Modicon Steuerungssysteme

Cybersicherheit

Benutzerhandbuch

Übersetzung der Originalbetriebsanleitung

11/2024

EIO0000002000.10

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.

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 5
Bevor Sie beginnen 6
Start und Test 7
Betrieb und Einstellungen 8
Informationen zum Dokument 9
Beschreibung 17
Richtlinien von Schneider Electric 17
Sicherung der Architektur 19
Systemansicht 19
Festlegung von Passwörtern in Control Expert 21
Härten des PC 23
Deaktivierung nicht verwendeter integrierter Kommunikationsdienste 32
Einschränkung des Datenflusses vom Steuerungsnetzwerk (Zugriffskontrolle) 33
Einrichtung verschlüsselter Kommunikation 36
CSPN-Sicherheitsziel 43
Einrichtung des Cybersicherheit-Audits (Ereignisprotokollierung) 53
Beschreibung der Ereignisprotokollnachrichten für Control Expert 63
Beschreibung der Ereignisprotokollnachrichten für M580-Steuerungen (ab Firmwareversion V4.10) und BMENOR2200H (ab Firmwareversion 3.01) 69
Beschreibung der Ereignisprotokollmeldungen für M580-Steuerungen (Firmware vor Version 4.10), BMENUA0100 und BMENOR2200H (Firmware vor Version 3.01) 84
Steuerungsidentifikation und - authentifizierung 101
Kontrollberechtigungen 107
Verwaltung der Datenintegritätsprüfungen 112
Konfiguration einer sicheren Engineering-Verbindung zwischen Control Expert und einer M580-Ethernet-Steuerung 115
Merkmale einer sicheren Verbindung 116
Konfiguration einer sicheren Verbindung 119
Hinweise zu Betriebsarten 120

Kompatibilität und Einschränkungen der erzwungenen sicheren Programmierung 121
Kompatibilität des Kommunikationsadapters 123
M580-Ethernet-Dienste und -Ports 128
Cybersicherheit-Dienste pro System 130
Cybersicherheit-Dienste 130
Modicon M340-Sicherheitsdienste 138
Modicon M580-Sicherheitsdienste 138
Modicon Quantum-Sicherheitsdienste 138
Modicon X80-Sicherheitsdienste 140
Modicon Premium/Atrium-Sicherheitsdienste 143
Modicon Momentum MDI-Sicherheitsdienste 144
Modicon MC80-Sicherheitsdienste 144
Schutz der M580-, M340-, Momentum MDI- und MC80-Architektur mit EAGLE40 über VPN 145
EAGLE40-Firewall 145
Voraussetzungen 146
Typische Architektur 148
Konfiguration der Firewall 148
Glossar 157
Index 183

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

Ziel dieses Dokuments

In diesem Handbuch werden die Elemente der Cybersicherheit definiert, mit denen Sie ein System konfigurieren können, das weniger anfällig für Cyberangriffe ist.

HINWEIS: Die Begriffe „Sicherheit“, „sicher“, „gesichert“ und „Sicherung“ werden in diesem Dokument mit Bezug auf Aspekte der Cybersicherheit verwendet.

Gültigkeitsbereich

Dieses Dokument wurde für EcoStruxure™ Control Expert V16.0 aktualisiert.

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

Verfügbare Sprachen des Dokuments

Dieses Dokument ist in folgenden Sprachen verfügbar:

- Chinesisch (EIO0000002004)
- Englisch (EIO0000001999)
- Französisch (EIO0000002001)
- Deutsch (EIO0000002000)
- Italienisch (EIO0000002002)
- Spanisch (EIO0000002003)

Informationen zur Cybersicherheit

Informationen zur Cybersicherheit finden Sie auf der Website von Schneider Electric: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Dokumente zum Download im Supportbereich für Cybersicherheit:

Titel der Dokumentation	Webseitenadresse
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations	www.se.com/ww/en/download/document/STN v2

Weiterführende Dokumente

Titel der Dokumentation	Handelsreferenz
Modicon M580 Systemplanungshandbuch	HRB65322 (CHS) HRB62666 (ENG) HRB65318 (FRE) HRB65319 (GER) RB65320 (ITA) HRB65321 (SPA)
Modicon M580 Hardware-Referenzhandbuch	EIO0000001583 (CHS) EIO0000001578 (ENG) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001582 (ITA) EIO0000001581 (SPA)
Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Kommunikationsmodul, Installations- und Konfigurationshandbuch	HRB65316 (CHS) HRB62665 (ENG) HRB65311 (FRE) HRB65313 (GER) HRB65314 (ITA) HRB65315 (SPA)
Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch	31007493 (CH) 31007131 (ENG) 31007132 (FRE) 31007133 (GER) 31007494 (ITA) 31007134 (SPA)
Quantum mit EcoStruxure™ Control Expert, TCP/IP-Konfiguration, Benutzerhandbuch	31007110 (CH) 33002467 (ENG) 33002468 (FRE) 33002469 (GER) 31008078 (ITA) 33002470 (SPA)
Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet-Netzwerkmodule, Benutzerhandbuch	31007102 (CH) 35006192 (ENG) 35006193 (FRE) 35006194 (GER) 31007214 (ITA) 35006195 (SPA)
EcoStruxure™ Control Expert - Betriebsarten	33003697 (CH) 33003101 (ENG) 33003102 (FRE)

Titel der Dokumentation	Handelsreferenz
	33003103 (GER) 33003696 (ITA) 33003104 (SPA)
Quantum mit EcoStruxure™ Control Expert - Hardware-Referenzhandbuch	35012184 (CH) 35010529 (ENG) 35010530 (FRE) 35010531 (GER) 35013975 (ITA) 35010532 (SPA)
Quantum mit EcoStruxure™ Control Expert, 140NOC77101, Ethernet Kommunikationsmodul, Benutzerhandbuch	S1A33993 (CHS) S1A33985 (ENG) S1A33986 (FRE) S1A33987 (GER) S1A33989 (ITA) S1A33988 (SPA)
Premium mit EcoStruxure™ Control Expert, TSXETC101, Ethernet Kommunikationsmodul, Benutzerhandbuch	S1A34008 (CHS) S1A34003 (ENG) S1A34004 (FRE) S1A34005 (GER) S1A34007 (ITA) S1A34006 (SPA)
Modicon M340, BMXNOC0401 Ethernet Kommunikationsmodul, Benutzerhandbuch	S1A34014 (CHS) S1A34009 (ENG) S1A34010 (FRE) S1A34011 (GER) S1A34013 (ITA) S1A34012 (Spanisch)
Quantum EIO, Steuerungsnetzwerk, Installations- und Konfigurationshandbuch	S1A48999 (CHS) S1A48993 (ENG) S1A48994 (FRE) S1A48995 (GER) S1A48997 (ITA) S1A48998 (Spanisch)
EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek	33003683 (CH) 33002527 (ENG) 33002528 (FRE) 33002529 (GER) 33003682 (ITA) 33002530 (SPA)
Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch	31007112 (CH) 33002479 (ENG) 33002480 (FRE) 33002481 (GER) 31007213 (ITA) 33002482 (SPA)
Modico M580 BMECXM CANopen-Module, Benutzerhandbuch	EIO0000002134 (CHS) EIO0000002129 (ENG) EIO0000002130 (FRE) EIO0000002131 (GER) EIO0000002132 (ITA)

Titel der Dokumentation	Handelsreferenz
	EIO0000002133 (SPA)
EcoStruxure Automation Device Maintenance, Tool zur Firmwareaktualisierung	EIO0000004050 (CHS) EIO0000004033 (ENG) EIO0000004046 (GER) EIO0000004048 (FRE) EIO0000004049 (ITA) EIO0000004047 (SPA)
Momentum für EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Prozessoren, Benutzerhandbuch	HRB44124 (ENG)
Modicon MC80 Program Logic Controller (SPS), Benutzerhandbuch	EIO0000002071 (ENG)

Produktinformationen

⚠⚠ GEFAHR

GEFAHR VON STROMSCHLAG, EXPLOSION ODER LICHTBOGENENTLADUNG

- Trennen Sie alle Geräte, einschließlich der angeschlossenen Komponenten, von der Spannungsversorgung, bevor Sie Abdeckungen oder Türen entfernen oder Zubehörteile, Hardware, Kabel oder Drähte anbringen bzw. abnehmen, ausgenommen unter den im Hardwarehandbuch des jeweiligen Geräts angegebenen Bedingungen.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um sicherzustellen, dass an den angegebenen 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.
- Betreiben Sie das Gerät und alle zugehörigen Produkte nur mit der angegebenen Spannung.

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

⚠WARNUNG

STEUERUNGSAUSFALL

- Führen Sie vor der Implementierung eine Fehlermodus- (Fallback) und Auswirkungsanalyse (FMEA, Failure Mode and Effects Analysis) oder eine gleichwertige Risikoanalyse Ihrer Anwendung durch und wenden Sie vorbeugende und erkennende 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.
- Überprüfen Sie die Auswirkungen von Übertragungsverzögerungen und ergreifen Sie Maßnahmen, um diese zu mindern.
- Überprüfen Sie die Auswirkungen von Unterbrechungen der Kommunikationsverbindung und ergreifen Sie Maßnahmen, um diese zu mindern.
- Stellen Sie unabhängige Pfade für Steuerungsfunktionen bereit (z. B. Not-Aus, Bedingungen bei Grenzüberschreitung und Fehler), die Ihrer Risikobewertung sowie den geltenden Vorschriften entsprechen.
- 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 den aktuellen Versionen von NEMA ICS 1.1 *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* sowie von NEMA ICS 7.1, *Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems* oder den entsprechenden vor Ort geltenden Vorschriften.

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Verwenden Sie mit diesem Gerät nur von Schneider Electric genehmigte Software.
- Aktualisieren Sie Ihr Anwendungsprogramm jedes Mal, wenn Sie die physische Hardwarekonfiguration ändern.

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

⚠WARNUNG
UNBEABSICHTIGTER GERÄTEBETRIEB, STEUERUNGSVERLUST, DATENVERLUST Sie sowie alle Personen, die Geräte mit EcoStruxure Control Expert besitzen, gestalten, betreiben und/oder warten, müssen die in diesem Dokument enthaltenen Anweisungen lesen, verstehen und befolgen. **Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.**

Marken

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 61496-1:2020	Sicherheit von Maschinen: Berührungslos wirkende Schutzeinrichtung Teil 1: Allgemeine Anforderungen und Tests
ISO 12100:2010	Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
EN 60204-1:2006	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

Norm/Standard	Beschreibung
ISO 13850:2015	Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
IEC 62061:2021	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Steuerungssysteme
IEC 61508-1:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Allgemeine Anforderungen
IEC 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme: Anforderungen für sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme
IEC 61508-3:2010	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 in diesem Dokument verwendeten Begriffe unter Umständen auch anderen Normen/Standards entnommen, u. a.:

Norm/Standard	Beschreibung
IEC 60034-Reihe	Drehende elektrische Maschinen
IEC 61800-Reihe	Drehzahlveränderbare elektrische Umrichter
IEC 61158-Reihe	Industrielle Kommunikationsnetze – Feldbus für industrielle Steuerungssysteme

Des Weiteren kann der Begriff *Betriebsbereich* in Verbindung mit der Beschreibung spezifischer Gefahren verwendet werden und wird in diesem Fall für eine *Gefahrenzone* bzw. einen *Gefahrenbereich* in folgenden *Maschinenrichtlinien* definiert: *2006/42/EC* und *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 Eigenschaftstabellen für die entsprechenden Produktreferenzen.

Informationen zu nicht-inklusiver oder unsensibler Terminologie

Als verantwortungsbewusstes, integratives Unternehmen aktualisiert Schneider Electric kontinuierlich seine Kommunikationen und Produkte, die nicht-integrative oder unsensible Terminologie enthalten. Trotz dieser Bemühungen können unsere Inhalte jedoch nach wie vor Begriffe enthalten, die von einigen Kunden als unangemessen betrachtet werden.

Beschreibung

Einführung

Ziel dieses Handbuchs ist die Beschreibung der in die Modicon-Steuerungen implementierten Cybersicherheit-Lösungen und der zugehörigen Softwareanwendungen. Zusätzlich zu den in diesem Handbuch vorgestellten Lösungen sollten Sie die technischen Hinweise zur Cybersicherheit von Schneider Electric auf der Schneider Electric website beachten.

Richtlinien von Schneider Electric

Einführung

Ihr PC-System kann verschiedene Anwendungen ausführen, um die Sicherheit in Ihrer Steuerungsumgebung zu erhöhen. Das System verfügt über werksseitige Standardeinstellungen, die neu konfiguriert werden müssen, um den Richtlinien von Schneider Electric für die Gerätehärtung gemäß dem Defense-in-Depth-Ansatz zu entsprechen.

Einen Abschnitt zur Cybersicherheit finden Sie im Supportbereich auf der Website von Schneider Electric.

„Defense-In-Depth“-Ansatz

Halten Sie sich zusätzlich zu den in diesem Dokument beschriebenen Lösungen an die Anweisungen im Defense-in-Depth-Ansatz von Schneider Electric, wie in den folgenden Dokumenten beschrieben:

- **Dokumenttitel:** How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations
- **Beschreibung des Website-Links (Dokumentbeschreibung):** How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures?

Verwalten von Schwachstellen

Gemeldete Schwachstellen von Schneider Electric-Geräten sind auf der Webseite zur **Unterstützung der Cybersicherheit** unter http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page aufgeführt.

Eine Liste der Sicherheitsbenachrichtigungen kann durch Klicken auf **Sicherheitshinweise** aufgerufen werden. Sie gelangen dadurch zu: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp.

Wenn Sie mit einem Cybersicherheitsvorfall oder einer Sicherheitslücke konfrontiert sind, die nicht in der von Schneider Electric bereitgestellten Liste aufgeführt ist, können Sie diesen Vorfall bzw. diese Sicherheitslücke melden, indem Sie auf **Melden einer Schwachstelle** auf der Webseite zur **Unterstützung der Cybersicherheit** klicken. Dadurch wird folgende Seite geöffnet: https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp

Sicherung der Architektur

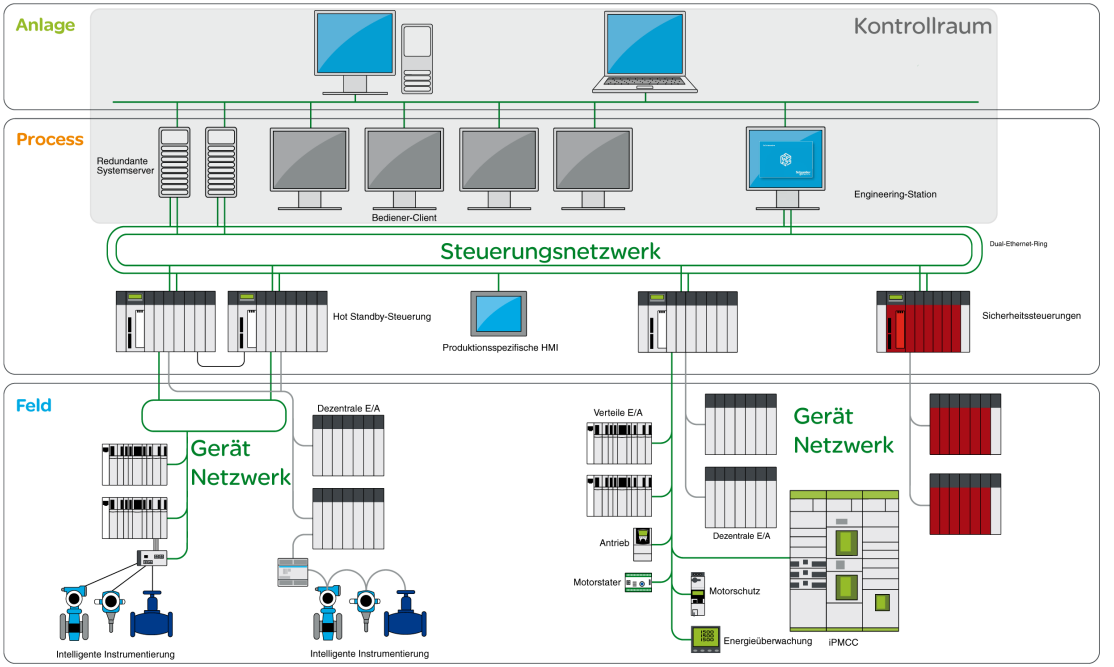
Einführung

Dieses Kapitel beschreibt, wie Sie zur Sicherung von Modicon-Steuerungen beitragen können.

Systemansicht

Systemarchitektur

Die folgende Architektur illustriert, wie wichtig eine mehrschichtige Architektur (mit einem Steuerungs- und einem Gerätenetzwerk) ist, da dies höhere Sicherheit ermöglicht. Eine flache Architektur (wenn alle Geräte mit dem gleichen Netzwerk verbunden sind) kann nicht ordnungsgemäß gesichert werden.



Sichere Kommunikation

Geräte im Kontrollraum sind wesentlich anfälliger für Angriffe als Geräte, die mit dem Gerätenetzwerk verbunden sind. Aus diesem Grund ist eine gesicherte Kommunikation zwischen dem Kontrollraum, der Steuerung und den Geräten zu implementieren. Isolieren Sie das Gerätenetzwerk von den anderen Netzwerkebenen (wie z. B. den Steuerungs- und den dezentralen Netzwerken).

In der obigen Systemarchitektur ist der Bereich des Kontrollraums grau hinterlegt, um ihn von der Steuerung und den anderen Geräten zu unterscheiden.

Sicherer Zugriff auf die USB-Ports

Der physische Zugriff auf die USB-Ports muss kontrolliert werden.

HINWEIS: Die Sicherung der USB-Ports können nur über physische Hilfsmittel erfolgen (z. B. Schaltschrank oder physischer Schlüssel).

Sicherer Zugriff auf die Hot Standby-Verbindung und das Gerätenetzwerk

Kontrollieren Sie den physischen Zugriff auf die Hot Standby-Verbindung und das Gerätenetzwerk.

Test

Control Expert stellt einen Simulator bereit, mit dem Sie Ihre Anwendung vor der Inbetriebnahme als Teil Ihres industriellen Automatisierungssystems testen können. Der Simulator entspricht den Anforderungen an die Cybersicherheit:

- Der Simulator kann nur über eine Anwendung bedient werden, die in Control Expert geöffnet ist.
- Die im Simulator geöffnete Anwendung kann nicht vom Simulator in die Steuerung hochgeladen werden.

Informationen zur Bedienung des Simulators finden Sie in der Hilfe zum *EcoStruxure™ Control Expert, Steuerungssimulator* (https://youtu.be/RrkorSe0G8s).

Festlegung von Passwörtern in Control Expert

Verwenden Sie die Control Expert-Software, um Passwörter festzulegen, die zur Sicherung Ihres Projekts beitragen. Die folgenden Passwörter können festgelegt werden:

- Anwendungspasswort, mit oder ohne Dateiverschlüsselung
- Passwort für den sicherheitsbezogenen Bereich
- Passwort für Firmwareaktualisierungen
- Passwort für Programmeinheiten, Sections und Unterprogrammen
- Passwort für Datenspeicherung/Webpasswort

Anwendungspasswort

Control Expert stellt einen Passwortmechanismus bereit, der den unberechtigten Zugriff auf die Anwendung verhindert. Control Expert greift in folgenden Situationen auf das Passwort zurück:

- Sie öffnen die Anwendung in Control Expert.
- Sie stellen in Control Expert eine Verbindung zur Steuerung her.

Durch den passwortbasierten Anwendungsschutz kann eine unerwünschte Anwendungsänderung, ein unbeabsichtigtes Herunterladen oder Öffnen von Anwendungsdateien verhindert werden. Das Passwort wird verschlüsselt in der Anwendung gespeichert.

Zusätzlich zum Passwortschutz können Sie die Dateien .STU, .STA und .ZEF verschlüsseln. Die Dateiverschlüsselungsfunktion in Control Expert trägt dazu bei, unbefugte Änderungen durch nicht qualifiziertes Personal zu verhindern, und verstärkt den Schutz vor Diebstahl geistigen Eigentums und anderen böswilligen Handlungen. Die Dateiverschlüsselungsoption ist durch einen Passwortmechanismus geschützt.

HINWEIS: Wenn eine Steuerung als Teil eines Systemprojekts verwaltet wird, sind Anwendungspasswort und Dateiverschlüsselung im Control Expert-Editor deaktiviert und müssen über den Topology Manager verwaltet werden.

Informationen zum Festlegen und Verwenden von Anwendungspasswörtern finden Sie im Abschnitt zum *Anwendungsschutz* im *Handbuch EcoStruxure™ Control Expert - Betriebsarten*.

Passwort für den sicherheitsbezogenen Bereich

Sicherheitssteueurngen verfügen über eine Passwortschutzfunktion für den sicherheitsbezogenen Bereich, auf den über das Fenster **Eigenschaften** des Projekts

zugegriffen werden kann. Diese Funktion wird verwendet, um Projektelemente zu schützen, die sich innerhalb des sicherheitsbezogenen Bereichs des Projekts für funktionale Sicherheit befinden.

Wenn die Passwortschutzfunktion für den sicherheitsbezogenen Bereich aktiv ist, können die sicherheitsbezogenen Teile der Anwendung nicht geändert werden.

Informationen zum Festlegen und Verwenden von Passwörtern für sicherheitsbezogene Bereiche finden Sie im Abschnitt zum *Passwortschutz für den sicherheitsgerichteten Bereich* im *Handbuch EcoStruxure™ Control Expert - Betriebsarten*.

Passwort für Firmwareaktualisierungen

Durch den passwortbasierten Firmwareschutz wird ein unerwünschter Zugriff auf die Modul-Firmware verhindert.

Bei M580-Steuerungen hängt die Verwaltung der Firmwareaktualisierungen von der Firmwareversion der Steuerung ab, mit der die Anwendung erstellt wurde.

- Bei Steuerungs-Firmwareversionen vor 4.01:
  - Firmwareaktualisierungen werden über FTP verwaltet.
  - Der Zugriff auf Firmwareaktualisierungen *kann* passwortgeschützt sein.
- Bei Steuerungs-Firmwareversionen ab 4.01:
  - Der Zugriff auf Firmwareaktualisierungen wird über HTTPS verwaltet (sicherer als FTP).
  - Der Zugriff auf Firmwareaktualisierungen *muss* passwortgeschützt sein.
  - Der Zugriff auf die Datenspeicherung und die Webseiten ist durch das gleiche Passwort geschützt.

Informationen zum Festlegen und Verwenden von Firmware-Passwörtern finden Sie im Abschnitt zum *Firmware-Schutz* im *Handbuch EcoStruxure™ Control Expert - Betriebsarten*.

Passwort für Programmeinheiten, Sections und Unterprogramme

Die Schutzfunktion für Programmeinheiten, Sections und Unterprogramme - aktiviert - nutzt ein Passwort, um diese Programmelemente zu schützen. Diese Funktion kann im Offline-Modus im Fenster der Eigenschaften des Projekts eingestellt und aufgerufen werden.

Informationen zum Festlegen und Verwenden von Passwörtern für Programmeinheiten, Sections und Unterprogramme finden Sie im Abschnitt zum *Schutz für Programmeinheiten, Sections und Unterprogramme* im *Handbuch EcoStruxure™ Control Expert - Betriebsarten*.

Passwort für Datenspeicherung/Webpasswort

Der Passwortschutz verhindert den unerwünschten Zugriff auf den Datenspeicherbereich der SD-Speicherkarte (wenn eine gültige Karte in die Steuerung eingesetzt ist).

