Modicon M580

Sicherheitssystem - Planungshandbuch

Übersetzung der Originalbetriebsanleitung

QGH60285.10
06/2024

www.se.com

Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument 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 Dokument 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 Dokuments 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 Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

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 sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

Inhaltsverzeichnis

Sicherheitshinweise 7
Bevor Sie beginnen 8
Start und Test 9
Betrieb und Einstellungen 10
Informationen zum Dokument 11
Vom M580-Sicherheitssystem unterstützte Module 17
Für das M580-Sicherheitssystem zertifizierte Module 18
Nicht-störende Module 20
Auswahl der Topologie für ein M580-Sicherheitssystem 25
Planung der Topologie eines M580-Sicherheitssystems 26
M580-Sicherheitstopologien 30
CPU und Koprozessor des M580-Sicherheitssystems 38
Physische Merkmale von CPU und Koprozessor eines M580-Sicherheitssystems 39
Physische Beschreibung der M580 Sicherheits-CPU und des Koprozessors 39
LED-Anzeigen für M580 Safety-CPU und Koprozessor 45
Ethernet-Ports 47
USB-Port 50
SFP-Steckbuchse 52
SD-Speicherkarte 52
Sicherheitsetiketten und verriegelbare SD-Kartenabdeckung 54
Leistungsmerkmale von CPU und Koprozessor eines M580-Sicherheitssystems 57
Leistungskenndaten von M580-CPU und Koprozessor 57
M580-Sicherheitsspannungsversorgungen 60
Physische Beschreibung der M580-Sicherheitsspannungsversorgungen 61
Leistungskenndaten der M580-Sicherheitsspannungsversorgung 67
Alarmrelais der M580-Sicherheitsspannungsversorgungen 73
M580-E/A-Sicherheitsmodule 74
Physische Beschreibung der M580-E/A-Sicherheitsmodule 75
Physische Abmessungen der M580-E/A-Module 75
Leistungsmerkmale der M580-E/A-Sicherheitsmodule 81

Leistungskenndaten des analogen BMXSAI0410-Sicherheitseingangsmoduls 81
Leistungskenndaten des digitalen BMXSDI1602-Sicherheitseingangsmoduls 83
Leistungskenndaten des digitalen BMXSDO0802-Sicherheitsausgangsmoduls 84
Leistungsmerkmale des digitalen Sicherheits-Relais-Ausgangsmoduls BMXSRA0405 86
Installation des M580-Sicherheits-PAC 88
Installation von M580-Racks und -Erweiterungsmodulen 89
Planung der Installation des lokalen Racks 89
Montage der Racks 94
Erweiterung eines Racks 96
Installation von CPU, Koprozessor, Spannungsversorgung und E/A eines M580-Sicherheitssystems 99
Installation von CPU und Koprozessor 99
Installation eines Spannungsversorgungsmoduls 103
Installation von M580-Sicherheits-E/A 107
Installation einer SD-Speicherkarte in einer CPU 109
Firmware-Upgrade für die M580-Sicherheitssteuerung 112
Aktualisierung der Firmware auf Version 4.21 113
Downgrade der Firmware von Version 4.21 oder höher 114
Bedienung eines M580-Sicherheitssystems 115
Prozess-, sicherheitsspezifische und globale Datenbereiche in Control Expert 116
Datentrennung in Control Expert 117
Betriebsarten, Betriebszustände und Tasks 121
Betriebsarten des M580-Sicherheits-PAC 121
Betriebszustände des M580-Sicherheits-PA 126
Anlaufsequenzen 132
Tasks des M580-Sicherheits-PAC 136
Gestaltung eines M580-Sicherheitsprojekts 140
Generierung eines M580-Sicherheitsprojekts 140
SAFE-Signatur 140
Sperre der Konfiguration der M580-E/A-Sicherheitsmodule 148

Sperre der Konfiguration der M580-E/A-Sicherheitsmodule ... 148
Initialisierung der Daten in Control Expert ... 151
Initialisierung der Daten in Control Expert für den M580-Sicherheits-PAC ... 151
Verwendung der Animationstabellen in Control Expert ... 152
Animationstabellen und Bedienerfenster ... 152
Hinzufügen von Code-Sections ... 157
Hinzufügen von Code zu einem M580-Sicherheitsprojekt ... 157
Diagnose-Anforderung ... 161
Die Befehle „Swap“ und „Clear“ ... 164
Verwaltung der Anwendungssicherheit ... 168
Application Protection ... 168
Safety-Related Area Password Protection ... 175
Program Unit, Section and Subroutine Password and Protection ... 179
Firmwareschutz ... 182
Data Storage/Web Protection ... 184
Passwortverlust ... 186
Verwaltung der Workstation-Sicherheit ... 193
Verwaltung des Zugriffs auf EcoStruxure Control Expert ... 193
Zugriffsrechte ... 197
Einstellungen für M580-Sicherheitsprojekte ... 209
Projekteinstellungen für ein M580-Sicherheitsprojekt in Control Expert ... 209
Anhang ... 215
IEC 61508 ... 216
Allgemeine Informationen zur Norm IEC 61508 ... 217
SIL-Richtlinie ... 219
Systemobjekte ... 224
Bits des M580-Sicherheitssystems ... 225
Wörter des M580-Sicherheitssystems ... 228
SRAC-Referenzen ... 232
Glossar ... 235
Index ... 237

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 Vorsichtsmaßnahmen stammen aus der NEMA Standards Publication ICS 7.1-1995:

(Im Falle einer Abweichung oder eines Widerspruchs zwischen einer Übersetzung und dem englischen Original hat der Originaltext in der englischen Sprache Vorrang.)

- 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.
- Nur die vom Bediener unbedingt vorzunehmenden betriebsspezifischen Einstellungen sollten für den Bediener zugänglich sein. Der Zugriff auf andere Steuerungsfunktionen sollte eingeschränkt sein, um unbefugte Änderungen der Betriebskenngrößen zu vermeiden.

Informationen zum Dokument

Geltungsbereich des Dokuments

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 Control Expert XL Safety 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.

Gültigkeitshinweis

Dieses Dokument ist gültig für EcoStruxure™ Control Expert 16.0 mit ControlExpert_V160_HF001 M580 Safety oder höher.

Die Kenndaten der in diesem Dokument beschriebenen Produkte entsprechen den auf www.se.com verfügbaren Kenndaten. Im Rahmen unserer Unternehmensstrategie zur kontinuierlichen Verbesserung überarbeiten wir den Inhalt im Laufe der Zeit ggf., um Klarheit und Genauigkeit zu verbessern. Wenn Sie einen Unterschied zwischen den Eigenschaften in diesem Dokument und den Eigenschaften auf www.se.com feststellen, sollten Sie sich auf www.se.com berufen, um die neuesten Informationen zu enthalten.

Weiterführende Dokumente

Titel der Dokumentation	Referenznummer
M580 Safety, Sicherheitsbezogene Anwendungsbedingungen - Prüfplan	EIO0000004540 (ENG) EIO0000004741 (FRE) EIO0000004742 (GER) EIO0000004744 (ITA) EIO0000004743 (SPA) EIO0000004745 (CHS)
Modicon M580, Sicherheitshandbuch	QGH46982 (Englisch), QGH46983 (Französisch), QGH46984 (Deutsch), QGH46985 (Italienisch), QGH46986 (Spanisch), QGH46987 (Chinesisch)
EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek	QGH60275 (Englisch), QGH60278 (Französisch), QGH60279 (Deutsch), QGH60280 (Italienisch), QGH60281 (Spanisch), QGH60282 (Chinesisch)
Modicon-Steuerungssysteme, Cybersicherheit, Benutzerhandbuch	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, Komplexe Topologien, Systemhandbuch	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)

Um Dokumente online zu finden, besuchen Sie das Schneider Electric Download-Center (www.se.com/ww/en/download/).

Produktbezogene Informationen

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENS

- Trennen Sie alle Geräte vom Netz, einschließlich der angeschlossenen Geräte, bevor Sie Abdeckungen oder Türen entfernen oder Zubehör, Hardware, Kabel oder Drähte anbringen bzw. abnehmen. Eine Ausnahme hiervon bilden die im Hardwarehandbuch dieses Geräts beschriebenen besonderen Bedingungen.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um sicherzustellen, dass an den betreffenden Stellen und zum jeweils angegebenen Zeitpunkt tatsächlich keine Spannung mehr anliegt.
- Bringen Sie alle Abdeckungen, Zubehörteile, Hardware, Kabel und Drähte wieder an, sichern Sie sie und vergewissern Sie sich, dass eine ordnungsgemäße Erdung vorhanden ist, bevor Sie die Spannungszufuhr zum Gerät einschalten.
- Verwenden Sie für den Betrieb dieses Geräts und jeglicher verbundener Produkte ausschließlich die vorgeschriebenen Spannungswerte.

Die Nichtbeachtung dieser Anweisungen hat Tod oder schwere Verletzungen zur Folge.

⚠WARNUNG

STEUERUNGSAUSFALL

- Führen Sie vor der Implementierung eine Fehlermöglichkeits- und Einflussanalyse (FMEA) oder eine entsprechende Risikoanalyse für Ihre Anwendung durch und wenden Sie präventive und detektive Kontrollen an.
- Stellen Sie einen Fallback-Zustand für den Fall unerwünschter Steuerungsereignisse oder -sequenzen bereit.
- Sorgen Sie für separate oder redundante Steuerungspfade, wann immer erforderlich.
- Stellen Sie geeignete Parameter bereit, insbesondere für Grenzwerte.
- Prüfen Sie die Auswirkungen von Übertragungsverzögerungen und ergreifen Sie Maßnahmen, um diese zu begrenzen.
- Überprüfen Sie die Auswirkungen von Unterbrechungen der Kommunikationsverbindung und ergreifen Sie Maßnahmen, um diese zu begrenzen.
- Stellen Sie unabhängige Pfade für die Steuerungsfunktionen (z. B. Not-Aus, Grenzüberschreitungen und Fehler) in Übereinstimmung mit der Sicherheitsanalyse und den geltenden Richtlinien und Vorschriften bereit.
- Wenden Sie geltende lokale Vorschriften und Richtlinien zur Unfallverhütung und Gewährleistung der Sicherheit an.[1]
- Jede Implementierung eines Systems muss auf ihre ordnungsgemäße Funktionsweise getestet werden, bevor sie in Betrieb genommen wird.

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

[1] Weitere Informationen finden Sie in NEMA ICS 1.1 (neueste Ausgabe), *Sicherheitsrichtlinien für die Anwendung, Installation und Wartung von Halbleitersteuerungen*, und NEMA ICS 7.1 (neueste Ausgabe), *Sicherheitsnormen für die Konstruktion und Anleitung für die Auswahl, Installation und den Betrieb von Frequenzumrichtersystemen*, oder deren Entsprechung, die für Ihren spezifischen Standort gilt.

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Verwenden Sie mit diesem Gerät nur von Schneider Electric genehmigte Software.
- Aktualisieren Sie Ihr Anwendungsprogramm bei jeder Änderung der physischen Hardwarekonfiguration.

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

Marken

QR Code ist eine eingetragene Marke von DENSO WAVE INCORPORATED in Japan und anderen Ländern.

Terminologie gemäß den geltenden Standards

Die technischen Begriffe, Terminologie, Symbole und die entsprechenden Beschreibungen in den hierin enthaltenen oder in bzw. auf den Produkten selbst angegebenen Informationen sind im Allgemeinen von den Begriffen oder Definitionen internationaler Normen abgeleitet.

Im Bereich der funktionalen Sicherheitssysteme, Antriebe und allgemeinen Automatisierungssysteme kann dies unter anderem Begriffe wie *Sicherheit*, *Sicherheitsfunktion*, *Sicherer Zustand*, *Störung*, *Fehlerreset*, *Fehlfunktion*, *Versagen/Ausfall*, *Fehler*, *Fehlermeldung*, *Gefährlich* usw. umfassen.

Zu diesen Normen und Standards zählen unter anderem:

Norm/Standard	**Beschreibung**
IEC 61131–2–2007	Speicherprogrammierbare Steuerungen, Teil 2: Betriebsmittelanforderungen und Prüfungen
ISO 13849-1:2023	Sicherheit von Maschinen: Sicherheitsbezogene Teile von Steuerungen Allgemeine Gestaltungsleitsätze
EN 61496-1:2013 Sicherheit	Sicherheit von Maschinen: Berührungslos wirkende Schutzeinrichtung Teil 1: Allgemeine Anforderungen und Tests
ISO 12100:2010:	Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
EN 60204-12006	Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen
ISO 14119:2013:	Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
ISO 13850:2015:	Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
IEC 62061:2021	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Steuerungssysteme
IEC 61508-12010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Allgemeine Anforderungen
IEC 61508-22010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Anforderungen für

Norm/Standard	Beschreibung
	sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme
IEC 61508-32010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Softwareanforderungen
IEC 61784-3:2021	Industrielle Kommunikationsnetzwerke – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile
2006/42/EC	Maschinenrichtlinie
2014/30/EU	EMV-Richtlinie (Elektromagnetische Verträglichkeit)
2014/35/EU	Niederspannungsrichtlinie

Darüber hinaus wurden einige der Begriffe in den hier enthaltenen Informationen ggf. auch anderen Normen/Standards entnommen, u. a.:

Norm/Standard	Beschreibung
IEC 60034:	Drehende elektrische Maschinen
IEC 61800:	Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl
IEC 61158:	Digitale Datenkommunikation für Messung und Steuerung - Feldbus für den Einsatz in industriellen Steuerungssystemen

Bei einer Verwendung des Begriffs *Betriebsumgebung/Betriebsbereich* in Verbindung mit der Beschreibung bestimmter Gefahren und Risiken entspricht der Begriff der Definition von Gefahrenbereich oder Gefahrenzone in der Maschinenrichtlinie (2006/42/EC) und der Norm ISO 12100:2010.

HINWEIS: Die zuvor erwähnten Normen/Standards können auf die spezifischen Produkte in der vorliegenden Dokumentation zutreffen oder nicht. Für weitere Informationen hinsichtlich individueller Normen/Standards, die auf hier beschriebene Produkte zutreffen, siehe die Kenndatentabellen für die entsprechenden Produktreferenzen.

Informationen zu nicht-inklusiver oder unsensibler Terminologie

Als verantwortungsbewusstes, integratives Unternehmen aktualisiert Schneider Electric ständig seine Kommunikationen und Produkte, um nicht-inklusive und unsensible Terminologie zu vermeiden. Trotz dieser Bemühungen können unsere Inhalte jedoch immer noch Begriffe enthalten, die von einigen Kunden als unangemessen erachtet werden.

Vom M580-Sicherheitssystem unterstützte Module

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

Nur die Versionen des Sicherheitsprodukts und der Control Expert-Software, die in der TÜV-Zertifikatrevisionsliste aufgeführt sind, sind mit einer Sicherheitsanwendung konform.

Aktuelle Informationen zu den zertifizierten Produkt-, Firmware- und Softwareversionen finden Sie auf der Website der TÜV Rheinland Group: www.certipedia.com oder www.fs-products.com.

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

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

HINWEIS: Zusätzlich zu den oben aufgeführten Sicherheitsmodulen können in ein Sicherheitsprojekt ebenfalls nicht-störende, nicht-sichere Module, Seite 20 aufgenommen werden.

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

HINWEIS:

- Wenn im Dokument SIL2 oder SIL3 ohne eine Standardreferenz erwähnt wird, bezieht sich dies auf IEC 61508 / IEC 61511.
- Wenn SIL2 erwähnt wird, bezieht sich dies ebenfalls auf SIL3 gemäß EN 50126 / EN 50128 / EN 50129.
- Wenn SIL3 erwähnt wird, bezieht sich dies ebenfalls auf SIL4 gemäß EN 50126 / EN 50128 / EN 50129.

Ersetzen einer CPU

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

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

Siehe folgende Themen:

- *Konfigurationskompatibilität* im *Modicon M580 Hot Standby Systemplanungshandbuch für häufig verwendete Architekturen* für eine Beschreibung von Control Expert-Anwendungen, die mit Sicherheits- und Hot Standby-CPUs kompatibel sind.
- Unter *Leistungskenndaten von M580-CPU und Koprozessor*, Seite 57 im *Modicon M580 Safety Systemplanungshandbuch* finden Sie eine Beschreibung der CPU-Beschränkungen.

Nicht-störende Module

Einführung

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

Definition eines nicht-störenden Moduls

HINWEIS: Stellen Sie sicher, dass weder die Eingangs- noch die Ausgangsdaten nicht-störender Module zur Steuerung sicherheitsbezogener Ausgänge verwendet werden. Nicht-Sicherheitsmodule können nur Daten ohne Bezug zur Sicherheit verarbeiten.

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

- **Typ 1**: Ein Modul vom Typ 1 kann im selben Rack installiert werden wie Sicherheitsmodule (ungeachtet der Position des Sicherheitsmoduls, ob im Haupt- oder Erweiterungsrack).
- **Typ 2**: Ein nicht-störendes Modul vom Typ 2 kann nicht im selben Rack installiert werden wie Sicherheitsmodule (ungeachtet der Position des Sicherheitsmoduls, ob im Haupt- oder Erweiterungsrack).

  HINWEIS: Eine Liste der Module vom Typ1 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 vom Typ 1 für SIL3-Anwendungen

Die folgenden Nicht-Sicherheitsmodule können als nicht-störende Module vom Typ 1 in einem M580-Sicherheitssystem eingesetzt werden.

HINWEIS: Die Liste der nicht-störenden Nicht-Sicherheitsmodule vom Typ 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 16 Steckplätzen	BMEXBP1600
Baugruppenträger mit 4 Steckplätzen	BMXXBP0400
Baugruppenträger mit 6 Steckplätzen	BMXXBP0600
Baugruppenträger mit 8 Steckplätzen	BMXXBP0800
Baugruppenträger mit 12 Steckplätzen	BMXXBP1200
Baugruppenträger mit 16 Steckplätzen	BMXXBP1600
Baugruppenträger mit 6 Steckplätzen und Dual-Steckplätzen für redundante Spannungsversorgungen	BMEXBP0602
Baugruppenträger mit 10 Steckplätzen und Dual-Steckplätzen für redundante Spannungsversorgungen	BMEXBP1002
Baugruppenträger mit 14 Steckplätzen und Dual-Steckplätzen für redundante Spannungsversorgungen	BMEXBP1402
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
Zählfunktion: SSI-Modul, 3 K	BMXEAE0300
Zählfunktion: Hochgeschwindigkeitszähler 2 K	BMXEHC0200
Zählfunktion: Hochgeschwindigkeitszähler 8 K	BMXEHC0800
Bewegung: Impulswellenausgang, 2 unabhängige K	BMXMSP0200

Modultyp	Modulreferenz
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, 8 Aus, Source, Tr	BMXDDM16022
Digital: Dig 8 Ein, 24 VDC, 8 Aus, Relais	BMXDDM16025
Digital: Dig 16 Ein, 24 VDC, 16 Aus, Source, Tr	BMXDDM3202K
Digital: Dig 16 Aus, Trans, Source, 0,5 A	BMXDDO1602

Modultyp	Modulreferenz
Digital: Dig 16 Aus, Trans, Sink	BMXDDO1612
	BMXDDO3202
	BMXDDO3202H
Digital: Dig 32 Aus, Trans, Source, 0,1 A	BMXDDO3202K
Digital: Dig 64 Aus, Trans, Source, 0,1 A	BMXDDO6402K
Digital: Dig 8 Aus, 125 VDC	BMXDRA0804T
Digital: Dig 8 Aus, 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 16 Aus, 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-Switch für Netzwerkoptionen	BMENOS0300
Turbomaschinen Frequenzeingang, 2 Kanäle	BMXETM0200
Unterstützung für Profibus DP/DPV1-Mastermodul	PMEPXM0100
Mx80 Erweitertes RTU-Modul	BMENOR2200H

Nicht-störende Module vom Typ 2 für SIL2/3-Anwendungen

Die folgenden rackinternen Nicht-Sicherheitsmodule können als nicht-störende Module vom Typ 2 in einem M580-Sicherheitssystem eingesetzt werden.

HINWEIS: Die Liste der nicht-störenden Nicht-Sicherheitsmodule vom Typ 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
Hochleistungsspannungsversorgung 24 bis 48 VDC, potentialgetrennt	BMXCPS3020
Redundante Standardspannungsversorgung, 125 VDC	BMXCPS3522

Modultyp	Modulreferenz
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 Baureihen Quantum und STB Advantys (nicht im gleichen Rack wie M580-Sicherheitsmodule einsetzbar) nicht-störende Module vom Typ 2.

Auswahl der Topologie für ein M580-Sicherheitssystem

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 89.

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 und 8 RIO-Stationen für die BME•582040S-CPU, die jeweils aus einem dezentralen Hauptrack und einem optionalen dezentralen Erweiterungsrack bestehen.

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

HINWEIS: Ein Rack mit Sicherheitsmodulen kann ebenfalls nicht-störende Module vom Typ 1, Seite 20 enthalten. Allerdings dürfen keine nicht-störenden Module vom Typ 2, Seite 23 im gleichen Rack wie Sicherheitsmodule untergebracht werden. Nicht-störende Module vom Typ 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. Verbinden Sie jedes Paar Erweiterungsmodule mit BMXXBC•••K-Steckerkabeln und schließen Sie jedes Ende der Kette mit TSXELYEX-Leitungsabschlüssen ab.

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 Daisy-Chain mit offenem Regelkreis verwenden.

HINWEIS: Nehmen Sie ausschließlich nicht-störende Module vom Typ 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 vom Typ 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 mit dem RIO-Hauptring verbinden 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 zu gewährleisten, sollten Sie nicht die maximale Anzahl aller E/A-Typen in derselben Architektur verwenden.

Basieren Sie eine typische M580 CIP Safety-Architektur auf einer dezentralen oder verteilten Topologie:

Dezentrale Topologie - Einschränkungen:

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

Verteilte Topologie - Einschränkungen:

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

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

M580-Sicherheitstopologien

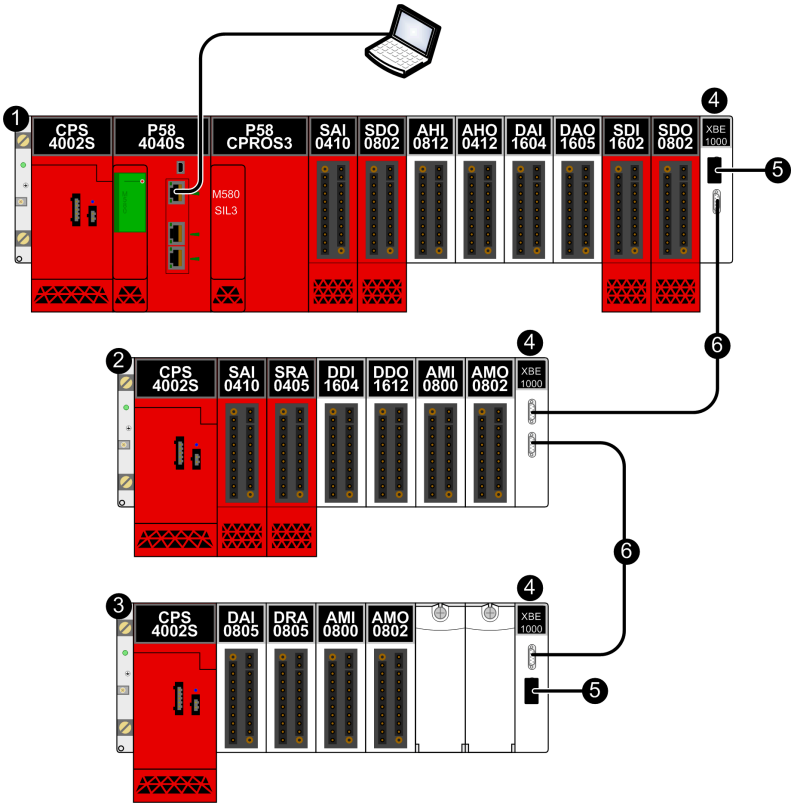
Einführung

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 vom Typ 1

2 Lokales Erweiterungsrack mit Sicherheits- und nicht-störenden Modulen vom Typ 1

3 Lokales Erweiterungsrack mit nicht-störenden Modulen vom Typ 1

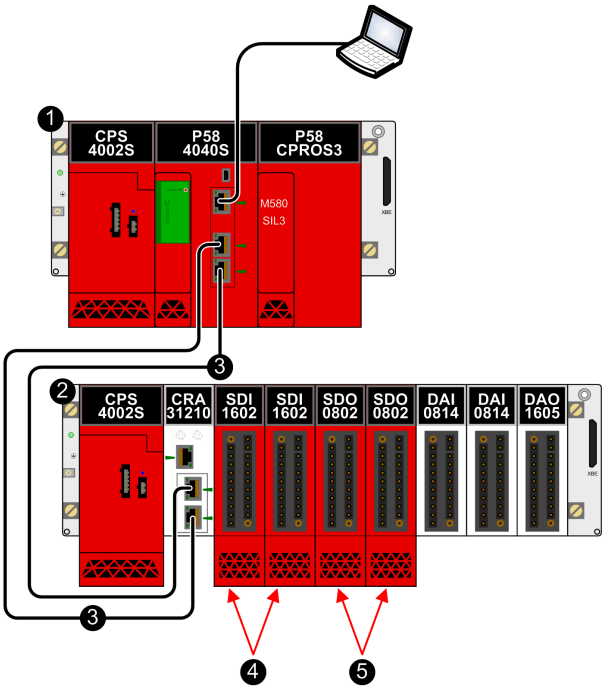
4 BMXXBE1000 Rack-Erweiterungsmodule

5 TSXELYEX Leitungsabschlüsse

6 BMXXBC•••K Anschlusskabel

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

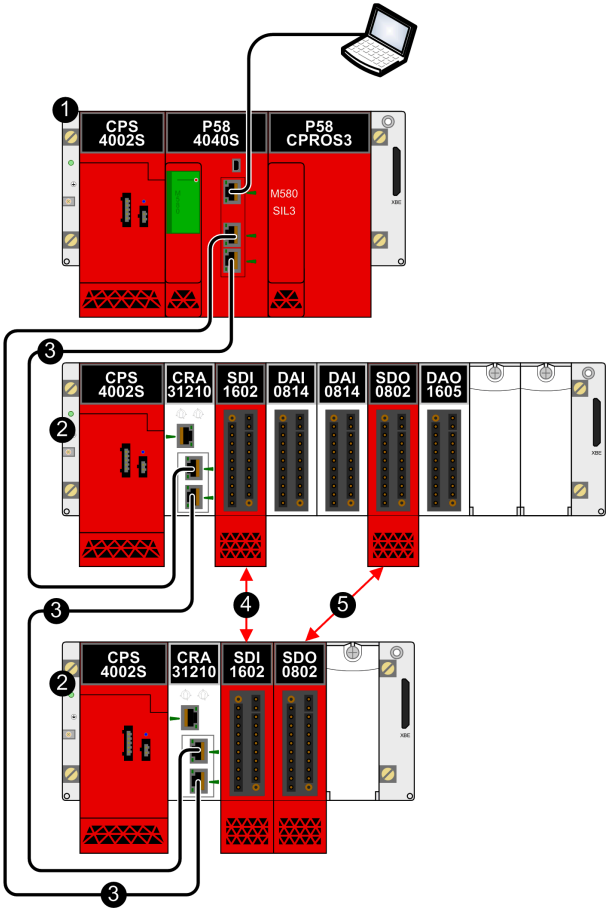
3 RIO-Hauptring

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

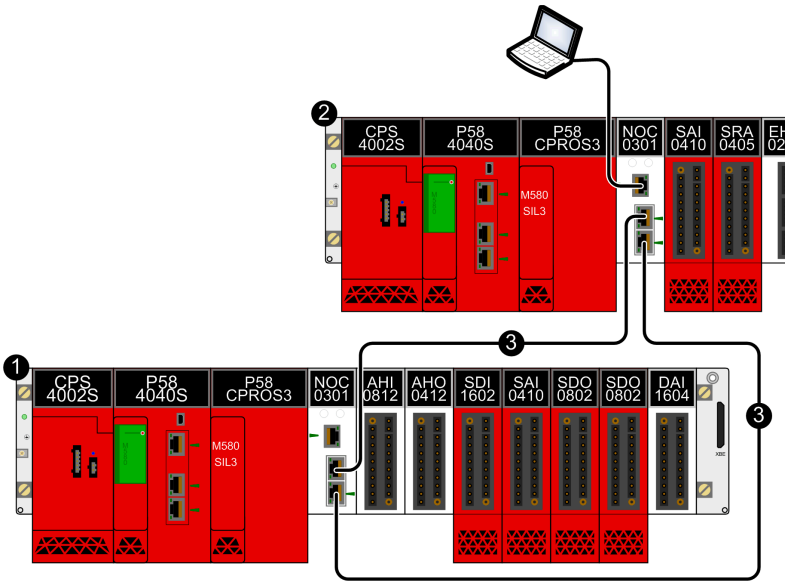
5 Zwei redundante Ausgangsmodule in separaten RIO-Stationen