Für M580-Steuerungen in einem mit Control Expert der folgenden Version erstellten Projekt:

- Bis Version 15.1 können Sie Passwortschutz für den Datenspeicherzugriff bereitstellen.
- Ab Version 15.1 (einschließlich) können Sie einen Passwortschutz sowohl für die Webdiagnose als auch für den Zugriff auf die Datenspeicherung bereitstellen.

Bei M580-Steuerungen hängt die Verwaltung der Datenspeicherung und Webschnittstellen von der Firmwareversion der Steuerung ab, die zur Erstellung der Anwendung verwendet wird:

- Bei Steuerungs-Firmwareversionen vor 4.01:
  - Die Datenspeicherung wird über FTP verwaltet.
  - Der Zugriff auf die Datenspeicherung *kann* passwortgeschützt sein.
  - Der Zugriff auf die Webseiten kann nicht passwortgeschützt sein.
- Bei Steuerungs-Firmwareversionen ab 4.01:
  - Die Datenspeicherung wird über HTTPS verwaltet (sicherer als FTP).
  - Der Zugriff auf die Datenspeicherung und die Webseiten *muss* passwortgeschützt sein.
  - Der Zugriff auf die Datenspeicherung und die Webseiten ist durch das gleiche Passwort geschützt.

Informationen zum Festlegen und Verwenden von Datenspeicherungs-/Webpasswörtern finden Sie im Abschnitt zum *Datenspeicherung/Web-Schutz* im *Handbuch EcoStruxure™ Control Expert - Betriebsarten*.

Härten des PC

Workstation-PCs, die sich im Kontrollraum befinden, sind in hohem Maß Angriffen ausgesetzt. Die PCs, die EcoStruxure™ Control Expert oder EcoStruxure™ Server Expert unterstützen, müssen gehärtet werden (Hardening).

Da diese Anwendungen alle unter dem Betriebssystem Windows ausgeführt werden, enthält dieses Kapitel Richtlinien zum Härten eines PC mit Fokussierung auf die Sicherheit für Windows 10.

Härten der Engineering-Workstation

Die folgenden Schlüsseltechniken werden verwendet, um eine Workstation zu sichern. Klicken Sie auf einen Punkt, um weitere Informationen zur jeweiligen Technik zu erhalten:

- Reduzierung der Angriffsfläche, Seite 24
- Konfiguration und Überprüfung von Sicherheitsrichtlinien, Seite 25
- Benutzerkontenverwaltung, Seite 25
- Verwaltung der Zugriffskontrolle, Seite 26
- Sicherung der Netzwerkdienste, Seite 27, einschließlich:
  - Deaktivierung des Remote-Desktop-Protokolls, Seite 28
  - Deaktivierung von LANMAN und NTLM, Seite 28
  - Deaktivierung nicht verwendeter Netzwerkschnittstellenkarten, Seite 28
  - Konfiguration der LAN-Verbindung, Seite 29
- Aktivierung oder Installation eines Tools zum Antivirenschutz, Seite 29
- Systematisches Patch-Management, Seite 30
- Backup-Management, Seite 30
- Vertraulichkeitsmanagement, Seite 31
- Audit-Management, Seite 31

Dieser Abschnitt enthält außerdem Verweise auf verschiedene Konfigurationsleitfäden für die Cybersicherheit unter Windows 10, Seite 31.

Reduzierung der Angriffsfläche

Die Angriffsfläche Ihres Netzwerksystems umfasst sämtliche Bereiche, die es einem Eindringling ermöglichen können, Daten hinzuzufügen oder zu extrahieren.

Um die potenzielle Angriffsfläche zu reduzieren:

- Deaktivieren Sie alle Softwareanwendungen, Dienste und Kommunikationsports, die nicht verwendet werden.
- Deaktivieren oder beschränken Sie den Zugriff auf Wechselspeichergeräte (z. B. USB).
- Verwenden Sie die Workstation nur für eine einzige Funktion (installieren Sie beispielsweise OPC UA Server Expert und Control Expert auf verschiedenen PCs).

Konfiguration und Überprüfung der Sicherheitsrichtlinien

Die Windows-Sicherheitsrichtlinien können über Gruppenrichtlinien-Objekte festgelegt werden.

Ein Gruppenrichtlinien-Objekt (GPO: Group Policy Object) ist eine Sammlung von Konfigurationsänderungen, die auf eine PC-Workstation angewendet werden können. Weitere Informationen über den lokalen Gruppenrichtlinien-Editor finden Sie in den unten genannten, Seite 31 Sicherheits-Konfigurationsleitfäden des Center for Internet Security (CIS).

Domain GPOs können auch in Windows Active Directory definiert werden.

Sicherheitskonfigurationen müssen regelmäßig und automatisch überprüft werden.

Benutzerkontenverwaltung

- **Ändern der Standardpasswörter**:

  Ändern Sie vor der Implementierung einer neuen Komponente alle Standardpasswörter in Werte, die mit den Konten auf Administrationsebene übereinstimmen.

  Deaktivieren Sie die automatische Windows-Anmeldung.

  Eine Beschreibung der Passworteinstellungen für Windows-Konten finden Sie in den unten genannten, Seite 31 Sicherheits-Konfigurationsleitfäden des Center for Internet Security (CIS).

- **Einrichten der Benutzerkonten**:

  Die Benutzerkonten können entweder lokal (Arbeitsgruppe) auf einem eigenständigen Computer oder über einen Windows Active Directory-Domänencontroller definiert werden, der die zentrale Verwaltung aller Benutzer in einem System ermöglicht.

  Befolgen Sie beim Einrichten von Benutzerkonten die folgenden Richtlinien:

  - Verwenden Sie ein standardmäßiges individuelles Benutzerkonto (ohne Administratorrechte), um die Softwareanwendungen auszuführen, die für eine Ausführung als eigenständige Anwendungen (z. B. Control Expert) konfiguriert sind.
  - Verwenden Sie ein lokales Systemkonto für die Softwareanwendungen, die für eine Ausführung als Dienst konfiguriert sind (z. B. OFS UA).
  - Verwenden Sie ein spezifisches Administratorkonto, um die Softwareanwendungen zu installieren und IPSec zu konfigurieren.
  - Richten Sie einen Passwortmanager ein, um Ihre Passwörter zu verwalten (z. B. KeyPass).
  - Deaktivieren Sie alle Konten, die nicht mit dem Unternehmensbetrieb verknüpft sind (z. B. Debug-Konten). Siehe CIS Control 16.8, Seite 31.
  - Deaktivieren Sie inaktive Konten nach einer festgelegten Zeit der Inaktivität automatisch. Siehe CIS Control 16.9, Seite 31.
  - Sperren Sie Workstation-Sitzungen nach einem Standardzeitraum der Inaktivität automatisch. Siehe CIS Control 16.11, Seite 31.

Verwaltung der Zugriffskontrolle

Der Zugriff auf alle Daten, die in Systemen mit Dateisystem, Netzwerkfreigabe, Claims, Anwendungen oder Datenbanken gespeichert sind, muss kontrolliert werden. Durch diese Kontrollen wird das **Least-Privilege-Prinzip** umgesetzt, d. h. nur jeweils befugte Personen können auf Daten zugreifen und die Daten, auf die sie zugreifen können, entsprechen den Mindestinformationen, die sie für ihren Aufgabenbereich benötigen.

Berechtigungen beziehen sich auf Objekte. Je nach Objekt können Berechtigungen auf folgender Grundlage implementiert werden:

- Windows Active Directory-Objekte
- NTFS-Dateizugriff über eine diskretionäre Zugriffskontrollliste (Discrete Access Control List (DACL))
- Berechtigungen für freigegebene Ordner
- Remote-Registry-Dienst (aktivieren/deaktivieren)

Privilegien sind Benutzerrechte, die nicht mit einem Objekt verknüpft sondern gerätespezifisch sind. Sie können über Gruppenrichtlinien-Einstellungen verwaltet werden. So kann z. B. über die Einstellungen für den „Zugriff auf Wechseldatenträger“ im lokalen

Gruppenrichtlinien-Editor der Zugriff auf den Speicher von USB-Geräten eingeschränkt werden (Lesen oder Schreiben)

Sicherung der Netzwerkdienste

Deinstallieren oder deaktivieren Sie nicht benötigte oder nicht verwendete Netzwerkdienste.

Es gibt verschiedene Möglichkeiten, einen Dienst zu deaktivieren (Dienst-Tool, Sicherheitsvorlage, Gruppenrichtlinien-Objekt, PowerShell, SC.exe).

Verwenden Sie die Windows-Firewall mit einer Standardverweigerungsregel, die den gesamten Datenverkehr mit Ausnahme der Dienste und Ports verwirft, die explizit zulässig sind.

- **Firewall-Nutzung**:

  Die Windows-Firewall wird für die IPSEC-Konfiguration unter Windows 10 benötigt. In den neuesten Versionen der Windows-Betriebssysteme, einschließlich Windows 10, ist die Firewall standardmäßig aktiviert. Weitere Informationen zu den Windows-Firewalleinstellungen finden Sie in den unten genannten Sicherheits-Konfigurationsleitfäden des Center for Internet Security (CIS).

- **Server-Manager-Tool**:

  Mit dem Server-Manager können Sie alle Abhängigkeiten einer Funktion anzeigen, sodass Sie feststellen können, ob es sinnvoll ist, diese von einem Windows-Server zu entfernen.

  Serverrollen können ausgewählt werden (z. B. Webserver (IIS), DNS-Server usw.).

  Serverfunktionen können ausgewählt werden (z. B. BitLocker, .NET Framework usw.).

- **Internet Information Server (IIS) - Webserver-Sicherheit**:

  Verwenden Sie die Minimalinstallation der neuesten Version.

  Konfigurieren Sie die IIS-Zugriffskontrolle (TLS und Benutzerauthentifizierung).

  Aktivieren Sie die Protokollierung und überprüfen Sie die Protokolle auf Hacking-Signaturen.

  Weitere Informationen zu den IIS-Einstellungen finden Sie im CIS-Benchmark-Dokument (Link siehe unten)., Seite 31

- **Deaktivierung von SMBv1**:

  Server Message Block Version 1 (SMBv1) ist ein Protokoll, das für die gemeinsame Nutzung von Diensten (wie Druck, Dateien und Kommunikation) zwischen PCs in einem Netzwerk verwendet wird. SMBv1ist nachweislich anfällig für eine Remote-Code-Ausführung auf dem Host-PC.

  Sie können SMBv1 deaktivieren, um Schwachstellen zu minimieren.

Deaktivierung des Remote-Desktop-Protokolls

Zu den Richtlinien für tiefgreifende Sicherheit von Schneider Electric gehört die Deaktivierung des Remote-Desktop-Protokolls (RDP), es sei denn, Ihre Anwendung benötigt das RDP. So deaktivieren Sie das Protokoll:

Schritt	Aktion
1	Deaktivieren Sie in Windows 10 das RDP über **Computer > Systemeigenschaften > Erweiterte Systemeinstellungen**.
2	Deaktivieren Sie auf der Registerkarte **Dezentral** das Kontrollkästchen **Remoteunterstützungsverbindungen mit diesem Computer zulassen**.
3	Aktivieren Sie das Kontrollkästchen **Keine Verbindung mit diesem Computer zulassen**.

Deaktivierung von LANMAN und NTLM

Deaktivieren Sie sowohl das Microsoft LAN Manager-Protokoll (LANMAN)) als auch dessen Nachfolger NT LAN Manager (NTLM), um Schwachstellen zu minimieren.

So deaktivieren Sie LANMAN und NTLM in einem Windows 10-System:

Schritt	Aktion
1	Führen Sie `secpol.msc` in einem Befehlsfenster aus, um das Fenster **Lokale Sicherheitsrichtlinie** zu öffnen.
2	Öffnen Sie **Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen**.
3	Wählen Sie **Nur NTLMv2-Antworten senden. LM & NTLM ablehnen** im Feld **Netzwerksicherheit: LAN Manager-Authentifizierungsstufe** aus.
4	Aktivieren Sie das Kontrollkästchen **Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern**.
5	Geben Sie `gpupdate` in einem Befehlsfenster ein, um die geänderten Sicherheitsrichtlinien zu übergeben.

Deaktivierung nicht verwendeter Netzwerkschnittstellenkarten

Deaktivieren Sie Netzwerkschnittstellenkarten, die für die Anwendung nicht erforderlich sind. Wenn Ihr System beispielsweise über zwei Karten verfügt, die Anwendung jedoch nur eine davon verwendet, vergewissern Sie sich, dass die zweite Netzwerkkarte (LAN-Verbindung 2) deaktiviert ist.

So deaktivieren Sie eine Netzwerkkarte in Windows 10:

Schritt	Aktion
1	Öffnen Sie **Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern**.
2	Klicken Sie mit der rechten Maustaste auf die nicht verwendete Verbindung. Wählen Sie **Deaktivieren** aus.

Konfigurieren der LAN-Verbindung

Verschiedene Windows-Netzwerkeinstellungen bieten eine verbesserte Sicherheit, die auf den Defense-in-Depth-Ansatz abgestimmt ist.

Greifen Sie in Windows 10-Systemen auf diese Einstellungen zu, indem Sie **Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern > LAN-Verbindung (x)** aufrufen.

Die folgende Liste ist ein Beispiel für Konfigurationsänderungen, die Sie im Fenster **Eigenschaften von LAN-Verbindung** an Ihrem System vornehmen können:

- Deaktivieren Sie alle IPv6-Stacks auf den entsprechenden Netzwerkkarten.
- Heben Sie die Auswahl aller Elemente in **Eigenschaften der LAN-Verbindung** auf, mit Ausnahme von **QoS-Paketplaner** und **Internetprotokoll Version 4**.
- Deaktivieren Sie auf der Registerkarte **Wins** in **Erweiterte TCP/IP-Einstellungen** die Kontrollkästchen **LMHOSTS aktivieren** und **NetBIOS über TCP/IP deaktivieren**.
- Aktivieren Sie **Datei- und Druckerfreigabe für Microsoft Network**.

Zu den Defense-in-Depth-Richtlinien von Schneider Electric gehören außerdem folgende Maßnahmen:

- Definieren Sie ausschließlich statische IPv4-Adressen, Subnetzmasken und Gateways.
- Verwenden Sie DHCP oder DNS nicht im Kontrollraum.

Aktivierung oder Installation eines Tools zum Antivirenschutz

Sie können die Systemreaktion gegen Viren und bösartigen Code mit den integrierten Tools in Windows 10 verbessern. Sie können bei Bedarf auch zusätzliche Antivirensoftware installieren.

Die Enterprise-Edition von Windows 10 umfasst *Windows Defender Advanced Threat Protection*, eine Sicherheitsplattform, die Endpunkte überwacht, z. B. Windows 10-PCs,

unter Rückriff auf Verhaltenssensoren. Die *SmartScreen*-Technologie von Microsoft ist eine weitere integrierte Funktion, die den Zugriff auf Websites und Downloads, von denen bekannt ist, dass sie bösartig sind, scannt, herunterlädt und blockiert.

Weitere Informationen zu den Einstellungen für *Windows Defender* finden Sie im unten genannten CIS-Dokument (Center for Internet Security), einschließlich:

- Stellen Sie sicher, dass die Anti-Malware-Software des Unternehmens ihre Scan-Engine und Signaturdatenbank regelmäßig aktualisiert (CIS Control 8.2).
- Konfigurieren Sie das Anti-Malware-Scannen von Wechseldatenträgern: USB (siehe CIS Control 8.4), Seite 31.
- Konfigurieren Sie die Geräte so, dass Inhalte von Wechselmedien nicht automatisch ausgeführt werden: USB (siehe CIS Control 8.5), Seite 31.

Systematisches Patch-Management

Installieren Sie stets die letzte stabile Version aller sicherheitsrelevanten Updates des Betriebssystems, der Anwendungen (einschließlich Webbrowser und E-Mail-Client) und der Treiber.

Aktivieren Sie automatische Updates in Windows 10.

Weitere Informationen finden Sie im unten genannten, Seite 31 CIS-Dokument (Center for Internet Security).

Backup-Management

Stellen Sie Folgendes sicher:

- Alle Systemdaten werden automatisch regelmäßig gesichert (siehe CIS Control 10.1), Seite 31.
- Die wichtigsten Systeme des Unternehmens werden als komplettes System durch Prozesse wie Imaging gesichert, um die schnelle Wiederherstellung eines gesamten Systems zu ermöglichen (siehe CIS Control 10.2), Seite 31.
- Backups werden ordnungsgemäß durch physische Sicherheit oder Verschlüsselung geschützt, wenn sie gespeichert und über das Netzwerk verschoben werden. Dies gilt auch für Remote-Backups und Cloud-Dienste (siehe CIS Control 10.4)., Seite 31
- Alle Backup-Vorgänge verfügen über mindestens ein Ziel für die Offline-Sicherung (Zugriff über Netzwerkverbindung nicht möglich) (siehe CIS Control 10.5), Seite 31.

Sie haben folgende Möglichkeiten:

- Verwenden Sie den *Dateiversionsverlauf* und andere kostenlose Tools in Windows 10, um Datei-Backups zu erstellen.

- Richten Sie ein Wiederherstellungslaufwerk ein, um Ihr System aus einem Image-Backup wiederherzustellen.
- Verwenden Sie einen Storage-Sync-and-Share-Dienst, um Ihre Backups in die Cloud zu verlagern, z. B. *OneDrive*, *Dropbox* oder *Google Drive*.

Weitere Informationen zum Windows-Dateiversionsverlauf sowie zu den Einstellungen für die Sicherung/Wiederherstellung finden Sie im unten genannten CIS-Dokument.

Vertraulichkeitsmanagement

Entfernen Sie sensible Daten oder Systeme, auf die das Unternehmen nicht regelmäßig zugreift, aus dem Netzwerk. Diese Systeme können als eigenständige (vom Netzwerk getrennte) Systeme von der Geschäftseinheit verwendet werden, die sie gelegentlich nutzen muss, oder sie können vollständig virtualisiert und abgeschaltet werden, bis sie benötigt werden. Siehe das unten genannte CIS-Dokument (siehe CIS Control 13.2), Seite 31.

Aktivieren Sie die Festplattenverschlüsselung mit *BitLocker*. Weitere Informationen zu den *BitLocker*-Einstellungen finden Sie im unten genannten CIS-Dokument.

Audit-Management

Stellen Sie sicher, dass die lokale Sicherheitsprotokollierung auf Windows-Hosts konfiguriert wurde. Detaillierte Informationen zur Konfiguration der Audit-Richtlinien finden Sie im unten genannten CIS-Dokument, Seite 31.

Konfigurationsleitfäden für die Cybersicherheit unter Windows 10

Vergewissern Sie sich, dass Sie unter Windows 10 mit Einstellungen für die Cybersicherheit arbeiten, um auf die nachstehenden Konfigurationsleitfäden für Windows Bezug nehmen zu können:

- Sicherheits-Konfigurationsleitfäden des Center for Internet Security – CIS

  https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/

  - IG1-Ebene:

    https://www.cisecurity.org/cis-benchmarks/

    https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

    https://www.cisecurity.org/benchmark/microsoft_iis/

- Richtlinien für die Sicherheitskonfiguration vom US-amerikanischen Verteidigungsministerium (DISA STIG)

  https://www.stigviewer.com/stig/windows_10/2020-06-15/

Sowohl das Dokument „CIS benchmarks“ als auch „STIG Windows 10 Security technical implementation guide“ schlagen optionale Profile vor. Die Auswahl eines Profils hängt von der Kritikalität Ihrer unter Windows ausgeführten Anwendungen ab.

Deaktivierung nicht verwendeter integrierter Kommunikationsdienste

Integrierte Kommunikationsdienste

Integrierte Kommunikationsdienste sind Kommunikationsdienste, die auf IP basieren und auf einem integrierten Produkt im Servermodus verwendet werden (zum Beispiel HTTP oder FTP).

Deaktivieren nicht verwendeter Dienste

Deaktivieren Sie alle nicht verwendeten integrierten Dienste, z. B. HTTP und FTP, um das Angriffsrisiko zu verringern und potenzielle Kommunikationskanäle zu schließen.

Deaktivieren der Ethernet-Dienste in Control Expert

Sie können die Ethernet-Dienste auf den Ethernet-Registerkarten in control Expert aktivieren/deaktivieren. Die Registerkarten werden für die folgenden Systeme beschrieben:

- Modicon M340, Seite 138
- Modicon M580, Seite 138

- Modicon Quantum, Seite 138
- Modicon X80 modules, Seite 140
- Modicon Premium/Atrium, Seite 143
- Modicon Momentum MDI, Seite 144
- Modicon MC80, Seite 144

Stellen Sie die Parameter auf den Ethernet-Registerkarten ein, bevor Sie die Anwendung in die Steuerung herunterladen.

Die Standardeinstellungen (maximale Sicherheitsebene) verringern die Kommunikationskapazität. Wenn Dienste benötigt werden, müssen diese aktiviert werden.

HINWEIS: Bei einigen Produkten ermöglicht der `ETH_PORT_CTRL (see EcoStruxure™ Control Expert, Communication, Block Library)`-Funktionsbaustein die Deaktivierung eines nach der Konfiguration in der Control Expert-Anwendung aktivierten Dienstes. Der Dienst kann mithilfe desselben Bausteins wieder aktiviert werden.

Einschränkung des Datenflusses vom Steuerungsnetzwerk (Zugriffskontrolle)

Datenfluss vom Steuerungsnetzwerk

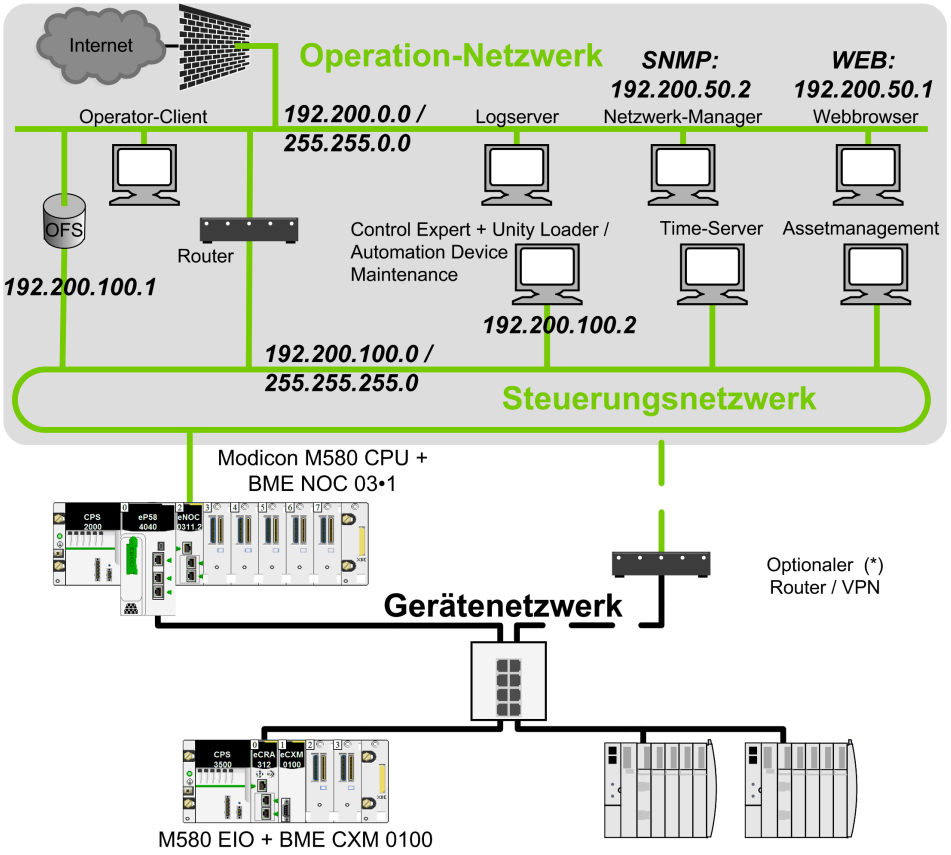
Der Datenfluss vom Steuerungsnetzwerk ist ein Datenfluss, der auf IP basiert und vom Steuerungsnetzwerk initiiert wird.

Beschreibung

Um den Zugriff auf Kommunikationsserver in einem eingebetteten Produkt zu steuern, beschränkt die Zugriffskontrollverwaltung den IP-basierten Datenfluss vom Steuerungsnetzwerk auf eine autorisierte Quell- oder Subnetz-IP-Adresse.

Architekturbeispiel

Die folgende Abbildung zeigt die Rolle und den Einfluss der Zugriffskontrolleinstellungen. Die Zugriffskontrolle verwaltet den Ethernet-Datenfluss von Geräten, die in Betriebs- und Steuerungsnetzwerken (grau hinterlegter Bereich) kommunizieren.



(*) Einige Dienste benötigen Zugriff auf das Gerätenetzwerk (z. B. Firmwareaktualisierung, Zeitstempelung an Quelle). In diesen Fällen wird über den optionalen Router/VPN ein sicherer Zugriff zur Verfügung gestellt.

Festlegen der autorisierten Adressen im Architekturbeispiel

Ziele der Zugriffskontrolle:

- Alle mit dem Betriebsnetzwerk verbundenen Geräte (IP-Adresse = 192.200.x.x) können auf den Webserver der Steuerung zugreifen.
- Alle mit dem Steuerungsnetzwerk verbundenen Geräte (IP-Adresse = 192.200.100.x) können mit der Steuerung über Modbus TCP kommunizieren und auf den Webserver zugreifen.

Zur Einschränkung des Datenflusses im vorstehenden Architekturbeispiel werden die autorisierten Adressen und Dienste wie folgt in der EcoStruxure Control Expert-Zugriffskontrolltabelle festgelegt:

Quelle	IP-Adresse	Sub-netz	Subnetz-maske	FTP	TFTP	HTTP / HTTPS	Por-t502	EIP	SN-MP
Netzwerkmana-ger	192.200.50.2	Nein	–	–	–	–	–	–	+
Betriebsnetz-werk	192.200.0.0	Ja	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance	192.200.100-.2	Nein	–	+ [1)]	–	- [2)]	+	–	–
Steuerungs-netzwerk	192.200.100-.0	Ja	255.255.255-.0	–	–	–	+	–	–

+ Ausgewählt

– Nicht ausgewählt oder kein Inhalt

[1)] Für M580-Firmwareversionen ab v4.10 ist FTP nicht ausgewählt.

[2)] Für M580-Firmwareversionen ab v4.10 ist HTTP/HTTPS ausgewählt.

Beschreibung der Einstellungen

Für Geräte, die zur Kommunikation mit der Steuerung über Modbus TCP oder EtherNet/IP berechtigt sind, wird eine autorisierte Adresse festgelegt.

Erklärung der Diensteinstellungen für jede IP-Adresse im vorherigen Beispiel:

192.200.50.2 (SNMP)	Genehmigt dem Netzwerkmanager den Zugriff über SNMP.
192.200.0.0 (HTTP/HTTPS)	Das Subnetz des Betriebsnetzwerks genehmigt allen mit dem Betriebsnetzwerk verbundenen Webbrowsern den Zugriff auf den Webbrowser der Steuerung.
192.200.100.2 (FTP) [1)]	Genehmigt Automation Device Maintenance den Zugriff über FTP.
192.200.100.0 (Port502)	Das Subnetz des Steuerungsnetzwerks genehmigt allen mit dem Steuerungsnetzwerk verbundenen Komponenten (OFS, Control Expert, Automation Device Maintenance) den Zugriff auf die Steuerung über Port502 Modbus.
[1)] Bei M580-Firmwareversionen ab v4.10 wird FTP nicht verwendet. Verwenden Sie stattdessen HTTP/HTTPS.	

HINWEIS: Die Analyse der Zugriffsliste durchläuft jeden Eintrag in der Zugriffskontrollliste. Wenn eine Übereinstimmung (IP-Adresse + zugelassener Dienst) gefunden wird, werden die anderen Einträge ignoriert.

Geben Sie im Fenster EcoStruxure Control Expert **Sicherheit** für ein bestimmtes Subnetz die spezifischen Regeln vor der Subnetzregel ein. Beispiel: Um Gerät 192.200.50.2 ein spezifisches SNMP-Recht zu gewähren, geben Sie die Regel vor der globalen Subnetzregel 192.200.0.0/255.255.0.0 ein, die allen Geräten des Subnetzes HTTP-Zugriff gewährt.

Einrichtung verschlüsselter Kommunikation

Einführung

Ziel der verschlüsselten Kommunikation ist der Schutz der Kommunikationskanäle, die einen Fernzugriff auf die kritischen Ressourcen des Systems ermöglichen (z. B. integrierte Anwendung, Firmware des Modicon M580 PAC). IPsec (Internet Protocol Security) ist ein von der IETF definierter offener Standard, der unter Verwendung einer Kombination aus kryptografischen und protokollspezifischen Sicherheitsmechanismen eine geschützte und private Kommunikation in IP-Netzwerken bereitstellt. Unsere Implementierung des IPsec-Schutzes umfasst Anti-Replay, Integritätsprüfung bei der Nachrichtenübertragung und Authentifizierung der Nachrichtenherkunft.

IPsec wird unter Microsoft Windows Versionen 7 und 10 unterstützt. Es wird vom Betriebssystem des PC initiiert.

Beschreibung

Die IPsec-Funktion ermöglicht die Sicherung der folgenden Aspekte:

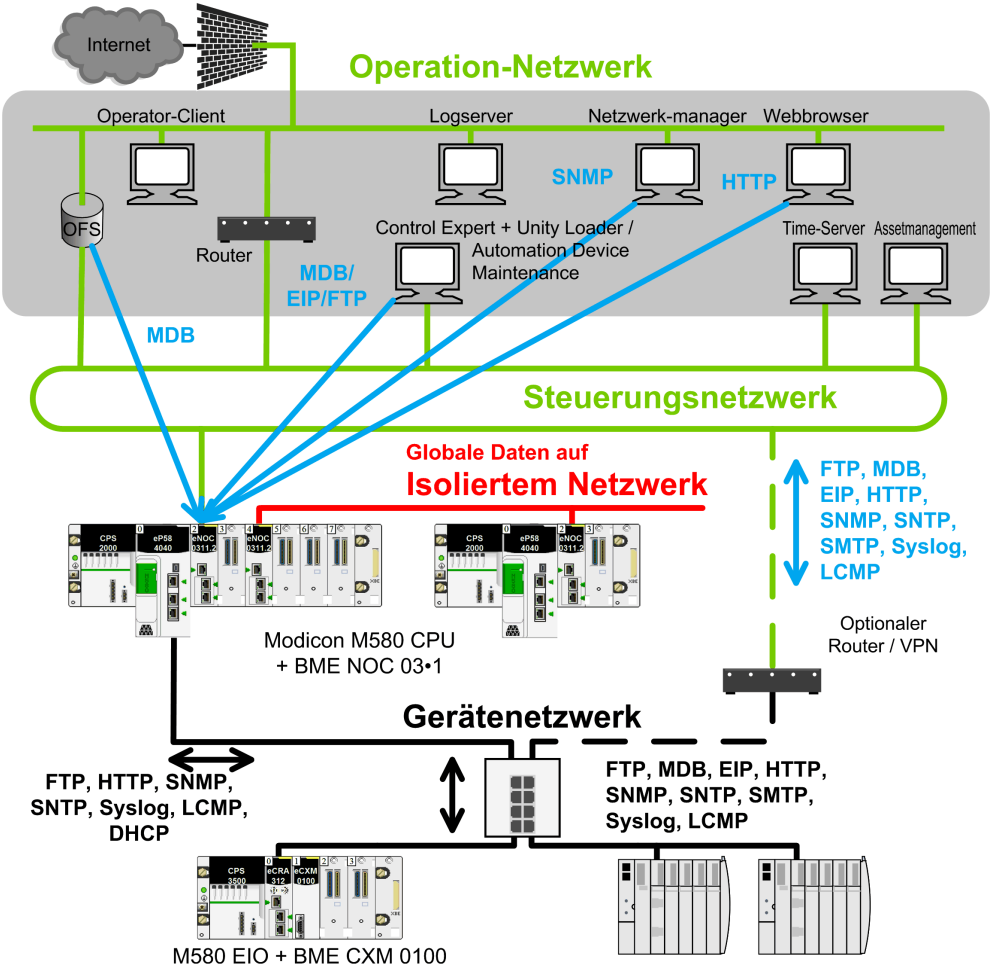
- Modbus-Zugriff des Kontrollraums auf die Steuerung über BMENOC0301 and BMENOC0311 -Module.
- Kontrollraum-Zugriff auf die in den BMENOC0301 and BMENOC0311-Modulen im Servermodus ausgeführten Kommunikationsdienste (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

  HINWEIS: IPsec trägt zur Sicherung der Dienste bei, die im Servermodus in der Steuerung ausgeführt werden. Vom Modicon M580 PAC initiierte sichere Client-Dienste fallen nicht in den Geltungsbereich dieses Handbuchs.

Wireless-Verbindung: Wenn ein Wireless-Modul PMXNOW0300 verwendet wird, um eine Wireless-Verbindung einzurichten, konfigurieren Sie dieses Modul mit den maximal verfügbaren Sicherheitseinstellungen (WPA2-PSK).

Architekturbeispiel

In der folgenden Abbildung werden anhand eines Beispiels die verschiedenen Protokolle oder Dienste veranschaulicht, die an einer verschlüsselten Kommunikation zwischen Kontrollraum und Modicon M580 controller beteiligt sind.



Datenfluss mit verschlüsselter Kommunikation

Verwenden Sie die folgenden Dienste, um die Kommunikation bei aktiviertem IPsec zu erleichtern:

Ethernet-Dienst	Sicherheit des Datenflusses
Server der EIP-Klasse 3	Diese Dienste werden über verschlüsselte Verbindungen unterstützt.
FTP-Server, TFTP-Server	
HTTP	
ICMP	
Modbus-Server (Port 502)	
ARP	Diese Dienste werden über verschlüsselte und unverschlüsselte Verbindungen unterstützt. **HINWEIS:** Dieser Datenverkehr umgeht das IPsec-Protokoll-Handling im BMENOC und verwendet daher nicht IPsec.
LLDP	
Loop-Check-Protokoll (Schleifenprüfung)	
Modbus-Scanner	
RSTP	
DHCP-, BootP-Client	Diese Dienste werden bei aktiviertem IPSec nicht unterstützt. **HINWEIS:** Vor der Initiierung von IKE/IPsec durch den Peer (PC) wird dieser Datenverkehr nicht per IPSec gesichert. Nach der Einrichtung von IKE/IPSec wird dieser Datenverkehr mit IPsec verschlüsselt. Das Protokoll kann unterstützt werden, aber nur, wenn es sich beim Paketempfänger um einen PC mit konfiguriertem und aktiviertem IPSec handelt.
DHCP-, BootP-Server	
EIP-Klasse 1, TCP (Forward Open)	
EIP-Klasse 1, UDP (Datenaustausch)	
Modbus-Client	
NTP-Client	
SNMP-Agent	
SNMP-Traps	
Syslog-Client (UDP)	

HINWEIS:

- IPsec ist ein Schutz der OSI-Schicht 3. Protokolle der OSI-Schicht 2 (ARP, RSTP, LLDP, Loop-Check-Protokoll) werden nicht durch IPsec geschützt.
- Der **Globale Daten**-Kommunikationsfluss (mit BMXNGD0100-Modulen) können nicht per IPsec gesichert werden. Verwenden Sie eine derartige Konfiguration in einem isolierten Netzwerk.

Einschränkungen

IPsec-Einschränkungen in der Architektur: BMENOC0301 and BMENOC0311-Module bieten keine Unterstützung für eine IP-Weiterleitung an das Gerätenetzwerk.

Wenn zwischen dem Steuerungs- und dem Gerätenetzwerk Transparenz benötigt wird, muss ein externer Router bzw. ein externes VPN eine verschlüsselte Kommunikation zwischen dem Steuerungs- und dem Gerätenetzwerk bereitstellen (wie in der vorherigen Abbildung eines Architekturbeispiels, Seite 38 gezeigt).

Transparenz wird benötigt, um die folgenden Vorgänge vom Steuerungsnetzwerk aus auszuführen:

- Aktualisieren einer M580-Steuerungsfirmware mithilfe von Automation Device Maintenance über den HTTPS-Dienst.
- Durchführen einer Netzwerkdiagnose für die M580-Steuerung mithilfe eines Netzwerkmanagementtools über den SNMP-Dienst.
- Diagnose einer M580-Steuerung mithilfe eines DTM über den EIP-Dienst.
- Diagnose einer M580-Steuerung mithilfe eines Webbrowsers über den HTTP-Dienst.
- Protokollieren von Cybersicherheit-Ereignissen für eine M580-Steuerung in einem syslog-Server über den syslog-Dienst.
- Synchronisieren der Zeit einer M580-Steuerung mit einem globalen Zeitserver über den NTP-Dienst.

Einrichtung der IPsec-Kommunikation in der Systemarchitektur

Gehen Sie vor wie folgt, um die IPsec-Kommunikation einzurichten:

- Identifizieren Sie im Kontrollraum die vom Client autorisierten Anwendungen, die mit dem Modicon M580 PAC -System über Modbus kommunizieren müssen (Control Expert, Automation Device Maintenance, OFS, Kundenanwendungen wie SGBackup usw.).

  Konfigurieren Sie IPsec auf jedem PC, der diese autorisierten Anwendungen unterstützt.
- Identifizieren Sie im Kontrollraum die vom Client autorisierten Anwendungen, die mit den im lokalen Rack konfigurierten BMENOC0301 and BMENOC0311-Modulen kommunizieren müssen (Control Expert DTM, Automation Device Maintenance, SNMP-Manager, Webbrowser, Webdesigner für FactoryCast BMENOC0301 and BMENOC0311-Module).

  Konfigurieren Sie IPsec auf jedem PC, der diese autorisierten Anwendungen unterstützt.

- Integrieren Sie die BMENOC0301 and BMENOC0311-Module mit IPsec-Funktion in den Baugruppenträger jedes mit dem Steuerungsnetzwerk verbundenen Modicon M580 PAC -Systems.

  Führen Sie zur Konfiguration der IPsec-Funktion in BMENOC0301 and BMENOC0311-Modulen die folgenden 2 Schritte aus:

  - Aktivieren Sie die IPsec-Funktion.
  - Konfigurieren Sie einen Pre-Shared-Key: Ein Pre-Shared-Key wird verwendet, um ein gemeinsames Geheimnis (Shared Secret) zu generieren, das es beiden Geräten ermöglicht, sich gegenseitig zu authentifizieren.

    HINWEIS: Da IPsec auf diesem gemeinsamen Geheimnis basiert, handelt es sich um ein Schlüsselelement der Sicherheitsrichtlinien, die vom Sicherheitsadministrator verwaltet wird. Um die Sicherheit des Pre-Shared-Key zu erhöhen, verwenden Sie ein externes Tool wie KeePass, Seite 41, um eine angemessene Zeichenfolge zu generieren.

Die Konfiguration der BMENOC0301 and BMENOC0311-Module erfolgt mit Control Expert. Um diese Konfiguration zu sichern, sollte der erste Download über eine Punkt-zu-Punkt-Verbindung durchgeführt werden, z. B. über den USB-Port. Alle weiteren Downloads können dann über Ethernet mit einer IPsec-Funktion durchgeführt werden, vorausgesetzt, IPsec ist aktiviert.

Jeder PC, der IPsec unterstützt, muss für die IPsec-Konfiguration die folgenden Anforderungen erfüllen:

- Verwendet das Betriebssystem Microsoft Windows 10.
- Verfügt über die erforderlichen Administratorrechte zur Konfiguration von IPsec.

  Sobald die IPsec-Konfiguration durchgeführt wurde, legen Sie das Windows-Konto als normales Benutzerkonto ohne Administratorrechte fest.
- **Härten Sie den PC wie im Abschnitt *Härten des PC*, Seite 23** beschrieben.

Weitere Informationen zur Konfiguration finden Sie im Abschnitt *Konfiguration der sicheren IP-Kommunikation* (siehe Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Kommunikationsmodul, Installations- und Konfigurationshandbuch).

Generierung von Pre-Shared-Keys mit höchster Sicherheitsebene

Die Sicherheit der IPsec-Kommunikation beruht auf der Komplexität des Pre-Shared-Key. Verwenden Sie spezielle Tools, um Pre-Shared-Keys mit höchster Sicherheitsebene zu erstellen.

Ein in Frage kommendes Tool ist z. B. KeePass, das als Freeware vom Internet heruntergeladen werden kann. Laden Sie KeePass in Ihren PC herunter, installieren und starten Sie das Tool.

Konfigurieren und verwenden Sie KeePass v2.34, um Passwörter zu erzeugen, die als Pre-Shared-Key verwendet werden können:

Schritt	Aktion
1	Erstellen Sie einen neuen Schlüsseldatenbankordner (**File > New**).
2	Geben Sie im Dialogfeld **Create New Password Database** im Feld **File name** einen Ordnernamen ein und speichern Sie Ihre Änderungen.
3	Geben Sie im Dialogfeld **Create Composite Master Key** im Feld **Master password** ein Master-Passwort ein. Geben Sie das Passwort dann erneut im Passwortfeld **Repeat** ein.
4	Klicken Sie auf **OK**, um **Step 2** zu öffnen, und klicken Sie dann erneut auf **OK**.
5	Erweitern Sie im Dialogfeld für neue Datenbanken die Option **New Database**.
6	Wählen Sie **Network** aus und fügen Sie einen Eintrag hinzu (**Edit > Add Entry**).
7	Geben Sie im Feld **Title** einen Namen für Ihr Modul ein (z. B. eNOC).
8	Geben Sie im Feld **User name** einen Benutzernamen ein.
9	Klicken Sie auf das Symbol **Generate a password**.
10	Wählen Sie **Open password generator** aus.
11	Klicken Sie auf **OK**, um die Felder **Password** und **Repeat** zu füllen.
12	Öffnen Sie das Dialogfeld **Password Generation Options** (**Tools > Generate Password**).
13	Treffen Sie die folgende Auswahl unter **Generate using character set**: • Großbuchstaben: Upper-case (A, B, C, ...) • Kleinbuchstaben: Lower-case (a, b, c, ...) • Ziffern: Digits (0, 1, 2, ...) • Minuszeichen: Minus (-) • Unterstreichung: Underline (_) • Sonderzeichen: Special (!, $, %, &, ...) • Klammern: Brackets ([,], [, (,), <, >) **HINWEIS:** Die folgenden Zeichen sind in einem Pre-Shared-Key nicht zulässig: • { • } • ; • #
14	Klicken Sie auf **OK**.
15	Klicken Sie mit der rechten Maustaste auf Ihr Gerät in der Liste **Database** und navigieren Sie zu **Copy Password**.
16	Öffnen Sie das Fenster zur Sicherheitskonfiguration in Control Expert.
17	Fügen Sie den Schlüssel im IPsec-Konfigurationsfenster ein.

Diagnose der IPsec-Kommunikation in der Systemarchitektur

Informationen zur IPsec-Diagnose in der Systemarchitektur finden Sie im Abschnitt *Konfiguration der verschlüsselten IP-Kommunikation* (siehe Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Kommunikationsmodul, Installations- und Konfigurationshandbuch).

CSPN-Sicherheitsziel

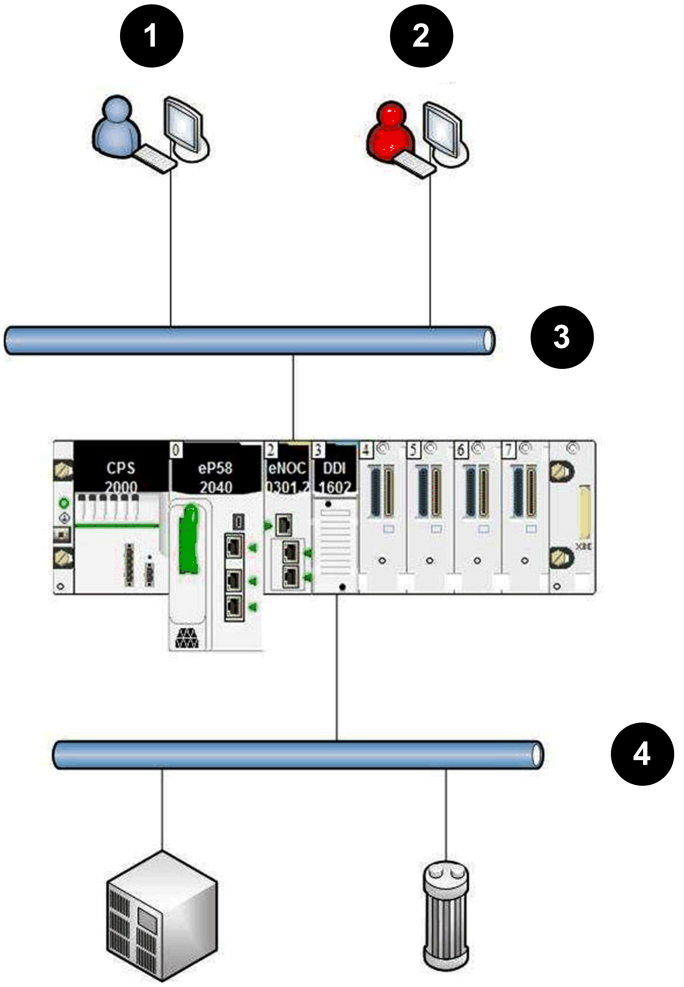
Einführung in die CSPN-Zertifizierung

CSPN (Certification de Sécurité de Premier Niveau) ist eine Cybersicherheit-Zertifizierung, die derzeit in Frankreich verwendet wird. Es wird erwartet, dass ein Produkt mit CSPN-Zertifizierung einem Cyberangriff standhält, der in zwei Personenmonaten von erfahrenen Hackern durchgeführt wird. Das M580-System ist CSPN-zertifiziert. In diesem Abschnitt werden die Umgebung, die Konfigurationen der speicherprogrammierbaren Automatisierungssteuerung und die Parameter beschrieben, die die CSPN-Anforderungen erfüllen, um ein Höchstmaß an Sicherheit zu gewährleisten.

Modicon M580 - Einführung

Das Modicon M580-PAC-System ist für die kontinuierliche Kontrolle und Steuerung eines industriellen Prozesses ohne menschliche Eingriffe ausgelegt. Bei jedem Schritt verarbeitet die Steuerung die von ihren Eingängen, den Sensoren, empfangenen Daten und sendet Befehle an ihre Ausgänge, die Aktoren. Der Austausch mit dem Überwachungssystem (HMI, SCADA) erfolgt über BMENOC0301 and BMENOC0311-Ethernet-Kommunikationsmodule im lokalen Rack mit der Steuerung.