HINWEIS:

- Platzieren Sie redundante 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 Aktors auszulösen:



1 Standalone-M580-Sicherheits-PAC 1

2 M580-Sicherheits-PAC 2

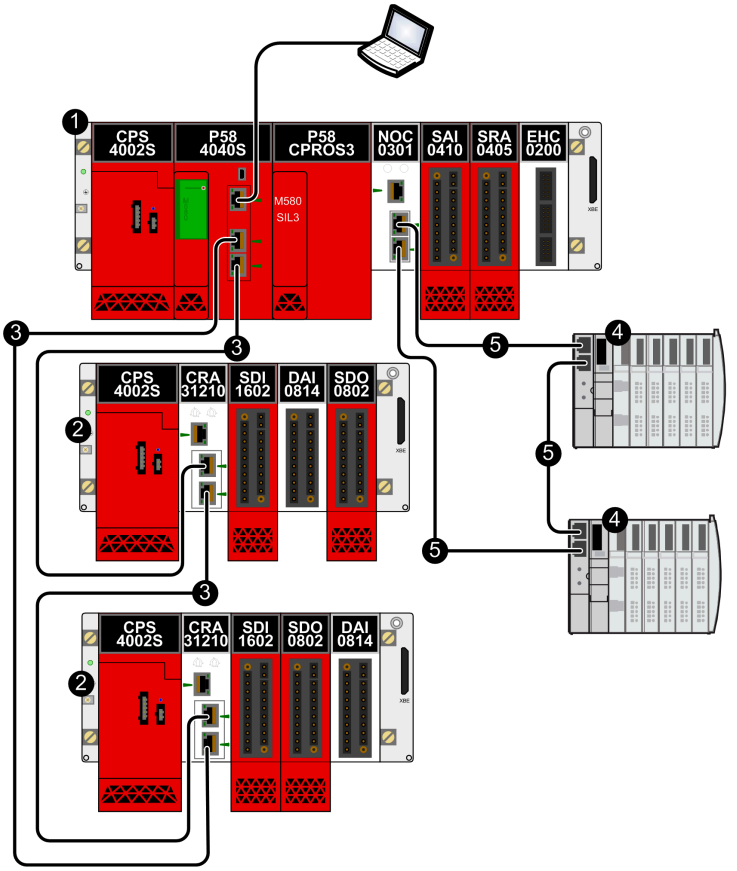
3 „Black-Channel“-Kommunikation zwischen PACs

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 vom Typ 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 Daisy-Chain mit offenem Regelkreis hinzugefügt wurden. In diesem Beispiel werden die verteilten Geräte in einer Daisy-Chain 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 vom Typ 1

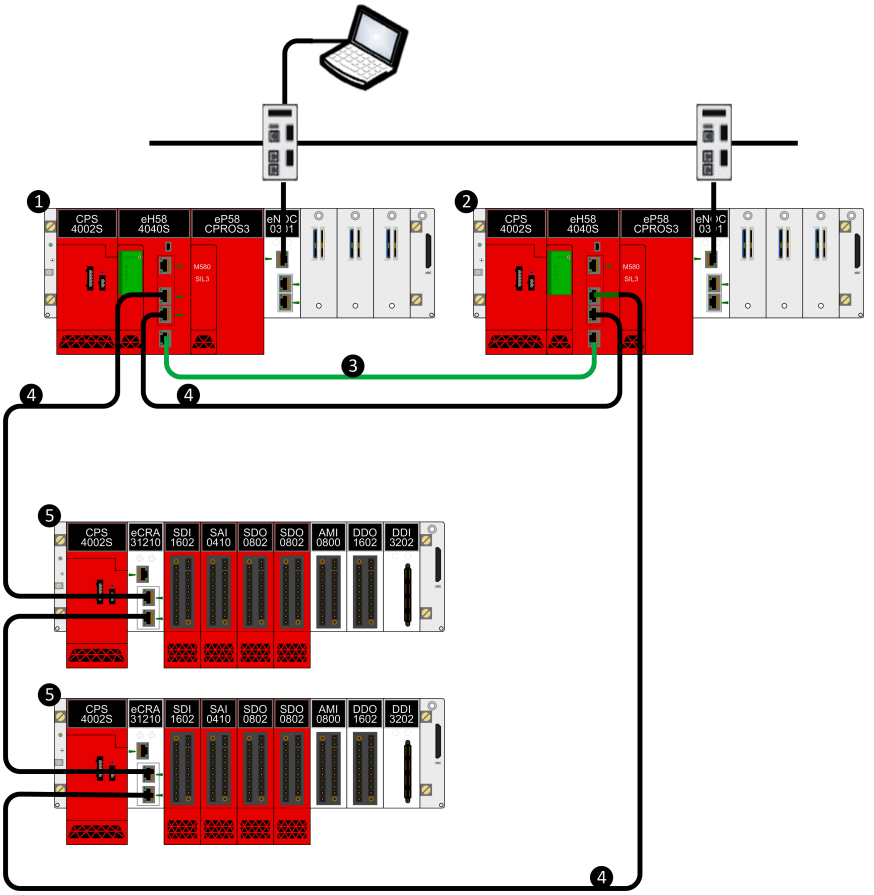
3 RIO-Hauptring

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

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

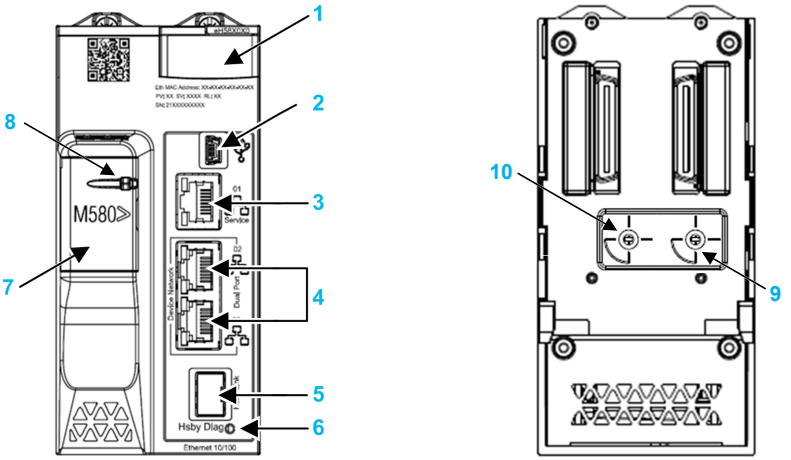
Jedes M580-Standalone-SIL3-Sicherheitssystem benötigt eine BME•58•040S-CPU und einen BMEP58CPROS3-Koprozessor (Kopro). Für die CPU sind zwei Modulsteckplätze erforderlich. Sie wird in den Steckplätzen 0 und 1 direkt rechts neben der Spannungsversorgung im lokalen Hauptrack installiert. Der Koprozessor 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.

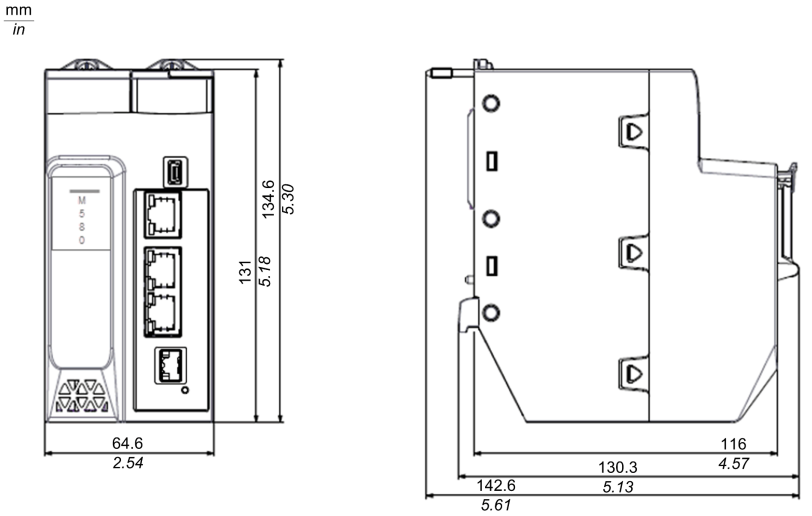
10 A/B/Löschen-Drehwahlschalter, der verwendet wird, um den PAC entweder als PAC A oder PAC B zu bestimmen oder um die bestehende Control Expert-Anwendung zu löschen.

Koprozessor-Frontplatte

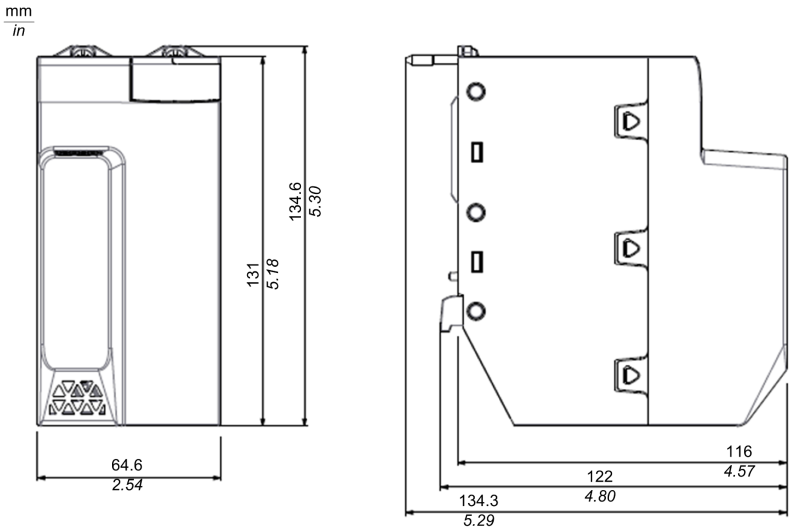
Der BMEP58CPROS3-Koprozessor verfügt nur über eine LED-Anzeige an seiner Frontplatte.

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.

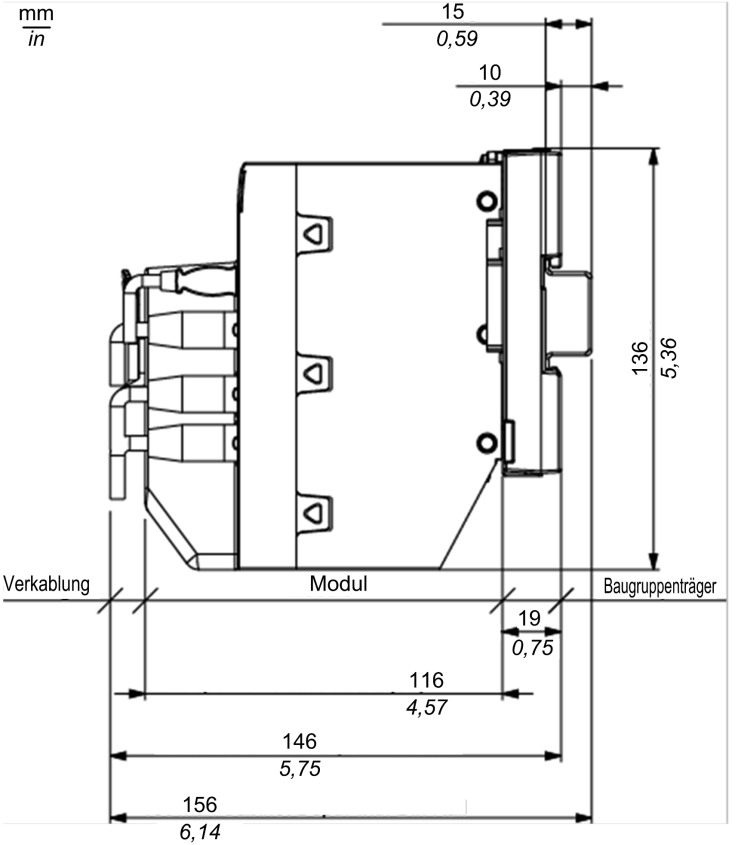


HINWEIS: Bei der Planung der Installation des lokalen Racks ist die Höhe der CPU und des Koprozessors zu berücksichtigen. Sowohl die CPU als auch der Koprozessor stehen um folgende Länge über den unteren Rand des Racks hervor:

- 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:

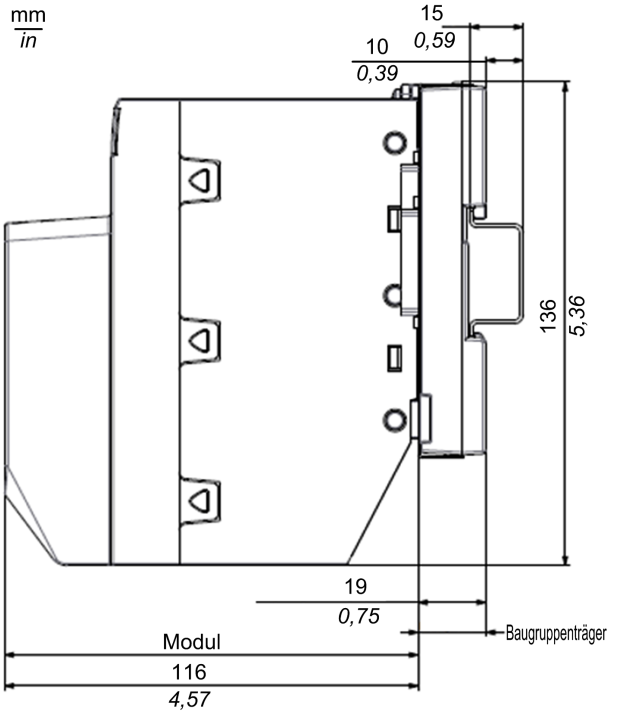


Globale Tiefe für die CPU:

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

Abmessungen der Koprozessor-Verkabelung

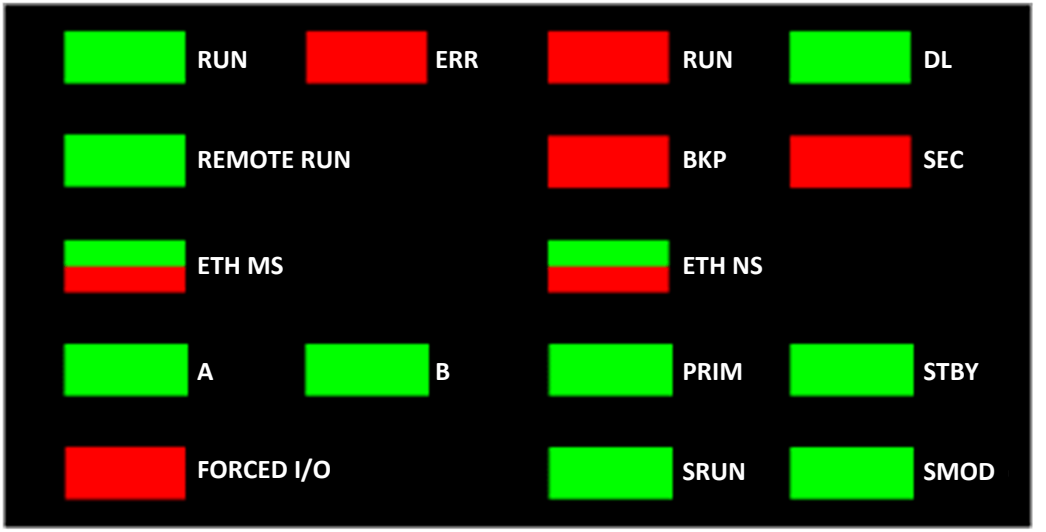
Für den BMEP58CPROS3-Koprozessor gelten folgende Abmessungen bei einer DIN-Schienenmontage:



LED-Anzeigen für M580 Safety-CPU und Koprozessor

LED Display-Anzeige der CPU

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*.
- Siehe *LED-Diagnose für M580 Hot Standby-CPUs* im *Modicon M580 Hot Standby Systemplanungshandbuch für häufig verwendete Architekturen* für Informationen zur Verwendung des LEDs **A**, **B**, **PRIM**, **STBY** und **REMOTE RUN** der Hot Standby-CPU.

LED-Anzeige	Gilt für ...		Beschreibung
	CPU	Kopro	
RUN	✓	–	**EIN**: CPU verwaltet die eigenen Ausgänge und mindestens eine Task befindet sich im RUN-Zustand.
ERR	✓	✓	**EIN**: CPU hat einen internen CPU-Fehler erkannt (z. B. keine Konfiguration, Watchdog-Fehler, Selbsttest-Fehler).
I/O	✓	–	**EIN**: CPU hat einen CPU-externen Fehler in einem oder mehreren E/A-Modulen erkannt.
DL (*Download*)	✓	+	• **EIN**: Eine Firmwareaktualisierung für CPU, Koprozessor, BKP oder ein anderes rackinternes Modul wird durchgeführt. • **AUS**: Es wird keine Firmwareaktualisierung durchgeführt.
BKP	✓	–	**EIN**: • Speicherkarte oder CPU-Flash-Speicher fehlt oder ist nicht funktionsfähig. • Die Speicherkarte kann nicht verwendet werden (falsches Format, unbekannter Typ). • Der Inhalt der Speicherkarte oder des CPU-Flash-Speichers ist nicht kohärent mit der aktuellen Anwendung. • Die Speicherkarte wurde entnommen und wieder eingesetzt. • Ein Befehl **SPS > Projekt-Backup... > Löschen** wurde ausgeführt, obwohl keine Speicherkarte vorhanden ist. Die **BKP**-LED bleibt **EIN**, bis das Projekt erfolgreich gesichert wurde.
			AUS: Der 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 **ETH MS**-LED grün oder rot leuchten 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**: PAC verwaltet die eigenen Sicherheitsausgänge und die SAFE-Task befindet sich im RUN-Zustand.
SMOD	✓	✓	• **EIN**: PAC befindet sich im Sicherheitsmodus, Seite 121. • **BLINKEN**: PAC befindet sich im Wartungsmodus, Seite 122.
✓: Anwendbar – : 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.

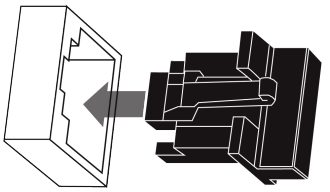
Gemeinsame Merkmale

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.

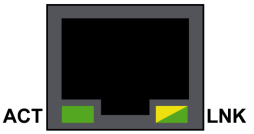
Staubschutz

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

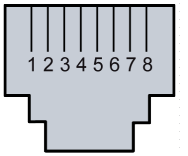


Ethernet-Ports

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 hat Tod oder schwere Verletzungen zur Folge.

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

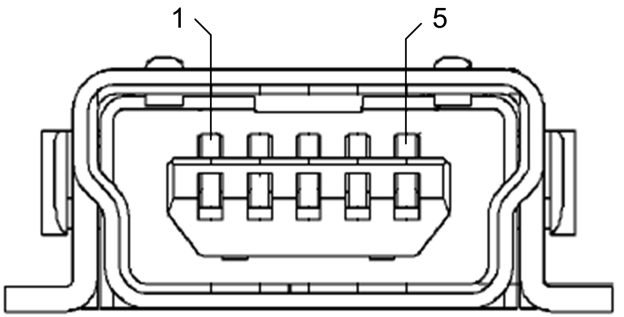
Wenn für Ihr System Transparenz zwischen dem an den USB-Port angeschlossenen Gerät und dem M580-Gerätenetzwerk erforderlich ist, müssen Sie in der Routing-Tabelle des Geräts eine persistente statische Route hinzufügen.

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

BMXRMS004GPF SD-Speicherkarte

Die BMXRMS004GPF-Speicherkarte ist eine Karte der Klasse 6 mit 4 GB für den industriellen Einsatz. Der Steckplatz für die SD-Speicherkarte befindet sich hinter der Klappe an der Frontseite der Steuerung.

Sie können eine BMXRMS004GPF-Speicherkarte zur Speicherung von Anwendungen und Daten einsetzen.

Eine BMXRMS004GPF-Speicherkarte ermöglicht die Speicherung von:

- Anwendung des M580-Sicherheitsprojekts
- 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 im RUN-Modus der Steuerung ein- und ausstecken. Um jedoch Datenverluste zu vermeiden, verwenden Sie das Systembit %S65, um einen Systemrequest zum Stopp des Datenzugriffs auf die Karte auszugeben, bevor Sie die Karte aus der Steuerung entnehmen.

HINWEIS: Andere Speicherkarten, einschließlich der in M340-Steuerungen verwendeten Karten, sind nicht mit M580-Steuerungen kompatibel. Wenn Sie eine inkompatible SD-Speicherkarte in die Steuerung einstecken:

- Die Steuerung verbleibt im NOCONF-Zustand (siehe Modicon M580, Hardware, Referenzhandbuch).
- Die Steuerung **BKP** LED schaltet sich EIN.
- Die LED für den Zugriff auf die Speicherkarte blinkt.

Die BMXRMS004GPF-Speicherkarte wurde speziell für die M580-Steuerung formatiert. Wenn Sie diese Karte mit einer anderen Steuerung oder einem anderen Tool verwenden, wird die Karte möglicherweise nicht erkannt.

Kenndaten der Speicherkarte

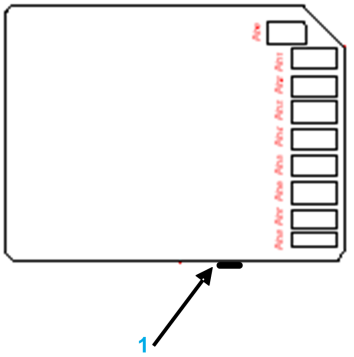
Die BMXRMS004GPF-Speicherkarte weist folgende Merkmale auf:

Merkmal	Wert
Globale Speichergröße	4 GB
Größe der Anwendungssicherung	200 MB
Größe der Datenspeicherung	3,8 GB
Schreib-/Löschzyklen (typisch)	100.000
Betriebstemperatur	-40 bis +85 °C (-40 bis +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.

Kartenschalter für Lese-/Schreibzugriff

Die BMXRMS004GPF-Speicherkarte ist an der nicht abgeschrägten Kante mit einem Lese-/Schreibzugriffsschalter ausgestattet, mit dem Sie die Karte vor unerlaubtem Schreibzugriff schützen können:



1 Lese-/Schreibzugriffsschalter

Formatieren der Speicherkarte

Das Formatierungsverfahren wird im Abschnitt *Formatieren der Speicherkarte* im Dokument der *EcoStruxure™ Control Expert Systembausteinbibliothek* beschrieben.

Sicherheitsetiketten und verriegelbare SD-Kartenabdeckung

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. dem hinteren Bereich des Modulcontainers). Diese Etiketten geben an, ob das Modul geöffnet und möglicherweise manipuliert wurde.

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

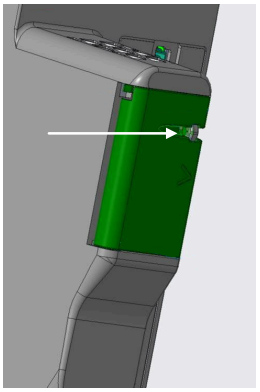


Der Modulcontainer wurde geöffnet, wenn die Sicherheitsetiketten wie folgt aussehen:



Verriegelbare SD-Kartenabdeckung

Die Abdeckung des SD-Kartensteckplatzes kann verriegelt oder verplombt werden.



Gehen Sie dazu wie folgt vor:

1. Schließen Sie die SD-Kartenabdeckung.

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

Leistungskenndaten 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 Gerätenetzwerk	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-Kommunikationsmodule im lokalen Rack	Max. Ethernet-Kommunikationsmodule	2	4	4	2	4	4
	Max. BMENOC0301/ 0311	2	3	3	2	3	3
	Max. BMENOC0321	2	2	2	2	2	2
Speicherzuweisung (max.)	Nicht-sicheres Anwendungsprogramm	8 MB	16 MB	64 MB[4]	8 MB	16 MB	64 MB[4]
	Sicheres Anwendungsprogramm	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
	Max. 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	40K Anweisungen / ms	40K Anweisungen / ms	50K Anweisungen / ms	40K Anweisungen / ms	40K Anweisungen / ms	50K Anweisungen / ms
	Typisiert	30K Anweisungen / ms	30K Anweisungen / ms	40K Anweisungen / ms	30K Anweisungen / ms	30K Anweisungen / ms	40K Anweisungen / ms
	SAFE-Task:						
	Boolesch	40K Anweisungen / ms	40K Anweisungen / ms	40K Anweisungen / ms	40K Anweisungen / ms[3]	40K Anweisungen / ms[3]	40K Anweisungen / ms[3]
	Typisiert	30K Anweisungen / ms	30K Anweisungen / ms	30K Anweisungen / ms	30K 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-Retain-Daten) + Anwendungsprogramm (sicher) + Anwendungsdaten (sicher) machen weniger als 64 MBytes aus. In der CPU BME•586040S ist für das Anwendungsprogramm und die Anwendungsdaten ein globaler Speicherpool von 64 MBytes vorhanden.