Die folgende Abbildung zeigt eine typische M580-Systemarchitektur, die anfällig für einen Sicherheitsangriff sein kann:



1 Bediener mit EcoStruxure Control Expert

2 Angreifer

3 Überwachungsnetzwerk

4 Feldnetzwerk ohne Angreifer

Funktionen der Baureihe M580

Die M580-Steuerungen bieten die folgenden Funktionen:

Funktion	Beschreibung
Ausführung des Benutzerprogramms	Eine M580-Steuerung führt ein Benutzerprogramm aus, das die Eingänge verarbeitet und die Ausgänge aktualisiert.
Verwaltung der Ein-/Ausgänge	Eine M580-Steuerung kann lokale Eingänge lesen und lokale Ausgänge schreiben. Diese Ein-/Ausgänge können digital oder analog sein und ermöglichen der M580-Steuerung die Kontrolle und Steuerung des industriellen Prozesses.
Kommunikation mit dem Überwachungssystem	Eine M580-Steuerung kann mit SCADA kommunizieren, um Befehle zu empfangen und Prozessdaten über das Modbus-Protokoll zu übertragen.
Administrationsfunktionen	Eine M580-Steuerung umfasst administrative Funktionen, die in EcoStruxure Control Expert zur Konfiguration und Programmierung zur Verfügung stehen.
Dezentrale Anmeldung	Eine M580-Steuerung unterstützt die Definition einer dezentralen Protokollierungsrichtlinie. Sie kann Sicherheits- und Verwaltungsereignisse protokollieren.

Konfiguration der Baureihe M580

Eine CSPN-zertifizierte M580-Konfiguration umfasst folgende Komponenten:

Modul	Firmware	Beschreibung
BMEP58•0•0	ab Version 2.20	Die Steuerung befolgt die in den Sicherheitsdokumenten beschriebenen Sicherheitsregeln (siehe Annahmen).
BMENOC0301 and BMENOC0311	ab Version 2.11	Dieses Ethernet-Modul verwaltet die verschlüsselte Kommunikation mit der oberen Schicht (Überwachungs- und Engineering-Software EcoStruxure Control Expert).

HINWEIS: Die Programmiersoftware EcoStruxure Control Expert, PCs, andere Steuerungsmodule und Baugruppenträgerkomponenten fallen nicht in den Geltungsbereich der Zertifizierung.

Benutzerprofile

Benutzer, die mit der Steuerung interagieren, um eine verbesserte Implementierung zu erzielen, verfügen über die folgenden vordefinierten Profile des Sicherheitseditors von EcoStruxure Control Expert:

Benutzerprofil	Beschreibung
ReadOnly (Nur Lesen)	Eine Änderung der Anwendung ist nicht zulässig.
Operate (Betrieb)	Nur die Ausführung der Anwendung und die Änderung von Parametern sind zulässig.
Program (Programm)	Alle Funktionen sind aktiviert.

Verbesserte Implementierung

Folgende Elemente tragen zu einer funktionsfähigen Umgebung zur Gewährleistung einer verbesserten Implementierung bei:

Element	Sicherheitshinweise
Sicherheitsspezifische Dokumentation	Alle Anweisungen in der Dokumentation (z. B. Benutzerhandbücher, Whitepaper) werden vor der Bewertung angewendet.
Administratoren	Systemadministratoren sind kompetent, geschult und vertrauenswürdig.
Räumlichkeiten	Der Zugriff auf den SPS-Standort ist auf vertrauenswürdige Personen beschränkt. Insbesondere hat ein Angreifer keinen Zugriff auf die physischen Ports der Steuerungen. Da identische Produkte ohne jegliche Einschränkungen erworben werden können, können Angreifer derartige Produkte frei untersuchen und anhand unterschiedlichster Verfahren potenzielle Schwachstellen aufspüren.
Deaktivierung nicht bewerteter Dienste	Alle Dienste, die nicht in Bezug auf das Sicherheitsziel bewertet wurden, werden in der Konfiguration oder über ein Benutzerprogramm deaktiviert (wie in der Sicherheitsdokumentation beschrieben).
Prüfung der Benutzeranwendung	Die Integrität der EcoStruxure Control Expert-Anwendung wird vom Administrator kontrolliert, bevor sie in die Steuerung geladen wird.
Aktive Protokollierung	Die Protokollierungsfunktion ist funktionstüchtig und die Protokolle sind nicht beschädigt.
Protokollprüfung	Systemadministratoren führen eine regelmäßige Prüfung der lokalen und dezentralen Protokolle durch.
Erstkonfiguration	Die Ausgangskonfiguration wird über die USB-Schnittstelle in die Steuerung übertragen, die Steuerung ist vom Netzwerk getrennt.

Element	Sicherheitshinweise
Firmwareaktualisierung	Die Firmwareaktualisierung erfolgt über die USB-Schnittstelle, die Steuerung ist vom Netzwerk getrennt.
Starke Passwörter	Systemadministratoren wenden starke Passwörter an, die Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen umfassen.

Betriebsarten

Folgende Betriebsarten sind mit den CSPN-Anforderungen konform:

- Im Rahmen der Inbetriebnahmephase kann die Erstkonfiguration der Steuerung über eine Control Expert-Engineering-Station erfolgen, die **entweder** Punkt-zu-Punkt mit dem Ethernet-Port **oder** mit dem lokalen USB-Port der Steuerung verbunden ist.
- Bei normalen Betriebsbedingungen (RUN-Modus, SCADA verbunden mit dem Ethernet-Steuerungsnetzwerk) ist sicherzustellen, dass Control Expert getrennt ist.
- Nehmen Sie alle weiteren Änderungen an der Konfiguration oder am Anwendungsprogramm mit Control Expert über eine Verbindung mit dem USB-Port der Steuerung vor.

Parameter für die Cybersicherheit

In der folgenden Tabelle werden die Parameter für die Cybersicherheit beschrieben:

Parameter	Abschnitt	Benutzerhandbuch
ACL aktiviert	Konfiguration von Sicherheitsdiensten	Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Kommunikationsmodul, Installations- und Konfigurationshandbuch
IPsec aktiviert auf BMENOC0301/0311 mit maximaler Sicherheit	Konfiguration von Sicherheitsdiensten	
Sicherheitsverstärkung ausgewählt (Protokolle FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP deaktiviert)	Konfiguration von Sicherheitsdiensten	
Protokoll aktiviert	Protokollierung von DTM- und Modulereignissen im Syslog Server	
RUN/STOP nur über Eingang aktiviert	Verwaltung des Run/Stop-Eingangs	M580 Hardware - Referenzhandbuch
Speicherschutz aktiviert	Speicherschutz	
Sichern eines Projekts: • Anwendung durch Anmeldung mit Benutzernamen und Passwort gesperrt • Section-Schutz aktiviert	Sicherung eines Projekts in Control Expert	
In der Steuerung sind keine Auslese-Informationen gespeichert.	In Steuerung eingebettete Daten	EcoStruxure™ Control Expert - Betriebsarten
Standardpasswörter für FTP-Dienst geändert	Firmwareschutz	
Anwendungs-Sections ohne Lese-/Schreibzugriff konfiguriert	Schutz der Sections und Unterprogramme	

Kritische Komponenten

Umgebung: Die nachstehende Tabelle enthält die kritischen Komponenten für die Umgebung:

Komponente	Beschreibung für einen ordnungsgemäßen Einsatz
Kontrolle-Steuerung des Industrieprozesses	Die Steuerung kontrolliert und steuert einen industriellen Prozess, indem sie Eingänge liest und Befehle an Aktoren sendet. Die Verfügbarkeit dieser Aktionen ist geschützt.
Datenflüsse der Engineering-Workstation	Die Datenflüsse zwischen der Steuerung und der Engineering-Workstation sind in Bezug auf Integrität, Vertraulichkeit und Authentizität geschützt.

Sicherheitsanforderungen an die für die Umgebung kritischen Komponenten:

Komponente	Verfügbarkeit	Vertraulichkeit	Integrität	Authentizität
Kontrolle-Steuerung des Industrieprozesses	X			
Datenflüsse der Engineering-Workstation		X	X	X

Steuerung: Die nachstehende Tabelle enthält die für die Steuerungen kritischen Komponenten:

Komponente	Beschreibung für einen ordnungsgemäßen Einsatz
Firmware	Die Firmware ist sowohl in Bezug auf Integrität als auch auf Authentizität geschützt.
Steuerungsspeicher	Der Speicher der Steuerung enthält die Konfiguration der Steuerung sowie ein vom Benutzer geladenes Programm. Integrität und Authentizität des Speichers sind während des Betriebs geschützt.
Ausführungsmodus	Integrität und Authentizität des Ausführungsmodus der Steuerung sind geschützt.
Benutzergeheimnisse	Alle zur Gewährleistung der Authentizität verwendeten Passwörter werden von den jeweiligen Benutzern vertraulich gehandhabt.

Sicherheitsanforderungen für die kritischen Komponenten der Steuerungen:

Komponente	Verfügbarkeit	Vertraulichkeit	Integrität	Authentizität
Firmware			X	X
Steuerungsspeicher			X	X
Ausführungsmodus			X	X
Benutzergeheimnisse		X	X	

Sicherheitsbedrohungen

Bedrohungen, die von Angreifern, die ein an das Überwachungsnetz angeschlossenes Gerät kontrollieren, in Betracht gezogen werden:

Art der Bedrohung	**Kontrolle-Steuerung des Industrieprozesses**	**Datenflüsse der technischen Workstations**	**Firmware**	**SPS-Speicher**	**Ausführungsmodus**	**Benutzergeheimnisse**
Denial of Service	Vf					
Änderung der Firmware		I, Au				
Änderung des Ausführungsmodus					Au, I	
Änderung des Speicherprogramms				I, Au		
Änderung der Datenflüsse	Vf	Au, Vt, I				Vt, I
Vf: Verfügbarkeit I: Integrität Vt: Vertraulichkeit Au: Authentizität						

Art der Bedrohung	**Beschreibung**
Denial of Service	Dem Angreifer gelingt es, einen Denial of Service in der Steuerung zu generieren, indem er eine unerwartete Aktion ausführt oder eine Schwachstelle nutzt (Senden eines fehlerhaften Requests, Verwenden einer beschädigten Konfigurationsdatei usw.). Die Denial-of-Service-Attacke wirkt sich auf die gesamte Steuerung oder einige ihrer Funktionen aus.
Änderung der Firmware	Dem Angreifer gelingt es, eine beschädigte Firmware in die Steuerung einzuschleusen und dort auszuführen. Die Code-Injection kann vorübergehend oder permanent sein und umfasst keine unerwartete oder unberechtigte Codeausführung. Ein Benutzer versucht unter Umständen, das Update auf vollkommen rechtmäßigem Weg in der Steuerung zu installieren. Daraufhin gelingt es dem Angreifer, die Version der in der Steuerung installierten Firmware zu ändern, ohne dazu berechtigt zu sein.
Änderung des Ausführungsmodus	Dem Angreifer gelingt es, den Ausführungsmodus der Steuerung zu ändern, ohne dass er dazu autorisiert ist (z. B. ein Stoppbefehl).
Änderung des Speichers	Der Angreifer ändert das Benutzerprogramm oder die Konfiguration, die im Speicher der Steuerung ausgeführt wird, vorübergehend oder permanent.
Änderung der Datenflüsse	Der Angreifer beschädigt den Datenaustausch zwischen der Steuerung und einer externen Komponente, ohne dass dies erkannt wird. Der Angreifer kann Angriffe ausführen, wie z. B. den Diebstahl von Anmeldedaten, eine Verletzung der Zugriffskontrolle oder eine Behinderung der Kontrolle/Steuerung des industriellen Prozesses.

Art der Bedrohung	Anhaltender Denial of Service	Änderung der Firmware	Änderung des Ausführungsmodus	Änderung des Speichers	Änderung der Datenflüsse
Verwaltung fehlerhafter Eingänge	X				
Speicherung von Geheimnissen				X	
Authentifizierung auf Administrationsschnittstelle					X
Richtlinien für die Zugriffskontrolle					X
Firmwaresignatur		X			
Integrität und Authentizität des Steuerungsspeichers				X	
Integrität des Steuerungsausführungsmodus			X		
Gesicherte Kommunikation					X

Art der Bedrohung	Beschreibung
Verwaltung fehlerhafter Eingänge	Die Steuerung wurde entwickelt, um fehlerhafte Eingänge, insbesondere fehlerhaften Netzwerkverkehr, ordnungsgemäß zu handhaben.
Stärke der Geheimnisse	Die Steuerung wurde entwickelt, um fehlerhafte Eingänge, insbesondere fehlerhaften Netzwerkverkehr, ordnungsgemäß zu handhaben. • PSK zur Einrichtung des IPsec-Tunnels • Anwendungspasswort zum Lesen der .STU-Datei von Control Expert und Verbinden der Datei mit der Steuerung • Andere Dienstepasswörter (wie FTP)
Authentifizierung auf Administrationsschnittstelle	Sitzungstoken sind vor Entwendung und Wiederholung geschützt. Sie besitzen nur eine kurze Lebensdauer. Identität und Berechtigungen des Benutzerkontos werden vor jeder privilegierten Aktion systematisch überprüft. In jeder Konfiguration wird ein Anwendungspasswort festgelegt, um jede Änderung der Steuerung durch einen nicht authentischen Benutzer zu verhindern.
Richtlinien für die Zugriffskontrolle	Die Richtlinien für die Zugriffskontrolle tragen dazu bei, die Authentizität von privilegierten Vorgängen zu kontrollieren, d. h. von Vorgängen, die identifizierte kritische Komponenten ändern können. Die Zugriffskontrollliste (ACL: Access Control List) ist in jeder Konfiguration aktiviert, und nur identifizierte IP-Adressen können eine Verbindung zur Steuerung herstellen.
Firmwaresignatur	Bei jeder Firmwareaktualisierung werden Integrität und Authentizität der neuen Firmware vor der Durchführung der Aktualisierung überprüft.

Art der Bedrohung	Beschreibung
Integrität und Authentizität des Steuerungsspeichers	Die Speicherschutzfunktion wird in jeder Konfiguration aktiviert. Dadurch lassen sich Änderungen am laufenden Programm ohne Einwirkung auf spezifische Ein- oder Ausgänge verhindern. Wenn kein Ein-/Ausgangsmodul installiert ist, ist die Programmierschnittstelle blockiert. Die Steuerung gewährleistet die Integrität und Authentizität des Benutzerprogramms, sodass autorisierte Benutzer Änderungen am Programm vornehmen können. Der Speicherschutz sorgt darüber hinaus für den Schutz der Konfiguration, wozu verschiedene Sicherheitsparameter beitragen: • Richtlinien für die Zugriffskontrolle • RUN/STOP nur über Eingang aktiviert • Speicherschutz aktiviert • Aktivierte/Deaktivierte Dienste (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP) • IPsec-Parameter • Syslog-Parameter
Integrität des Steuerungsausführungsmodus	Die Steuerung stellt sicher, dass der Ausführungsmodus von autorisierten und authentifizierten Benutzern geändert werden kann. Die Funktion „RUN/STOP nur über Eingang“ ist aktiviert, um eine Änderung des RUN/STOP-Status über die Ethernet-Schnittstelle zu verhindern.
Verschlüsselte Kommunikation	Die Steuerung unterstützt eine verschlüsselte Kommunikation, die in Bezug auf Integrität, Vertraulichkeit und Authentizität (IPsec, verschlüsselt mit ESP) geschützt ist. Das FTP-Protokoll ist deaktiviert, und IPsec gewährleistet eine sichere Modbus-Kommunikation über die Module BMENOC0301 and BMENOC0311.

Einrichtung des Cybersicherheit-Audits (Ereignisprotokollierung)

Die Ereignisprotokollierung und die Protokollierungsanalyse sind von entscheidender Bedeutung. Die Analyse durchsucht Benutzeraktionen nach Wartung und ungewöhnlichen Ereignissen, die auf einen möglichen Angriff hinweisen.

Das gesamte System benötigt ein zuverlässiges Protokollierungssystem, das in allen Geräten vorhanden ist. Die Ereignisse im Zusammenhang mit Cybersicherheit werden lokal protokolliert und über das Syslog-Protokoll an einen Remote-Server gesendet.

In der Systemarchitektur betrifft die Ereignisprotokollierung zwei Parteien:

- Einen Protokollserver, der alle Cybersicherheit-bezogenen Systemereignisse über das Syslog-Protokoll empfängt.
- Protokollclients (Ethernet-Verbindungspunkte, an denen Cybersicherheit-Ereignisse überwacht werden: Gerät, Control Expert).

Beschreibung des Ereignisprotokollierungsdienstes

Jeder Protokollclient hat die folgenden Aufgaben:

- Erfassen von Ereignissen und Hinzufügen eines Zeitstempels.

  Eine einzige NTP-Referenz muss im System konfiguriert werden, um die Cybersicherheit-Ereignisse mit einem Zeitstempel zu versehen.

- Senden der erfassten Ereignisse an den Ereignisprotokollserver.

  Die Ereignisse werden zwischen Client und Server mithilfe des Syslog-Protokolls (RFC 5424-Spezifikation) übermittelt.

  Die Syslog-Nachrichten entsprechen dem in der RFC 5424-Spezifikation beschriebenen Format.

  Der Syslog-Austausch erfolgt über das TCP-Protokoll.

  Auf den Geräten gehen Ereignisse im Fall eines vorübergehenden Netzwerkausfalls nicht verloren. Bei einem Geräte-Reset gehen Ereignisse verloren (außer Modicon M580-Steuerungsfirmware ≥ 4.0).

Facility-Werte (Ursprung) für Ereignistypen

Facility-Werte für Syslog-Nachrichten nach der RFC 5424-Spezifikation, die Ereignistypen zugeordnet sind:

Facility-Wert	Beschreibung
0	Kernel-Nachrichten
1	Nachrichten auf Benutzerebene
2	Mailsystem
3	System-Daemons
4	Sicherheits-/Autorisierungsnachrichten
5	Intern von Syslog erstellte Nachrichten
6	Linienschreiber-Subsystem
7	Netzwerk-News-Subsysteme
8	UUCP-Subsystem
9	Uhr-Daemon
10	Sicherheits-/Autorisierungsnachrichten
11	FTP-Daemon
12	NTP-Subsystem

Facility-Wert	Beschreibung
13	Protokoll-Audit
14	Protokoll-Alarm
15	Uhr-Daemon
16 bis 23	Lokale Verwendung 0 bis 7

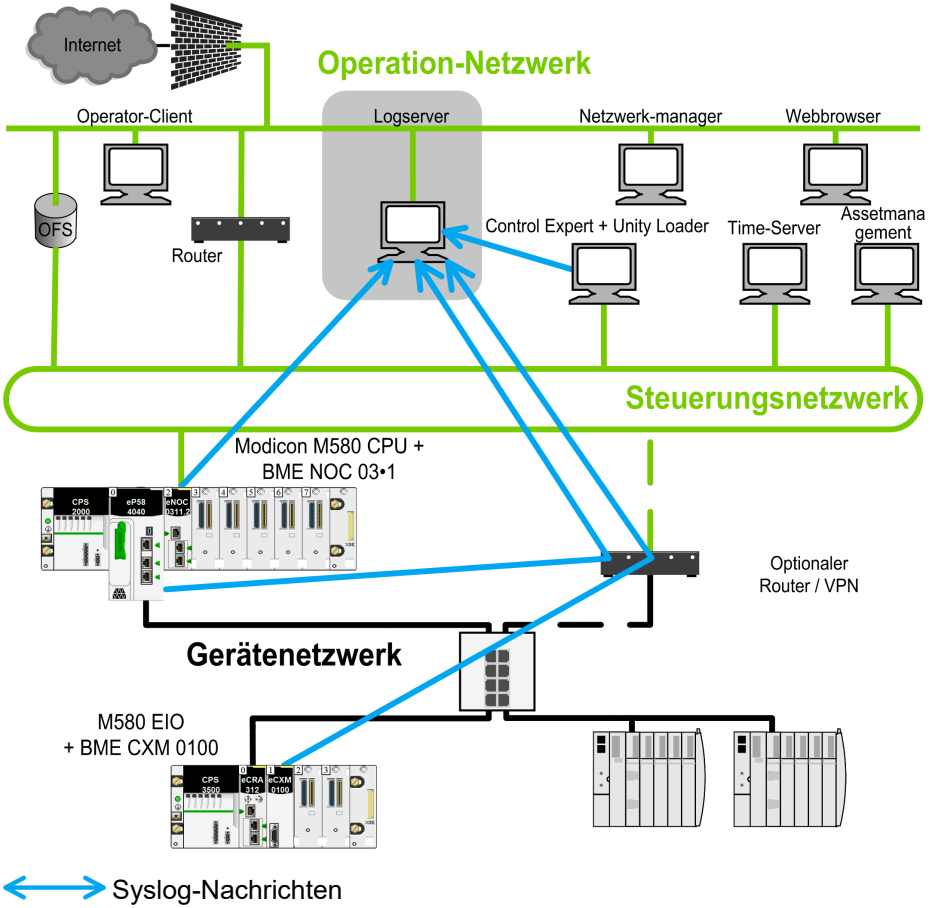
Severity-Werte (Schweregrad) für Ereignistypen

Severity-Werte für Syslog-Nachrichten nach der RFC 5424-Spezifikation, die Ereignistypen zugeordnet sind:

Severity-Wert	Schlüsselwort	Beschreibung
0	Emergency	System ist nicht verwendbar.
1	Alert	Maßnahmen müssen sofort ergriffen werden.
2	Critical	Kritische Zustände.
3	Error	Fehlerzustände.
4	Warning	Hinweise auf spezifische Zustände.
5	Notice	Normaler aber signifikanter Zustand.
6	Informational	Informelle Nachrichten.
7	Debug	Nachrichten auf Debug-Ebene.

Architekturbeispiel

Die folgende Abbildung zeigt die Position eines Protokollservers in einer Systemarchitektur:



Struktur der protokollierten Ereignisnachrichten für Modicon M580-Steuerungen (ab Firmwareversion 4.10) und BMENOR2200H (ab Firmwareversion 3.01)

Felder	Beschreibung
PRI	Informationen zu Ursprung (Facility) und Schweregrad (Severity): „FACILITY“ = 10 für Cybersicherheit-Ereignisse.
VERSION	Version der Syslog-Protokollspezifikation (Version = 1 für RFC 5424).
TIMESTAMP	Das Zeitstempelformat wird ausgegeben von RFC 3339, der das folgende Internet-Datums- und Uhrzeitformat nach ISO8601 empfiehlt: YYY-MM-DD**T**hh:mm:ss.nnn**Z** **HINWEIS: -**, **T**, **:**, **.** und **Z** sind Pflichtzeichen und Teil des Zeitstempelfelds. **T** und **Z** müssen in Großbuchstaben geschrieben werden. **Z** gibt an, dass die Zeit UTC ist. Beschreibung des Inhalts des Zeitfelds: • YYY: Jahr • MM: Monat • DD: Tag • hh: Stunde • mm: Minute • ss: Sekunde • nnn: Bruchteil einer Sekunde in Millisekunden (0, wenn nicht verfügbar)
HOSTNAME	Identifiziert den Computer, der die Syslog-Nachricht ursprünglich gesendet hat: Vollqualifizierter Domänenname (FQDN) oder statische IP-Quelladresse, wenn FQDN nicht unterstützt wird. Quelle @IP-Adresse = @IP-Adresse A ODER @IP-Adresse B im Fall einer HSBY-Steuerung
APP-NAME	Identifiziert die Anwendung, die die Syslog-Nachricht initiiert hat. Enthält Informationen zur Identifikation der Einheit, die die Nachricht gesendet hat (z. B. Teil der Handelsreferenz).
PROCID	Prozess- oder Protokollname, von dem die Nachricht stammt (z. B. Modbus, HTTPS, LocalHMI).
MSGID	Kennung für den Typ des Ereignisses (zum Beispiel CONNECTION_FAILURE_AND_ BLOCK).
Ereignisinformationen	<ac:Structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="30296255-e8b7-4cf1-982e-2c45b17b1f06"><ac:plain-text-body><![CDATA[**[authn@3833]**, **[authz@3833]**, **[config@3833]**, **[cred@3833], [backup@3833], [plc@3833] [system@3833]** Siehe die Beschreibung von STRUCTURED-DATA unten.
MSG	Nachricht mit dem ereignisspezifischen Ergebnis (siehe Beschreibung der Ereignisprotokollnachrichten für Control Expert, Seite 63).

- **STRUCTURED-DATA** - Beschreibung: Obligatorische Ereignisinformationen.
  - **[meta]**: Obligatorische strukturierte Daten, um Metadaten zur Nachricht bereitzustellen. Mit folgenden Parametern:
    - **sequenceId**: Ereigniskennung (Überlauf auf 1, wenn der Höchstwert 2147483647 erreicht ist).
    - **sysUpTime**: Dieser Wert sollte berücksichtigt werden, wenn die Komponente nicht in der Lage ist, die Systemzeit zu erhalten (Ganzzahl, die die Zeit in 1/100 Sekunden seit der letzten Neuinitialisierung des Systems enthält).

- **STRUCTURED-DATA** - Beschreibung: Ereignisinformationen in Abhängigkeit von der Ereigniskategorie.
  - **[authn@3833]**: Strukturierte Daten, die für Authentifizierungsereignisse verwendet werden. Mit folgenden Parametern:
    - **itf**: Die Schnittstelle, mit der der Benutzer verbunden ist, entweder ein Netzwerk-Port oder eine lokale Schnittstelle (HMI, USB usw.).
    - **peer**: Die FQDN- oder IP-Adresse der Komponente, mit der der Benutzer verbunden ist, sowie deren Port (ipAddress:port), optional bei lokaler Schnittstelle.
    - **user**: Der Benutzername (Komponente oder Person), optional bei unbekanntem Benutzernamen.
  - **[authz@3833]**: Strukturierte Daten, die für Autorisierungsereignisse verwendet werden. Mit folgenden Parametern:
    - **user**: Der Benutzername (Komponente oder Person)-
    - **object**: Der Objektzugriff durch den Benutzer, Objekt ist produktabhängig.
    - **action**: Die für das Objekt ausgeführte Aktion: Erstellen, Lesen, Aktualisieren, Löschen (CRUD: Create, Read, Update, Delete).
  - **[config@3833]**: Strukturierte Daten, die für Konfigurationsereignisse verwendet werden. Mit folgenden Parametern:
    - **object**: Der Name des zu konfigurierenden Sicherheitsobjekts (Firmware, RBAC, Sicherheitsrichtlinie, Geräteeinstellung, Vertrauensanker, produktabhängige Objekte).
    - **value**: Optionale Version oder Wert des neuen Objekts.
  - **[cred@3833]**: Strukturierte Daten, die für Ereignisse in Verbindung mit der Anmeldedatenverwaltung verwendet werden. Mit folgenden Parametern:
    - **name**: Der gemeinsame Name des Zertifikats oder der Benutzername für die Anmeldung.
  - **[system@3833]**: Strukturierte Daten für Systemereignisse. Mit folgenden Parametern:
    - **object**: Der Name des Systemobjekts, das sich ändert (Steuerung, Modul, Drehschalter, SD-Karte, produktabhängiges Objekt).
  - **[backup@3833]**: Strukturierte Daten, die für die Sicherung verwendet werden. Mit folgenden Parametern:
    - **object**: Der Teil der Komponente, der gesichert/wiederhergestellt wurde, Objekt ist produktabhängig.
  - Strukturierte Daten können auch von jeder Anwendung für bestimmte Ereignisse definiert werden.

Struktur der protokollierten Ereignisnachrichten für Modicon M580-Steuerungen (Firmware vor Version 4.10), BMENUA0100 (Firmwareversionen 1.10 und 2.0) und BMENOR2200H (Firmware vor Version 3.01)

Syslog-Nachrichtenstruktur für Modicon M580-Steuerungsfirmware und BMENUA0100:

Feld	Beschreibung
PRI	Informationen zu Ursprung (Facility) und Schweregrad (Severity) (eine Beschreibung finden Sie in den folgenden Tabellen).
VERSION	Version der Syslog-Protokollspezifikation (Version = 1 für RFC 5424).
TIMESTAMP	Das Zeitstempelformat wird ausgegeben von RFC 3339, der das folgende Internet-Datums- und Uhrzeitformat nach ISO8601 empfiehlt: YYY**-**MM**-**DD**T**hh**:**mm**:**ss**.**nnn**Z** **HINWEIS: -**, **T**, **:**, **.** und **Z** sind Pflichtzeichen und Teil des Zeitstempelfelds. **T** und **Z** müssen in Großbuchstaben geschrieben werden. **Z** gibt an, dass die Zeit UTC ist. Beschreibung des Inhalts des Zeitfelds: • YYY: Jahr • MM: Monat • DD: Tag • hh: Stunde • mm: Minute • ss: Sekunde • nnn: Bruchteil einer Sekunde in Millisekunden (0, wenn nicht verfügbar)
HOSTNAME	Identifiziert den Computer, der die Syslog-Nachricht ursprünglich gesendet hat. Vollständig qualifizierter Domänenname (FQDN) oder statische IP-Quelladresse, wenn FQDN nicht unterstützt wird.
APP-NAME	Identifiziert die Anwendung, die die Syslog-Nachricht initiiert hat. Enthält Informationen zur Identifikation der Einheit, die die Nachricht gesendet hat (z. B. Teil der Handelsreferenz).
PROCID	Prozess- oder Protokollname, von dem die Nachricht stammt (z. B. Modbus, HTTPS, LocalHMI usw.) Erhält NILVALUE, wenn nicht verwendet.

Feld	Beschreibung
MSGID	Identifiziert den Nachrichtentyp, auf den sich das Ereignis bezieht. Beispiel: HTTP, FTP, Modbus. Erhält NILVALUE, wenn nicht verwendet.
MESSAGE TEXT	Dieses Feld enthält: • Issuer address: IP-Adresse der Einheit, die das Protokoll generiert hat. • Peer ID: Peer-ID, wenn ein Peer am Vorgang beteiligt ist (z. B. Benutzername für eine Protokollierung). Erhält Null, wenn nicht verwendet. • Peer address: Peer-IP-Adresse, wenn ein Peer am Vorgang beteiligt ist. Nicht verwendet (Null). • Type: Eindeutige Nummer zur Identifizierung einer Nachricht (siehe Beschreibung der Ereignisprotokollnachrichten für Control Expert, Seite 63). • Comment: Zeichenfolge, die die Nachricht beschreibt (siehe Beschreibung der Ereignisprotokollnachrichten für M580-Steuerungen (ab Firmwareversion V4.10) und BMENOR2200H (ab Firmwareversion 3.01), Seite 69).

Einrichten eines Syslog-Servers in der Systemarchitektur

Mehrere Syslog-Server sind für verschiedene Betriebssysteme verfügbar.

HINWEIS: Syslog-Server müssen mit RFC 5424 kompatibel sein.

Beispiele für Anbieter von Syslog-Servern:

- WinSyslog: Für das Windows-Betriebssystem.
  Link: www.winsyslog.com/en/.
- Kiwi Syslog: Für das Windows-Betriebssystem.
  Link: www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx.
- Splunk: Für das Windows- und Unix-Betriebssystem.
  Link: www.splunk.com/.
- Rsyslog: Für das Unix-Betriebssystem.
  Link: www.rsyslog.com/.
- Syslog-ng: Open Source für das Unix-Betriebssystem.
  Link: www.balabit.com/network-security/syslog-ng/opensource-logging-system.
- Syslog Server: Open Source für das Windows-Betriebssystem.
  Link: sourceforge.net/projects/syslog-server/.

Einrichten eines Syslog-Clients in der Systemarchitektur

Die Ereignisprotokollierung wird für alle Geräte und Device Type Manager (DTMs) in Control Expert verwaltet.

Die Ereignisprotokollierungsfunktion, die Serveradresse und die Portnummer werden wie folgt in Control Expert konfiguriert. Diese Parameter werden nach der Aktion **Generieren** an jeden Client im System gesendet:

Schritt	Aktion
1	Klicken Sie auf **Extras > Projekteinstellungen**.
2	Klicken Sie **Projekteinstellungen > Allgemein > SPS-Diagnose**.
3	Aktivieren Sie das Kontrollkästchen **Ereignisprotokollierung** (standardmäßig deaktiviert). **HINWEIS:** Ein Projekt mit dieser Einstellung kann nur ab Unity Pro 10.0 geöffnet werden. Unity Pro ist die vorherige Bezeichnung von Control Expert bis Version 13.1.
4	Geben Sie einen gültigen Wert für **SYSLOG-Serveradresse** und **Nummer des SYSLOG-Serverports** ein.
5	Führen Sie eine Aktioni **Generieren** nach der Konfiguration dieser Einstellung durch (Sie brauchen nicht die Aktion **Projekt analysieren** auszuwählen).

Diagnose der Ereignisprotokollierung

Die folgende Tabelle zeigt die für verschiedene Geräte verfügbaren Diagnosetypen für die Ereignisprotokollierung:

Geräte	Diagnoseinformationen
Control Expert	Wenn ein Kommunikationsfehler mit einem Syslog-Server auftritt, wird der erkannte Fehler in der Ereignisanzeige aufgezeichnet. Um die Ereignisanzeige in Control Expert zu aktivieren, aktivieren Sie das Kontrollkästchen **Prüfung** auf der Registerkarte **Richtlinien** im Sicherheitseditor (siehe EcoStruxure™ Control Expert, Sicherheitseditor, Betriebshandbuch.
Geräte-DDT von BMENOC0301 and BMENOC0311 (Parameter *SERVICE_STATUS2*)	Zwei Diagnoseinformationen sind verfügbar: • EVENT_LOG_STATUS: Wert = 1, wenn der Ereignisprotokolldienst betriebsbereit ist. Wert = 0, wenn der Protokollierdienst nicht betriebsbereit ist. • LOG_SERVER_NOT_REACHABLE: Wert = 1, wenn der Syslog-Client keine Quittierung der TCP-Nachrichten vom Syslog-Server empfängt. Wert = 0, wenn die Quittierung empfangen wird.
Geräte-DDT der Modicon M580-Steuerung	
Geräte-DDT von BMECXM	

Beschreibung der Ereignisprotokollnachrichten für Control Expert

Protokolliertes Ereignis: Anwendungsaktion

Die folgende Tabelle enthält eine Beschreibung der Nachrichten, wenn es sich bei dem protokollierten Ereignis um Folgendes handelt: Aktion der Anwendung.

MSG(1)	Facility	Severity	Beschreibung
Neues Projekt erstellen	10	6	Neue Control Expert-Anwendung erstellen
Vorhandenes Projekt öffnen	10	6	Bestehende Control Expert-Anwendung öffnen
Projekt speichern	10	6	Aktuell geöffnete Anwendung speichern
Als Projekt speichern	10	6	Aktuell geöffnete Anwendung in einer anderen Datei speichern
Projekt importieren	10	6	Eine Anwendung importieren
Offline generieren	10	6	Anwendung im Offline-Modus generieren
Online generieren in Stop	10	6	Anwendung im Online-Modus und mit der Steuerung im STOP-Modus generieren
Online generieren in Run	10	6	Anwendung im Online-Modus und mit der Steuerung im RUN-Modus generieren
PAC starten, stoppen oder initialisieren	10	6	Die Steuerung starten/stoppen/ initialiseiren
Initialwerte mit aktuellen Werten aktualisieren	10	6	Initialwerte mit den aktuellen Werten aktualisieren
Projekt vom PAC übertragen	10	6	Die Anwendung aus der Steuerung hochladen
Projekt an PAC übertragen	10	6	Die Anwendung in die Steuerung herunterladen
Datenwerte von Datei in PAC übertragen	10	6	Datenwerte aus einer Datei in die Steuerung übertragen
Projektsicherung in PAC wiederherstellen	10	6	Projektsicherung in der Steuerung wiederherstellen
In Projektsicherung in PAC speichern	10	6	Projektsicherung in der Steuerung speichern
Adresse festlegen	10	6	Steuerungsadresse für die Verbindung ändern
Optionen ändern	10	6	Änderung von Control Expert-Optionen

MSG[1]	Facility	Severity	Beschreibung
Variablenwerte ändern	10	6	Änderung von Variablenwerten in der Steuerung
Interne Bits forcieren	10	6	Änderung der Forcierungswerte von Variablen in der Steuerung: Interne Bits
Ausgänge forcieren	10	6	Änderung der Forcierungswerte von Variablen in der Steuerung: Ausgänge
Eingänge forcieren	10	6	Änderung der Forcierungswerte von Variablen in der Steuerung: Eingänge
Taskverwaltung	10	6	Taskverwaltung
Änderung der Task-Zykluszeit	10	6	Änderung der Task-Zykluszeit
Meldung in Diagnoseanzeige unterdrücken	10	6	Meldung in Diagnoseanzeige unterdrücken
Debugging ausführbar	10	6	Debugging ausführbar
Projektvariable ersetzen	10	6	Projektvariable ersetzen
Bibliotheken oder Familien erstellen	10	6	Bibliotheken oder Familien innerhalb der Bibliothek erstellen
Bibliotheken oder Familien löschen	10	6	Bibliotheken oder Familien innerhalb der Bibliothek löschen
Objekt in Bibliothek setzen	10	6	Element (DFB/DDT) aus der Anwendung in die Bibliothek kopieren
Objekt aus Bibliothek löschen	10	6	Element (DFB/DDT) in der Bibliothek löschen
Objekt aus Bibliothek abrufen	10	6	Element (DFB/DDT/EF/EFB) aus der Bibliothek in die Anwendung kopieren
Dokumentation ändern	10	6	Dokumentation ändern (aus Anwendung drucken)
Funktionsansicht ändern	10	6	Funktionsansicht ändern
Animationstabellen ändern	10	6	Animationstabellen ändern
Konstantenwerte ändern	10	6	Konstantenwerte ändern
Programmstruktur ändern	10	6	Programmstruktur ändern
Programm-Sections ändern	10	6	Programm-Sections ändern
Projekteinstellungen ändern	10	6	Projekteinstellungen ändern
Variable hinzufügen/entfernen	10	6	Variable erstellt/entfernt im Dateneditor
Änderung der Hauptattribute von Variablen	10	6	Variablenattribut geändert
Änderung der Nebenattribute von Variablen	10	6	Variablenattribut geändert

MSG[1]	Facility	Severity	Beschreibung
DDT hinzufügen/entfernen	10	6	DDT erstellt/entfernt im Dateneditor
DDT-Änderung	10	6	DDT geändert im Dateneditor
DFB-Typ hinzufügen/entfernen	10	6	DFB erstellt/entfernt im Dateneditor
Änderung der Struktur eines DFB-Typs	10	6	DFB-Struktur geändert im Dateneditor
Änderung der Sections eines DFB-Typs	10	6	DFB-Sections geändert
Änderung der DFB-Instanz	10	6	Änderung der DFB-Instanz im Dateneditor
Änderung der Nebenattribute einer DFB-Instanz	10	6	Änderung der Nebenattribute einer DFB-Instanz im Dateneditor
Konfiguration ändern	10	6	Änderung der Steuerungskonfiguration
E/A-Sniffing	10	6	SPS-E/A-Sniffing
E/A-Konfiguration ändern	10	6	Änderung der E/A-Konfiguration der Steuerung
E/A anpassen	10	6	E/A-Konfiguration der Steuerung anpassen
Parameter speichern	10	6	Parameter der E/A-Konfiguration der Steuerung im E/A-Fenster speichern
Parameter wiederherstellen	10	6	Parameter der E/A-Konfiguration der Steuerung im E/A-Fenster wiederherstellen
Fenster ändern	10	6	Änderung der Bedienerfenster
Meldungen ändern	10	6	Meldungen ändern
Fenster oder Familien hinzufügen/entfernen	10	6	Bedienerfenster: Familie/Fenster hinzugefügt/entfernt
Komponente verschieben	13	6	FFB-Baustein verschieben
Komponente verschieben	13	6	Kontakt/Spule verschieben
Komponente einfügen	13	6	FFB-Baustein einfügen
Komponente einfügen	13	6	Kontakt/Spule einfügen
Komponente löschen	13	6	FFB-Baustein löschen
Komponente löschen	13	6	Kontakt/Spule löschen
Variable hinzufügen	13	6	Effektivparameter für FFB-Baustein festlegen
Variable hinzufügen	13	6	Effektivparameter für Kontakt/Spule festlegen

MSG[1]	Facility	Severity	Beschreibung
Variable löschen	13	6	Effektivparameter für FFB-Baustein entfernen
Variable löschen	13	6	Effektivparameter für Kontakt/Spule entfernen
Variable ändern	13	6	Effektivparameter für FFB-Baustein ändern
Variable ändern	13	6	Effektivparameter für Kontakt/Spule ändern
Verbindungs-Pin	13	6	Verbindung zwischen zwei Pins herstellen
Komponente skalieren	13	6	Größe eines erweiterbaren FFB-Bausteins ändern
Komponente skalieren	13	6	Größe einer vertikalen/horizontalen Verbindung ändern
Variable umbenennen	13	6	Effektivparameter umbenennen
Zeile löschen	13	6	Eine einzelne Zeile löschen
Zeilen löschen aus	13	6	Mehrere Zeilen löschen
Spalte löschen	13	6	Eine einzelne Spalte löschen
Spalten löschen aus	13	6	Mehrere Spalten löschen
Zeile einfügen	13	6	Eine einzelne Zeile einfügen
Zeilen einfügen aus	13	6	Mehrere Zeilen einfügen
Spalte einfügen	13	6	Eine einzelne Spalte einfügen
Spalten einfügen aus	13	6	Mehrere Spalten einfügen
[1] MSG-Inhalt umfasst die Verkettung des Benutzernamens, der PID von Control Expert sowie der Nachricht.			

HINWEIS: Die Felder HOSTNAME, APP-NAME, PROCID, MSGID und STRUCTURED-DATA gelten nicht für Control Expert-Nachrichten.

Protokolliertes Ereignis: DTM-Aktion

Die folgende Tabelle enthält eine Beschreibung der Nachrichten, wenn es sich bei dem protokollierten Ereignis um Folgendes handelt: DTM-Aktion.

MSG[1]	Facility	Severity	Beschreibung
Dienst für Parameter-Download in Gerät fehlerhaft beendet	9	6	DTM Parameter-Download fehlerhaft beendet
Dienst für Parameter-Download in Gerät fehlerfrei beendet	9	6	DTM Parameter-Download fehlerfrei beendet
Dienst für Parameter-Upload aus Gerät fehlerhaft beendet	9	6	DTM Parameter-Upload fehlerhaft beendet
Dienst für Parameter-Upload aus Gerät fehlerfrei beendet	9	6	DTM Parameter-Upload fehlerfrei beendet
„Go online“-Dienst fehlgeschlagen	9	6	Verbindung zum DTM nicht hergestellt
„Go online“-Dienst erfolgreich	9	6	Verbindung zum DTM erfolgreich
„Go offline“-Dienst fehlgeschlagen	9	6	Verbindung zum DTM nicht getrennt
„Go offline“-Dienst erfolgreich	9	6	Verbindung zum DTM erfolgreich getrennt
FDR-Dienst für Parameter-Download fehlgeschlagen	9	6	DTM FDR-Dienst für Parameter-Download wird nicht ausgeführt
FDR-Dienst für Parameter-Download erfolgreich	9	6	DTM FDR-Dienst für Parameter-Download erfolgreich
FDR-Dienst für Parameter-Upload fehlgeschlagen	9	6	DTM FDR-Dienst für Parameter-Upload wird nicht ausgeführt
FDR-Dienst für Parameter-Upload erfolgreich	9	6	DTM FDR-Dienst für Parameter-Upload erfolgreich
Dienst für Parameter-Download in Gerät fehlgeschlagen	9	6	Dienst für Parameter-Download in Gerät wird nicht ausgeführt
Dienst für Parameter-Download in Gerät erfolgreich	9	6	Dienst für Parameter-Download in Gerät erfolgreich
Dienst für Parameter-Upload aus Gerät fehlgeschlagen	9	6	Dienst für Parameter-Upload aus Gerät wird nicht ausgeführt
Dienst für Parameter-Upload aus Gerät erfolgreich	9	6	Dienst für Parameter-Upload aus Gerät erfolgreich
Funktionsereignis Audit-Trail	9	6	Funktionsereignis Audit-Trail
Gerätestatusereignis Audit-Trail	9	6	Gerätestatusereignis Audit-Trail
Keine Gerätestatusmeldung	9	6	Keine Gerätestatusmeldung
Statusinformationen	9	6	Statusinformationen
Zugriffsrecht: Lesen / Schreiben	9	6	Zugriffsrecht: Lesen / Schreiben
Enumeratoreintrag	9	6	Enumeratoreintrag
[1] MSG-Inhalt umfasst die Verkettung des Benutzernamens, der PID von Control Expert sowie der Nachricht.			

Protokolliertes Ereignis: Passwortaktion

Die folgende Tabelle enthält eine Beschreibung der Nachrichten, wenn es sich bei dem protokollierten Ereignis um Folgendes handelt: Passwortaktion.

MSG(1)	Facility	Severity	Beschreibung
Cybersicherheit - Änderung des Passworts > Falsches Passwort	2	6	Problem bei Änderung des Anwendungspassworts
Cybersicherheit - Verifizierung des Passworts > Falsches Passwort	2	6	Problem bei der Überprüfung des Anwendungspassworts
Cybersicherheit - Verifizierung des Section-Passworts > Falsches Passwort	2	6	Problem bei der Überprüfung des Section-Passworts
Cybersicherheit - Passwort für die Datenspeicherung geändert	2	6	Passwort für die Datenspeicherung („DataStorage“) geändert
Cybersicherheit - Firmware-Passwort geändert	2	6	Passwort für den Firmware-Download („FW Download“) geändert
Cybersicherheit - Verifizierung des Passworts > Falsches Passwort	2	6	Problem bei der Überprüfung des Anwendungspassworts
(1) MSG-Inhalt umfasst die Verkettung des Benutzernamens, der PID von Control Expert sowie der Nachricht.			

Protokolliertes Ereignis: Änderung der SYSLOG-Konfiguration

Die folgende Tabelle enthält eine Beschreibung der Nachrichten, wenn es sich bei dem protokollierten Ereignis um Folgendes handelt: Änderung der SYSLOG-Konfiguration.

MSG(1)	Facility	Severity	Beschreibung
SYSLOG-Adresse geändert	-	-	Cybersicherheit - Projekteinstellung für die Ereignisprotokollierung geändert - Ereignisprotokollierung, SYSLOG-Serveradresse, Port oder Protokoll
(1) MSG-Inhalt umfasst die Verkettung des Benutzernamens, der PID von Control Expert sowie der Nachricht.			

Protokolliertes Ereignis: Dateiaktion

Die folgende Tabelle enthält eine Beschreibung der Nachrichten, wenn es sich bei dem protokollierten Ereignis um Folgendes handelt: Dateiaktion.

MSG(1)	Facility	Severity	Beschreibung
Datei XXXXX wurde geöffnet	0	6	Datei XXXXX geöffnet
Trennung von PAC @=XXXXXX Treiber = YYYYY	0	6	Steuerung getrennt = @XXXXXX = YYYYY
Anwendung XXXXXX schließen	0	6	Anwendung XXXXXX schließen
Projekt wurde von PAC in PC übertragen	0	6	Übertragung von Steuerung in PC
(1) MSG-Inhalt umfasst die Verkettung des Benutzernamens, der PID von Control Expert sowie der Nachricht.			