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

6. 2 GB ohne externe Speicherkarte.

M580-Sicherheitsspannungsversorgungen

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:

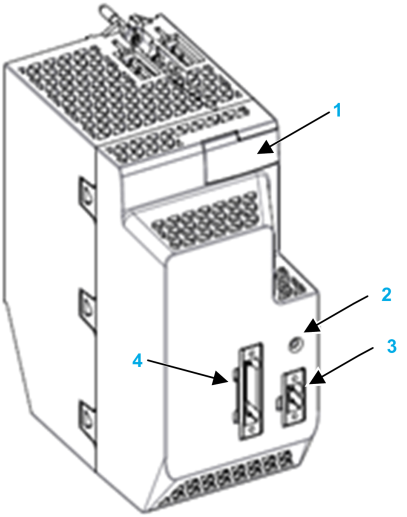
- Lokales Hauptrack
- Lokales Erweiterungsrack
- Dezentrales Hauptrack
- Dezentrales Erweiterungsrack

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-Anzeigetafel

2 RESET-Taste

3 Alarmrelaiskontakt

4 5-poliger Anschluss für die Haupteingangsversorgung

LED-Array

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



Die LED-Anzeigetafel umfasst folgende LED-Anzeigen:

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

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

Siehe das Thema *Diagnose der Spannungsversorgungs-LED* (siehe Modicones M580 Sicherheitshandbuch) im *M580 Sicherheitshandbuch* für Informationen zur Verwendung dieser LEDs für die Diagnose des Status der Spannungsversorgung.

RESET

Das Drücken der **RESET**-Taste an der Spannungsversorgung bewirkt die Reinitialisierung aller Module im selben Rack wie die Spannungsversorgung. Wenn sich das M580-Sicherheitsspannungsversorgungsmodul im lokalen Hauptrack befindet, wird durch Drücken der **RESET**-Taste die CPU reinitialisiert.

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

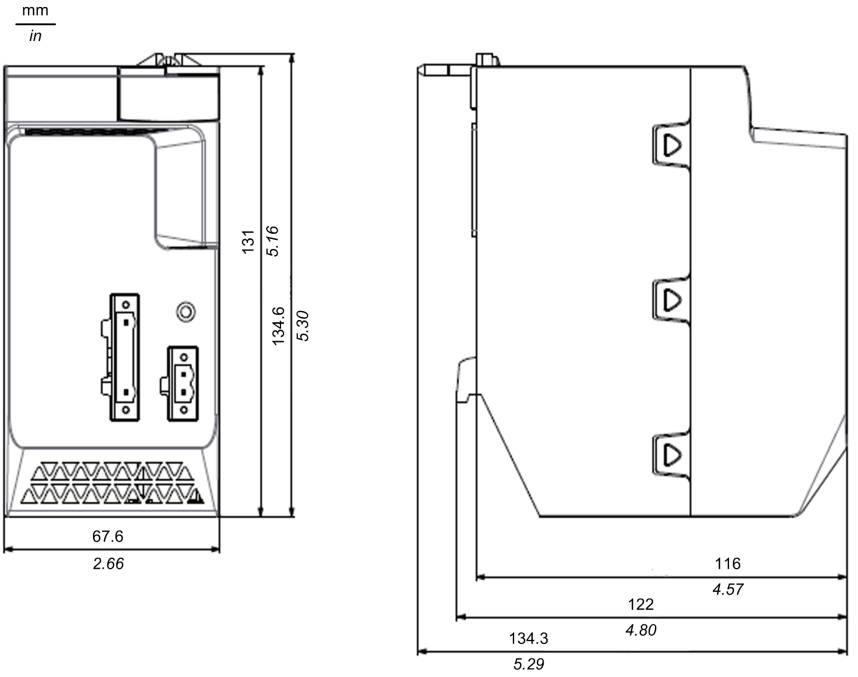
Die M580-Sicherheitsspannungsversorgungen weisen folgende Eingangsleistung und Pinzuweisung auf:

Beschreibung	**BMXCPS4002S**	**BMXCPS4022S**	**BMXCPS3522S**
Haupteingangsleistung	100 bis 240 VAC	24 bis 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.

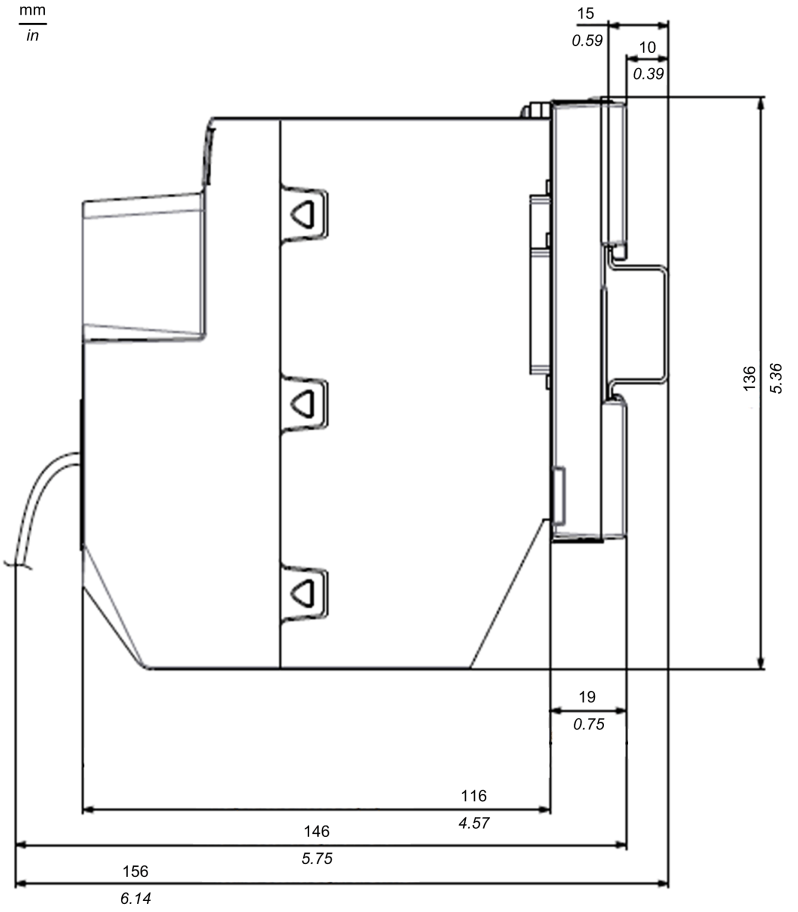
Abmessungen der Spannungsversorgungen

Die M580-Sicherheitsspannungsversorgungen weisen folgende Abmessungen auf:



Abmessungen der Verkabelung der Spannungsversorgungen

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



Leistungskenndaten der M580-Sicherheitsspannungsversorgung

Sicherheitsspannungsversorgung BMXCPS4002S

Die Sicherheitsspannungsversorgung BMXCPS4002S weist folgende Leistungsmerkmale auf:

Eingangsmerkmale		
Nennspannung		100 bis 240 V effektiv
Spannungsbereich		85 bis 132 V effektiv 170 bis 264 V effektiv
Frequenzbereich		47 bis 63 Hz
Maskierte Eingangsversorgungsausfälle		Max. 10 ms bei 100 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 1. Inbetriebnahme bei 25 °C	Spitzenwert	≤ 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
Integrierter Schutz		Interne, nicht zugängliche Sicherung an L-Eingang

Ausgangskenndaten		
Max. Ausgangsstrom 3V3_BAC		5,5 A (18,2 W)
Max. Ausgangsstrom 24V_BAC		1,67 A (40W)
Max. Ausgangsgesamtleistung		40 W
Erkennung	Überlast	Ja - Trennung
	Kurzschluss	Ja - Trennung

Ausgangskenndaten		
	Überspannung	Ja - Trennung

Sonstige Kenndaten		
Dielektrikum	Primär/Alle Sekundär	SELV/PELV
Festigkeit	Primär/Masse	SELV/PELV
Isoliationswiderstand	Primär/Alle Sekundär	100 MΩ
	Primär/Masse	100 MΩ

Sicherheitsspannungsversorgung BMXCPS4022S

Eingangskenndaten		
Nennspannungstyp		24 bis 48 VDC
Spannungsbereich		18 bis 62,4 VDC
Effizienz		Max. Verlust ≤ 7 W (Effizienz ≥ 84,8 %) bei maximaler Dauerlast, für den gesamten Eingangsspannungs- und Temperaturbereich
Eingangsnennstrom		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 Ausgangskenndaten kommen. Zeitraum zwischen Unterbrechungen: 1 Sek.

Eingangskenndaten	
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.

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

Ausgangskenndaten:	
	• Imax = 2 A.
Überspannungsschutz	Trennung der Spannungsversorgung bei einem Anstieg des Ausgangs auf 30,0 VDC ±,8 V.
Externe kapazitive Lastkapazität	Alle obigen Eigenschaften müssen mit der folgenden externen kapazitiven Last erfüllt sein. Diese Funktion muss insbesondere für Stromanstieg, Regelkreisstabilität und Überlasterkennung/-schutz in Betracht gezogen werden.
	11500 µF kapazitive Last

Sicherheitsspannungsversorgung BMXCPS3522S

Eingangskenndaten:		
Nennspannungstyp		125 VDC
Eingangsspannungsbereich		100 bis 150 VDC
Effizienz		Max. Verlust ≤ 7 W (Effizienz ≥ 84,8 %) bei maximaler Dauerlast, für den gesamten Eingangsspannungs- und Temperaturbereich
Eingangsnennstrom		0,6 A bei 125 VDC
Einschaltstrom beim ersten Einschalten bei 25 °C	Spitzenstrom	≤ 60 A bei 125 VDC
	I^2t (Bemessung externe Sicherung)	≤ 0,15 A^2s bei 125 VDC
	It (Bemessung externer Leistungsschalter)	≤ 0,025 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 Ausgangskenndaten kommen. Zeitraum zwischen Unterbrechungen: 1 Sek.

Eingangskenndaten:	
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.

	Hochleistungsmodul BMXCPS3522 /S
Ausgangsnennspannung	24,35 V
Ruhespannungsbereich der Ausgänge	23,3 bis 24,7 V für den gesamten Eingangsspannungsbereich, den gesamten Ausgangslastbereich und den kompletten Temperaturbereich
Rauschen und Welligkeit der Ausgänge	240 mV Spitze zu Spitze (gemessen mit einer Bandbreite ≥ 100 MHz, an den Anschlusspins des Moduls)
Dauerstrombereich der Ausgänge	• Max. 1,63 A
	• Min. 0 A
Ausgleichsstromkapazität der Ausgänge	Max. 1,9 A während 500 ms, Mindestzeitraum 20 Sek.
Ausgangsimpedanz mit Bezug auf die Frequenz	180 mΩ
Ausgangsansprechspannung bei transienter Last an 24V_BAC	Für folgende transiente Ausgangslast an 24V_BAC:
	• Lastschwankung I von min. Dauerstromgrenze bis max. Ausgleichsstromgrenze (und umgekehrt)
	• Übergangszeit 4 µs – Pulsbreite 500 ms – Zeitraum 20 Sek.
	• Die Ausgangsausgleichsspannung an 24V_BAC muss innerhalb des Bereichs 23,0 bis 25,0 V bleiben, die Ansprechzeit muss ≤ 50 ms sein.
	• Ungeachtet des Werts der kapazitiven Last an 24V_BAC innerhalb der vorgegebenen Grenzen.
Überlast-/Kurzschlussschutz	• Bei Überlast oder Kurzschluss an 24V_BAC (d. h. ungeachtet von Pegel, Dauer, Temperatur, Eingangsspannung) muss die Platine vor jeglichen Schäden geschützt werden.

	Hochleistungsmodul BMXCPS3522 /S
	• Der globale Höchstwert der Überlasterkennungsschwelle (d. h. einschließlich aller Toleranzen, Abweichungen usw.) muss kleiner sein als Imax.
	• Imax = 2 A.
Überspannungsschutz	Trennung der Spannungsversorgung bei einem Anstieg des Ausgangs auf 30,0 VDC ±,8 V.
Externe kapazitive Lastkapazität	Alle obigen Eigenschaften müssen mit der folgenden externen kapazitiven Last erfüllt sein. Diese Funktion muss insbesondere für Stromanstieg, 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

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

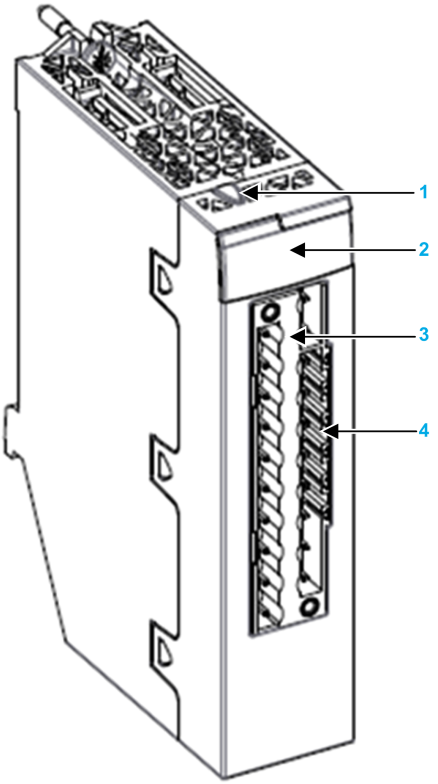
Sie können ein M580-E/A-Sicherheitsmodul in folgenden Positionen installieren:

- 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

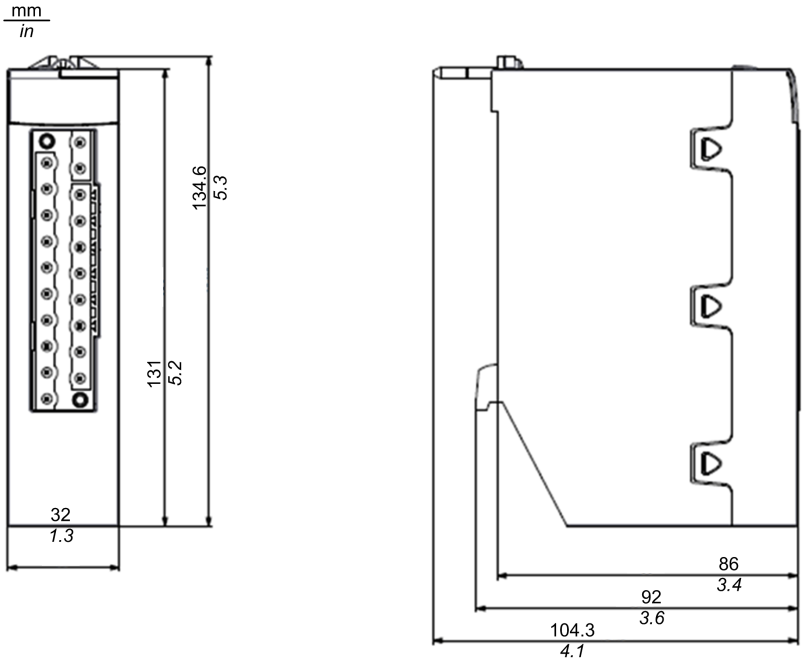
2 LED-Panel

3 20-poliger Steckverbinder

4 Steckplätze für Kodierstifte

Abmessungen der E/A-Sicherheitsmodule

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

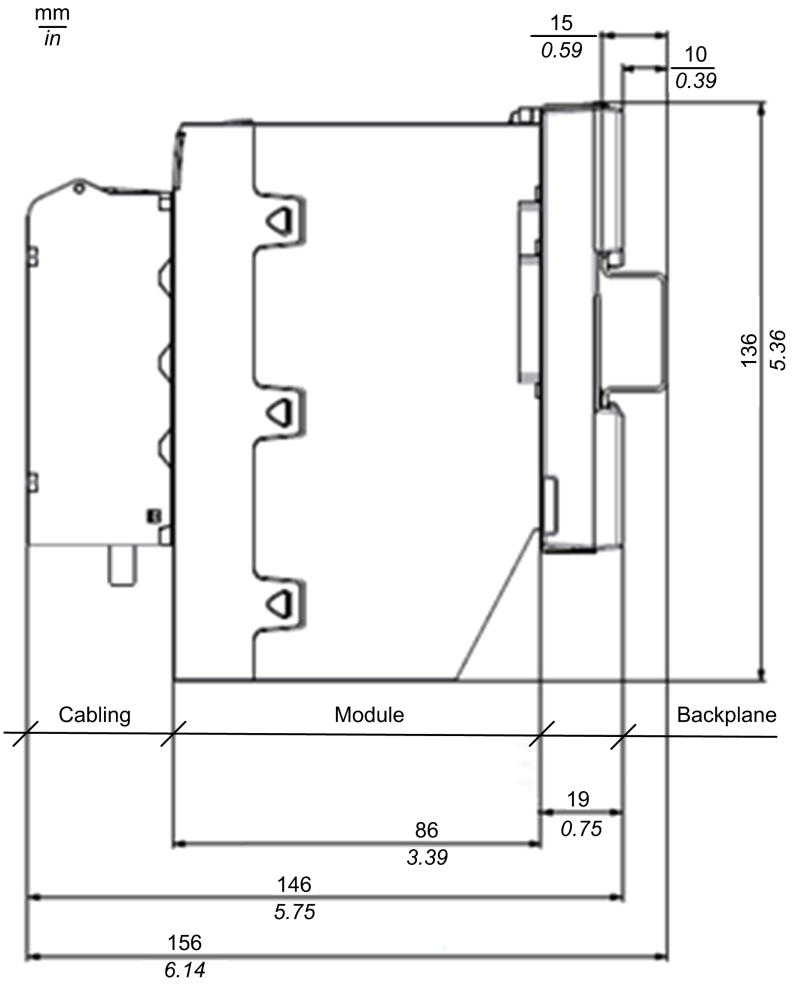


HINWEIS: Berücksichtigen Sie bei der Planung einer Rackinstallation die Höhe der E/A-Sicherheitsmodule. Jedes E/A-Sicherheitsmodul steht über die untere Kante des Racks hervor:

- 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

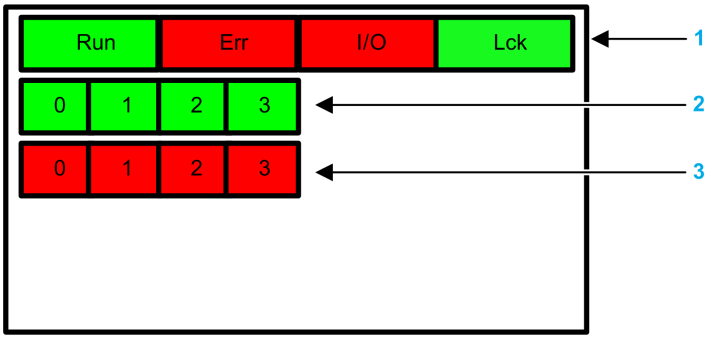
An der Frontplatte jedes E/A-Sicherheitsmoduls stehen LEDs zur Modul- und Kanaldiagnose bereit:

- 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:

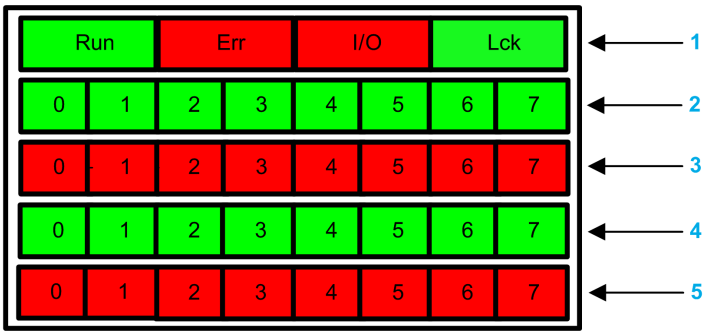


1 Modulstatus-LEDs

2 Kanalstatus-LEDs

3 Kanalfehler-LEDs

LEDs der digitalen BMXSDI1602-Sicherheitseingangsmodule:



1 Modulstatus-LEDs

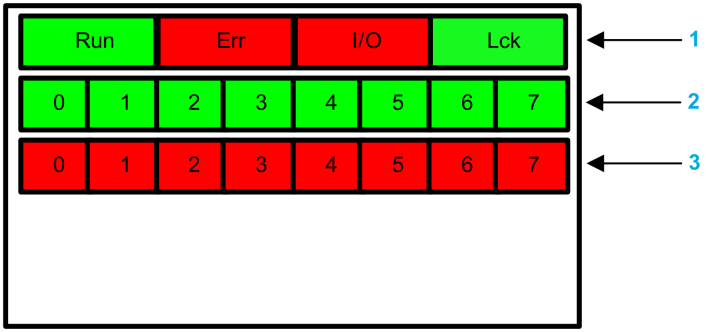
2 Kanalstatus-LEDs für Rang A

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.

Leistungskenndaten des analogen BMXSAI0410-Sicherheitseingangsmoduls

Leistungskenndaten des analogen Eingangsmoduls

Das analoge Sicherheitseingangsmodul BMXSAI0410 weist folgende Leistungsmerkmale auf:

Statische Kenndaten		**Wert**
Eingangsimpedanz im Signalbereich		286 Ω
Analoger Eingangsfehler	Max. Gesamtskalenfehler bei 25 °C	0,30 %
Analoger Eingangsfehler (= Sicherheitstoleranz)	Max. Gesamtskalenfehler, voller 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)
Bereichsüberschreitung (Erkennung)		< 3,75 mA und > 20,75 mA
Digitale Auflösung	Auflösung	16 Bit
	Anzahl gleichzeitig konvertierter Kanäle	4
Vom Anwendungsprogramm zurückgegebenes Datenformat		Binär
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 Kenndaten		**Wert**
	Typ	Potentialfreie, galvanisch getrennte Eingänge
	Max. Eingangsbereich	0 bis 25 mA
Gleichtakt-Kenndaten	Gleichtaktunterdrückung	Zu messen

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

Allgemeine Kenndaten		**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 - 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 Kenndaten		**Wert**
Monotonie ohne fehlenden Code		Ja
Übersprechen zwischen Gleichstrom und Wechselstrom 50 Hz und AC 60 Hz		–
Nicht-Linearität	+/-	0,006 % (LSB)
Wiederholgenauigkeit bei stabiler Temperatur nach vorgegebener Stabilisierungszeit		–
Aufnahme 3,3 V	Typisch	223 mA
	Maximal	256 mA
Aufnahme 24 V	Typisch	92 mA
	Maximal	115 mA
Verlustleistung	Maximal	3,98 W

Leistungskenndaten des digitalen BMXSDI1602-Sicherheitseingangsmoduls

Leistungskenndaten des digitalen Eingangsmoduls

Das Sicherheitseingangsmodul BMXSDI1602 weist folgende Leistungsmerkmale auf:

Merkmal		**Wert**
Eingangsbemessung	Spannung	24 VDC
Spannungsversorgung vom Typ 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)	Von 19 bis 30 V (möglich bis 33, begrenzt auf 1 Stunde pro Tag)
Eingangsimpedanz	Bei Unom	7,5 kΩ
Ansprechzeit	Typisch/Max.	100 µs / 250 µs
Zuverlässigkeit	MTTF bei Tamb = 25 °C	31,5 Jahre
Verpolung		Geschützt
IEC61131-2 - Ausgabe 3.0 (2007)		Typ 3
Kompatibilität	(Näherungssensoren 2 Drähte, 3 Drähte)	IEC 947-5-2
Dielektrische Spannungsfestigkeit	Primär/Sekundär	1500 Veff (bei 4000 m) 50/60 Hz für 1 min
Isolationswiderstand		> 10 µH (bei 500 VDC)
Eingangstyp		Sink (Strom ziehend)
Eingangsparallelschaltung(1)		Ja
Sensorspannung Überwachungsschwellen-wert	OK	> 18,6 VDC < 32 VDC
	Außerhalb des Betriebsbereichs	< 18,6 VDC > 33 VDC

Merkmal		Wert
Sensorspannungsüberwachung Ansprechzeit	Bei Verschwinden	4,4 ms < T < 30 ms
	Bei Auftreten	0,18 ms < T < 0,3 ms
Max. externe Kapazität bei SV-Verwendung für 24-V-Kurzschlusserkennung	Maximal	80 nF
Aufnahme 3,3 V	Typisch	200 mA
	Maximal	256 mA
Aufnahme 24 V	Typisch	63 mA
	Maximal	100 mA
Max. Verlustleistung		3,57 W
(1) Diese Eigenschaft ermöglicht die Verdrahtung mehrerer Eingänge am gleichen Modul oder an verschiedenen Modulen, wenn redundante Eingänge erforderlich sind.		

Leistungskenndaten des digitalen BMXSDO0802-Sicherheitsausgangsmoduls

Leistungskenndaten 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
Spannungsversorgung vom Typ externer Aktor		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
	Falsche Polarität	Ja
	Übertemperatur	Ja
Mindestlast Widerstandswert (für Voraktor)		48 Ω
Vollständige Drahtbrucherkennung: Maximaler Wert der Kabellastkapazität (einschließlich Voraktorkapazität) zwischen Ausgang und Voraktor		10 nF
Ansprechzeit(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 internen Überspannungsbegrenzer
	Gegen Verpolung	Ja - über umgekehrt montierte Diode. Bringen Sie eine Sicherung an die 24-V-Voraktoren an.
	Gegen Kurzschluss und Überlast	Ja - über Strombegrenzer und elektronischen Leistungsschalter 1,5 In < Id < 2 In
Spannung 24-V-Voraktor Überwachungs-schwellenwert	OK	> 19,0 V und < 31,8 V
	Bereichsüberschreitung	< 18,0 V und > 31,8 V
Voraktor-Spannungsüberwa-chung Ansprechzeit	Bei Verschwinden	2 ms < T < 5,6 ms
	Bei Auftreten	10 ms < T < 15,6 ms
Aufnahme 3,3 V	Typisch	240 mA
	Maximal	264 mA
Aufnahme 24-V-Baugruppenträger	Typisch	80 mA
	Maximal	90 mA
Aufnahme 24-V-Voraktor (ohne Laststrom)	Typisch	5 mA
	Maximal	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 h. **(2)** Alle Ausgänge verfügen über elektromagnetische Schnellentmagnetisierungsschaltungen. 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

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.