Beschreibung der Ereignisprotokollnachrichten für M580-Steuerungen (ab Firmwareversion V4.10) und BMENOR2200H (ab Firmwareversion 3.01)

Dieser Abschnitt enthält eine Beschreibung der Ereignisprotokollnachrichten für:

- M580-Steuerungen ab Firmwareversion 4.10 (kurz **CPU** in der Spalte **Geräte**)
- RTU-Module BMENOR2200H ab Firmwareversion 3.01 (kurz „eNOR“ in der Spalte **Geräte**)

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
Erfolgreiche Verbindung	Erfolgreiche Verbindung von einem Benutzer (Person oder Komponente) zu einer Komponente, entweder über ein verschlüsseltes oder ein unverschlüsseltes Protokoll, sofern dies gemäß der Sicherheitsrichtlinien des Kunden zulässig ist.	Erfolgreiche Anmeldung (Webserver über HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Anmelden	CPU eNOR
		Erfolgreiche Anmeldung (Firmwareaktualisierung über HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Anmelden	CPU eNOR
		Erfolgreiche Anmeldung (OPC-UA)	6	OPC-UA	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Socket-Verbindung	CPU
		Erfolgreiche Anmeldung (Unity-	6	MODBUS-UMAS	CONNECTION_	[meta sequenceId=*Zahl*]	Anmelden	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
		Anwendungspasswort über Modbus-Umas)**Nur Standardmodus**			SUCCESS	[authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]		
		Erfolgreiche Modbus TCP-Verbindung (kein Benutzer)	6	MODBUS	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Socket-Verbindung	CPU eNOR
		Erfolgreiche HTTP/ DPWS-Verbindung	6	HTTP	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Socket-Verbindung	CPU
		Erfolgreiche explizite EIP-TCP-Verbindung (kein Benutzer)	6	EIP	CONNECTION_SUCCESS	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort*	Socket-Verbindung	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						| *LokaleSchnittstelle*Peer= *PeerFQDN:PeerPort* user= *Benutzername*]		
		Erfolgreiche DNP3-Verbindung (kein Benutzer)	6	DNP3	CONNECTION_SUCCESS	[meta sequenceId=Zahl] [authn@3833 itf= LokalerPort | LokaleSchnittstelle peer= PeerFQDN:PeerPort user= Benutzername]	Socket-Verbindung	eNOR
		Erfolgreiche IEC 60870-Verbindung (kein Benutzer)	6	IEC60870	CONNECTION_SUCCESS	[meta sequenceId=Zahl] [authn@3833 itf= LokalerPort | LokaleSchnittstelle peer= PeerFQDN:PeerPort user= Benutzername]	Socket-Verbindung	eNOR
Verbindungsproblem	Alle nicht erfolgreichen Verbindungen von einem Benutzer (Person oder Komponente) zu	Anmeldeproblem (Unity-Anwendungspasswort über Modbus-Umas)	5	MODBUSUMAS	CONNECTION_FAILURE	[meta sequenceId=*Zahl*] [authn@3833 itf= *LokalerPort* | *LokaleSchnittstelle*Peer=	Ungültiges Passwort	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
	einer Komponente, entweder über ein verschlüsseltes oder ein unverschlüsseltes Protokoll, sofern dies gemäß der Sicherheitsrichtlinien des Kunden zulässig ist.					*PeerFQDN: PeerPort* user= *Benutzername*]		
		Modbus TCP-Verbindungsproblem (kein Benutzer)	5	MODBUS	CONNECTION_FAILURE	[meta sequenceId=*Zahl*] [authn@3833 itf= *LokalerPort* | *LokaleSchnittstelle*Peer= *PeerFQDN: PeerPort* user= *Benutzername*]	Max. Anzahl Verbindungen erreicht - Gefilterter Datenfluss	CPU eNOR
		Explizites EIP-TCP-Verbindungsproblem (kein Benutzer)	5	EIP	CONNECTION_FAILURE	[meta sequenceId=*Zahl*] [authn@3833 itf= *LokalerPort* | *LokaleSchnittstelle*Peer= *PeerFQDN: PeerPort* user= *Benutzername*]	Max. Anzahl Verbindungen erreicht - Gefilterter Datenfluss	CPU
		DNP3-Verbindungsproblem (kein Benutzer)	5	DNP3	CONNECTION_FAILURE	[meta sequenceId=Zahl] [authn@3833 itf= LokalerPort | LokaleSchnittstelle peer= PeerFQDN: PeerPort user=	Max. Anzahl Verbindungen erreicht	eNOR

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						Benutzername]		
		IEC60870-Verbindungsproblem (kein Benutzer)	5	IEC60870	CONNECTION_FAILURE	[meta sequenceId=Zahl] [authn@3833 itf=LokalerPort | LokaleSchnittstelle peer=PeerFQDN:PeerPort user=Benutzername]	Max. Anzahl Verbindungen erreicht	eNOR
Benutzerkonto-Sperre einer Person aufgrund zu vieler Probleme bei den Authentifizierungsversuchen	Die Sicherheitsrichtlinien können vorgeben, dass das Benutzerkonto einer Person nach einer konfigurierbaren Anzahl von Versuchen gesperrt wird. Dieses Ereignis informiert den Administrator über einen potenziellen Angriff und darüber, dass das Benutzerkonto der Person gesperrt	Anmeldeproblem (Webserver über HTTPS). Benutzerkonto-Sperre einer Person aufgrund zu vieler Probleme bei den Authentifizierungsversuchen	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Ungültiges Zertifikat, ungültiges Passwort	CPU eNOR
		Anmeldeproblem (Firmwareaktualisierung über HTTPS). Benutzerkonto-Sperre einer Person aufgrund zu vieler fehlgeschlagener	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Ungültiges Zertifikat, Ungültiges Passwort	CPU eNOR

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
	werden muss.	Authentifizierungsversuche						
		Anmeldeproblem (OPC-UA) Benutzerkonto-Sperre einer Person aufgrund zu vieler Probleme bei den Authentifizierungsversuchen	1	OPC-UA	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Ungültiges Zertifikat, Ungültiges Passwort	—
Anmeldung verweigert (Konto gesperrt)	Ein Benutzer (eine Person) versucht, eine Verbindung mit einem bereits gesperrten Konto herzustellen.	Anmeldeproblem (Webserver über HTTPS). Anmeldung verweigert (Konto gesperrt)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]		CPU eNOR
		Anmeldeproblem (Firmwareaktualisierung über HTTPS). Anmeldung verweigert (Konto gesperrt)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]		CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
		Anmeldeproblem (OPC-UA) Anmeldung verweigert (Konto gesperrt)	1	OPC-UA	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]		—
Verbindungstrennung	Eine Person oder eine Komponente trennt die Verbindung manuell oder Trennung nach einem Timeout aufgrund von Inaktivität.	HTTPS-Verbindungstrennung (Webserver)	6	HTTPS	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Manuelle Abmeldung	CPU eNOR
		HTTPS-Verbindungstrennung (Firmwareaktualisierung)	6	HTTPS	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Manuelle Abmeldung	CPU eNOR
		OPC-UA-Verbindungstrennung	6	OPC-UA	DISCONNECTION	[meta sequenceId=*Zahl*]	Socket-Verbindungstrennung	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						[authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]		
		Modbus-Verbindungstrennung	6	MODBUS	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Socket-Verbindungstrennung	CPU
		Explizite EIP-Verbindungstrennung	6	EIP	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort* | *LokaleSchnittstelle*Peer=*PeerFQDN:PeerPort* user=*Benutzername*]	Socket-Verbindungstrennung	CPU
		HTTP-Verbindungstrennung (DPWS)	6	HTTP	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf=*LokalerPort*	Socket-Verbindungstrennung	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						| *LokaleSchnittstelle*Peer= *PeerFQDN:PeerPort* user= *Benutzername*]		
		HTTPS-Verbindungstrennung ausgelöst durch Timeout	6	HTTPS	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf= *LokalerPort* | *LokaleSchnittstelle*Peer= *PeerFQDN:PeerPort* user= *Benutzername*]	Timeout-Abmeldung	CPU eNOR
		OPC-UA-Verbindungstrennung ausgelöst durch Timeout	6	OPC-UA	DISCONNECTION	[meta sequenceId=*Zahl*] [authn@3833 itf= *LokalerPort* | *LokaleSchnittstelle*Peer= *PeerFQDN:PeerPort* user= *Benutzername*]	Timeout-Abmeldung	—
		DNP3-Verbindungstrennung	6	DNP3	DISCONNECTION	[meta sequenceId=Zahl] [authn@3833 itf= LokalerPort | LokaleSchnittstelle peer=	Socket-Verbindungstrennung	eNOR

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						PeerFQDN: PeerPort user= Benutzername]		
		IEC 60870-Verbindungstrennung	6	IEC60870	DISCONNECTION	[meta sequenceId=Zahl] [authn@3833 itf= LokalerPort | LokaleSchnittstelle peer= PeerFQDN: PeerPort user= Benutzername]	Socket-Verbindungstrennung	eNOR
Wichtige Parameteränderung zur Laufzeit	Wichtige Parameteränderung zur Laufzeit mit potenziell signifikaten Auswirkungen auf das System	Änderung der Parameter der Steuerungsanwendung: Zykluszeit	6	Konfiguration	PARAMETER_SET	[meta sequenceId=*Zahl*] [config@3833 object= "SPS-Anwendung" value= *Wert*]	Zykluszeit	CPU
Sicherungsvorgang	Sicherung eines Komponententeils oder einer gesamten Komponente	Download der Anwendung aus der Steuerung	6	Sicherung	BACKUP	[meta sequenceId=*Zahl*] [backup@3833 object= "SPS-Anwendung"]		CPU
		Export der Cybersicherheit-Konfiguration über BME NUA- oder BME	6	Sicherung	BACKUP	[meta sequenceId=*Zahl*] [backup@3833 object= "Cybersi-		eNOR

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
		NOR-Webseiten				cherheit-Konfiguration"]		
Wiederherstellungsvorgang	Wiederherstellung eines Komponententeils oder einer gesamten Komponente	Upload der Steuerungsanwendung/-konfiguration in die Steuerung	6	Konfiguration	CONFIGURATION_CHANGE	[meta sequenceId=*Zahl*] [config@3833 object=*Objekt*] *Objekt* = "SPS-Anwendung" oder "SPS-Konfiguration"		CPU
		Wiederherstellung der Steuerungsanwendung in der Steuerung	6	Sicherung	RESTORE	[meta sequenceId=*Zahl*] [backup@3833 object= "SPS-Anwendung"]		CPU
		Import der Cybersicherheit-Konfiguration über BME NUA- oder BME NOR-Webseiten	6	Sicherung	RESTORE	[meta sequenceId=*Zahl*] [backup@3833 object= "Cybersicherheit-Konfiguration"]		eNOR
Firmwareaktualisierung	Eine neue Firmware wurde erfolgreich überprüft und installiert.	Upload einer neuen Firmware in die Steuerung	6	Konfiguration	FIRMWARE_UPDATE	[meta sequenceId=*Zahl*] [config@3833 object= *Objekt* value= *Version*] Objekt = "Firmware", "Sicherheits-Kopro",		CPU eNOR

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
						"Webseiten"		
Ungültige Firmwareaktualisierung	Eine neue Firmware wurde aufgrund eines Fehlers nicht installiert.	Eine neue Firmware wurde aufgrund einer inkompatiblen Version oder ungültigen Signatur nicht installiert	1	Konfiguration	FIRMWARE_INVALID	[meta sequenceId=*Zahl*] [config@3833 object=*Objekt* value=*Version*] Objekt = "Firmware", "Sicherheits-Kopro", "Webseiten"	Inkompatible Version, ungültige Signatur	CPU eNOR
Änderung der Gerätezeit	Benutzer-Request einer Person zur Änderung von Uhrzeit und Datum.	—	5	Konfiguration	TIME_CHANGE	[meta sequenceId=*Zahl*] [config@3833 object=*"Uhrzeit"* value=*Datum/Uhrzeit*]		CPU
Zeitsignal außerhalb des Toleranzbereichs	Die Komponente validiert die über die Zeitsynchronisationskanäle empfangenen Zeitsynchronisationsnachrichten und gibt einen Alarm aus, wenn die Zeitsynchronisationsnachricht nicht innerhalb	—	1	Konfiguration	TIME_UNEXPECTED	[meta sequenceId=*Zahl*] [config@3833 object="Uhrzeit" value=*Datum/Uhrzeit*]	Zeitsignal außerhalb des Toleranzbereichs	

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
	der Toleranzen der internen/ lokalen Uhr der Komponente liegt (Zeit in der Vergangenheit, weit entfernt usw.)							
Hardwareänderung	In der Netzwerktopologie erkannte Änderung	Änderung des physischen Netzwerkports: Verbindungsaufbau/-abbau	6	System	HARDWARE_CHANGE	[system@3833 object= *Objekt*] Objekt = "Eth" gefolgt von Dezimalzahl	Port-Verbindung aktiv, Port-Verbindung inaktiv	CPU
		Jede von RSTP / HSR / PRP erkannte Topologieänderung	6	System	HARDWARE_CHANGE	[system@3833 object= *Objekt*] Objekt = "Eth" gefolgt von Dezimalzahl	Port-Aktivierung, Port-Deaktivierung, Port-Learning, Port-Weiterleitung, Port-Blockierung	CPU
	Hardwareänderung erkannt	Einsetzen/ Entnehmen der M580 SD-Karte	6	System	HARDWARE_CHANGE	[system@3833 object= "SDKarte"]	Einsetzen, Entnehmen	CPU
Änderung der Betriebsart	Änderung der Programmbetriebsart (Run, Stop, Init, Halt), Wartungsmodus / SafeRun / Anhalten der SAFE-Task	—	5	System	OPERATING_MODE_CHANGE	[system@3833 object= Objekt] Objekt = "SPS" oder "SPS-SAFE-Task" oder "Modul"	„Init“ „Run“ „Stop“ „Halt“ „Wartungsmodus“ „Sicherheitsmodus“ „HSBY primär“ „HSBY sekundär“ „HSBY warten“ „Master“	CPU

Protokolliertes Ereignis	Beschreibung	Zusätzliche Beschreibung	Severity	PROCID	MSGID	STRUCTURED-DATA	MSG	Geräte
							„Nicht-Master“	
Ungültige Konfiguration (außerhalb Cybersicherheit)	Eine neue (nicht Cybersicherheit) Konfiguration wurde aufgrund eines Fehlers nicht installiert.	Dateninte-gritätsfehler (Steuerung-sanwen-dung usw.)	1	Konfigu-ration	CONFI-GURATI-ON_ INVALID	[meta sequenc-eId=*Zahl*] [con-fig@3833 object= *Objekt* value= *Version*] *Objekt*= "SPS-Anwen-dung" oder "Modulkon-figuration”	Ungültiges Format, inkompatib-le Version	
Neustart	Hardware-Reset oder automati-scher Reset nach Firmware-Upload	—	1	System	REBOOT	—	Firmwa-reaktuali-sierung, Reset-Taste	CPU
Änderung des Produkt-zertifikats (und/oder der Schlüssel)	Zertifikat-manage-ment: SL1-Erstellung eines selbstsig-nierten Produkt-zertifikats	—	6	Anmelde-daten	CERTIFI-CATE_ CHANG-E	[meta sequenc-eId=*Zahl*] [cre-d@3833 name= *Allgemei-nerName*]	Zertifikater-stellung	CPU

HINWEIS: Zusätzlich zu der oben beschriebenen Struktur enthält jede Nachricht die folgenden Felder und Werte:

- Facility = 10
- HOSTNAME = Vollqualifizierter Domänenname (FQDN) oder lokale IP-Adresse
- APPNAME = Handelsreferenz, z. B. BMEP584040

Beispiele für Syslog-Servernachrichten

Date	Time	Priority	Hostname	Message
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="331"][authn@3833 if="eth" peer="192.168.11.50:52470"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="330"][authn@3833 if="eth" peer="192.168.11.50:52468"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="329"][authn@3833 if="eth" peer="192.168.11.50:52466"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="328"][authn@3833 if="eth" peer="192.168.11.50:52464"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="327"][authn@3833 if="eth" peer="192.168.11.50:52462"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="326"][authn@3833 if="eth" peer="192.168.11.50:52460"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="325"][authn@3833 if="eth" peer="192.168.11.50:52458"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="324"][authn@3833 if="eth" peer="192.168.11.50:52456"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="323"][authn@3833 if="eth" peer="192.168.11.50:52454"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="322"][authn@3833 if="eth" peer="192.168.11.50:52452"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="321"][authn@3833 if="eth" peer="192.168.11.50:52450"] Socket connection
11-08-2021	11:54:33	System0.Info	192.168.11.1	1 2021-08-26T11:22:12.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="320"][authn@3833 if="eth" peer="192.168.11.50:52442"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:07.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="319"][authn@3833 if="eth" peer="192.168.1.100:34246"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="318"][authn@3833 if="eth" peer="192.168.11.50:52440"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="317"][config@3833 object="Module"]
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:04.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="316"][config@3833 object="Module"]
11-08-2021	11:54:24	System0.Notice	192.168.11.1	1 2021-08-26T11:22:03.000Z 192.168.11.1 BMEP585040 System OPERATING_MODE_CHANGE [meta sequenceId="315"][system@3833 object="PLC"] Init
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="314"][config@3833 object="PLC application"]
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Backup RESTORE [meta sequenceId="313"][backup@3833 object="PLC application"]
11-08-2021	11:54:07	System0.Info	192.168.11.1	1 2021-08-26T11:21:46.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="312"][authn@3833 if="eth" peer="192.168.1.100:34235"] Socket connection
11-08-2021	11:53:20	System0.Info	192.168.11.1	1 2021-08-26T11:20:59.000Z 192.168.11.1 BMEP585040 Backup BACKUP [meta sequenceId="311"][backup@3833 object="PLC application"]

Beschreibung der Ereignisprotokollmeldungen für M580-Steuerungen (Firmware vor Version 4.10), BMENUA0100 und BMENOR2200H (Firmware vor Version 3.01)

Dieser Abschnitt enthält eine Beschreibung der Ereignisprotokollmeldungen für:

- M580-Steuerungen mit einer Firmware vor Version 4.10 (in der Spalte **Geräte** kurz als „CPU“ bezeichnet)
- OPC UA-Kommunikationsmodule BMENUA0100 (in der Spalte **Geräte** kurz als „NUA“ bezeichnet)
- Dezentrale Bedienterminals BMENOR2200H (in der Spalte **Geräte** kurz als „eNOR“ bezeichnet)

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
Erfolgreiche Verbindung mit einem Tool oder Gerät: * Erfolgreiche Anmeldung * Erfolgreiche TCP-Verbindung	Erfolgreiche Anmeldung (Datenspeicherung über FTP, FDR-Server über FTP, Firmware-Upload über FTP)	10	6	FTP	Dezentrale IP-Adresse	Li1: Erfolgreiche Verbindung (MNT_ENG_MSG_TYP_CNCTN_SUCCESS)	„Erfolgreiche Anmeldung“	CPU
	Erfolgreiche Anmeldung (Webserver mit HTTPS)			HTTPS	„(Null)“		„Erfolgreiche Anmeldung“	NUA
	Erfolgreiche Anmeldung (Firmwareaktualisierung über HTTPS)			HTTPS	„(Null)“		„Erfolgreiche Anmeldung“	NUA
	Erfolgreiche Anmeldung (OPC-UA)			OPC-UA	„(Null)“		„Erfolgreiche Anmeldung“	NUA
	Erfolgreiche Anmeldung (Unity-Anwendungspasswort über Modbus-Umas)			DEVICE_MANAGER	„(Null)“		„Erfolgreiche Anmeldung“	CPU
	Erfolgreiche Anmeldung			HTTP	„(Null)“		„Erfolgreiche Anmeldung“ ODER	CPU

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
	(Webserver über HTTP)						„Erfolgreiche Verbindung“ (falls keine M580-Webseiten für die Benutzeranmeldung)	
	Erfolgreiche TCP-Verbindung (kein Benutzer)			MODBUS	Dezentrale IP-Adresse		„Erfolgreiche Verbindung“	CPU
	Erfolgreiche TCP-Verbindung (kein Benutzer)			EIP	„(Null)“		„Erfolgreiche Verbindung“	CPU
	Erfolgreiche Verbindung auf dem DNP3-Kommunikationsprotokoll (über DNP3-Master und -Outstation)			DNP3	Dezentrale IP-Adresse		„Erfolgreiche Verbindung“	eNOR
	Erfolgreiche Verbindung auf dem IEC60870-Kommunikationsprotokoll (über IEC60870-Client und -Server)			IEC60870	Dezentrale IP-Adresse		„Erfolgreiche Verbindung“	eNOR

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
Verbindungsproblem mit einem Tool oder Gerät: *TCP-Verbindungsproblem aufgrund von ACL-Prüfung (Filterung von Quell-IP-Adresse/ TCP-Port) * Problem bei der Anmeldung	Problem bei der Anmeldung (Datenspeicherung über FTP, FDR-Server über FTP, Firmware-Upload über FTP)	10	4	FTP	Dezentrale IP-Adresse	Li2: Verbindung nicht erfolgreich (falsche Anmeldedaten) (MNT_ ENG_ MSG_ TYP_ CNCTN_ FAILURE)	„Anmeldung fehlgeschlagen“	CPU
	Problem bei der Anmeldung (Webserver mit HTTPS)			HTTPS	„(Null)“		„Anmeldung fehlgeschlagen“	NUA
	Problem bei der Anmeldung (Firmwareaktualisierung über HTTPS)			HTTPS	„(Null)“		„Anmeldung fehlgeschlagen“	NUA
	Problem bei der Anmeldung (OPC-UA)			OPC-UA	„(Null)“		„Anmeldung fehlgeschlagen“	NUA
	Problem bei der Anmeldung (Webserver mit HTTP)			HTTP	Dezentrale IP-Adresse		„Anmeldung fehlgeschlagen“ ODER „Verbindung fehlgeschlagen“ (falls keine Benutzeranmeldung)	CPU
	Problem bei der Anmeldung			DEVICE_ MANAGER	Dezentrale IP-Adresse		„Anmeldung fehlgeschlagen“	CPU

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
	(Unity-Anwendungspasswort über Modbus-Umas)							
	TCP-Verbindungsproblem (kein Benutzer)			MODBUS	Dezentrale IP-Adresse		„Verbindung fehlgeschlagen“	CPU
	TCP-Verbindungsproblem (kein Benutzer)			EIP	Dezentrale IP-Adresse		„Verbindung fehlgeschlagen“	CPU
	Verbindungsproblem auf dem DNP3-Kommunikationsprotokoll (über DNP3-Master und -Outstation)			DNP3	Dezentrale IP-Adresse		„Verbindung fehlgeschlagen“	eNOR
	Verbindungsproblem auf dem IEC60870-Kommunikationsprotokoll (über IEC60870-Client und -Server)			IEC60870	Dezentrale IP-Adresse		„Verbindung fehlgeschlagen“	eNOR
Verbindungstrennung lokal ausgelöst	Verbindungstrennung ausgelöst	10	6	FTP	„(Null)“	Li5: Verbindungstrennung	„Trennen der Verbindung“	—

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
oder durch Peer: * TCP-Verbindungstrennung * Abmeldung auf Anfrage	durch Peer/ Benutzer/ Lokal					ausgelöst durch Peer/ Benutzer (MNT_ ENG_ MSG_ TYP_ DISCONNECTION)		
	Verbindungstrennung ausgelöst durch Peer/ Benutzer/ Lokal			HTTPS	„(Null)“		„Trennen der Verbindung“	NUA
	Verbindungstrennung ausgelöst durch Peer/ Benutzer/ Lokal			OPC-UA	„(Null)“		„Trennen der Verbindung“	NUA
	Verbindungstrennung ausgelöst durch Peer/ Benutzer/ Lokal			MODBUS	Dezentrale IP-Adresse		„Trennen der Verbindung“	CPU
	—			DNP3	„(Null)“ oder dezentrale IP-Adresse		„Trennen der Verbindung“	eNOR
	—			IEC60870	„(Null)“ oder dezentrale IP-Adresse		„Trennen der Verbindung“	eNOR
Automatische Abmeldung (Inaktivitäts-	Verbindungstrennung ausgelöst durch Timeout	10	6	HTTPS	„(Null)“	Li6: Verbindungstrennung ausgelöst durch	„Automatische Abmeldung“	NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
Timeout) HTTPS OPC-UA						Timeout (MNT_ ENG_ MSG_ TYP_ DSCNCT_ TIME-OUT)		
	Verbindungstrennung ausgelöst durch Timeout			OPC-UA			„Automatische Abmeldung“	NUA
Wichtige Änderungen im System: Änderung der Laufzeit der Parameter außerhalb der Konfiguration	Wesentliche Änderung der Zykluszeit oder Änderung der Watchdog-Parameter der Steuerungsanwendung (Zykluszeit, Watchdog)	13	5	DEVICE_ MANAGER	„(Null)“	Li87: Aktualisierung der Systemparameter (MNT_ ENG_ MSG_ TYP_ PARAMETER_ UPDATE)	„XXXX-Parameteraktualisierung“ (wobei XXXX den Parameter identifiziert) XXXX = „Zykluszeit“ Beispiel: Aktualisierung der Zykluszeit-Parameter	CPU
Wichtige Änderungen im System: * Download der Anwendung oder Konfiguration aus dem Gerät	Download einer Konfigurationsdatei aus dem Gerät	13	6	MODBUS	„(Null)“	Li8: Download einer Konfigurationsdatei aus dem Gerät (MNT_ ENG_ MSG_ TYP_ CONF_ DL)	„Anwendungsdownload“ oder „Konfigurationsdownload“	CPU
* Export (Aufzeichnung) der Cybersicherheit-Konfigura-				HTTPS			„Cybersicherheit-Konfigurationssicherung“	NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
tionsdateien aus dem Gerät								
Wichtige Änderungen im System	Upload der Anwendung/ Konfiguration oder nur der Konfiguration in das Gerät (einschließlich CCOTF)	13	6	MODBUS	„(Null)“	Li9: Upload einer Konfigurationsdatei in das Gerät (MNT_ ENG_ MSG_ TYP_ CONF_ UL)	„Anwendungsupload“ oder „Konfigurationsupload“	CPU NUA
	Import (Wiederherstellung) der Cybersicherheit-Konfigurationsdatei in das Gerät			HTTPS			„Cybersicherheit-Konfigurationswiederherstellung“	NUA
Wichtige Änderungen im System	Upload von Webseiten in das Gerät	13	6	FTP	„(Null)“	Li10: Upload einer neuen Firmware in das Gerät (MNT_ ENG_ MSG_ TYP_ FIRMWARE_ UPDATE)	„Webseiten-Upload“	CPU
	Upload einer neuen Firmware für den Sicherheitskoprozessor			FTP			„Sicherheits-Koprozessor-Firmware-Upload“	CPU
	Upload einer neuen			FTP			„Firmware-Upload“	CPU

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
	Firmware in das Gerät							
	Upload einer neuen Firmware in das Gerät			HTTPS			„Firmware-Upload“	NUA
Wichtige Änderungen im System	Änderung der Gerätezeit	13	6	DEVICE_MANAGER	„(Null)“	LI15: Änderung der IED-Zeit	„Wichtiges Update Zeit“	NUA
Laufzeit der Kommunikationsparameter - Erfolgreiche Änderung außerhalb der Konfiguration	Aktivierung/ Deaktivierung von Kommunikationsdiensten	10	4	DEVICE_MANAGER	„(Null)“	Li18: Aktivierung/ Deaktivierung von Ports, physisch (serieller Port, USB-Port) oder logisch (Telnet, FTP) (MNT_ENG_MSG_TYP_PORT_MANAGEMENT)	„Wichtige Aktualisierung der Kommunikationsparameter: XXXX YYYY“ XXXX = „EIP“, „DHCP“, „FTP“, „MODBUS“, „SNMP“, „HTTP“, „SECURITY“, „NTP“, „IPSEC“ oder „DEVICE_MANAGER“ Nur für NUA: XXXX = „Nur Control Expert-Datenflüsse zur Steuerung“ oder „Control Expert-Datenflüsse zum	CPU NUA eNOR

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
							Gerätenetzwerk“ oder „CPU-zu-CPU-Datenflüsse“ - Nur für NOR: XXXX = „DNP3 über TLS-Kanal [„*Kanalname*“]“ oder „IEC60870 über TLS“ - YYYY = „aktivieren“ oder „deaktivieren“ - Beispiel: „Aktualisierung der Hauptkommunikationsparameter: FTP aktivieren“	
Änderung des physischen Netzwerkports: Verbindungsaufbau/-trennung	Alle Statusänderungen des physischen Netzwerkports. Kann der Status eines Ethernet-Ports sein oder Informationen betreffen, die vom RSTP-/HSR-/PRP-Algorithmus für	10	4	DEVICE_MANAGER	„(Null)“	LI19: Alle Statusänderungen des physischen Netzwerkports. Kann der Status eines Ethernet-Ports sein oder Informationen betreffen, die vom RSTP-/HSR-/PRP-Algorithmus für	„Wichtige Statusänderung des physischen Netzwerkports: XXXX Verbindung YYYY“ - XXXX = „ETH“ gefolgt von der Dezimalzahl für den Port oder „FRONT-Port“ - YYYY =	CPU NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
	redundante Systeme erfasst werden.					redundante Systeme erfasst werden. (MNT_ ENG_ MSG_ TYP_ NETWK_ PORT_ CHG)	„Verbindung aktiv“ oder „Verbindung nicht aktiv“ - Beispiel: „Wichtige Statusänderung des physischen Netzwerkports: ETH1-Verbindung aktiv)“	
Jede erkannte Topologieänderung:	Jede von RSTP / HSR / PRP erkannte Topologieänderung	10	4	RSTP	„(Null)“	LI20: Alle von RSTP-/ HSR-/ PRP-Algorithmen für redundante Systeme erkannten Topologieänderungen (MNT_ ENG_ MSG_ TYP_ NTWK_ TPLGY_ CHG)	„Topologieänderung erkannt“ oder „Topologieänderung erkannt: XXXX YYYY“ - XXXX = „ETH“ gefolgt von einer Dezimalzahl für den Port oder „FRONT-Port“ - YYYY = „aktivieren“, „deaktivieren“, „lernen“, „vorwärts“, „blockieren“	CPU NUA
Fehler bei der Integritätsprüfung:	Firmware-Integritätsfehler	10	6	DEVICE_ MANAGER	„(Null)“	LI84: Datenintegritätsfehler MNT_ ENG_	„Firmware-Integritätsfehler“	CPU NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
* Fehler bei der digitalen Signatur * Nur Integrität (HashMac)	Datenintegritätsfehler: CS-Konf., Zert., Whitelist oder RBAC)			DEVICE_MANAGER		MSG_DATA_INTEGRITY_ERROR	„Datenintegritätsfehler“	NUA
Wichtige Änderungen im System: Neustart	Neustart nach Firmware-Upload	13	4	DEVICE_MANAGER	„(Null)“	LI14: MNT_ENG_MSG_TYP_REBOOT ORDER	„Neustart“	CPU NUA
Wichtige Änderungen im System	Änderung der Betriebsart der Steuerung (Run, Stop, Init, Halt) Wartungsmodus Änderung der sicherheitsbezogenen Betriebsarten (SafeRun, Stop Safe Task)	13	5	DEVICE_MANAGER	„(Null)“	LI85: Änderung der Betriebsart MNT_ENG_MSG_OPERATING_MODE_CHANGE	„XXXX-Statusaktualisierung: YYYY“ (wobei XXXX das Objekt angibt, dessen Zustand sich ändert, und YYYY den neuen Zustand identifiziert) - XXXX = „SPS“ oder „SPS-SAFE-Task“ oder „Gerät“ - YYYY = „INIT“, „STOP“, „RUN“, „HALT“, „Wartungsmodus“ oder „Sicherheitsmodus“ -	CPU

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
							BEISPIEL: „SPS-Statusaktualisierung: RUN“ „SPS-Statusaktualisierung: Wartungsmodus“	
Wichtige Änderungen im System: Hardwareänderung	Betrieb auf der SD-Karte	13	6	DEVICE_MANAGER	„(Null)“	LI26: Hardwareänderung MNT_ENG_MSG_HARDWARE_CHANGE	„Hardwareaktualisierung: XXXX“ (wobei XXXX die Aktualisierung beschreibt) - XXXX = „Einsetzen der SD-Karte“ oder „Herausnehmen der SD-Karte“	CPU
	Positionsänderung des Drehrads: Reset, Erweitert			DEVICE_MANAGER			„Hardwareaktualisierung: XXXX“ (wobei XXXX die Aktualisierung beschreibt) - XXXX = „Zurück zum Werksmodus“ oder „Sicherer Modus“	NUA
Wichtige Änderung in Cybersicherheit-	Erstellung eines Benutzerkontos			HTTPS	„(Null)“	Li11: MNT_ENG_MSG_TYP_	„RBAC aktualisieren“	NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
RBAC (durchgeführt über die Webseiten zur Cybersicherheit-Konfiguration)	Löschen eines Benutzerkontos Aktualisierung eines Benutzerkontos					RBAC_ UPDATE		
Wichtige Änderung der Cybersicherheit-Richtlinie (durchgeführt über die Webseiten zur Cybersicherheit-Konfigurations)	Netzwerkdienste Ereignisprotokoll Sicherheitsstrategie Sicherheitsbanner	10	4	HTTPS	„(Null)“	Li12: MNT_ ENG_ MSG_ TYP_ SECURITY_ UPDATE_ UPDATE	„Wichtige Cybersicherheit-Parameteraktualisierung: Netzwerkdienste“ „Wichtige Cybersicherheit-Parameteraktualisierung: Ereignisprotokoll“ „Wichtige Cybersicherheit Parameteraktualisierung: Sicherheitsrichtlinie“ „Wichtige Cybersicherheit-Parameteraktualisierung: Sicherheitsbanner“	NUA
Wichtige Änderung der gerätespezifischen Cybersicherheit-Parameter (durchgeführt über	Aktivierung/ Deaktivierung und Konfiguration von IPSEC Aktivierung/	10	4	HTTPS	„(Null)“	Li13: MNT_ ENG_ MSG_ TYP_ DSS_ UPDATE	„Wichtige Cybersicherheit-Parameteraktualisierung: IPSEC“ „Wichtige Cybersicherheit-	NUA

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
die Webseiten zur Cybersicherheit-Konfiguration)	Deaktivierung und Konfiguration von OPC-UA Aktivierung/ Deaktivierung und Konfiguration von DNP3						Parameteraktualisierung: OPC-UA“	
Autorisierungsproblem	Eine Aktion von einem Benutzer oder einer Maschine mit einer Ressource nicht autorisiert	10	4	HTTPS	„(Null)“	Li21: MNT_ ENG_ MSG_ TYP_ AUTH_ REQ	„Autorisierung fehlgeschlagen“	—
Zertifikatverwaltung	Hinzufügen/ Entfernen eines Client-Zertifikats	10	4	HTTPS	„(Null)“	Li89: Zertifikatverwaltung (MNT_ ENG_ MSG_ TYP_ CERT_ MGT)	„Client-Zertifikat hinzufügen“ „Client-Zertifikat entfernen“	NUA
Zertifikatverwaltung: * Zertifikat abgelaufen	Erkennung des Gültigkeitsendes des Serverzertifikats bei Neustart	10	3	DEVICE_ MANAGER	„(Null)“	Li29: Zertifikatverwaltung (MNT_ ENG_ MSG_ TYP_ CERT_ EXPIRE)	„Zertifikat abgelaufen“	NUA
Spezifisch für eNOR-Projekt:								
Authentifizierungsproblem	—	10	4	„DNP3_ Master“ oder „DNP3_ Outstation“	Dezentrale IP-Adresse	Li100: MNT_ ENG_ MSG_ TYPE_ AUTHEN-	„Authentifizierung Kanal [„*Kanalname*“] fehlgeschlagen“	eNOR

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
						TICATION_FAILURE		
Nicht erwartete Antwort	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li101: MNT_ENG_MSG_TYPE_UNEXPECTED_RESPONSE	„Nicht erwartete Antwort Kanal [„*Kanalname*“]“	eNOR
Keine Reaktion	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li102: MNT_ENG_MSG_TYPE_NO_RESPONSE	„Keine Antwort Kanal [„*Kanalname*“]“	eNOR
Aggressiver Modus nicht unterstützt	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li103: MNT_ENG_MSG_TYPE_AGGRESSIVE_MODE_NOT_SUPPORTED	„Aggressiver Modus Kanal [„*Kanalname*“] nicht unterstützt“	eNOR
MAC-Algorithmus nicht unterstützt	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li104: MNT_ENG_MSG_TYPE_MAC_ALGORITHM_NOT_SUPPORTED	„MAC-Algorithmus Kanal [„*Kanalname*“] nicht unterstützt“	eNOR
Key-Wrap-Algorithmus (Schlüsselumbruch) nicht unterstützt	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li105: MNT_ENG_MSG_TYPE_KEYWRAP_ALGORITHM_NOT_	„Key-Wrap-Algorithmus Kanal [„*Kanalname*“] nicht unterstützt“	eNOR

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
						SUPPORTED		
Autorisierungsproblem	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li86: MNT_ENG_MSG_TYP_AUTHORIZATION_FAILURE)	„Autorisierung Kanal [„*Kanalname*“] fehlgeschlagen“	eNOR
Methode zur Änderung des Aktualisierungsschlüssels nicht zulässig	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li106: MNT_ENG_MSG_TYPE_UPDATE_KEY_CHANGE_METHOD_NOT_PERMITTED	„Methode zur Änderung des Aktualisierungsschlüssels Kanal [„*Kanalname*“] nicht zulässig“	eNOR
Ungültige Signatur	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li107: MNT_ENG_MSG_TYPE_INVALID_SIGNATURE	„Ungültige Signatur Kanal [„*Kanalname*“]“	eNOR
Ungültige Zertifizierungsdaten	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li108: MNT_ENG_MSG_TYPE_INVALID_CERTIFICATION_DATA	„Ungültige Zertifizierungsdaten Kanal [„*Kanalname*“]“	eNOR
Unbekannter Benutzer	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li109: MNT_ENG_MSG_TYPE_UNKNOWN_USER	„Unbekannter Benutzer Kanal [„*Kanalname*“]“	eNOR

Protokolliertes Ereignis	Beschreibung	Facility (Ursprung)	Severity (Schweregrad)	MSGID	MSG: PeerAddr	MSG: type	MSG: appMsg	Geräte
Max. Anzahl Statusanforderungen des Sitzungsschlüssels überschritten	—	10	4	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li110: MNT_ENG_MSG_TYPE_MAX_SESSION_KEY_STATUS_REQ_EXCEED	„Max. Anzahl Statusanforderungen des Sitzungsschlüssels Kanal [„*Kanalname*“] überschritten“	eNOR
Änderung des Sitzungsschlüssels erfolgreich	—	10	6	„DNP3_Master“ oder „DNP3_Outstation“	Dezentrale IP-Adresse	Li111: MNT_ENG_MSG_TYPE_SESSION_KEY_CHANGE_SUCCESS	„Änderung des Sitzungsschlüssels Kanal [„*Kanalname*“] erfolgreich“	eNOR

HINWEIS: Zusätzlich zu der oben beschriebenen Struktur enthält jede Meldung die folgenden Felder und Werte, die auf das Feld des Schweregrads folgen:

- HOSTNAME = Lokale IP-Adresse oder Null.
- APPNAME = Handelsreferenz, z. B. BMEP584040.
- PROCID - nicht verwendet.
- MSG:Issuer-Adresse = Lokale IP-Adresse.
- MSG:Peer - nicht verwendet.

Steuerungsidentifikation und - authentifizierung

Kontoverwaltung

Die folgenden Best Practices gelten für die Kontoverwaltung:

- Erstellen Sie ein Standardbenutzerkonto ohne Administratorrechte.

- Nutzen Sie das Standardbenutzerkonto zum Starten von Anwendungen. Verwenden Sie Konten mit höheren Berechtigungen nur dann zum Starten einer Anwendung, wenn die Anwendung eine höhere Berechtigungsebene erfordert, um ihre Aufgabe im System zu erfüllen.
- Nutzen Sie ein Konto mit Administratorrechten, um Anwendungen zu installieren.

Verwalten von Benutzerkontensteuerungen (UAC) mit Windows 10

Um unbefugte Änderungen am PC-Betriebssystem zu minimieren, gewährt Windows 10 Anwendungen die Berechtigungsebenen eines normalen Benutzers ohne Administratorrechte. Ohne Administratorrechte können Anwendungen keine Änderungen am System vornehmen. UAC fordert den Benutzer auf, einer Anwendung zusätzliche Berechtigungen zu erteilen oder zu verweigern. Stellen Sie UAC auf die höchste Ebene ein. Auf der höchsten Ebene erhält der Benutzer von UAC eine entsprechende Aufforderung, bevor eine Anwendung die Berechtigung erhält, Änderungen vorzunehmen, die Administratorrechte erfordern.

Um auf UAC-Einstellungen in Windows 10 zuzugreifen, öffnen Sie **Systemsteuerung > Benutzerkonten und Family Safety > Benutzerkonten > Benutzerkontensteuerungseinstellungen ändern** oder geben Sie **UAC** in das Suchfeld des Windows 10-**Startmenüs** ein.

Verwalten von Passwörtern

Die Passwortverwaltung ist eines der grundlegenden Werkzeuge zum Geräte-Hardening, also dem Prozess, bei dem ein Gerät zum Schutz vor kommunikationsbasierten Bedrohungen konfiguriert wird. Es hat sich als vorteilhaft erwiesen, die folgenden Richtlinien zur Passwortverwaltung anzuwenden:

- Aktivieren Sie die Passwortauthentifizierung für alle E-Mails und Web-Server, Steuerungen und Ethernet-Schnittstellenmodule.

- Ändern Sie direkt nach der Installation alle Standardpasswörter, einschließlich derjenigen für:
  - Benutzer- und Anwendungskonten in Windows, SCADA, HMI und anderen Systemen
  - Skripte und Quellcode
  - Netzwerksteuerungsgeräte
  - Geräte mit Benutzerkonten
  - FTP-Server
  - SNMP- und HTTP-Geräte
  - Control Expert
- Weisen Sie nur Benutzern, die Zugriff benötigen, ein Passwort zu. Untersagen Sie die gemeinsame Nutzung von Passwörtern.
- Lassen Sie Passwörter bei der Eingabe nicht anzeigen.
  - Fordern Sie Passwörter, die schwer zu erraten sind. Sie sollten mindestens 8 Zeichen enthalten und aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (sofern zulässig) bestehen.
- Verlangen Sie, dass Benutzer und Anwendungen Passwörter in regelmäßigen Abständen ändern.
- Entfernen Sie die Zugriffskonten von Benutzern, wenn deren Anstellung beendet ist.
- Fordern Sie unterschiedliche Passwörter für verschiedene Konten, Systeme und Anwendungen.
- Verwalten Sie eine sichere Master-Liste mit Administrator-Passwörtern, sodass diese in einem Notfall schnell zur Hand sind.
- Setzen Sie die Passwortverwaltung auf eine Weise um, die nicht die Fähigkeit eines Bedieners behindert, bei einem Ereignis (z. B. einer Notabschaltung) schnell zu reagieren.
- Übertragen Sie Passwörter nicht per E-Mail oder auf andere Weise über das unsichere Internet.

Verwalten von HTTP

Hypertext Transfer Protocol (HTTP) ist das vom Web verwendete Basisprotokoll. Es wird in Steuerungssystemen zur Unterstützung eingebetteter Webserver in Steuerungsprodukten verwendet. Schneider Electric Webserver verwenden die HTTP-Kommunikation zur Anzeige von Daten und zum Senden von Befehlen über Webseiten.

Wenn der HTTP-Server nicht erforderlich ist, deaktivieren Sie ihn. Andernfalls verwenden Sie anstatt von HTTP, sofern möglich, *Hypertext Transfer Protocol Secure* (HTTPS), eine Kombination aus HTTP und einem kryptografischen Protokoll. Lassen Sie nur Datenverkehr

zu bestimmten Geräten zu, indem Sie Zugriffskontrollmechanismen wie beispielsweise eine Firewall implementieren, die den Zugriff von bestimmten Geräten auf bestimmte Geräte beschränken.

Sie können HTTPS als Standard-Web-Server auf den Produkten konfigurieren, die diese Funktion unterstützen.

Importieren Sie die selbstsignierten Zertifikate Ihrer M580-Steuerungen in Ihren Webbrowser über ein vertrauenswürdiges Netzwerk und kennzeichnen Sie sie als vertrauenswürdig. Dadurch wird verhindert, dass eine Benachrichtigung angezeigt wird, wenn eine Verbindung zu den Webseiten Ihrer vertrauenswürdigen Steuerungen hergestellt wird.

HINWEIS: Dieser Vorgang muss wiederholt werden, wenn die Zertifikate Ihrer Steuerungen erneuert werden, z. B. wenn Sie die IP-Adressen Ihrer Steuerungen über die Anwendung ändern.

Verwalten von FTP

File Transfer Protocol (FTP) bietet dezentrale Dateiverwaltungsdienste über ein TCP/IP-basiertes Netzwerk, wie z. B. Internet. FTP verwendet eine Client-Server-Architektur sowie separate Steuerungs- und Datenverbindungen zwischen Client und Server.

Beachten Sie das folgende Verhalten des von Schneider Electric bereitgestellten FTP-Dienstes:

- Das FTP-Protokoll ist standardmäßig deaktiviert.
- Das FTP-Protokoll ist nur für spezifische Wartungs- und Konfigurationsaktivitäten erforderlich. Es hat sich bewährt, den gesamten Satz an FTP-Diensten zu deaktivieren, wenn sie nicht benötigt werden.

- Das FTP-Protokoll ist ein unsicheres Protokoll und muss mit Vorsicht eingesetzt werden, um die Offenlegung sensibler Informationen und den unbefugten Zugriff auf die Steuerungen zu vermeiden:
  - Ändern Sie nach Möglichkeit die Standardpasswörter auf allen Geräten, die FTP unterstützen.
  - Verwenden Sie eine Zugriffskontrollliste, um die Kommunikation auf die autorisierten IP-Adressen zu beschränken. Siehe „Cybersicherheit pro System“ für detaillierte Informationen zum jeweiligen Modul.
  - Konfigurieren Sie bei Verwendung des BMENOC-Moduls die IPSEC-Funktion (Einrichtung verschlüsselter Kommunikation, Seite 36).
  - Blockieren Sie sämtlichen ein- und ausgehenden FTP-Datenverkehr an der Grenze des Unternehmensnetzwerks und des Betriebsnetzwerks des Kontrollraums.
  - Filtern Sie FTP-Befehle zwischen dem Steuerungsnetzwerk und dem Betriebsnetzwerk an bestimmte Hosts oder übertragen Sie sie über ein separates, verschlüsseltes Verwaltungsnetzwerk.
  - Verwenden Sie ein externes Modul, um ein VPN zwischen den von der Steuerung betroffenen Modulen und der Engineering-Workstation im Steuerungsnetzwerk einzurichten.
- BMENOC0301 and BMENOC0311-Module unterstützen keine IP-Weiterleitung an das Gerätenetzwerk.