Planung der Installation des lokalen Racks

Einführung

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

UNBEABSICHTIGTER GERÄTEBETRIEB

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 Spannungsversorgung, CPU, Koprozessor und E/A werden durch natürliche Konvektion gekühlt. 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.

Verwendung der Racks

Die in Control Expert verfügbaren Racks und ihre zulässige Verwendung werden im Folgenden 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 1600	16	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
BME XBP 1402	14	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
BMX XBP 1600	16	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						

Mindestabstand um die Racks

Lassen Sie auf der rechten Seite jedes Racks mindestens 12 mm (0.472 in.) Platz für die Kühlung.

Halten Sie einen Mindestabstand von 35 mm (1.378 in) vor den Modulen ein, wenn Sie Erweiterungsracks einplanen. Für das BMX XBE 1000-Rack-Erweiterungsmodul ist dieser Freiraum für den lokalen Busanschluss und den Abschlusswiderstand erforderlich.

Erforderliche Abstände für einen M580 CPU in einem lokalen Hauptrack

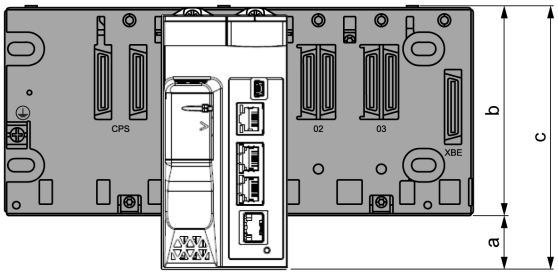
⚠WARNUNG

ÜBERHITZUNG UND UNBEABSICHTIGTER GERÄTEBETRIEB

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

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

Achten Sie im lokalen Hauptrack auf zusätzlichen Freiraum im unteren Teil des Racks für CPU. Diese Abbildung zeigt die Montageabmessungen, wenn ein X Bus-Rack oder ein Ethernet-Rack verwendet wird. Die Gesamthöhe des lokalen Hauptracks beträgt in beiden Fällen 134,6 mm (5.299 in.).



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

b: Höhe des Racks. Bei einem X Bus-Rack beträgt die Höhe 103,7 mm (4.083 in), bei einem Ethernet-Rack 105,11 mm (4.138 in).

c: Höhe des lokalen Hauptracks, 135,7 mm (5.343 in.).

Thermische Faktoren innerhalb eines Gehäuses

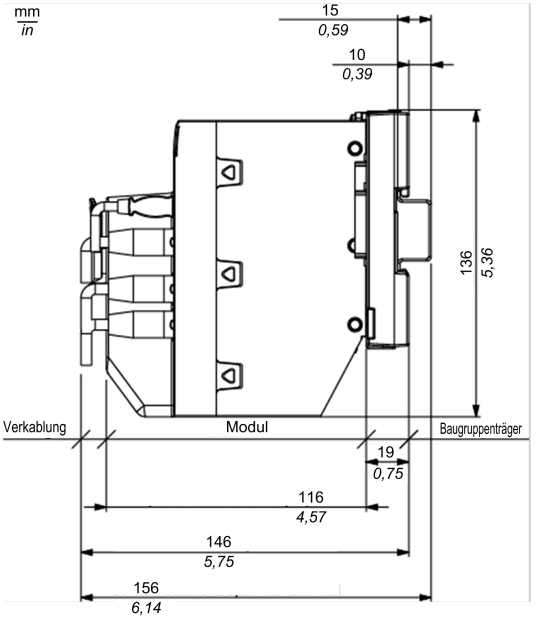
Wenn die Racks in einem Gehäuse installiert werden, muss für eine ausreichende Luftzirkulation gesorgt werden. Verwenden Sie ein Gehäuse mit folgenden Mindestabständen:

- 80 mm (3.15 in.) über der Oberseite der Module im Rack
- 60 mm (2.36 in.) unter der Unterseite der Module im Rack
- 60 mm (2.36 in.) zwischen Modulen und Kabelkanälen

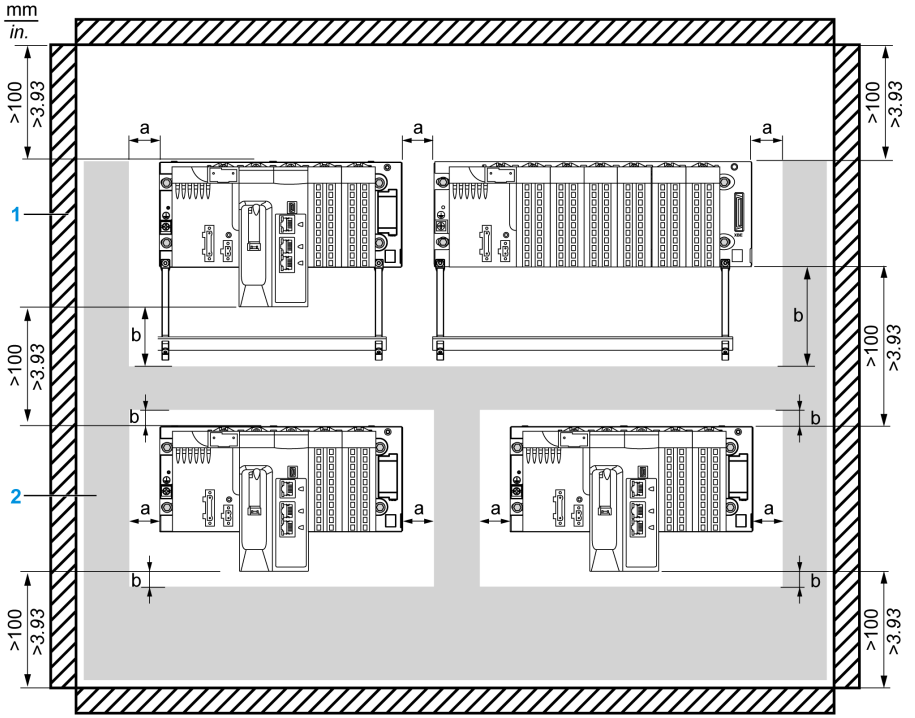
Mindesttiefe des Gehäuses:

- 150 mm (5.91 in.), wenn das Rack an einer Platte befestigt wird.
- 160 mm (6.30 in.) bei Montage des Racks auf einer DIN-Schiene 15 mm (0.59 in.).
- Wenn BMX XBE 1000-Rack-Erweiterungsmodule angeschlossen sind, verwenden Sie BMX XBC •••K-Kabel mit 45° abgewinkelten Steckverbindern.

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



Die folgende Abbildung zeigt die Regeln für eine typische Installation in einem Schaltschrank mit Kabelkanälen:



1 Installation oder Gehäuse

2 Kabelkanal oder -rinne

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

b Oberer und unterer Abstand zu umgebenden Objekten: > 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 ein Derating von 5 °C (9 °F) der maximal zulässigen Umgebungstemperatur. Das bedeutet 55 °C (131 °F) bei Standard- 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.

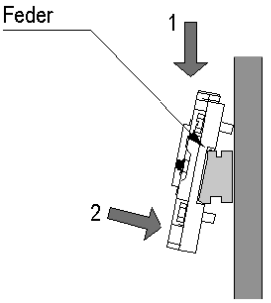
Montage auf einer DIN-Schiene

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.	

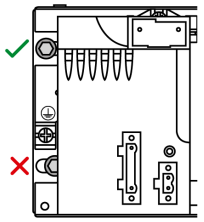
Gehen Sie zur Demontage eines Racks von einer DIN-Schiene vor wie folgt:

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

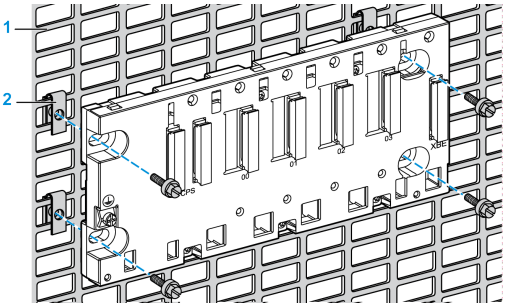
Sie können ein Rack an einer Wand innerhalb oder außerhalb eines Gehäuses mithilfe von M4-, M5-, M6- oder UNC #6-Schrauben in den Befestigungslöchern anbringen.

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.

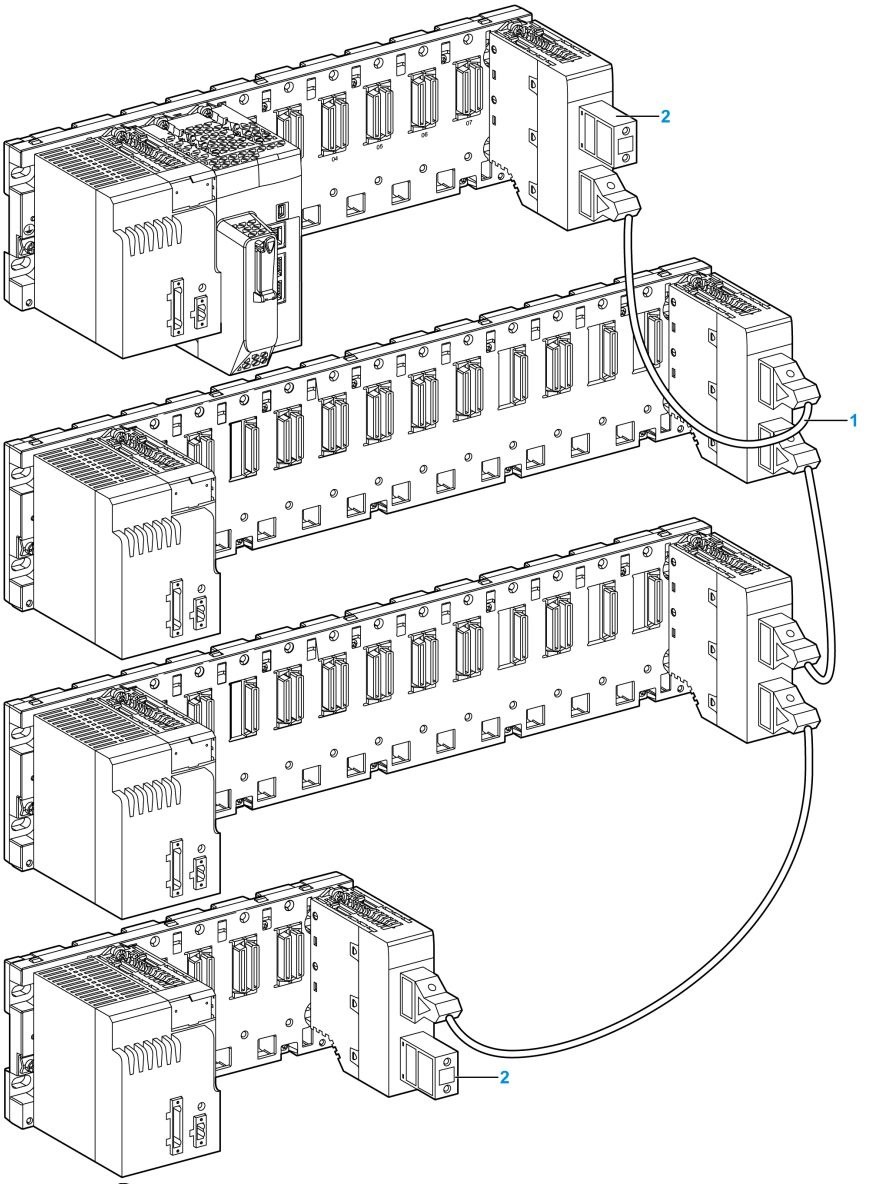
HINWEIS: Informationen zur Installation und Verbindung von Rack-Erweiterungsmodulen finden Sie unter *Installation von Modicon X80-Rack-Erweiterungsmodulen* im *Modicon M580 Hardware-Referenzhandbuch*.

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

Vorsichtsmaßnahmen bei der Installation

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

⚠⚠GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENS

- Trennen Sie alle Geräte vom Netz, einschließlich der angeschlossenen Geräte, bevor Sie Abdeckungen oder Türen entfernen oder Zubehör, Hardware, Kabel oder Drähte anbringen oder abnehmen. Eine Ausnahme hiervon bilden die im Hardwarehandbuch dieses Geräts beschriebenen besonderen Bedingungen.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um sicherzustellen, dass an den betreffenden Stellen und zum angegebenen Zeitpunkt tatsächlich keine Spannung mehr anliegt.
- Bringen Sie alle Abdeckungen, Zubehörteile, Hardware, Kabel und Drähte wieder an, sichern Sie sie und vergewissern Sie sich, dass eine ordnungsgemäße Erdung vorhanden ist, bevor Sie die Spannungszufuhr zum Gerät einschalten.
- Verwenden Sie für den Betrieb dieses Geräts und jeglicher verbundener Produkte ausschließlich die vorgeschriebenen Spannungswerte.

Die Nichtbeachtung dieser Anweisungen hat Tod oder schwere Verletzungen zur Folge.

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

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

Vergewissern Sie sich vor dem Einschalten, dass die Steuerung keine nicht unterstützte SD-Speicherkarte enthält.

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

HINWEIS:

- Stellen Sie sicher, dass die Abdeckung des Speicherkartensteckplatzes nach dem Einsetzen einer Speicherkarte in die Steuerung geschlossen ist.
- Siehe `%SW97` zur Überprüfung des Status der SD-Karte.

Installation von CPU und Koprozessor im Rack

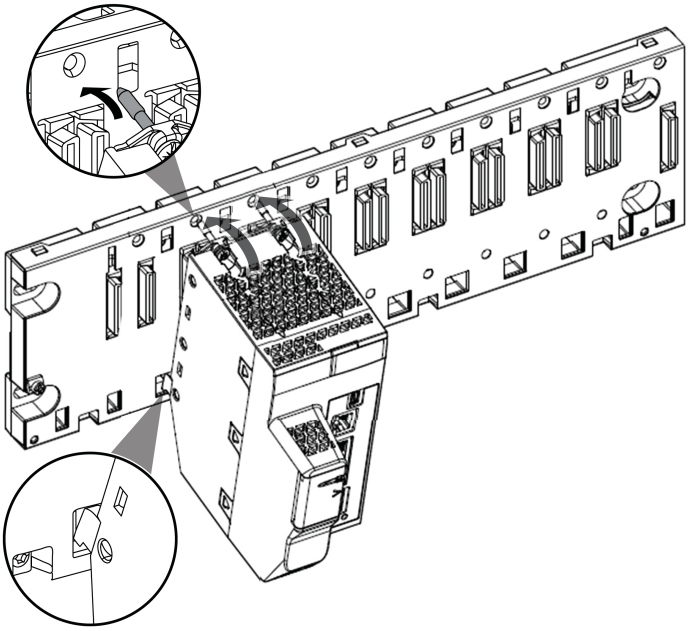
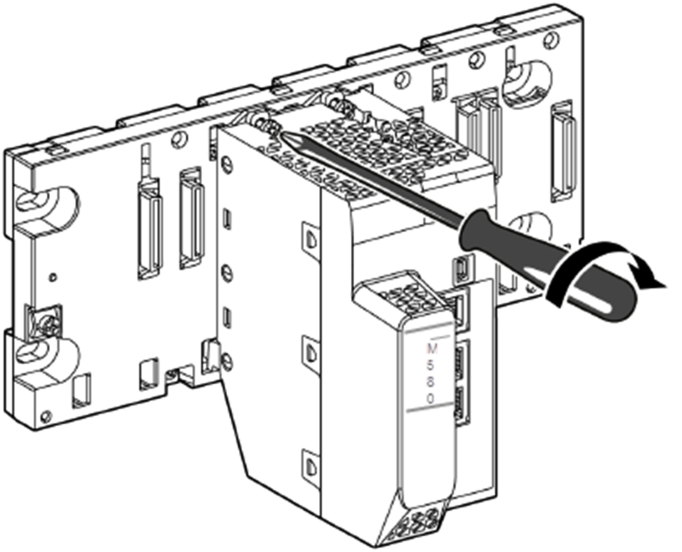
Installieren Sie CPU und Koprozessor im Rack in den folgenden Steckplätzen:

- CPU: Steckplätze **00** und **01**.

- Koprozessor: Steckplätze **02** und **03**

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

Schr-itt	Aktion
1	Stellen Sie sicher, dass die Spannungsversorgung ausgeschaltet ist.
2	Stellen Sie sicher, dass folgende Voraussetzungen erfüllt 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	Schwenken Sie das Modul gegen den oberen Rand 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 hat Tod oder schwere Verletzungen zur Folge.

Informationen zur Erdung von CPU und Koprozessor finden Sie im Abschnitt *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

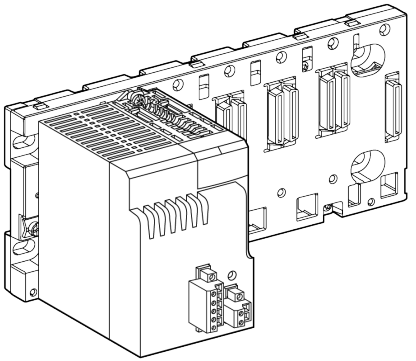
VERLUST DER FÄHIGKEIT ZUR AUSFÜHRUNG DER SICHERHEITSFUNKTION

Setzen Sie die Sicherheitsspannungsversorgung BMXCPS4002S, BMXCPS4022S oder BMXCPS3522S nur in einem Rack ein, das mindestens ein 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**. Für ein BMEXBP••02-Rack mit dualer Spannungsversorgung (siehe Modicon M580, Hardware, Referenzhandbuch) platzieren Sie zwei M580-Sicherheitsspannungsversorgungsmodule nebeneinander in die vier mit **CPS** markierten Steckplätzen.

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 einsetzen oder daraus entnehmen.

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.

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

⚠⚠GEFAHR

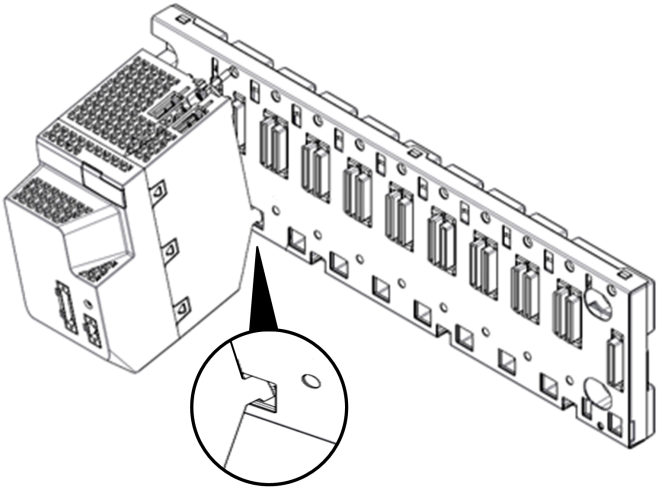
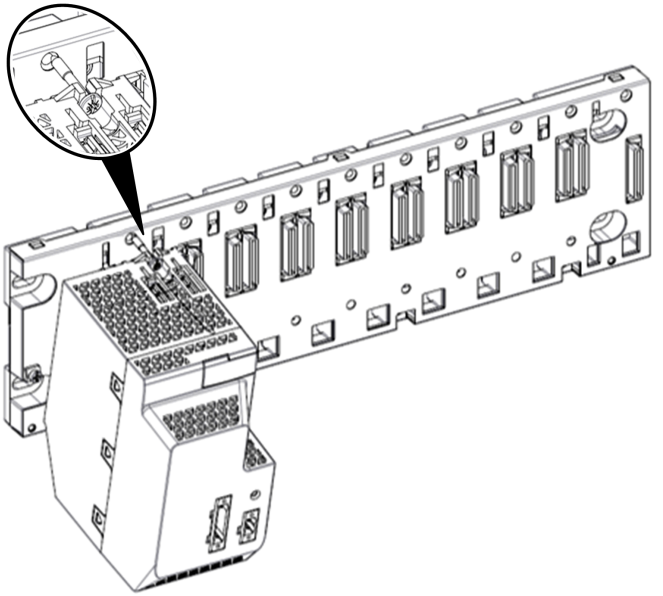
GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENS

- Trennen Sie alle Geräte vom Netz, einschließlich der angeschlossenen Geräte, bevor Sie Abdeckungen oder Türen entfernen oder Zubehör, Hardware, Kabel oder Drähte anbringen oder abnehmen. Eine Ausnahme hiervon bilden die im Hardwarehandbuch dieses Geräts beschriebenen besonderen Bedingungen.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um sicherzustellen, dass an den betreffenden Stellen und zum jeweils angegebenen Zeitpunkt tatsächlich keine Spannung mehr anliegt.
- Bringen Sie alle Abdeckungen, Zubehörteile, Hardware, Kabel und Drähte wieder an, sichern Sie sie und vergewissern Sie sich, dass eine ordnungsgemäße Erdung vorhanden ist, bevor Sie die Spannungszufuhr zum Gerät einschalten.
- Verwenden Sie für den Betrieb dieses Geräts und jeglicher verbundener Produkte ausschließlich die vorgeschriebenen Spannungswerte.

Die Nichtbeachtung dieser Anweisungen hat Tod oder schwere Verletzungen zur Folge.

Installation der Spannungsversorgung in einem Rack

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

Schr-itt	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	Schwenken Sie das Modul gegen den oberen Rand des Racks, sodass das Modul bündig an die Rackrückseite 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 hat Tod oder schwere Verletzungen zur Folge.

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.

Hot Swapping ist für M580-Sicherheits-E/A möglich.

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 eingehenden Eingangskabeln wie auch von den zu den Aktoren 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.

Verwenden Sie eine BMXXSP••••-Leiste, um das Rack vor elektromagnetischen Störungen zu schützen.

Verwenden Sie für das analoge BMXSAI0410-Sicherheitseingangsmodul eine BMXXSP••••-Leiste. Verbinden Sie den Kabelmantel mit der Erdungsleiste durch Anklemmen auf Modulseite.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENS

- Stellen Sie sicher, dass jede Klemmenleiste beim Anbringen oder Entfernen von E/A-Sicherheitsmodulen mit der BMXXSP••••-Erdungsleiste verbunden bleibt.
- Trennen Sie die Spannungsversorgung der Sensoren bzw. Aktoren.

Die Nichtbeachtung dieser Anweisungen hat Tod oder schwere Verletzungen zur Folge.

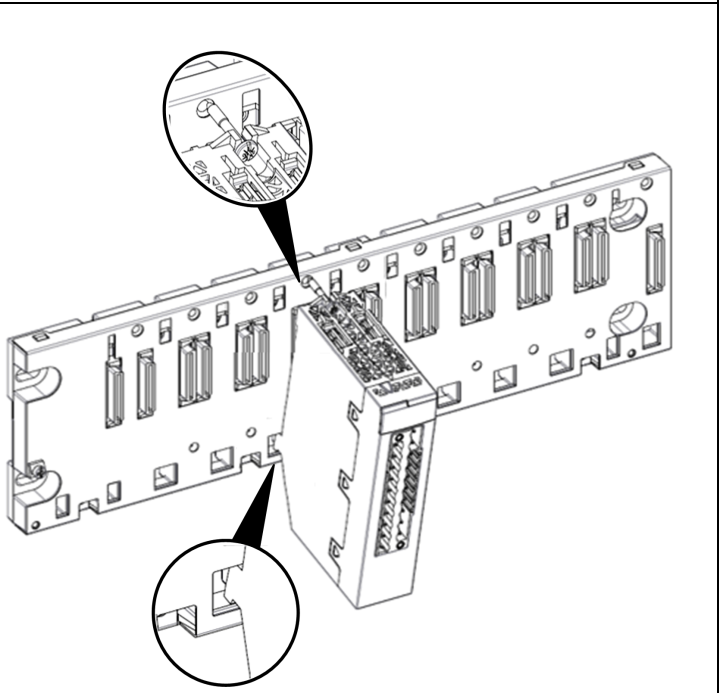
Installation von Eingangsmodulsensoren (in Bezug auf die Erdung)

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

- Positionieren Sie die Sensoren in nächster Nähe zueinander. Sie drüfen 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	Drehen Sie das Modul gegen den oberen Rand des Racks, sodass das Modul bündig an die Rackrückseite 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 Racks und des Spannungsversorgungsmoduls*.

HINWEIS: Verwenden Sie für das analoge BMXSAI0410-Sicherheitseingangsmodul eine BMXXSP••••-Erdungsleiste. Informationen zur Installation dieses Geräts finden Sie im Abschnitt *Schirmverbindungskit*.

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.
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.

Firmware-Upgrade für die M580-Sicherheitssteuerung

Das Verfahren ist von der ursprünglichen Version und der angestrebten Version der Steuerung abhängig. Ein neuer Bootloader wurde mit Version 4.x eingeführt. Daher erfordert die Aktualisierung von einer früheren Version (bis V3.22) auf die Version V4.x oder das Downgrade von einer V4.x-Version auf eine frühere Version spezifische Verfahren.

Detaillierte Anweisungen zur Firmwareaktualisierung finden Sie im *Modicon M580 Controller, Firmware-Installationshandbuch*.

Aktualisierung der Firmware auf Version 4.21

Sie können die Firmware der Sicherheitssteuerungen von den folgenden Vorgängerversionen auf Version 4.21 aktualisieren:

- 3.30.06 für BMEP586040S-Steuerungen
- 3.20.05 oder früher für die anderen M580-Sicherheitssteuerungen

Das Verfahren wird im Abschnitt *Firmware-Aktualisierung von v3.x auf v4.x* im Modicon M580 Controller Firmware-Installationshandbuch beschrieben.

Fallback-Firmwareversionen

Wenn die Firmwareaktualisierung nicht erfolgreich ist, wendet die Sicherheitssteuerung die folgende Fallback-Firmwareversion an:

- 3.30.06 für die BME58P6040S-Steuerung
- 3.20.05 für die anderen M580-Sicherheitssteuerungen

SPS-Anwendungsebene und Betriebszustand nach Abschluss der Aktualisierung

Wenn die Aktualisierung erfolgreich war, startet die Sicherheitssteuerung die zuvor in die Steuerung geladene Anwendung neu und arbeitet im STOP-Zustand.

HINWEIS: In diesem Fall befindet sich die Steuerung selbst dann im STOP-Zustand, wenn die Einstellung *Automatischer Start in RUN* ausgewählt ist.

Wenn die Aktualisierung nicht erfolgreich war und die zuvor in die Steuerung geladene Anwendung:

- nicht mit der Fallback-Firmwareversion kompatibel ist, startet die Steuerung im Betriebszustand NOCONF (Keine Konfiguration) neu.
- mit der Fallback-Firmwareversion kompatibel ist, startet die Steuerung die zuvor in die Steuerung geladene Anwendung neu und arbeitet im STOP-Zustand.

Downgrade der Firmware von Version 4.21 oder höher

Sie können ein Downgrade der Firmware von Sicherheitssteuerungen ab Version 4.21 auf die folgenden Vorgängerversionen durchführen:

- Version 3.30.06 für BMEP586040S
- Version 3.20.05 für die anderen M580-Sicherheitssteuerungen

Das Verfahren wird im *Modicon M580 Controller Firmware-Installationshandbuch*, Abschnitt *Firmware-Downgrade*, beschrieben.

Fallback-Firmwareversionen

Wenn das Firmware-Downgrade nicht erfolgreich ist, müssen Sie das Tool EcoStruxure Automation Device Maintenance (EADM) verwenden, um die Steuerung durch Installation einer Firmwareversion ab 4.21 zu regenerieren.

SPS-Anwendungsebene und Betriebszustand nach Abschluss des Downgrades

Wenn das Downgrade erfolgreich ist und die zuvor in die Steuerung geladene Anwendung:

- nicht mit der Fallback-Firmwareversion kompatibel ist, startet die Steuerung im Betriebszustand NOCONF (Keine Konfiguration) neu.
- mit der Fallback-Firmwareversion kompatibel ist, startet die Steuerung mit der zuvor in die Steuerung geladenen Anwendung neu und arbeitet im STOP-Zustand, selbst wenn die Einstellung *Automatischer Start in RUN* ausgewählt ist.

Wenn das Downgrade nicht erfolgreich ist, behält die Steuerung ihre ursprüngliche Firmware bei.

Bedienung eines M580-Sicherheitssystems

Einführung

Dieses Kapitel enthält Informationen zur Bedienung eines M580-Sicherheitssystems.

Prozess-, sicherheitsspezifische und globale Datenbereiche in Control Expert

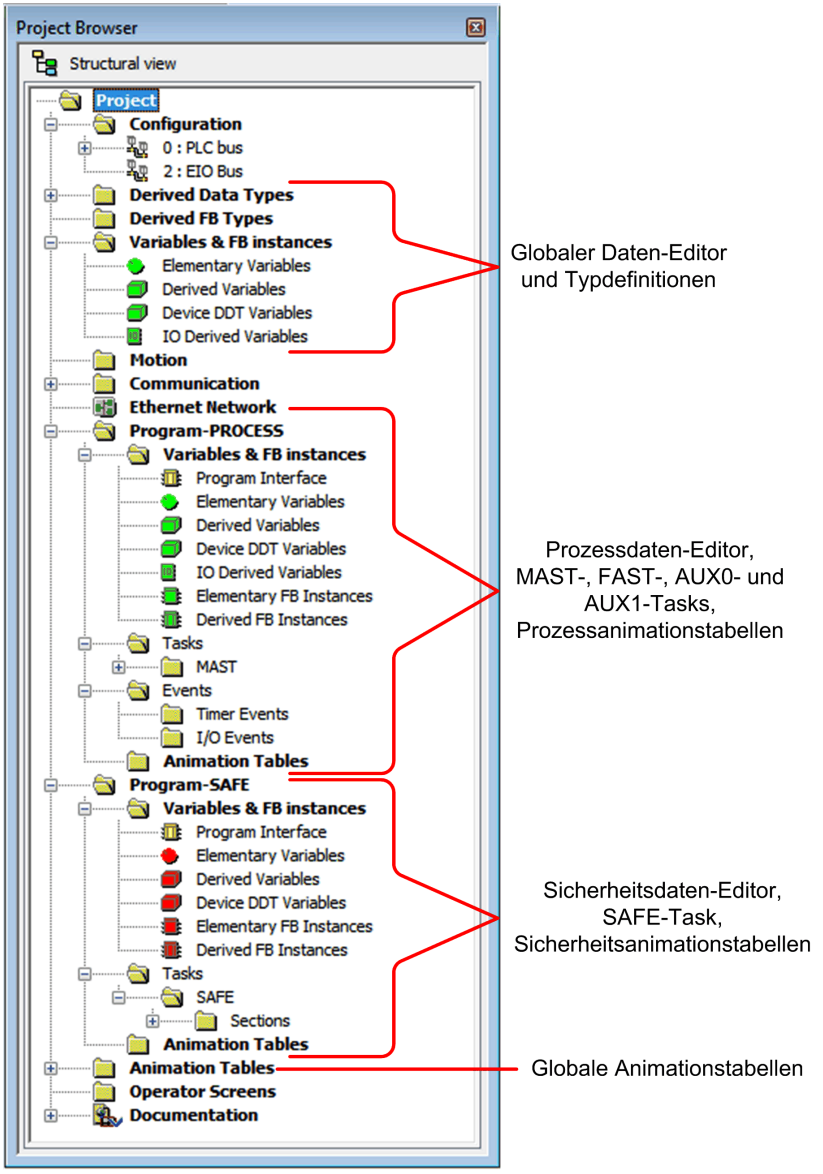
Einführung

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:



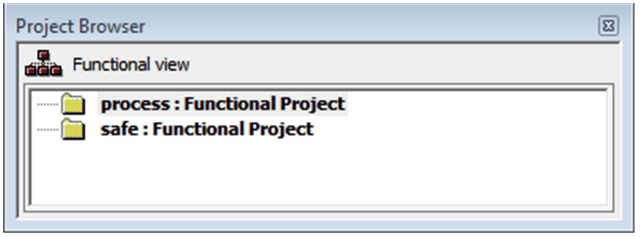
Eine Analyse des **Projekt-Browsers** ergibt Folgendes:

- 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. der Konfiguration aktiviert werden kann.

Die Software Control Expert XL Safety ist das exklusive Tool, das Sie zur Verwaltung der Betriebsartübergänge verwenden können.

HINWEIS: Die Betriebsarteinstellung für einen Hot Standby-Sicherheits-PAC - Sicherheits- oder Wartungsmodus - wird bei der Übertragung einer Anwendung vom Primär- 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.

Sicherheitsmodus und Einschränkungen

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 einem 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 temporär, da der Sicherheits-PAC automatisch in den Sicherheitsmodus wechselt, wenn die Kommunikation zwischen Control Expert und PAC unterbrochen wird bzw. bei Ausführung eines Trennbefehls. 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 einem 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 wird die SIL-Stufe der Sicherheitssteuerung nicht aufrechterhalten.

⚠WARNUNG

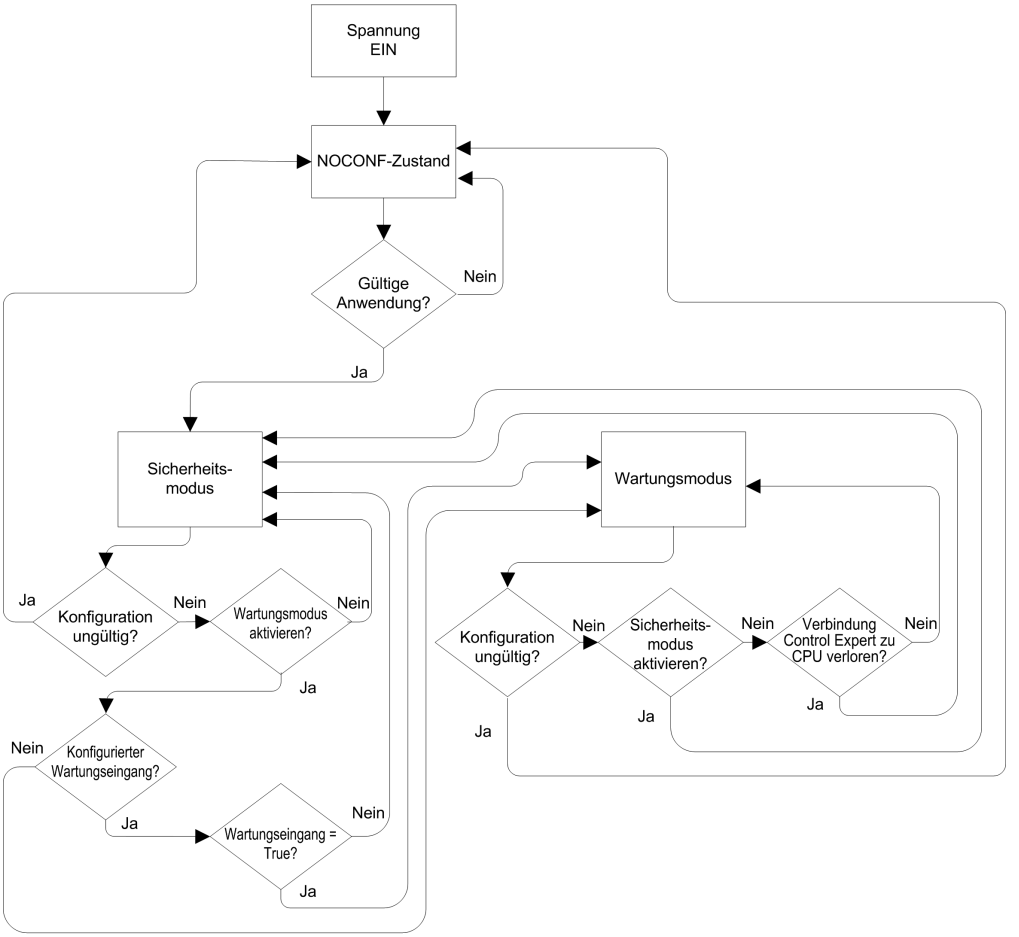
VERLUST DES SICHERHEITS-INTEGRITÄTSLEVELS

Ergreifen Sie geeignete Maßnahmen, um den sicheren Zustand des Systems zu gewährleisten, wenn sich die Sicherheitssteuerung im Wartungsmodus befindet.

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 der einen in die andere Betriebsart wechselt.



Bei der 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 den entsprechenden Menü- oder Symbolleistenbefehl in Control Expert.
  - Automatisch durch den Sicherheits-PAC, wenn die Kommunikation zwischen Control Expert und für ca. 50 Sekunden unterbrochen wird.
- Wenn die Wartungseingangsfunktion konfiguriert ist, dient sie zur Überprüfung des Übergangs vom Sicherheits- in den Wartungsmodus. Die Wartungseingangsfunktion wird in Control Expert auf der Registerkarte zur CPU-**Konfiguration** konfiguriert:
  - Durch Auswahl der Einstellung **Wartungseingang**. Und:
  - Durch 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 ist, wird der PAC im Sicherheitsmodus gesperrt. Wenn das Bit auf 1 (True) gesetzt ist, kann ein Übergang in den Wartungsmodus erfolgen.

Umschalten 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 Section der SAFE-Task ist ein Haltepunkt aktiviert.
- In einer Section der SAFE-Task ist ein Überwachungspunkt aktiviert.

Wenn der Debug-Modus nicht aktiv, kein SAFE-Task-Haltepunkt aktiviert und kein SAFE-Task-Überwachungspunkt festgelegt ist, können Sie einen Übergang zwischen dem Sicherheits- und dem Wartungsmodus manuell aktivieren. Gehen Sie dazu vor wie folgt:

- Zur Umschaltung vom Sicherheits- in den Wartungsmodus haben Sie folgende Möglichkeiten:
  - Auswählen von **SPS > Wartung** oder
  - Klicken auf die Schaltfläche  in der Symbolleiste

- Zur Umschaltung vom Wartungs- in den Sicherheitsmodus haben Sie folgende Möglichkeiten:
  - Auswählen von **SPS > Sicherheit** oder
  - Klicken auf die Schaltfläche  in der Symbolleiste

  HINWEIS: Das Aktivieren und Beenden des Sicherheitsmodus werden als Ereignisse im SYSLOG-Server in der CPU gespeichert.

Identifizieren der Betriebsart

Sie können die aktuelle Betriebsart eines M580-Sicherheits-PAC anhand der **SMOD**-LEDs der CPU und des Koprozessors oder über Control Expert bestimmen.

Wenn die **SMOD**-LEDs von CPU und Koprozessor:

- *Blinken*: Der PAC befindet sich im Wartungsmodus.
- *Permanent leuchten*: Der PAC befindet sich im Sicherheitsmodus.

Wenn Control Expert mit dem PAC verbunden ist, wird die Betriebsart des M580-Sicherheits-PAC anhand folgender Elemente identifiziert:

- Systemwörter %SW12 (Koprozessor) und %SW13 (CPU), Seite 228 - 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 beiden Systemwörter oder beide den Wert 16#5AFE (hex.) aufweisen, dann befindet sich der PAC im Sicherheitsmodus.
- Auf den zwei Unterregisterkarten **Task** und **Information** der CPU-Registerkarte **Animation** wird die Betriebsart des PAC angezeigt.
- Die 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*.

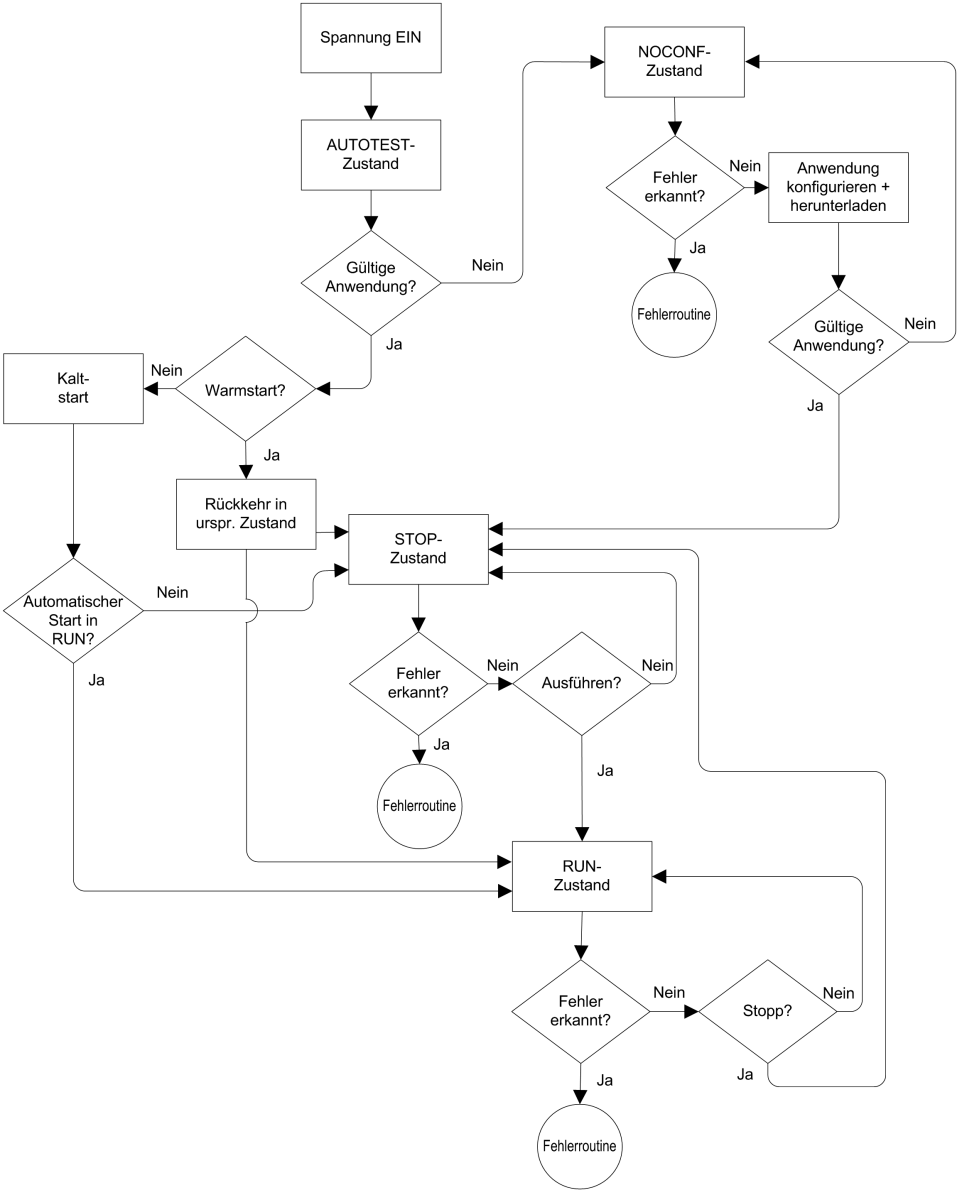
Betriebszustand	Gilt für ...	Beschreibung
AUTOTEST	PAC	Die CPU führt interne Selbsttests durch. **HINWEIS:** Wenn Erweiterungsracks mit dem lokalen Hauptrack verbunden sind und nicht verwendete Anschlüsse am Rack-Erweiterungsmodul nicht mit Leitungsabschlüssen versehen wurden, verbleibt die CPU auch 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 121). • Die Ausführung wurde durch einen STOP-Befehl abgebrochen (sicherer Modus, Seite 121 oder Wartungsmodus, Seite 122). • 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.

Betriebszustand	Gilt für ...	Beschreibung
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 121: Die Sicherheitsfunktion wird ausgeführt und sämtliche Einschränkungen werden angewendet. • Im Wartungsmodus, Seite 122: 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 135 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 135 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 130 finden Sie Informationen zur Fehlerverwaltung durch das Sicherheitssystem.

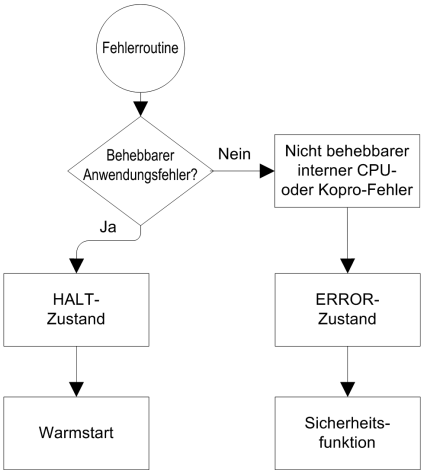
Fehlerverwaltung

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

Der M580-Sicherheits-PAC kann in den folgenden Situationen in die Anlaufsequenz wechseln:

- 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 135 oder einen Warmstart, Seite 135 aus.

Anlauf bei Erstinbetriebnahme

Bei der ersten Inbetriebnahme führt der M580-Sicherheits-PAC einen Kaltstart durch. Alle Tasks, einschließlich der SAFE-Task und der Nicht-SAFE-Tasks (MAST, FAST, AUX0, AUX1), wechseln in den STOP-Zustand, es sei denn, **Automatischer Start in RUN** ist aktiviert. In diesem Fall wechseln alle Tasks in den RUN-Zustand.

Anlauf nach einer Unterbrechung der Spannungsversorgung

Die Sicherheitsspannungsversorgung M580 bietet eine Spannungsreserve, die im Falle einer Unterbrechung der Spannungsversorgung alle Module im Rack für bis zu 10 ms 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 bis %SW58)
- Zustand jeder Task
- Zustand der Ereignis-Timer
- Werte der aktiven Zähler
- Signatur der Anwendung
- Anwendungsdaten (aktuelle Werte der Anwendungsvariablen)
- Prüfsumme der Anwendung

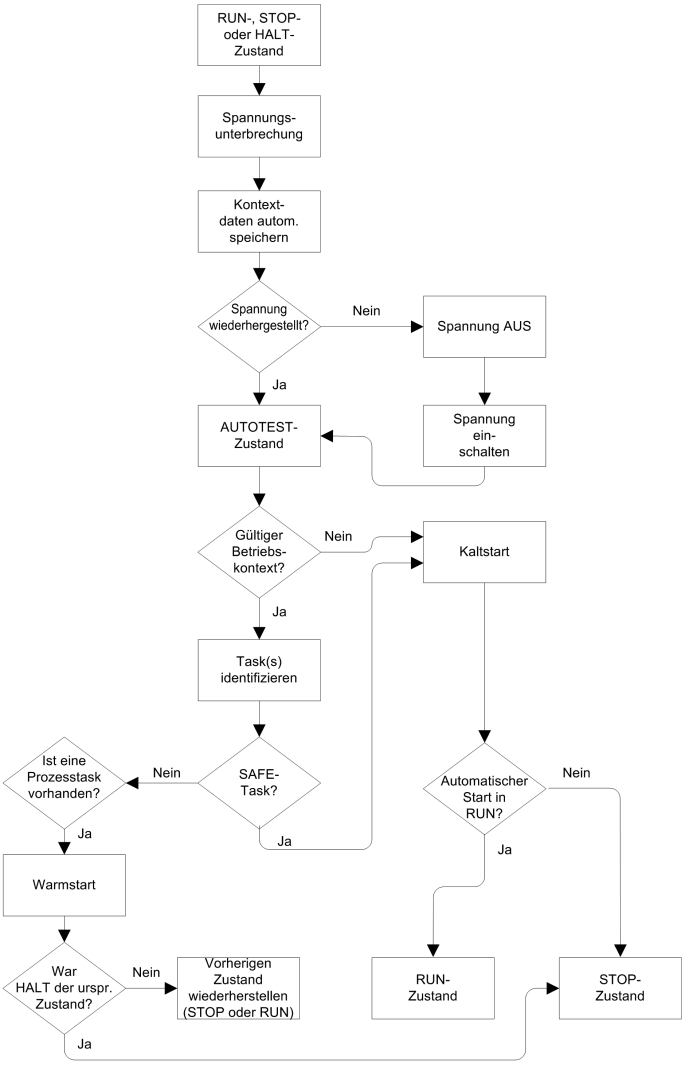
Nach dem Herunterfahren kann der Systemanlauf entweder automatisch (wenn die Spannungsversorgung vor Abschluss des Herunterfahrens wiederhergestellt wurde) oder manuell (wenn nicht) erfolgen.

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 wechseln alle Tasks, einschließlich der SAFE-Task und der nicht-sicheren Tasks (MAST, FAST, AUX0, AUX1), in den STOP-Zustand, es sei denn, **Automatischer Start in RUN** ist aktiviert. In diesem Fall wechseln alle Tasks in den RUN-Zustand.

Bei einem Kaltstart werden folgende Vorgänge ausgeführt:

- Den Anwendungsdaten (einschließlich der internen Bits, E/A-Daten, internen Wörter usw.) werden die von der Anwendung definierten Initialwerte 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 folgende Auswahl ausgeführt werden: **SPS > Init** in Control Expert, Seite 151, oder indem Sie das Systembit %S0 (COLDSTART) auf 1 setzen. 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, dass jede Prozesstask - einschließlich der Tasks (MAST, FAST, AUX0, AUX1) - in ihren Betriebszustand zum Zeitpunkt der Spannungsunterbrechung zurückgesetzt wird. Die SAFE-Task wechselt bei einem Warmstart dagegen in den STOP-Zustand, es sei denn, **Automatischer Start in RUN** ist 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 ab Beginn der Task wieder aufgenommen.

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

Stellen Sie sicher, dass die Option **Automatischer Start in RUN** mit dem ordnungsgemäßen Verhalten Ihres Systems kompatibel ist. Deaktivieren Sie andernfalls diese Funktion.

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	Priorität	Zeitmodell	Periodenbereich	Standardperiode	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. Wenn CCOTF aktiviert ist (durch Auswahl von **Online-Änderung im RUN- oder STOP-Modus** auf der Registerkarte **Konfiguration** im Dialogfeld der CPU-Eigenschaften), beträgt die minimale **Watchdog**-Einstellung 64 ms.

3. Unterstützt von BMEP58•040S-Sicherheits-PACs im Standalone-Betrieb. Von BMEH58•040S-Sicherheits-PACs im Hot Standby-Betrieb nicht unterstützt.

4. Standalone-BMEP58•040S-Sicherheits-PACs unterstützen das zyklische und periodische Zeitmodell, Hot Standby-BMEH58•040S-Sicherheits-PACs nur das periodische Zeitmodell.

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) arbeiten im gleichen Speicherbereich, während die SAFE-Task in einem eigenen, separaten Speicherbereich arbeitet. 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 Koprozessor 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-Tasks 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, müssen Sie die Ausführungszeit der FAST-Task so kurz wie möglich konfigurieren. Verwenden Sie einen Watchdog-Wert für die FAST-Task, der nicht viel größer ist als die FAST-Periode.

Wenn die zur Ausführung der FAST-Task erforderliche Zeit die Watchdog-Einstellung überschreitet, wechseln die FAST-Task sowie alle anderen Nicht-SAFE-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-SAFE-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 148 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 140 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 Standalone als auch Hot Standby - umfassen einen Mechanismus zur Erzeugung eines algorithmischen SHA256-Fingerabdrucks der Sicherheitsanwendung umfassen: die SAFE-Quellsignatur (SourceSafeSignature). Bei der Übertragung der Anwendung vom PC in den PAC vergleicht Control Expert die SAFE-Quellsignatur auf dem PC mit der SAFE-Quellsignatur im PAC, um festzustellen, ob die

Sicherheitsanwendung im PC mit der Sicherheitsanwendung im PAC identisch ist oder sich von ihr 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 SAFE-Quellsignatur erzeugen und diese zum neuesten Build hinzufügen möchten, oder
- überhaupt nicht

Aktionen, die eine Änderung der SAFE-Quellsignatur bewirken

Sowohl Änderungen an der Konfiguration als auch Änderungen von Variablenwerten können eine Änderung der SAFE-Quellsignatur zur Folge haben.

Konfigurationsänderungen: Die folgenden Konfigurationsaktionen führen zu einer Änderung der Signatur:

Gerät	Aktion
Sicherheits-CPU	Änderung der CPU-Referenz über **Prozessor ersetzen...**
	Änderung der CPU-Version über **Prozessor ersetzen...**
	Bearbeitung eines Parameters auf den Registerkarten zur CPU-**Konfiguration** oder **Hot Standby**-Konfiguration
	Bearbeitung eines Parameters auf einer Registerkarte des Ethernet-Kommunikationskopfmoduls der CPU (**Sicherheit**, **IP-Konfig.**, **RSTP**, **SNMP**, **NTP**, **ServicePort**, **Sicherheit** usw.)
Sicherheitskoprozessor	Nicht zutreffend, da der Koprozessor nicht konfiguriert werden kann.
Anderes Sicherheitsmodul	**Hinzufügen**/**Löschen**/**Verschieben** eines Moduls, entweder: • Direkt (über einen Befehl) oder • 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 eines Sicherheitsmodulparameters auf der Registerkarte **Konfiguration** (Beispiel: **Kurzschlusserkennung an 24 V**, **Offene Draht-Erkennung**) und im linken Bereich des Editors (z. B. **Funktion**, **Fehlerwert**)
	Änderung der Modul-ID über den Befehl **IDs erneuern und alle generieren**

Gerät	Aktion
	Änderung des Namens einer Geräte-DDT-Instanz
CIP Safety-Modul	**Hinzufügen**/**Löschen** eines Moduls
	Änderung eines CIP Safety-Modulparameters im DTM-Editor des CIP Safety-Geräts oder in der **Geräteliste** des CPU-Master-DTM-Editors
	Änderung des Namens einer 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: Sofern nicht anders angegeben, sind die folgenden Elemente in der Berechnung der SAFE-Quellsignatur enthalten. Eine Änderung der folgenden Werte bewirkt eine Änderung der SAFE-Quellsignatur:

Typ	Komponenten
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 **Anwendungsbereich** = sicher.
Gemeinsame Bereichseinstellungen	Die folgenden **Projekteinstellungen** für **Anwendungsbereich** = gemeinsam:
	Variablen • Führende Zahlen zulassen • Zeichensatz • Verwendung von EBOOL-Flanke zulässig • INT/DINT anstelle von ANY_BIT zulässig

Typ	Komponenten
	• Bit-Extraktion von BYTE, INT, UINT, DINT, UDINT, WORD und DWORD zulässig • Direkt dargestellte Array-Variablen • Schnellabfrage zur Trenderstellung aktivieren • Referenzinitialisierung forcieren
	Programm > Sprachen > Gemeinsam • 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 > Zeit[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, aber jede Änderung ihrer Werte ändert die Teilsignatur der Konfiguration.	

Verwalten der SAFE-Quellsignatur

Die SAFE-Quellsignatur wird verwaltet in Control Expert im Fenster **Extras > Projekteinstellungen** durch Auswahl von **Allgemein > Generierungseinstellungen** und dann einer der folgenden Einstellungen zur **Verwaltung der SAFE-Signatur**:

- **Automatisch** (Standard): Generiert bei jeder Ausführung des Befehls **Generieren** eine neue SAFE-Quellsignatur.
- **Auf Benutzeranforderung**: Generiert eine neue SAFE-Quellsignatur, wenn der Befehl **Generieren > SAFE-Signatur aktualisieren** ausgeführt wird.

  HINWEIS: Wenn Sie **Auf Benutzeranforderung** auswählen, generiert Control Expert bei jeder Generierung eine SAFE-Quellsignatur mit dem Wert 0. Wenn Sie den Befehl **Generieren > SAFE-Signatur aktualisieren** nicht ausführen, wird die SAFE-Signatur-Funktion nicht verwendet.

Übertragen einer Anwendung vom PC in den PAC

Wenn Sie eine Anwendung vom PC in den PAC herunterladen, vergleicht Control Expert die SAFE-Quellsignatur in der heruntergeladenen Anwendung mit einer Signatur im PAC. Control Expert verhält sich wie folgt:

Neue SAFE-Signatur	SAFE-Signatur des PAC	Control Expert-Anzeige
Beliebig	Keine Anwendung	Übertragungsbestätigung
Beliebig (außer 0)	0	Übertragungsbestätigung
0	0	Übertragungsbestätigung
0	Beliebig (außer 0)	Übertragungsbestätigung, gefolgt von einem Hinweis auf das Zurücksetzen der SAFE-Signatur und einer erneuten Übertragungsbestätigung
XXXX = YYYY[2]	YYYY	Übertragungsbestätigung
XXXX ≠ YYYY[3]	YYYY	Übertragungsbestätigung, gefolgt von einem Hinweis auf die Änderung der SAFE-Signatur und einer erneuten Übertragungsbestätigung

1. Der Wert „0“ gibt an, dass keine SAFE-Quellsignatur automatisch oder manuell generiert wurde.

2. Die Sicherheitsanwendung im PC (XXXX) und die Sicherheitsanwendung im PAC (YYYY) sind IDENTISCH.

3. Die Sicherheitsanwendung im PC (XXXX) und die Sicherheitsanwendung im PAC (YYYY) sind VERSCHIEDEN.

Anzeigen der SAFE-Quellsignatur

Sofern eine SAFE-Quellsignatur 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 SAFE-Quellsignatur zu kopieren und zum Vergleich in ein geeignetes Texttool einzufügen. Der Wert der SAFE-Quellsignatur ist in Control Expert in folgenden Speicherpfaden zu finden:

- Registerkarte **Eigenschaften des Projekts > Identifikation**: Klicken Sie im **Projekt-Browser** mit der rechten Maustaste auf **Projekt** und wählen Sie **Eigenschaften** aus.
- Registerkarte **PLCScreen > Information** (siehe 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** (siehe EcoStruxure™ Control Expert, Betriebsarten): Wählen Sie diesen Befehl im Menü **SPS** aus.

- Dialogfeld **Projekt an SPS übertragen**: Wählen Sie diesen Befehl im Menü **SPS** (oder im Dialogfeld **PC < - - > SPS-Vergleich**) aus.

Vergleichen der SAFE-Quellsignatur mit der SAId

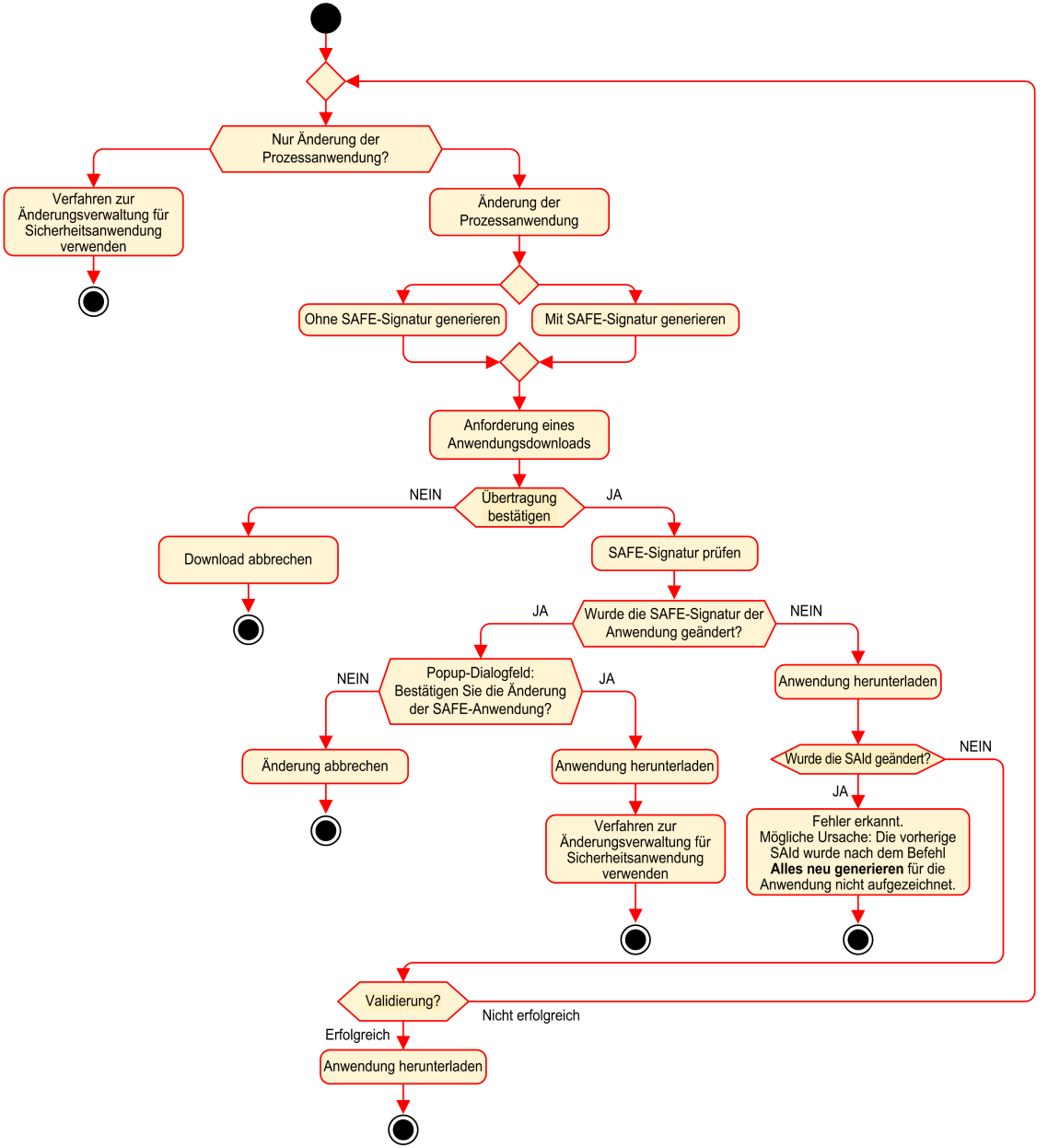
Die SAFE-Quellsignatur wurde eingeführt, um eine *Vorabkontrolle* zu ermöglichen und sicherzustellen, dass die Sicherheitsanwendung unverändert ist. Verwenden Sie diese Funktion bei jeder Änderung der Prozessanwendung, Seite 146, um eine unbeabsichtigte Änderung der Sicherheitsanwendung zu vermeiden.

Die SAFE-Quellsignatur 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 letzte Änderung des Sicherheitscodes.

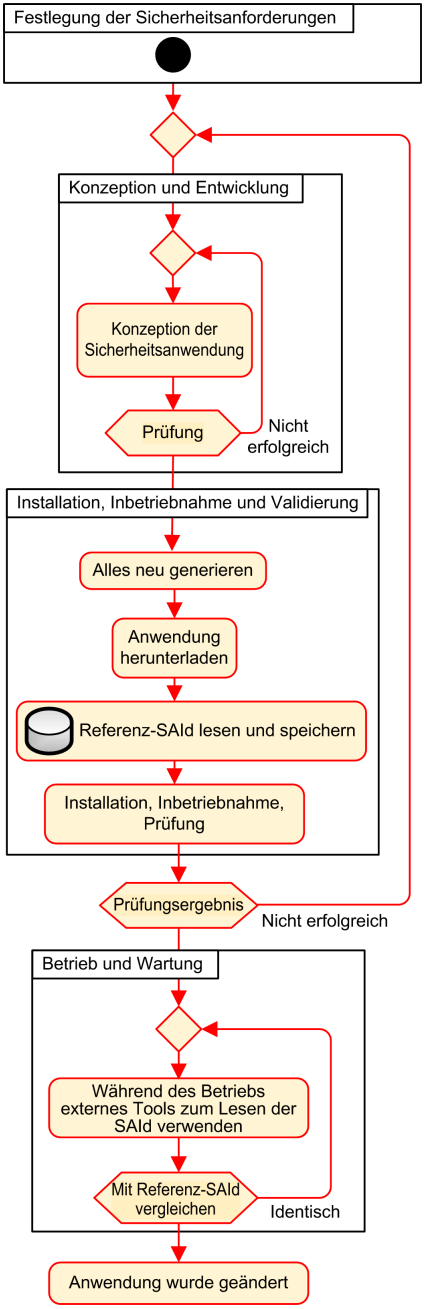
Die SAId kann nur während des Betriebs ausgewertet werden. Ihre Berechnung wird doppelt ausgeführt und sowohl von der CPU als auch vom KOPRO mit dem von der Sicherheitsanwendung ausgeführten Binärcode verglichen. Weil die SAId empfindlich auf alle Änderungen reagiert, einschließlich der Änderungen, die durch den Befehl **Alle neu generieren** nach einer Generierungsänderung ausgelöst werden können, verwenden Sie den Befehl **Alle neu generieren**, um eine Referenzversion der Sicherheitsanwendung zu generieren. Dieses Verfahren, Seite 147 ermöglicht die Verwendung jeder Art der Generierung (**Alle neu generieren**, **Änderungen generieren** - Online oder Offline) bei Prozessanwendungsänderungen ohne Änderung der SAId.

Die SAId ist die Best-Practice-Methode, mit der bestätigt werden kann, dass es sich bei der Sicherheitsanwendung um die validierte Anwendung handelt. Der SAId-Wert wird nicht automatisch von der Anwendung getestet. Überprüfen Sie aus diesem Grund die SAId regelmäßig anhand geeigneter Verfahren (z. B. mit Control Expert oder über ein HMI), indem Sie den Ausgang von Funktionsbaustein S_SYST_STAT_MX oder den Inhalt von Systemwort %SW169, Seite 228 auslesen.

Ändern der Prozessanwendung - Vereinfachtes Verfahren



SAId-Verwaltung



Sperre der Konfiguration der M580-E/A-Sicherheitsmodule

Sperre der Konfiguration der M580-E/A-Sicherheitsmodule

Sperre der Konfiguration der E/A-Sicherheitsmodule

Jedes E/A-Sicherheitsmodul verfügt über eine Konfigurationssperrtaste, Seite 76, die sich oben an der Modulfrontseite befindet. Aufgabe der Sperrfunktion ist die Verhinderung unbeabsichtigter Änderungen an der E/A-Modulkonfiguration. Beispielsweise kann die Sperre der aktuellen Konfiguration des E/A-Moduls den Versuch verhindern, dem Modul eine falsche Konfiguration zuzuweisen, oder zum Schutz vor Konfigurationsfehlern beitragen.

Um den gewünschten Sicherheits-Integritätslevel (SIL) zu erreichen, sollte jedes E/A-Sicherheitsmodul nach der Konfiguration vor (Wieder-) Aufnahme des Betriebs gesperrt werden.

⚠WARNUNG

VERLUST DES SICHERHEITS-INTEGRITÄTSLEVELS

Sperren Sie jedes E/A-Sicherheitsmodul nach der Konfiguration, jedoch vor Beginn des Betriebs.

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 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 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 Austausch (FDR) 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	Verwenden Sie den Befehl **Projekt von SPS übertragen** zum Laden des Projekts aus dem PAC in Control Expert.
3	Öffnen Sie im Fenster **SPS-Bus** in Control Expert jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert ist.
4	Prüfen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass die Konfiguration jedes Moduls mit der in Schritt 3 oben übereinstimmt.
5	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste, Seite 76 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 Austausch (FDR) 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 in Wartungsmodus, Seite 122.
3	Öffnen Sie im Fenster **SPS-Bus** in Control Expert jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert ist.
4	Prüfen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass sich die Konfiguration der Module nicht geändert hat und mit der Konfiguration in Schritt 3 oben übereinstimmt.
5	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste, Seite 76 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 in Wartungsmodus, Seite 122.
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 Fenster **SPS-Bus** in Control Expert jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert ist.
5	Prüfen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul und vergewissern Sie sich, dass sich die Konfiguration der Module nicht geändert hat und mit der Konfiguration in Schritt 3 oben übereinstimmt.
6	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste, Seite 76 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	Weisen Sie über das Menü **SPS** von Control Expert den PAC an, in den Sicherheitsmodus, Seite 121 zu wechseln.

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 135 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 Datenbereiche zugeordnet ist:

- Animationstabellen des Prozessbereichs enthalten ausschließlich Daten des prozessspezifischen 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 als „SAFE.<varname>“ angezeigt.
  - Eine Datenvariable aus dem Prozess-Namespace wird als „PROCESS.<Variablenname>“ angezeigt.
  - 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 wie folgt erstellen und bearbeiten:

- 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 in die Auslese-Informationen einbezogen oder von diesen ausgeschlossen werden. Wählen Sie in Control Expert dazu **Extras > Projekteinstellungen...** aus, um das Fenster **Projekteinstellungen...** zu öffnen und navigieren Sie dann zu **Projekteinstellungen > Allgemein > In SPS eingebettete Daten > Auslese-Information > Animationstabellen**.

Voraussetzungen für die Verwendung von Animationstabellen

Sie können Animationstabellen verwenden, um einen Variablenwert zu forcieren bzw. dessen Forcierung aufzuheben oder 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 Prozess-Namespace in Control Expert

Control Expert bietet zwei Möglichkeiten zum Erstellen von Animationstabellen für den sicherheits- oder prozessspezifischen Namespace:

- 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 aus:
  - **Animationstabelle initialisieren**, um das Datenobjekt in einer vorhandenen Animationstabelle im Sicherheits- oder Prozess-Namespace hinzuzufügen, oder
  - **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** im Bereich der Prozess- oder der Sicherheitsdaten mit der rechten Maustaste auf den Ordner **Animationstabellen** und wählen Sie **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 globalen Ordner **Animationstabellen** und 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 Dateneditor ziehen und in der globalen Animationstabelle ablegen. Da der Bereich der Animationstabelle die gesamte Anwendung umfasst, können Sie die Variable aus dem **Sicherheitsdateneditor**, dem **Prozessdaten-Editor** oder dem **Editor für globale Daten** ziehen.
- *Dialogfeld „Instanzauswahl“*: Sie können auf 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:
  - SICHER (SAFE): Anzeige der dem Sicherheitsbereich zugeordneten Datenobjekte.
  - PROZESS: Anzeige der dem Prozessbereich zugeordneten Datenobjekte.
  - ANWENDUNG: Anzeige der anwendungsspezifischen Datenobjekte einer höheren Ebene.

  Wählen Sie ein Datenobjekt aus und klicken Sie 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. einer HMI-, SCADA- oder FactoryCast-Anwendung - auf die gleiche Weise anzeigen, wie Sie Daten in einer Animationstabelle verknüpfen. Die zur Auswahl stehenden Datenvariablen sind diejenigen Variablen, die im Control Expert-Datenwörterbuch enthalten sind.

Sie können das Datenwörterbuch aktivieren, indem Sie das Fenster **Extras > Projekteinstellungen...** öffnen und dann im Bereich **Anwendungsbereich > Gemeinsam** des Fensters **Allgemein > In SPS eingebettete Daten > Datenwörterbuch** auswählen.

Das Datenwörterbuch stellt Datenvariablen in den Bedienerfenstern zur Verfügung:

- Sichere Namespace-Variablen enthalten immer 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.
- Über die Einstellung **Verwendung des Prozess-Namespace** wird festgelegt, wie ein Bedienerfenster auf die Variablen des Prozess-Namespace zugreifen kann.
  - Wenn Sie **Verwendung des Prozess-Namespace** auswählen, kann das Bedienerfenster die Variablen des Prozessbereichs nur über das Format „PROCESS.<Variablenname>“ lesen.
  - Wenn Sie die Auswahl von **Verwendung des Prozess-Namespace** aufheben, kann das Bedienerfenster die Variablen des Prozessbereichs nur über das Format „<Variablenname>“ ohne PROCESS-Präfix lesen.

    HINWEIS: Wenn zwei Variablen mit demselben Namen deklariert werden, eine 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.

Sie können das Dialogfeld **Instanzauswahl** verwenden, um auf einzelne Datenobjekte zuzugreifen.

⚠WARNUNG
UNBEABSICHTIGTER GERÄTEBETRIEB • Vergewissern Sie sich, 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 Tod, schwere 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. Oder:
- Wählen Sie **Verwendung des Prozess-Namespace** aus und verwenden Sie die folgende Syntax, um auf die Variablen mit demselben Namen zuzugreifen:
  - „PROCESS.<Variablenname>“ für Variablen, die im Prozess-Namespace deklariert sind.
  - „<Variablenname>“ ohne Präfix für die im globalen Namespace deklarierten Variablen.

Trendanalyse-Tool

Das Control Expert-Tool zur Trendanalyse kann nicht mit einem M580-Sicherheitsprojekt verwendet werden.

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 136.

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:

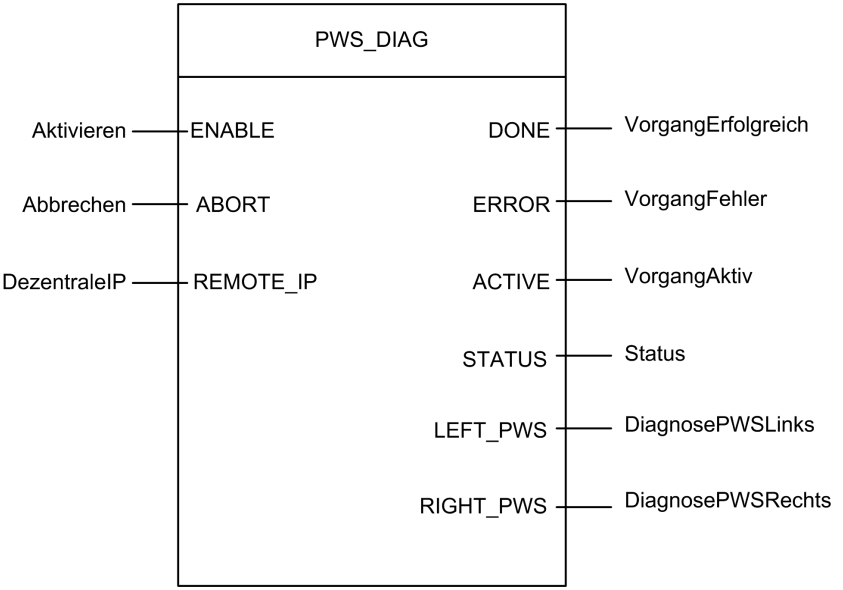
- Umgebungstemperatur der Spannungsversorgung
- Spannung und Strom auf der 3,3-V-Baugruppenträgerleitung
- Spannung und Strom auf der 24-VDC-Baugruppenträgerleitung
- Insgesamt kumulierte Energie der Spannungsversorgungen auf den 24-VDC- und 3,3-VDC-Baugruppenträgerleitungen seit Herstellung
- Betriebszeit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

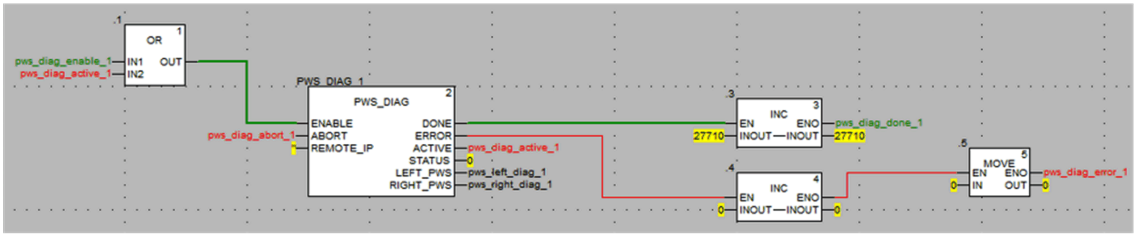
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine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

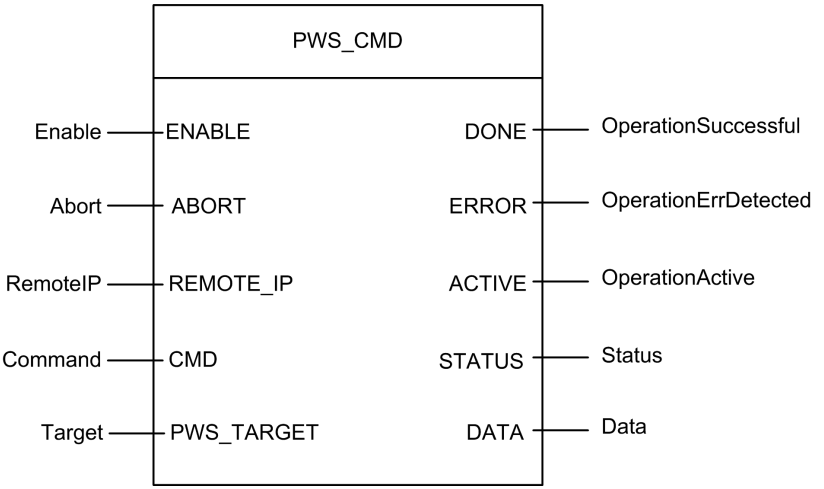
Der Funktionsbaustein PWS_CMD kann zur Ausgabe zweier Befehle genutzt werden:

- 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:

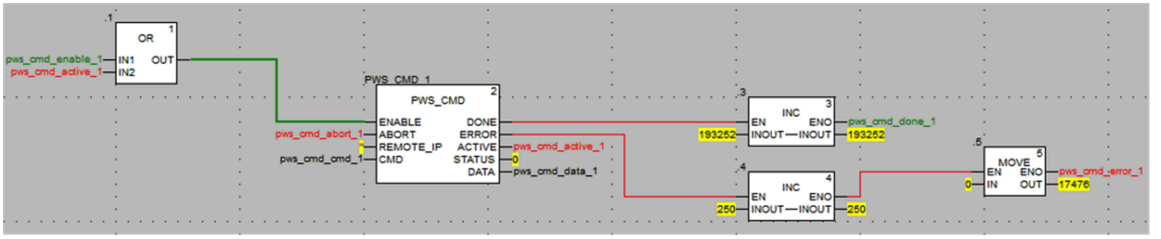
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine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

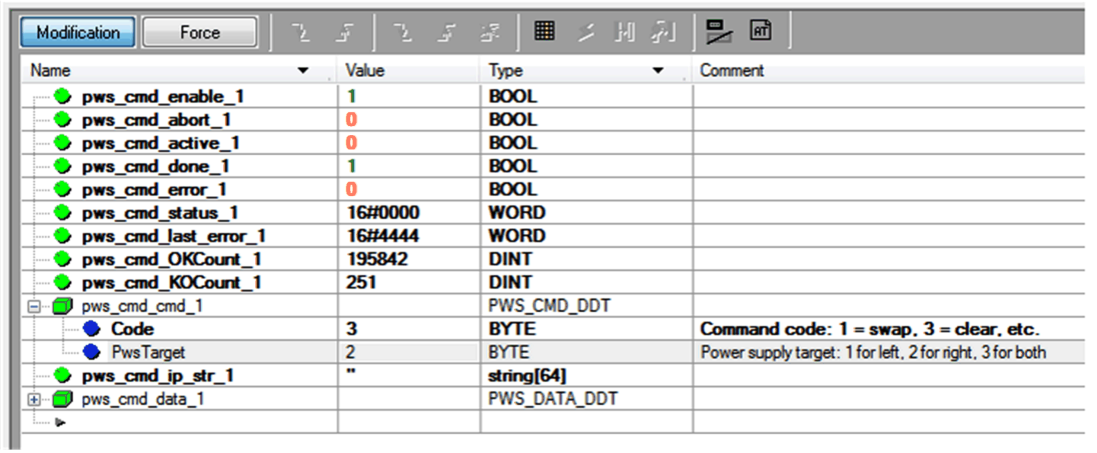
Parametername	Datentyp	Beschreibung
DONE	BOOL	EIN: Die Operation wurde erfolgreich abgeschlossen.
ERROR	BOOL	EIN: Die Operation wurde erfolglos abgebrochen.
ACTIVE	BOOL	EIN: Die Operation ist aktiv.
STATUS	WORT	Bezeichner des erkannten Fehlers
DATA	ANY	Antwortdaten (abhängig vom Befehlscode). Für Austausch-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

Application Protection

Overview

EcoStruxure Control Expert has a password mechanism to help guard against unauthorized access to the application.

EcoStruxure Control Expert password protects these actions:

- Open the application in EcoStruxure Control Expert.
- Connect to the controller in EcoStruxure Control Expert.

Setting an application password helps prevent unwanted application modification, download, or opening of application files. The password is encrypted within the application.

In addition to setting the password, you can encrypt `.STU`, `.STA`, and `.ZEF` files. The file encryption feature in EcoStruxure Control Expert helps prevent modifications and reinforces the protection of intellectual property. The file encryption option is protected by a password mechanism.

HINWEIS: When a controller is managed as part of a system project, the application password and file encryption are disabled in EcoStruxure Control Expert editor and managed with Topology Manager.

Password Construction

The construction of the password conforms to the IEEE 1686–2013 standard.

A valid password contains at least 8 characters and includes at least one uppercase letter, one lowercase letter, one number, and one non-alphanumeric character ($, %, &, etc.).

HINWEIS: The application password is cleared when you export a non-encrypted project to an `.XEF` or `.ZEF` file.

Create a New Project

By default, a new EcoStruxure Control Expert Classic application (project) has these characteristics:

- The project is not protected by a password.
- The project application files are not encrypted.

When you create a project, you can exercise these options in the **Security enforcement** dialog box:

- Set a password for the application.
- Apply encryption to your application files through a file-encryption password.

Access the **Security enforcement** dialog box in EcoStruxure Control Expert Classic:

Step	Action
1	Open the **New Project** window in EcoStruxure Control Expert (**File > New**).
2	Select a controller for the project.
3	Click the **OK** button to open the **Security enforcement** dialog box.
4	Choose to create a project with or without passwords and follow the directions in the appropriate table below.

No Passwords: Create a project without an application password:

Step	Action
1	Access the **Security enforcement** dialog box.
2	In the **Security enforcement** dialog box, select **I do not want to set an application password for this project**.
3	Click the **OK** button to continue.

With Passwords: Use the directions below to create a project with an application password and an (optional) file encryption password.

HINWEIS: You can configure an expiration date for these passwords on the **Policies** tab in the Security Editor.

Step	Action
1	Access the **Security enforcement** dialog box.
2	In the **Application password** group box, create a password to help protect the application and increase the security for access to the controller: • Enter a password in the **Entry** field. • Reenter the password in the **Confirmation** field.
3	In the **File encryption password** group box, create a password to help protect the intellectual property: • Enter a password in the **Entry** field. • Reenter the password in the **Confirmation** field. **HINWEIS:** • You can configure a file-encryption password only after you configure an application password. • Use different passwords for the application password and the file-encryption password.
4	Press the **OK** button to apply your password settings and close the **Security enforcement** dialog box.

HINWEIS:

- If no password is entered, the application files are not encrypted. In this case, the next time you open your EcoStruxure Control Expert project, the **Password** dialog box opens. To access your project, do not type a password and click **OK**. Then use the instructions below to set an application password and enable file encryption.
- You can create or change an application password at any time, but you cannot clear the application password when a file-encryption password is configured for the project.

Set an Application Password

Set the application password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select **Properties** from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.

Step	Action
4	In the **Application** field, click **Change password ...** to open the **Modify Password** window.
5	Enter the new password in the **Entry** field.
6	Enter the confirmation of the new password in the **Confirmation** field.
7	Click **OK** to confirm.
8	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

Change the Application Password

Change the application protection password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select **Project & Controller Protection** tab.
4	In the **Application** field, click **Change password ...** to open the **Modify Password** window.
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

Delete the Application Password

Use these steps to clear the application protection password.

HINWEIS: You cannot clear the application password while file encryption is enabled.

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	In the **Application** field, click **Clear password...** to open the **Password** window.

Step	Action
5	Enter the password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

Auto-Lock Feature

To exercise the option to limit access to the EcoStruxure Control Expert tool after a configured time of inactivity, select (check) the **Auto-lock** check box and enter a value in the **Minutes before lock** field to set the timeout for the time of inactivity.

An optional auto-lock feature limits access to the EcoStruxure Control Expert software programming tool after a configured time of inactivity. You can activate the auto-lock feature with the **Auto-lock** check box and select the time-out for the time of inactivity with **Minutes before lock**.

If the auto-lock feature is enabled and the configured inactivity time elapses, a dialog box for the application password appears. Behind the dialog box, editors remain open in the same position. As a result, anyone can read the content of the EcoStruxure Control Expert windows but cannot continue to work with EcoStruxure Control Expert.

HINWEIS: If you have not assigned a password to the project, the dialog box is not displayed.

Password Request Condition

Opening an existing application (project):

When you open an application file, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, the application opens. If the password is incorrect, an on-screen message indicates that the password is not valid, and a new **Application Password** dialog box opens.

If you click **Cancel**, the application is not opened.

Accessing the application in EcoStruxure Control Expert after an auto-lock, when EcoStruxure Control Expert is not connected to the controller or when the project in EcoStruxure Control Expert is *equal* to the project in the controller:

When the auto-lock time is elapsed, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, EcoStruxure Control Expert becomes active again. If the password is incorrect, a message box indicates that the password is not valid, and a new **Application Password** dialog box opens.

Click **Close** to close the unsaved application.

Accessing the application in the controller after an auto-lock, when EcoStruxure Control Expert is connected to the controller and the application in EcoStruxure Control Expert is *different* from the application in the controller:

On connection, if the EcoStruxure Control Expert software application and the controller application are not equal, an **Application Password** dialog box opens.

Enter the password and click **OK**.

Result: If the password is correct, the connection is established. If the password is incorrect, a message box indicates that an incorrect password was entered, and a new **Application Password** dialog box opens.

If you click **Cancel**, the connection is not established.

HINWEIS: On connection, if the EcoStruxure Control Expert software application and the controller applications are equal, there is no password request. If no password has been initially entered (left empty on project creation), click **OK** to establish the connection on password prompt.

HINWEIS:

- After three attempts with an invalid password, wait an increasing amount of time between subsequent password attempts. The delay increases from 15 seconds to 1 hour, with the wait increment increasing by a factor of 2 after each attempt with an invalid password.
- For forgotten passwords, refer to the instructions for addressing lost passwords, Seite 186.

Enable the File Encryption Option

HINWEIS: Set an application password *before* you enable file encryption.

Enable the file encryption option:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	Select the **File encryption active** check box to open the **Create Password** window.
5	Enter the password in the **Entry** field.

Step	Action
6	Enter the confirmation of the password in the **Confirmation** field.
7	Click **OK** to confirm.
8	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

Disable the File Encryption Option

Disable the file encryption option:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	Clear *(uncheck)* the **File encryption active** check box to open the **File Encryption Password** window.
5	Enter the password and click **OK** to confirm that the application is not encrypted.
6	Click **OK** or **Apply** in the **Properties of Project** window to confirm all changes.

Change the File Encryption Password

Change the file encryption password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	In the **File encryption** field, click **Change password ...** to open the **Modify Password** window.
5	Enter the previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

Clear the File Encryption Password

Clear the file encryption password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the pop-up menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	In the **File encryption** field, click **Clear password...** to open the **Password** window.
5	Enter the password in the **Password** field.
6	Click **OK** to confirm.
7	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes.

HINWEIS: For forgotten file-encryption passwords, refer to the instructions for addressing lost passwords, Seite 186.

Compatibility Rules

You cannot open encrypted `.STA` and `.ZEF` application files in EcoStruxure Control Expert 15.0 Classic or earlier versions.

You cannot import encrypted `.ZEF` application files to EcoStruxure Control Expert with Topology Manager.

The compatibility rules between the application version and the EcoStruxure Control Expert/ Unity Pro version apply to `.ZEF` files that are exported without encryption.

HINWEIS: When file encryption is enabled for your project, you cannot save archived application files (`.STA`) without encryption.

Safety-Related Area Password Protection

At a Glance

Safety-related controllers include a safety-related area password protection function, which is accessible from the **Properties** dialog box of the project. This function helps protect project elements located within the safety-related area of the functional safety-related project.

HINWEIS: When the safety-related area password protection function is active, the safety-related parts of the application cannot be modified

Modifications to the following safety-related parts are not permitted when safety-related area password protection is enabled:

Safety-related Part	**Forbidden action (offline AND online)**
Configuration	Modify controller characteristics
	Add, Delete, Modify a safety-related module in the rack
	Modify safety-related Power supply
Types	Create, Delete, Modify a safety-related DDT
	Change a DDT attribute: from NOT SAFE->defined SAFE-STATE
	Change a DDT attribute: from defined SAFE-STATE->NOT SAFE
	Create, Delete, Modify a safety-related DFB
	Change a DFB attribute: from NOT SAFE->defined SAFE-STATE
	Change a DFB attribute: from defined SAFE-STATE->NOT SAFE
Program-SAFE	Any Change under the **Variables an FB instances** node
	Create Task
	Import Task
	Modify Task
	Create Section
	Delete Section
	Import Section
	Modify Section
Project Settings	Modify SAFE project settings
	Modify COMMON project settings

HINWEIS:

- To access maintenance mode, enter the password when prompted.
- If you are prompted to enter the password due to inactivity while EcoStruxure Control Expert Classic is connected to the safety-related controller in programming mode and the safety-related controller is in maintenance mode, the safety-related controller transitions to safety mode after five minutes if you do not enter the password.

Encryption

The safety-related area password uses the standard encryption SHA-256.

Safety-Related Area Password Function versus Functional Safety-Related Project User Rights

The activation of the safety-related area password and the implementation of user rights created in the **Security Editor** are mutually exclusive security functions, as follows:

- If the user launching EcoStruxure Control Expert has been assigned a user profile, that user can access the safety-related areas of the safety-related application if the user enters the safety-related area password and has been granted access rights in the **Security Editor**.
- If user profiles have not been assigned, a user can access the safety-related areas of the safety-related application by entering the safety-related area password.

Visual Indicators in EcoStruxure Control Expert

The state of the safety-related area protection function can be visibly detected by viewing the **Program-SAFE** node in the **Project Browser**:

- A locked padlock indicates a safety-related area password has been created and activated.
- An unlocked padlock indicates a safety-related area password has been created but not activated.

  HINWEIS: If the safety-related application is closed then re-opened, the safety-related area password is automatically activated on reopening.
- No padlock indicates a safety-related area password has not been created.

Compatibility

As of EcoStruxure Control Expert version 14.0, the safety-related area password function exists for M580 safety-related controllers as of firmware version 2.80.

HINWEIS:

- Application program `.STU`, `.STA`, and `.ZEF` files (which are created as of EcoStruxure Control Expert version 14.0) cannot be opened in Unity Pro version 13.1 or earlier.
- Replacing an M580 safety-related controller in a EcoStruxure Control Expert version 14.0 application has the following effect:
  - Upgrading from firmware 2.70 to 2.80 (or any subsequent supporting version(s)) adds the safety-related area password functionality to the **Program & Safety Protection** tab of the **Project > Properties** window.
  - Downgrading from firmware 2.80 (and any subsequent comparable version(s)) to 2.70 removes the safety-related area password functionality.

Activating Protection and Creating Password

Activate the protection of sections and create the password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the popup menu to open the **Properties of Project** window.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, activate the protection by selecting the **Protection active** check box to open the **Modify Password** dialog box.
5	Enter a password in the **Entry** field.
6	Enter the confirmation of the password in the **Confirmation** field.
7	Follow the on-screen prompts to confirm and apply your modifications.

Changing the Password

Procedure for changing the project sections protection password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the popup menu to open the **Properties of Project** window.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, click **Change password ...** to open the **Modify Password** dialog box.

Step	Action
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Follow the on-screen prompts to confirm and apply your modifications.

Deleting the Password

Procedure for deleting the project sections protection password:

Step	Action
1	In the project browser right-click **Project**.
2	Select **Properties** command from the popup menu. **Result**: The **Properties of Project** window appears.
3	Select the **Program & Safety Protection** tab.
4	In the **Safety** area, click **Clear password...**. **Result**: The **Access control** dialog box appears:
5	Enter the previous password in the **Password** field.
6	Follow the on-screen prompts to confirm and apply your modifications.

Program Unit, Section and Subroutine Password and Protection

At a Glance

In offline mode, you can apply a password to your project and lock a section or program unit for editing.

It does not prevent you to:

- Connect to the controller
- Upload application from the controller
- Change the configuration
- Add new Program Units and/or sections

- Change the logic in a new section that is not password protected

  HINWEIS: To lock a section or Program Unit for editing, you need to both:

  - Activate **Protection active** on project level. Refer to the process *Activating Protection and Creating Password*, Seite 180.
  - Select the type of protection in the **Protection** field of a section or Program Unit. Refer to the process *Locking a Section or Program Unit for Editing*, Seite 180.

Activating Protection and Creating Password

Follow these steps to activate a password at the project level:

Step	Action
1	In the project browser, right-click **Project** and select **Properties**.
2	Select the **Program & Safety Protection** tab.
3	Select the **Protection active** checkbox. **Result**: The **Modify Password** dialog box appears.
4	Enter a password in the **Entry** field.
5	Enter the confirmation of the password in the **Confirmation** field.
6	Select **Crypted** check box if an enhanced password protection is required. **HINWEIS:** A project with a crypted password cannot be edited with Unity Pro V4.0 or earlier version.
7	Click **OK** to confirm.
8	Click **OK** or **Apply** in the **Properties** window to confirm the changes. If you click **Cancel** in the **Properties of Project** window, the changes are discarded.

Locking a Section or Program Unit for Editing

Follow these steps to lock a section or Program Unit for editing:

Step	Action
1	Right-click on your section or program unit and select **Properties**.
2	In the **General** tab, select the type of protection in the **Protection** field.
3	Click **OK** to confirm.

HINWEIS: To lock a section or Program Unit for editing, you also need to active **Protection active** on project level. Refer to the process *Activating Protection and Creating Password*, Seite 180.

HINWEIS:

- A locked padlock next to a section or Program Unit indicates that you locked it for editing and that you activated **Protection active** on project level.
- An unlocked padlock next to a section or Program Unit indicates that you locked it for editing but that you did not activate **Protection active** on project level. Therefore, the protection of your section or Program Unit is disabled.

Changing the Password

Procedure for changing the project protection password for sections and Program Units:

Step	Action
1	In the project browser, right-click **Project** and select **Properties**. **Result**: The **Properties of Project** window appears.
2	Select **Program & Safety Protection** tab.
3	In the **Sections & Program Units** field, click **Change password ...**. **Result**: The **Modify Password** dialog box appears:
4	Enter previous password in the **Old password** field.
5	Enter the new password in the **Entry** field.
6	Enter the confirmation of the new password in the **Confirmation** field.
7	Select **Crypted** check box if an enhanced password protection is required. **HINWEIS:** A project with a crypted password cannot be edited with Unity Pro V4.0 or earlier version.
8	Click **OK** to confirm.
9	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes. If you click **Cancel** in the **Properties of Project** window, the changes are discarded.

Deleting the Password

Procedure for deleting the project protection password for sections and Program Units:

Step	Action
1	In the project browser, right-click **Project** and select **Properties**. **Result**: The **Properties of Project** window appears.
2	Select **Program & Safety Protection** tab.
3	In the **Sections & Program Units** field, click **Clear password...**. **Result**: The **Access control** dialog box appears.
4	Enter the password in the **Password** field.
5	Click **OK** to confirm.
6	Click **OK** or **Apply** in the **Properties of Project** window to confirm the changes. If you click **Cancel** in the **Properties of Project** window, the changes are discarded.

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.

Schritt	Aktion
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.
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.

Data Storage/Web Protection

Overview

Protection by a password helps prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the controller).

For Modicon M580 controllers in a project created by EcoStruxure Control Expert with version:

- Earlier than version 15.1, you can provide password protection for data storage access.
- As of version 15.1, you can provide password protection for both web diagnostics and data storage access.

  HINWEIS: When a controller is managed as part of a system project, the **Web Diagnostic/Data Storage** password is disabled in EcoStruxure Control Expert editor and needs to be managed by using the Topology Manager.

Password

The password is case-sensitive and contains 8 to 16 alphanumeric characters. The password robustness is increased when it contains a mix of upper and lower case, alphabetical, numerical, and special characters.

HINWEIS: When importing a ZEF file, the Data Storage/Web password is stored inside the module only if the **File encryption** option is selected.

Changing the Password

It is possible to change a password at any time.

HINWEIS: Data Storage/Web password has a default value in the EcoStruxure Control Expert application. This default value depends on the version of EcoStruxure Control Expert:

- **`datadownload:`** EcoStruxure Control Expert versions earlier than 15.1
- **`webuser:`** EcoStruxure Control Expert versions as of 15.1

Changing the default password is mandatory, or not, depending on the module firmware version:

- As of firmware version 4.01, you need to change the Data Storage/Web password default value. Otherwise it is not possible to build the EcoStruxure Control Expert application.
- For firmware versions earlier than 4.01 it is not mandatory but strongly advised to change Data Storage/Web password default value.

Procedure for changing the Data Storage/Web password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the popup menu to open the **Properties of Project** window.
3	Select **Project & Controller Protection** tab.
4	In the **Data Storage** (or **Web Diagnostics/Data Storage**) field, click **Change password ...** to open the **Modify Password** window.
5	Enter previous password in the **Old password** field.
6	Enter the new password in the **Entry** field.
7	Enter the confirmation of the new password in the **Confirmation** field.
8	Follow the on-screen prompts to confirm and apply your modifications.

Resetting the Password

Resetting the password assigns its default value to the Data Storage/Web password in the EcoStruxure Control Expert application if the password is confirmed.

Program Unit, Section and Subroutine Password and Protection, Seite 179

Reset the password:

Step	Action
1	Right-click **Project** in the **Project Browser**.
2	Select the **Properties** command from the popup menu to open the **Properties of Project** window.
3	Select the **Project & Controller Protection** tab.
4	In the **Data Storage** (or **Web Diagnostic/Data Storage**) field, click **Reset password...** to open the **Password** window.
5	Enter your password in the **Password** field.
6	Follow the on-screen prompts to confirm and apply your modifications.

Passwortverlust

Überblick

Wenn Sie Ihr Passwort vergessen haben, halten Sie sich an die nachstehend beschriebenen Verfahren und setzen Sie sich mit dem Kundensupport 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

Das folgende Verfahren 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.

Zu Ihrer Unterstützung benötigt der Kundensupport von Schneider Electric die alphanumerische Zeichenfolge, die im Popup-Fenster **Passwort vergessen** angegeben wird, sobald Sie die Tastenkombination `SHIFT+F2` im Dialogfeld **Kennwort** drücken.

Das Dialogfeld **Kennwort** wird in folgenden Situationen angezeigt:

- Wählen Sie beim Öffnen die Anwendung. Daraufhin wird das Dialogfeld **Kennwort** angezeigt.
- Das Dialogfeld **Kennwort** wird zum Zeitpunkt der automatischen Sperre angezeigt. Wenn Sie sich nicht mehr an Ihr Passwort erinnern, wählen Sie **Schließen** aus. Öffnen Sie die Anwendung erneut. Dann wird das Dialogfeld **Kennwort** angezeigt.

  HINWEIS: Wenn die Anwendung im Anschluss an eine automatische Sperre ohne Eingabe eines Passworts geschlossen wird, gehen alle Änderungen verloren.

Verfahren zum Zurücksetzen des Anwendungspassworts:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Kennwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis**: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **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-Kundensupport 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 Kundensupport von Schneider Electric senden. Anschließend erhalten Sie die verschlüsselte Anwendungsdatei mit einem neuen Anwendungspasswort vom Schneider Electric-Kundensupport.

HINWEIS: Ändern Sie das Anwendungspasswort bei der ersten Verwendung.

SPS-Anwendungspasswort

Verfahren zum Zurücksetzen des controller-Anwendungspassworts, wenn die entsprechende **.STU*-Datei verfügbar ist:

Schritt	Aktion
1	Öffnen Sie die betroffene Datei **.STU*.
2	Sobald das Dialogfeld **Kennwort** angezeigt wird, drücken Sie `SHIFT+F2`. **Ergebnis**: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.

Schritt	Aktion
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **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-Kundensupport bereitgestellte Passwort).
7	**Verbinden** Sie sich mit der Steuerung.
8	Klicken Sie auf **Generieren > Änderungen generieren**.
9	**Speichern** Sie die Anwendung.

Verfahren zum Zurücksetzen des Passworts für die Steuerungsanwendung, wenn die entsprechende **.STU*-Datei 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 alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **Hinweis:** Das vom Schneider Electric-Kundensupport 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 aus der Steuerung.
7	**Speichern** Sie die Anwendung.
8	Ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundensupport bereitgestellte Passwort).
9	Klicken Sie auf **Generieren > Änderungen generieren**.
10	**Speichern** Sie die Anwendung.

Dateiverschlüsselungspasswort

Zu Ihrer Unterstützung benötigt der Kundensupport von Schneider Electric eine alphanumerische Zeichenfolge, die im Popup-Fenster **Passwort vergessen** angegeben wird, sobald Sie die Tastenkombination `SHIFT+F2` im Dialogfeld **Kennwort** drücken.

So greifen Sie auf das Dialogfeld **Kennwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Feld **Dateiverschlüsselung** auf **Passwort löschen...**. Das Dialogfeld **Kennwort** wird angezeigt.

Gehen Sie zum Zurücksetzen des Dateiverschlüsselungspassworts vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Kennwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis**: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **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 auf **OK**, um das Dialogfeld **Kennwort** zu schließen.
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundensupport bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** zu schließen, und klicken Sie dann im Fenster **Eigenschaften des Projekts** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften des Projekts** auf **Abbrechen** klicken, werden alle Änderungen verworfen.

Passwort für den sicheren Bereich

Zu Ihrer Unterstützung benötigt der Kundensupport von Schneider Electric eine alphanumerische Zeichenfolge, die im Popup-Fenster **Passwort vergessen** angegeben wird, sobald Sie die Tastenkombination `SHIFT+F2` im Dialogfeld **Kennwort** drücken.

So greifen Sie auf das Dialogfeld **Kennwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.

- Klicken Sie im Feld **Sicherheit** auf **Passwort ändern...**. Das Dialogfeld **Kennwort** wird angezeigt.

Gehen Sie zum Zurücksetzen des Passworts für den sicheren Bereich vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Kennwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis**: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **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 auf **OK**, um das Dialogfeld **Kennwort** zu schließen.
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundensupport bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** zu schließen, und klicken Sie dann im Fenster **Eigenschaften des Projekts** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften des Projekts** auf **Abbrechen** klicken, werden alle Änderungen verworfen.

Passwort für die Firmware

Zu Ihrer Unterstützung benötigt der Kundensupport von Schneider Electric eine alphanumerische Zeichenfolge, die im Popup-Fenster **Passwort vergessen** angegeben wird, sobald Sie die Tastenkombination `SHIFT+F2` im Dialogfeld **Kennwort** drücken.

So greifen Sie auf das Dialogfeld **Kennwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Feld **Firmware** auf **Passwort zurücksetzen...**. Das Dialogfeld **Kennwort** wird angezeigt.

Gehen Sie zum Zurücksetzen des Firmware-Passworts vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Kennwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`.

Schritt	Aktion
	Ergebnis: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport. **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 auf **OK**, um das Dialogfeld **Kennwort** zu schließen.
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundensupport bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** zu schließen, und klicken Sie dann im Fenster **Eigenschaften des Projekts** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften des Projekts** auf **Abbrechen** klicken, werden alle Änderungen verworfen.

Datenspeicher-/Webpasswort

Zu Ihrer Unterstützung benötigt der Kundensupport von Schneider Electric eine alphanumerische Zeichenfolge, die im Popup-Fenster **Passwort vergessen** angegeben wird, sobald Sie die Tastenkombination `SHIFT+F2` im Dialogfeld **Kennwort** drücken.

So greifen Sie auf das Dialogfeld **Kennwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Feld **Datenspeicherung** auf **Passwort zurücksetzen...**. Das Dialogfeld **Kennwort** wird angezeigt.

Gehen Sie zum Zurücksetzen des Passworts für den Datenspeicher vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Kennwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis**: Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine alphanumerische Zeichenfolge erscheint.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundensupport von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundensupport.

Schritt	Aktion
	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 auf **OK**, um das Dialogfeld **Kennwort** zu schließen.
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundensupport bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** zu schließen, und klicken Sie dann im Fenster **Eigenschaften des Projekts** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften des Projekts** auf **Abbrechen** klicken, werden alle Änderungen verworfen.

Verwaltung der Workstation-Sicherheit

Einführung

Schneider Electric stellt das Zugriffsmanagementtool **Sicherheitseditor** bereit, das Sie verwenden können, um den Zugriff auf die Workstation(s) zu beschränken und zu steuern, auf der/denen die Software EcoStruxure Control Expert installiert ist. In diesem Abschnitt werden die Eigenschaften dieses Tools beschrieben, das speziell auf M580-Sicherheitsprojekte ausgerichtet ist.

Verwaltung des Zugriffs auf EcoStruxure Control Expert

Einführung

Schneider Electric stellt das Konfigurationstool *Sicherheitseditor* bereit, mit dem Sie den Zugriff auf die auf einer Workstation installierte Software Control Expert verwalten können. Die Verwendung des *Sicherheitseditor*-Konfigurationstools zur Verwaltung des Zugriffs auf die Software Control Expert ist optional.

HINWEIS: Die Zugriffsverwaltung bezieht sich auf die Hardware - in der Regel eine oder mehrere Workstations -, auf der die Software EcoStruxure Control Expert installiert ist, und nicht auf das Projekt, das über ein eigenes Schutzsystem verfügt.

Weitere Informationen finden Sie hier: *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:

- **SecurityAdmin:** Der Sicherheitsadministrator (*SecurityAdmin*) ist die einzige Person, die die Zugriffssicherheit für die Software verwalten kann. Der *SecurityAdmin* bestimmt, wer auf die Software zugreifen darf, und legt die entsprechenden Zugriffsrechte fest. Während der Installation von EcoStruxure Control Expert auf der Workstation, kann nur der *SecurityAdmin*-Benutzer ohne Einschränkung der Rechte (ohne Passwort) auf die Sicherheitskonfiguration zugreifen.

  HINWEIS: Der für den Sicherheitsadministrator reservierte Benutzername lautet *SecurityAdmin*. Dieser Benutzer führt die administrative Rolle aus, die vom *Supervisor* (*Superuser*) in Vorgängerversionen EcoStruxure Control Expert (älter als Version 15.3) übernommen wurde.
- **Benutzer**: Software-Benutzer werden bei aktiver EcoStruxure Control Expert-Zugriffssicherheit vom *SecurityAdmin*-Benutzer in der Liste der Benutzer definiert. Wenn Ihr Name in der Benutzerliste enthalten ist, können Sie auf eine Software-Instanz zugreifen, indem Sie Ihren Namen (genau so, wie er in der Liste enthalten ist) und das entsprechende Passwort eingeben.

Benutzerprofil

Das Benutzerprofil enthält alle Zugriffsrechte eines Benutzers. Das Benutzerprofil kann vom *SecurityAdmin* bedarfsgerecht eingerichtet oder durch Anwendung eines der im **Sicherheitseditor**-Tool verfügbaren vorkonfigurierten Profile erstellt werden.

Vorkonfigurierte Benutzerprofile

Der **Sicherheitseditor** stellt folgende vorkonfigurierte Benutzerprofile für das Sicherheits- oder das Prozessprogramm zur Auswahl:

Profil	Anwendbarer Programmtyp		Beschreibung
	Prozess	Sicherheit	
ReadOnly (Nur Lesen)	✓	✓	Der Benutzer kann nur im schreibgeschützten Modus auf das Projekt zugreifen. Eine Ausnahme hiervon bildet 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**, kann jedoch darüber hinaus die Ausführungsparameter des Prozessprogramms (Konstanten, Initialwerte, Task-Zykluszeiten usw.) ändern.
Safety_Operate (Sicherheitsbetrieb)	—	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Operate**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen:

Profil	Anwendbarer Programmtyp		Beschreibung
	Prozess	Sicherheit	
			• Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Anforderung eines Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Adjust (Einstellung)	✓	—	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Operate**, kann jedoch darüber hinaus ein Projekt hochladen (in den PAC übertragen) und die Betriebsart des PAC (**Run**, **Stop** usw.) ändern.
Safety_Adjust (Sicherheitseinstellung)	—	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Adjust**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen: • Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Anforderung eines Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Debug (Debugging)	✓	—	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Adjust**, kann jedoch darüber hinaus die Debugging-Tools verwenden.
Safety_Debug (Sicherheitsdebugging)	—	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Debug**, 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 eines Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Program (Programm)	✓	—	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Debug**, kann jedoch darüber hinaus Änderungen am Programm vornehmen.

Profil	Anwendbarer Programmtyp		Beschreibung
	Prozess	Sicherheit	
Safety_Program (Sicherheitsprogramm)	—	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Program**, 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 eines Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Disabled (Deaktiviert)	✓	✓	Der Benutzer kann nicht auf das Projekt zugreifen.

Zuweisung eines vorkonfigurierten Benutzers

Der *SecurityAdmin* kann einen vorkonfigurierten Benutzer, der von einem vorkonfigurierten Profil abgeleitet ist, einem bestimmten Benutzer auf der Registerkarte **Benutzer** im **Sicherheitseditor**. zuweisen Folgende vorkonfigurierte Benutzerprofile stehen zur Auswahl:

- safety_user_Adjust (Sicherheitsbenutzer - Einstellung)
- safety_user_Debug (Sicherheitsbenutzer - Debugging)
- safety_user_Operate (Sicherheitsbenutzer - Betrieb)
- safety_user_Program (Sicherheitsbenutzer - Programm)
- user_Adjust (Benutzer - Einstellung)
- user_Debug (Benutzer - Debugging)
- user_Operate (Benutzer - Betrieb)
- user_Program (Benutzer - Programm)

Siehe das Thema *Benutzerfunktionen* (siehe EcoStruxure™ EcoStruxure Control Expert, Sicherheitseditor, Betriebshandbuch für weitere Informationen über die Zuweisung eines vorkonfigurierten Profils zu einem Benutzer durch den *SecurityAdmin*-Benutzer.

Zugriffsrechte

Einführung

In diesem Abschnitt werden die für jedes vorkonfigurierte Benutzerprofil verfügbaren Zugriffsrechte vorgestellt.
Die EcoStruxure Control Expert-Zugriffsrechte sind in den folgenden Kategorien zusammengefasst:

- Topology Manager

Die EcoStruxure Control Expert Classic-Zugriffsrechte sind in folgende Kategorien unterteilt:

- Projektdienste
- Einstellung/Debugging
- Bibliotheken
- Globale Änderung
- Elementare Änderung einer Variablen
- Elementare Änderung von DDT-Verbunddaten
- Elementare Änderung eines DFB-Typs
- Elementare Änderung einer DFB-Instanz
- Bus-Konfigurationseditor
- E/A-Konfigurationseditor
- Laufzeitfenster
- Cybersicherheit
- Sicherheit

  HINWEIS: Die EcoStruxure Control Expert Classic-Zugriffsrechte gelten ebenfalls für EcoStruxure Control Expert editor.

Topology Manager

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Create Systemprojekt	–	–	–	–	–	–	✓	✓
Modify Systemprojekt	–	–	–	–	–	–	✓	✓
Import Systemprojekt	–	–	–	–	–	–	✓	✓
Delete Systemprojekt	–	–	–	–	–	–	✓	✓
Manage Systemprojekt settings	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Projektdienste

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Neues Projekt erstellen	–	–	–	–	–	–	✓	✓
Vorhandenes Projekt öffnen	✓	✓	✓	✓	✓	✓	✓	✓
Projekt speichern	–	–	–	–	–	–	✓	✓
Projekt speichern unter	✓	✓	✓	✓	✓	✓	✓	✓
Projekt importieren	–	–	–	–	–	–	✓	✓
Offline generieren	–	–	–	–	–	–	✓	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Online-Generierung stoppen	–	–	–	–	–	–	✓	✓
Online-Generierung ausführen	–	–	–	–	–	–	✓	✓
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Anpassung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Dokumentation ändern	✓	✓	✓	✓	✓	✓	✓	✓
Funktionsansicht ändern	–	–	–	–	–	–	✓	✓
Animationstabellen ändern	✓	✓	✓	✓	✓	✓	✓	✓
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Variable hinzufügen/ entfernen	–	–	–	–	–	–	✓	✓
Sicherheitsvariablen - Hinzufügen/Entfernen	–	–	–	–	–	–	–	✓
Hauptattribute von Variablen ändern	–	–	–	–	–	–	✓	✓
Sicherheitsvariablen - Änderung der Hauptattribute	–	–	–	–	–	–	–	✓
Nebenattribute von Variablen ändern	✓	–	✓	–	✓	–	✓	✓
Sicherheitsvariablen - Änderung der Nebenattribute	–	✓	–	✓	–	✓	–	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Elementare Änderung von DDT-Verbunddaten

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
DFB-Typ hinzufügen/ entfernen	–	–	–	–	–	–	✓	✓
Sicherheits-DFB-Typ - Hinzufügen/ Entfernen	–	–	–	–	–	–	–	✓
Struktur eines DFB-Typs ändern	–	–	–	–	–	–	✓	✓
Sicherheits-DFB-Typ - Strukturänderung	–	–	–	–	–	–	–	✓
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
Konfiguration ändern	–	–	–	–	–	–	✓	✓
Sicherheitskonfiguration ändern	–	–	–	–	–	–	–	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
E/A-Sniffing	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

E/A-Konfigurationseditor

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 (Einstellen)	Safety_ Adjust (Sicherheitsbezogene Einstellung)	Debug (Debuggen)	Safety_ Debug (Sicherheitsbezogenes Debugging)	Operate (Betrieb)	Safety_ Operate (Sicherheitsbezogener Betrieb)	Program (Programm)	Safety_ Program (Sicherheitsbezogenes Programm)
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 **Extras > Projekteinstellungen...** im Control Expert-Hauptmenü 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 unterteilt, je nach **Anwendungsbereich** der Einstellungen:

- **Gemeinsam**: Diese Einstellungen gelten für die gesamte Anwendung und können sich auf den globalen, prozessspezifischen und sicheren Bereich des Projekts auswirken.
- **Prozess**: Diese Einstellungen gelten nur für den Prozessbereich „PROCESS“ des Projekts.
- **Sicher**: Diese Einstellungen gelten nur für den Sicherheitsbereich des Projekts.

In diesem Abschnitt werden nur die Teile des Fensters **Projekteinstellungen** beschrieben, die sich von einem nicht-sicherheitsbezogenen M580-Projekt unterscheiden. Im Abschnitt *Projekteinstellungen* des Handbuchs *EcoStruxure™ Control Expert-Betriebsarten* finden Sie Informationen zu Funktionen, die sowohl für M580-Sicherheits- als auch für Nicht-Sicherheitsprojekte verfügbar sind.

Gemeinsame Projekteinstellungen

Die folgenden Einstellungen **Anwendungsbereich > Gemeinsam** gelten für den globalen, sicheren und prozessspezifischen Projektbereich, unterscheiden sich jedoch von den gleichen Einstellungen in einem nicht-sicherheitsbezogenen M580-Projekt:

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

Gruppe	Einstellung	Beschreibung
		braucht kein Datenblock mit fester Größe reserviert zu werden.
	Virtueller Verbindungsmodus	Der virtuelle Verbindungsmodus ist für M580-Sicherheitssteuerungen möglich und standardmäßig deaktiviert. Wenn der virtuelle Verbindungsmodus aktiviert wird, sind Änderungen, die keine Neugenerierung des Projekts erfordern, im gemeinsamen, prozessspezifischen und sicherheitsbezogenen Teil des Programms zulässig. Um Änderungen im Sicherheitsbereich des Programms bei aktiviertem virtuellen Verbindungsmodus zu verhindern, legen Sie ein Sicherheitspasswort fest, um den Schutz zu aktivieren. **HINWEIS:** • Der virtuelle Verbindungsmodus ist für M580 Safety-Prozessoren aktiviert und standardmäßig nicht ausgewählt. • Der virtuelle Verbindungsmodus kann vom Benutzer ausgewählt werden. Wenn der virtuelle Verbindungsmodus ausgewählt wird, sind Änderungen, die keine Neugenerierung des Projekts erfordern, im gemeinsamen, prozessspezifischen und sicheren Teil des Programms zulässig. Wenn Sie Änderungen am sicheren Teil des Programms bei aktiviertem virtuellen Verbindungsmodus verbieten möchten, legen Sie ein Sicherheitspasswort fest und aktivieren den Schutz in den Eigenschaften des Projekts.
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 ausgewählter Option kann das Bedienerfenster die Variablen des Prozessbereichs nur unter Verwendung des Formats „PROCESS.<Variablenname>“ lesen. • Ist die Option nicht ausgewählt, dann kann das Bedienerfenster die Prozessbereichsvariablen nur unter Verwendung des Formats „<Variablenname>“ ohne PROCESS-Präfix lesen. **HINWEIS:** Auf alle Variablen im sicherheitsbezogenen Bereich wird über das Format „SAFE.<Variablenname>“ zugegriffen.
	Online-Änderung von Daten optimieren	Gilt für folgende Elemente: • Prozessprogramm im Sicherheits- und Wartungsmodus

Gruppe	Einstellung	Beschreibung
		• 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.
Zeit	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.

Gemeinsame Projekteinstellungen ohne Auswirkung auf den sicheren Projektbereich

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

Gruppe	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.
Variablen-Einstellungen:		
–	Direkt dargestellte Array-Variablen	Der %MW-Zugriff wird im Sicherheitsprogramm nicht unterstützt.
	Schnellabfrage zur Trenderstellung aktivieren	Das Trendanalyse-Tool wird im Sicherheitsprogramm nicht unterstützt. Es wird nur in der MAST-Task des Prozessprogramms unterstützt.
	Referenzinitialisierung forcieren	Referenzen sind im Sicherheitsprogramm nicht zulässig.
Programm-Einstellungen:		

Gruppe	Einstellung	Beschreibung
Sprachen • Gemeinsam	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 den prozess- und den sicherheitsspezifischen Projektbereich

Der **Anwendungsbereich > Sicher** und der **Anwendungsbereich > Prozess** verfügen über dieselben Programmeinstellungen. Allerdings werden die folgenden Einstellungen in jedem Bereich eines M580-Sicherheitsprojekts unterschiedlich gehandhabt.

Gruppe	Einstellung	Beschreibung
Allgemeine Einstellungen:		
Generierungsein-stellungen	Optimierter Code	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich.
	Verwaltung der sicheren Signatur	• Deaktiviert für den Prozessbereich. • Aktiviert und standardmäßig auf **Automatisch** gesetzt für den Sicherheitsbereich.
SPS-Diagnose	Anwendungsdiagnose • Stufe der Anwendungsdiagnose	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich.
Variablen-Einstellungen:		
–	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	

Gruppe	Einstellung	Beschreibung
Programm-Einstellungen:		
Sprachen	Funktionsbausteindiagramm (FBD)	Aktiviert sowohl für den Prozess- als auch für den Sicherheitsbereich.
	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 • Gemeinsam	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.
	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

IEC 61508 216
Systemobjekte 224
SRAC-Referenzen 232

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

Allgemeine Informationen zur Norm IEC 61508 217
SIL-Richtlinie 219

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 221.

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

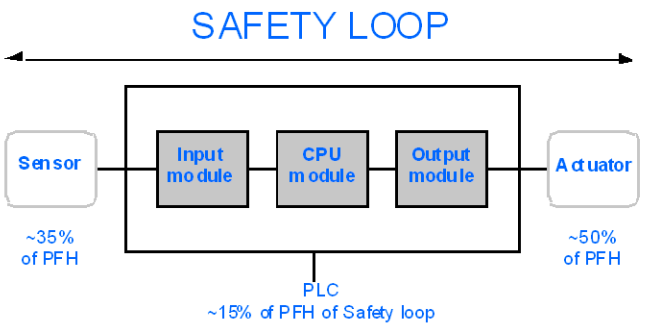
Beschreibung der Sicherheitsregelung

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

Bits des M580-Sicherheitssystems 225
Wörter des M580-Sicherheitssystems 228

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.

Wörter des M580-Sicherheitssystems

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 *Systemwörter* 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 den nicht-sicherheitsbezogenen 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-Taskperiode. 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 genutzter Prozentsatz der CPU-Systemlast.	R
%SW111	Von der MAST-Task genutzter Prozentsatz der CPU-Systemlast.	R
%SW112	Von der FAST-Task genutzter Prozentsatz der CPU-Systemlast.	R
%SW113	Von der SAFE-Task genutzter Prozentsatz der CPU-Systemlast.	R
%SW114	Von der AUX0-Task genutzter Prozentsatz der CPU-Systemlast.	R
%SW115	Von der AUX1-Task genutzter Prozentsatz der CPU-Systemlast.	R
%SW116	Gesamte CPU-Systemlast.	R

Wort	Funktion	Typ
%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 Koprozessor. • 0x5B01: Koprozessor 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 Koprozessor 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 Koprozessor erkannt). • 0x5AF3: Vergleichsfehler von der Haupt-CPU erkannt. • 0x5AFC: Vergleichsfehler vom Koprozessor erkannt. • 0x5AFD: Interner Fehler vom Koprozessor erkannt. • 0x5AFE: Synchronisationsfehler zwischen CPU und Koprozessor. • 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	Diese zwei Systemwörter enthalten Informationen zur internen Verwendung durch Schneider Electric bei der detaillierten Analyse erkannter Fehler.	R
%SW127		
%SW128	Mit einer CPU-Firmwareversion bis 3.10 wird die Zeitsynchronisation 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 Synchronisation. Weitere Informationen finden Sie im Abschnitt *Vorgehensweise zur Synchronisierung der NTP-Zeiteinstellungen* (siehe Modicon M580, Sicherheitshandbuch). • Andere Sequenzen und Werte forcieren keine Synchronisation.	R/W
%SW142	Enthält die Firmwareversion des Sicherheitskoprozessors 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	Mit einer CPU-Firmware bis Version 3.10 wird der Status der CPU-NTP-Zeit vom Ethernet-Kommunikationsmodul (z. B. BMENOC0301/11) über den X Bus-Baugruppenträger mittels 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	Sicherheitsanwendungs-ID: Enthält die ID des Sicherheitscodes der Anwendung. Die ID wird bei Änderung des Codes der Sicherheitsanwendung automatisch geändert. **HINWEIS:** • Wenn der Sicherheitscode geändert und der Befehl **Änderungen generieren** seit dem letzten Befehl **Alle neu generieren** ausgeführt wurde (wodurch die ID der Sicherheitsanwendung geändert wird), wird die ID der Sicherheitsanwendung durch Ausführung des Befehls **Alle neu generieren** u. U. erneut geändert. • Die eindeutige Kennung des SAFE-Programms kann über den `SAID`-Ausgang des `S_SYST_STAT_MX`-Systemfunktionsbausteins ausgelesen werden.	R
%SW171	Status der FAST-Tasks: • 0: Keine FAST-Tasks vorhanden • 1: Stop • 2: Run • 3: Haltepunkt • 4: Halt	R
%SW172	Status der SAFE-Task: • 0: Keine SAFE-Task vorhanden • 1: Stop • 2: Run • 3: Haltepunkt • 4: Halt	R
%SW173	Status der MAST-Task: • 0: Keine MAST-Task vorhanden • 1: Stop • 2: Run • 3: Haltepunkt • 4: Halt	R
%SW174	Status der AUX0-Task: • 0: Keine AUX0-Task vorhanden • 1: Stop • 2: Run • 3: Haltepunkt • 4: Halt	R

Wort	Funktion	Typ
%SW175	Status der AUX1-Task: • 0: Keine AUX1-Task vorhanden • 1: Stop • 2: Run • 3: Haltepunkt • 4: Halt	R
%SW176	Status der Zählung forcierter Bits für SAFE-Programmvariablen: • Wird bei jeder Forcierung eines digitalen Bits inkrementiert. • Wird dekrementiert, sobald die Forcierung eines digitalen Bits aufgehoben wird.	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 20
PG #4	Hinweise zur Erdung, Seite 50
PG #5	Planung der Installation des lokalen Racks, Einführung, Seite 89
PG #6	Platzbedarf für eine M580-CPU in einem lokalen Hauptrack, Seite 91
PG #7	Vorsichtsmaßnahmen bei der Installation, Seite 99
PG #8	Vorsichtsmaßnahmen bei der Installation, Seite 99
PG #9	Erdung, Seite 103
PG #10	Installation eines Stromversorgungsmoduls, Einführung, Seite 103
PG #11	Vorsichtsmaßnahmen bei der Installation, Seite 104
PG #12	Vorsichtsmaßnahmen bei der Installation, Seite 104
PG #13	Vorsichtsmaßnahmen bei der Installation, Seite 104
PG #14	Erdung des Spannungsversorgungsmoduls, Seite 107
PG #15	Sicherheitshinweise zur Erdung, Seite 108

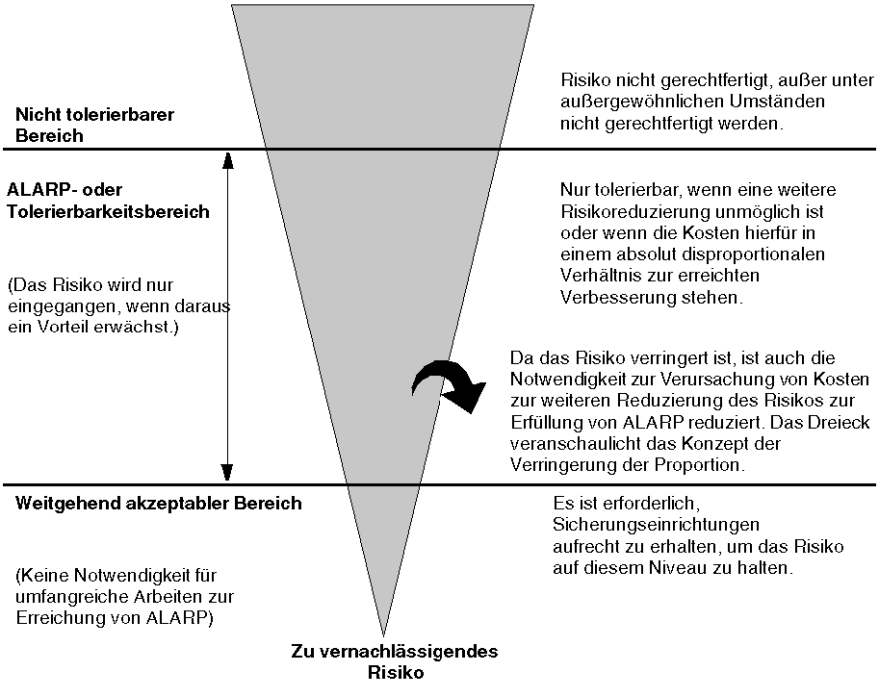
Anforderungen für Sicherheitsinformationsmeldungen	
Id	**An dieser Stelle**
PG #16	Funktion des Wartungsmodus, Seite 122
PG #17	Warmstart, Seite 135
PG #18	Sperren der Konfiguration der E/A-Sicherheitsmodule, Seite 148
PG #19	Anzeige der Daten in den Bedienerfenstern, Seite 155

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

61508
IEC 217
61511
IEC 217

A

Abmessung
CPU 39
Koprozessor 39
M580-Sicherheitsspannungsversorgung ... 61
Abmessungen
E/A-Sicherheitsmodul 75
Animationstabellen 152
Anlauf 132
Bei Erstinbetriebnahme 132
Kaltstart 135
Nach Spannungsunterbrechung 132
Warmstart 135
Anwendung 186
application
protecting 168
Ausfallrate 223
Ausfallwahrscheinlichkeit einer Sicherheitsfunktion pro Stunde (PFH) 220
Ausfallwahrscheinlichkeit im Anforderungsfall (PFD) 220

B

Befehl „Generieren“
Änderungen generieren 140
Gesamtes Projekt generieren 140
IDs erneuern & Alles generieren 140
Betriebsart 121
Betriebsart: Sicherheitsmodus 121
Betriebsart: Wartungsmodus 122
Betriebszustände 126
Bits des Sicherheitssystems 225
BMXRMS004GPF 52
BMXSAI0410
Leistungskenndaten 81
BMXSDI1602
Leistungskenndaten 83
BMXSDO0802
Leistungskenndaten 84
BMXSRA0405
Leistungsmerkmale 86
BMXXCAUSB018 USB-Kabel 50
BMXXCAUSB045 USB-Kabel 50

C

Control Expert
Datentrennung 117
Projekteinstellungen 209
Sicherheitseditor 197
Verwalten des Zugriffs auf 193
Vordefinierte Benutzerprofile 197
CPU
Abmessungen 39
Frontplatte 39
Installation 99
CPU BME•58•040S
Leistungskenndaten 57
CPU-LEDs 45

D

data storage
protecting 184
Dateninitialisierungsbefehl
Init 151
Init Safety 151
Datenspeicher 186
Datentrennung in Control Expert 117
Dual-Netzwerk-Ports 50

E

E/A-Konfiguration
Sperren 148
E/A-Modul
Installation 107
E/A-Sicherheitsmodul
Abmessungen 75
Frontplatte 76
LEDs 78
encryption

file 168
Ethernet-Ports 47
Dual-Netzwerk-Ports 50
LEDs 49
Service-Port 49
Stifte 48

F

file
encryption 168
Firmware 186
Schützen 182
Frontplatte
coprocessor 41
CPU 39
E/A-Sicherheitsmodul 76
Spannungsversorgung 62
FTP
SD-Speicherkarte 52

H

Hardwarefehlertoleranz(HFT) 220
HFT (Hardware Fault Tolerance) 220
HMI 155

I

IEC 61508
Funktionale Sicherheit 217
IEC 61511
Funktionale Sicherheit für die Prozessindustrie 217
Initialisieren der Daten 151
Installation
CPU 99
E/A-Modul 107
Lokales Rack 89
Spannungsversorgung 103
Speicherkarte 109

K

Kaltstart 135
Klemmenleiste mit Alarmrelais 73
Koprozessor
Abmessungen 39
Frontplatte 41
Koprozessor BMEP58CPROS3
Leistungskenndaten 57
Koprozessor-LEDs 45

L

LED-Anzeigen
CPU 45
Koprozessor 45
LED-Anzeigetafel
Spannungsversorgung 63
LEDs
E/A-Sicherheitsmodul 78
Leistungskenndaten
BMXSAI0410 81
BMXSDI1602 83
BMXSDO0802 84
CPU und Koprozessor 57
Spannungsversorgung 67
Leistungsmerkmale
BMXSRA0405 86
Lokales Rack
Installation 89

M

M580-Sicherheitsspannungsversorgung
Abmessungen 61
Frontplatte 62
LED-Anzeigetafel 63
RESET-Funktion 63
Maximale Geräteanzahl
CIP Safety-Topologie 28
Mittlere Betriebsdauer zwischen Ausfällen (MTBF) 223
Module
Nicht-störend 20
Nicht-störende Module vom Typ 1 20
Nicht-störende Module vom Typ 2 23
Zertifiziert 18
MTBF (Mean Time Between Failures) 223

P

password
section 175
Passwort
Vergessen 186
Verlust 186
PFD (Probability of Failure on Demand) 220
PFH (Probability of Failure per Hour) 220
Program Unit
protecting 179
Projekteinstellungen 209
protecting
application 168
data storage 184
Program Unit 179
section 179
Prozess-Namespace
Nutzung von 209
Verwendung über Bedienerfenster 209

R

Rack
Montage 94
Rack-Erweiterungsmodul 96
Redundanter Verbindungsport 52
RESET 63

S

SAFE-Quellsignatur 140
SAFE-Signatur 140
SAFE-Task
Konfigurieren 157
safety-related area
password 175
Schützen
Firmware 182
SD-Karte
Verriegelbare Abdeckung 55
SD-Speicherkarte
FTP 52
section
protecting 179
Service-Port 49
SFF (Safe Failure Fraction) 220
SFP-Steckbuchse 52
Sicherer Ausfallanteil(SFF) 220
Sicherheits-Integritätslevel (SIL) 219
Sicherheitseditor 193
Sicherheitsetiketten 54
Sicherheitsregelung 222
SIL (Sicherheits-Integritätslevel) 219
Spannungsversorgung
Installation 103
Leistungskenndaten 67
Speicherkarte
FTP 52
Installation 109
Sperre der E/A-Konfiguration 148
System
Bits 225
Wörter 228

T

Tasks 136, 157
Konfiguration 137
Topologie
Hohe Verfügbarkeit 32
Lokales Hauptrack mit Erweiterung 31
Peer-to-Peer 34
Planung 26
Verteilte Geräte 35
Trendanalyse-Tool 156

U

USB
Anschlussbelegung 50
Kabel 50
Transparenz 50

V

Vergessen
Passwort 186
Verlust
Passwort 186
Verwendung des Prozess-Namespace 209

W

Warmstart..... 135
Wartungseingang..... 125
Wörter des Sicherheitssystems 228

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, sollten Sie um Bestätigung der in dieser Veröffentlichung gegebenen Informationen nachsuchen.

© 2024 Schneider Electric. Alle Rechte vorbehalten.

QGH60285.10