  Wenn Transparenz zwischen dem Steuerungs- und dem Gerätenetzwerk benötigt wird, ist ein externer Router/VPN erforderlich, um eine verschlüsselte Kommunikation zwischen dem Steuerungs- und dem Gerätenetzwerk bereitzustellen (siehe Abbildung in CSPN-Sicherheitsziel, Seite 43).

Im FTP-Protokoll wird Transparenz benötigt, um die folgenden Operationen vom Steuerungsnetzwerk aus auszuführen:

- Aktualisierung der Firmware der M580-Steuerung über das Tool „Automation Device Maintenance“.
- Netzwerkdiagnose der M580-Steuerung, ausgeführt mit einem Netzwerkverwaltungstool über den SNMP-Dienst.

Verwalten von SNMP

Simple Network Management Protocol (SNMP) stellt Netzwerkverwaltungsdienste zwischen einer zentralen Verwaltungskonsole und Netzwerkgeräten wie Routern, Druckern und Steuerungen bereit. Das Protokoll besteht aus drei Teilen:

- Manager: Eine Anwendung, die SNMP-Agents in einem Netzwerk durch die Ausgabe von Requests, das Abrufen der Antworten und die Überwachung und Verarbeitung der von den Agents ausgegebenen Traps verwaltet.

- Agent: Ein Softwaremodul zur Netzwerkverwaltung, das sich auf einem verwalteten Gerät befindet. Der Agent ermöglicht die Änderung von Konfigurationsparametern durch Manager. Bei den verwalteten Geräten kann es sich um jeden Gerätetyp handeln: Router, Zugriffsserver, Switches, Bridges, Hubs, Steuerungen, Laufwerke.
- Netzwerkmanagementsystem (NMS): Das Endgerät, über das Administratoren administrative Aufgaben ausführen können.

Ethernet-Geräte von Schneider Electric verfügen über SNMP-Dienstfunktionen für das Netzwerkmanagement.

SNMP wird häufig automatisch mit **public** (öffentlich) als Lesezeichenfolge und **private** (privat) als Schreibzeichenfolge installiert. Diese Art der Installation bietet einem Angreifer die Möglichkeit, ein System auszuspionieren, um dann einen Denial-of-Service-Angriff durchzuführen.

Um das Risiko eines Angriffs mit SNMP zu begrenzen:

- Falls SNMP v1 erforderlich ist, schränken Sie die Geräte (IP-Adressen), die auf den Switch zugreifen können, mithilfe entsprechender Zugriffseinstellungen ein. Weisen Sie Geräten unterschiedliche Passwörter für den Lesezugriff und Lese-/Schreibzugriff zu.
- Ändern Sie die Standardpasswörter auf allen Geräten, die SNMP unterstützen.
- Blockieren Sie sämtlichen ein- und ausgehenden SNMP-Datenverkehr an der Grenze des Unternehmensnetzwerks und des Betriebsnetzwerks des Kontrollraums.
- Filtern Sie SNMP v1-Befehle zwischen dem Steuerungsnetzwerk und dem Betriebsnetzwerk an bestimmte Hosts oder übertragen Sie sie über ein separates, verschlüsseltes Verwaltungsnetzwerk.
- Kontrollieren Sie den Zugriff durch Identifizierung der IP-Adressen, die zur Abfrage eines SNMP-Geräts berechtigt sind.
- Verwenden Sie ein externes Modul, um ein VPN zwischen den von der Steuerung betroffenen Modulen und der Engineering-Workstation im Steuerungsnetzwerk einzurichten.

Verwalten der Passwörter für Control Expert-Anwendungen, Sections, Datenspeicherung und Firmware

In Control Expert gelten Passwörter für Folgendes (je nach Steuerung):

- **Anwendung**

  Der Passwortschutz für Control Expert und Steuerungsanwendung verhindert unerwünschte Änderungen, Downloads oder das Öffnen der Anwendung (.STU-, .STA and .ZEF -Dateien). Das Passwort wird verschlüsselt in der Anwendung gespeichert.

  Zusätzlich zum Passwortschutz können Sie die Dateien .STU, .STA und .ZEF verschlüsseln. Die Dateiverschlüsselungsfunktion in Control Expert verhindert unbefugte Änderungen durch nicht qualifiziertes Personal und verstärkt den Schutz vor Diebstahl geistigen Eigentums und anderen böswilligen Handlungen. Die Dateiverschlüsselungsoption ist durch einen Passwortmechanismus geschützt.

  HINWEIS: Wenn eine Steuerung im Rahmen eines Systemprojekts verwaltet wird, sind Anwendungspasswort und Dateiverschlüsselung im Control Expert-Editor deaktiviert und müssen über den Topology Manager verwaltet werden.

  Weitere Informationen finden Sie im Abschnitt *Anwendungsschutz* (siehe EcoStruxure™ Control Expert, Betriebsarten).

- **Section**

  Der Zugriff auf die Section-Schutzfunktion erfolgt über das Fenster **Eigenschaften** des Projekts im Offline-Modus Diese Funktion dient dem Schutz der Programm-Sections. Weitere Informationen finden Sie im Abschnitt *Schutz von Sections und Unterprogrammen* (siehe EcoStruxure™ Control Expert, Betriebsarten).

  HINWEIS: Der Section-Schutz ist nicht aktiv, solange der Schutz nicht im Projekt aktiviert wird.

- **Datenspeicherung/Web**

  Der Datenspeicherschutz durch ein Passwort verhindert unerwünschten Zugriff auf den Datenspeicherbereich der SD-Speicherkarte (wenn eine gültige Karte in die Steuerung eingesetzt ist). Er kann ebenfalls unerwünschten Zugriff auf die Webdiagnose verhindern (für M580-Steuerungsfirmware ≥ 4.0). Weitere Informationen finden Sie im Abschnitt *Schutz der Datenspeicherung* (siehe EcoStruxure™ Control Expert, Betriebsarten).

- **Firmware**

  Der Passwortschutz für den Firmware-Download verhindert den Download schädlicher Firmware. Weitere Informationen finden Sie im Abschnitt *Firmware-Schutz* (siehe EcoStruxure™ Control Expert, Betriebsarten).

Kontrollberechtigungen

Control Expert Sicherheitseditor

Ein Sicherheitskonfigurationstool wird verwendet, um Softwarebenutzer und ihre jeweiligen Berechtigungen zu definieren. Die Zugriffssicherheit von EcoStruxure Control Expert gilt für

die Endgeräte, auf denen die Software installiert ist, und nicht für das Projekt, das über ein eigenes Schutzsystem verfügt.

Weitere Informationen hierzu finden Sie in folgendem Handbuch: *EcoStruxure™ Control Expert, Security Editor, Operation Guide*.

Es hat sich als vorteilhaft erwiesen, ein spezielles Passwort für den Sicherheitsadministrator (*SecurityAdmin*) festzulegen und die Berechtigungen anderer Benutzer anhand eines eingeschränkten Profils zu begrenzen.

Programmier- und Überwachungsmodus

Für den Zugriff auf die Steuerung im **Online**-Modus stehen zwei Modi zur Verfügung:

- **Programmiermodus**: Das Steuerungsprogramm kann geändert werden. Wenn ein Endgerät zum ersten Mal mit der Steuerung verbunden wird, wird die Steuerung reserviert, und solange sie reserviert ist, kann kein anderes Endgerät verbunden werden.
- **Überwachungsmodus**: Das Steuerungsprogramm kann nicht geändert werden, aber die Variablen. Im Überwachungsmodus wird die Steuerung nicht reserviert, und es kann auf eine bereits reservierte Steuerung zugegriffen werden.

Zur Auswahl eines Modus in EcoStruxure Control Expert wählen Sie Folgendes aus: **Extras > Optionen... > Verbindung > Standard-Verbindungsmodus**.

Weitere Informationen zu diesen Modi finden Sie im Abschnitt *Dienste im Online-Modus* (siehe EcoStruxure™ Control Expert, Betriebsarten).

Es hat sich bewährt, den **Online**-Steuerungszugriffsmodus wann immer möglich auf **Überwachung** einzustellen.

Schutz der Programm-Sections

Auf die Section-Schutzfunktion kann vom Fenster **Eigenschaften** des Projekts aus im Offline-Modus zugegriffen werden. Diese Funktion ermöglicht es, die Programm-Sections zu schützen. Detaillierte Informationen finden Sie im Abschnitt *Schutz von Sections und Unterprogrammen* (siehe EcoStruxure™ Control Expert, Betriebsarten).

HINWEIS: Der Section-Schutz ist nicht aktiv, solange der Schutz nicht im Projekt aktiviert wurde.

Es hat sich als vorteilhaft erwiesen, den Section-Schutz zu aktivieren.

Schutz des Steuerungsspeichers

Der Speicherschutz verhindert die Übertragung eines Projekts in die Steuerung sowie Änderungen im Online-Modus, unabhängig vom jeweiligen Kommunikationskanal.

HINWEIS: Der Steuerungsspeicherschutz kann bei Hot Standby-Steuerungen nicht konfiguriert werden. Verwenden Sie in diesem Fall die verschlüsselte IPsec-Kommunikation.

Der Speicherschutz wird wie folgt aktiviert:

- Steuerung der Baureihe Modicon M340: Eingangsbit. Detaillierte Informationen finden Sie im Abschnitt *Konfiguration der Modicon M340-Prozessoren* (siehe EcoStruxure™ Control Expert, Betriebsarten).
- Steuerung der Baureihe Modicon M580: Eingangsbit. Detaillierte Informationen finden Sie im Abschnitt *Verwalten des Run/Stop-Eingangs* (siehe Modicon M580, Hardware, Referenzhandbuch).
- Steuerung der Baureihe Modicon Quantum: Physischer Schlüsselschalter am Steuerungsmodul, entweder für Low-End-Steuerungen (siehe Quantum mit EcoStruxure™ Control Expert, Hardware, Referenzhandbuch) oder für High-End-Steuerungen (siehe Quantum mit EcoStruxure™ Control Expert, Hardware, Referenzhandbuch).
- Steuerung der Baureihe Modicon Premium: Eingangsbit. Detaillierte Informationen finden Sie im Abschnitt *Konfiguration der Premium-Prozessoren* (siehe EcoStruxure™ Control Expert, Betriebsarten).
- Steuerung der Baureihe Modicon MC80: Eingangsbit. Detaillierte Informationen finden Sie im Benutzerhandbuch für Modicon MC80 Speicherprogrammierbare Steuerungen (SPS).
- Steuerung der Baureihe Modicon Momentum MDI: Eingangsbit. Detaillierte Informationen finden Sie im EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Prozessoren - Benutzerhandbuch.

Es hat sich als vorteilhaft erwiesen, den Speicherschutz der Steuerung nach Möglichkeit zu aktivieren.

Dezentraler Run/Stop-Zugriff auf die Steuerung

Die Verwaltung des dezentralen Run/Stop-Zugriffs legt fest, wie eine Steuerung dezentral gestartet oder gestoppt werden kann, und ist vom System abhängig.

HINWEIS: Der dezentrale Run/Stop-Zugriff auf die Steuerung kann für Hot Standby-Steuerungen nicht konfiguriert werden. Verwenden Sie in diesem Fall die verschlüsselte IPsec-Kommunikation.

Steuerung	Zugriff
Modicon M580:	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request. • Dezentrales Stoppen der Steuerung per Request. Dezentrales Zurückweisen von Ausführungsrequests für die Steuerung. Wenn ein gültiger Eingang konfiguriert wurde, ist nur eine über den Eingang gesteuerte Ausführung verfügbar. • Dezentrales Zurückweisen von Ausführungs- oder Stopprequests für die Steuerung per Request. Siehe den Abschnitt *Verwalten des Run/Stop-Eingangs* für Optionen der Steuerungskonfiguration, die verhindern, dass dezentrale Befehle auf die Run/Stop-Modi zugreifen können (siehe Modicon M580, Hardware, Referenzhandbuch).
Modicon M340:	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request. • Dezentrales Stoppen der Steuerung per Request. Dezentrales Zurückweisen von Ausführungsrequests für die Steuerung. Wenn ein gültiger Eingang konfiguriert wurde, ist nur eine über den Eingang gesteuerte Ausführung verfügbar. Siehe den Abschnitt *Konfiguration der Modicon M340-Prozessoren* (siehe EcoStruxure™ Control Expert, Betriebsarten).
Modicon Premium:	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request. • Dezentrales Stoppen der Steuerung per Request. Dezentrales Zurückweisen von Ausführungsrequests für die Steuerung. Wenn ein gültiger Eingang konfiguriert wurde, ist nur eine über den Eingang gesteuerte Ausführung verfügbar. Siehe den Abschnitt *Konfiguration der Premium/Atrium-Prozessoren* (siehe EcoStruxure™ Control Expert, Betriebsarten).
Modicon Quantum:	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request.

Modicon MC80:	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request. • Dezentrales Stoppen der Steuerung per Request. Dezentrales Zurückweisen von Ausführungsrequests für die Steuerung. Wenn ein gültiger Eingang konfiguriert wurde, ist nur eine über den Eingang gesteuerte Ausführung verfügbar. • Dezentrales Zurückweisen der Ausführung bzw. des Stopps der Steuerung per Request. Siehe den Abschnitt *Konfiguration der Modicon MC80-Prozessoren* im Benutzerhandbuch für Modicon MC80 Speicherprogrammierbare Steuerungen (SPS).
Modicon Momentum MDI	Der dezentrale Run/Stop-Zugriff auf die Steuerung ermöglicht folgende Aktionen: • Dezentrales Stoppen oder Ausführen der Steuerung per Request. • Stopp durch die Steuerung per Fernzugriff per Request. Dezentrales Zurückweisen von Ausführungsrequests für die Steuerung. Wenn ein gültiger Eingang konfiguriert wurde, ist nur eine über den Eingang gesteuerte Ausführung verfügbar. Siehe den Abschnitt *Konfiguration der Modiconen Momentum MDI-Prozessoren* im Benutzerhandbuch für Modicon Momentum für EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Prozessoren.

Es hat sich als vorteilhaft erwiesen, dezentrale Ausführungen bzw. Stopps der Steuerung per Request zurückzuweisen.

Zugriff auf Steuerungsvariablen

Um die Steuerungsdaten vor unberechtigtem Lese- oder Schreibzugriff zu schützen, sollten Sie nach Möglichkeit die folgenden Best Practices anwenden:

- Verwenden Sie nicht lokalisierte Daten.
- Konfigurieren Sie EcoStruxure Control Expert zur ausschließlichen Speicherung von HMI-Variablen: **Extras > Projekteinstellungen... > In SPS eingebettete Daten > Datenwörterbuch > Nur HMI-Variablen**.

  Nur HMI-Variablen kann nur ausgewählt werden, wenn **Datenwörterbuch** ausgewählt ist.
- Markieren Sie die Variablen als *HMI*, auf die vom HMI oder SCADA aus zugegriffen werden kann. Auf Variablen, die nicht als *HMI* markiert sind, können externe Clients nicht zugreifen.
- Die Verbindung mit SCADA muss auf OFS basieren.

Datenspeicherschutz

Sie können den Datenspeicherschutz in EcoStruxure Control Expert durch Navigation zu **Extras > Projekteinstellung > In SPS eingebettete Daten** und anschließende Auswahl von **Übernehmen** aktivieren. Diese Funktion schützt sowohl lokalisierte als auch nicht lokalisierte Daten.

Weitere Informationen zur Datenspeicherschutz-Funktion finden Sie im Dokument zum Datenspeicherschutz in den EcoStruxure Control Expert-Betriebsarten.

Verwaltung der Datenintegritätsprüfungen

Einführung

Die Funktion der automatischen Integritätsprüfung in Control Expert verhindert die Änderung von Control Expert-Dateien und Software durch Viren oder Malware. Sie können die Integritätsprüfung auch manuell starten.

Automatische Integritätsprüfung

Control Expert mit dem Topology Manager basiert auf einer Client/Server-Architektur.

Die Server sind so konfiguriert, dass sie automatisch gestartet werden, wenn der Computer eingeschaltet oder neu gestartet wird. Bevor die Server gestartet werden, wird eine Integritätsprüfung für beide durchgeführt.

Der Server startet nur, wenn die Integritätsprüfung abgeschlossen ist, ohne dass Datenbeschädigungen erkannt werden. Wenn bei der Integritätsprüfung eine Datenbeschädigung festgestellt wird, wird ein Fehler protokolliert, den Sie in der **Ereignisanzeige** prüfen können.

In einem Meldungsfeld werden die beschädigten Dateien ausgewiesen. Klicken Sie auf **OK**. Daraufhin wird die Control Expert-Instanz geschlossen. Detaillierte Informationen finden Sie im *EcoStruxure Control Expert - Installationshandbuch* sowie im Abschnitt *Aktivieren der Kommunikation mit dezentralen Clients und Erhöhen der Sicherheit*.

Manuelle Integritätsprüfung mit Control Expert Classic

Gehen Sie wie folgt vor, um eine manuelle Integritätsprüfung durchzuführen, wenn eine Instanz von Control Expert Classic gestartet wird:

Schritt	Aktion
1	Klicken Sie auf **Hilfe > Über Control Expert XXX**.
2	Klicken Sie im Feld **Integritätsprüfung** auf **Selbsttest durchführen**. **Ergebnis**: Die Integritätsprüfung wird im Hintergrund durchgeführt. Control Expert erstellt ein Protokoll der erfolgreichen und gescheiterten Komponentenanmeldungen. Die Protokolldatei enthält IP-Adresse, Datum und Uhrzeit sowie das Ergebnis der Anmeldungen. **HINWEIS:** Wenn bei einer Integritätsprüfung eine nicht erfolgreiche Komponentenanmeldung angezeigt wird, enthält die **Ereignisanzeige** eine entsprechende Meldung. Klicken Sie auf **OK**. Korrigieren Sie die im Protokoll aufgezeigten Elemente manuell.

Manuelle Integritätsprüfung mit Control Expert

Gehen Sie wie folgt vor, um eine manuelle Integritätsprüfung durchzuführen, wenn eine Instanz von Control Expert gestartet wird:

Schritt	Aktion
1	Klicken Sie auf **Hilfe > Info...** in der Symbolleiste des Topology Manager.
2	Klicken Sie im Feld **Info** auf den Link **Selbsttest durchführen**. **Ergebnis**: Die Integritätsprüfung wird im Hintergrund durchgeführt. Die lokalen Client-Server (lokal oder dezentral), mit denen der Client verbunden ist, werden abgefragt. Der Client und die Server laufen weiter, bis das Ergebnis der Integritätsprüfung zurückgegeben wird. In der folgenden Tabelle finden Sie Informationen zu den Ergebnissen der Integritätsprüfung.

WENN	DANN
Keine Datenbeschädigung erkannt	Die Meldung „Selbsttest erfolgreich abgeschlossen“ wird angezeigt. Klicken Sie auf **OK**.
Datenbeschädigung auf dem Client erkannt	In einem Meldungsfeld werden die beschädigten Dateien ausgewiesen. Klicken Sie auf **OK**. Der Control Expert-Client wird geschlossen.
Datenbeschädigung auf einem der Server erkannt	Der Server wird angehalten. Es wird ein Fehler protokolliert, den Sie in der **Ereignisanzeige** prüfen können.

M580-Firmware-Integritätsprüfung

Die Integritätsprüfung der Firmware der M580-Steuerung wird automatisch nach einem neuen Firmware-Upload oder einem Neustart des Modicon M580 PAC durchgeführt.

Verwaltung der SD-Karte

Aktivieren Sie die Anwendungssignatur, um zu vermeiden, dass eine falsche Anwendung über eine SD-Karte ausgeführt wird.

Die Signatur der SD-Karte wird über die Funktionen `SIG_WRITE` und `SIG_CHECK` verwaltet (siehe *EcoStruxure™ Control Expert, Communication, Block Library*).

Konfigurieren des Schutzes des SD-Kartenanschlusses

Für Steuerungen mit einer Firmwareversion ab 4.30 ist ein SD-Kartenschutzmechanismus verfügbar.

Diese Funktion kann auf der Registerkarte **Konfiguration** auf den Webseiten der Steuerung aktiviert bzw. deaktiviert werden.

Gehen Sie vor wie folgt, um die Seite **Home** zu öffnen:

Schritt	Aktion
1	Öffnen Sie einen Webbrowser.
2	Geben Sie in der Adressleiste die IP-Adresse der Steuerung ein.
3	Geben Sie den Benutzernamen **modbususer** und das Anwendungspasswort ein.
4	Drücken Sie die **Eingabetaste** und warten Sie, bis die Seite geöffnet wird.
5	Wählen Sie **Konfiguration > Cybersicherheit** aus.
6	Wählen Sie in der Dropdown-Liste **SD-Kartenanschluss** aus, um diese Funktion zu konfigurieren: • **Aktiviert** (SD-Karten werden von der Steuerung nicht berücksichtigt). • **Deaktiviert** (SD-Karten werden von der Steuerung berücksichtigt). **HINWEIS:** Wenn bereits eine SD-Karte in die Steuerung eingesetzt ist, wird der Schutz aktiviert, wenn die SD-Karte entfernt oder die Steuerung aus- und wiedereingeschaltet wird. **HINWEIS:** Wenn der Schutz des SD-Kartenanschlusses aktiviert ist, ist NAND der Sicherungsspeicherbereich der Steuerung. Daher führt das Löschen des Sicherungsbereichs bei aktiviertem Schutz zum Löschen des NAND der Steuerung.

Konfiguration einer sicheren Engineering-Verbindung zwischen Control Expert und einer M580-Ethernet-Steuerung

Kompatibilität

- M580 PV < 25 (weiße Steuerungen) und PV >= 25 (graue Steuerungen).
- Control Expert Classic und Control Expert Topology Manager ab Version V16.0.
- M580-Firmware ab V4.20.
- Control Expert-Anwendung ab Version V4.20.

Zweck einer sicheren Verbindung

Mithilfe der oben genannten Software-, Hardware- und Anwendungsversionen können Sie eine sichere Verbindung zwischen Control Expert und einer M580-Ethernet-Steuerung konfigurieren. Diese Verbindung basiert auf dem TLS-Protokoll (Transport Layer Security) und bietet eine verschlüsselte End-to-End-Kommunikation.

Eine sichere Engineering-Verbindung schützt die M580-Steuerung vor Cyberangriffen durch:

- Steuerungsauthentifizierung auf der Grundlage eines selbstsignierten M580-Zertifikats.
- Verschlüsselung der Datenflüsse zwischen Control Expert und der M580-Steuerung.
- Control Expert-Clientauthentifizierung, indem ein Anmeldename/Passwort erforderlich ist, um den HTTPS-Tunnel einzurichten.

Eine sichere Verbindung schützt vor den folgenden Netzwerkangriffen:

- Replay-Angriffe.
- Passwortwiederherstellung (Hash).
- Wiederherstellung der Anwendungsbinärdateien.
- Man-in-the-middle-Angriffe (MITM), die Daten oder die Anwendung ändern können.

Merkmale einer sicheren Verbindung

Die folgenden Funktionen wurden dem **Sicherheitseditor**, der M580-Steuerungsfirmware und Control Expert hinzugefügt, um die Erstellung einer sicheren Engineering-Verbindung zu unterstützen:

- Sichere Kommunikationsprotokolltreiber, Seite 116
- Drei Engineering-Verbindungsmodi, Seite 116

Kommunikationsprotokolltreiber

HTTPS und **HTTPS über USB** sind neue Treiber, die sichere Engineering-Verbindungen unterstützen.

HINWEIS: Der Übersichtlichkeit halber wurden zwei bereits vorhandene Treiber umbenannt:

- **TCP IP** ist jetzt **Modbus TCP**.
- **USB** ist jetzt **Modbus TCP über USB**.

Engineering-Verbindungsmodi

Je nach Ebene der angestrebten Cybersicherheit können Sie einen der folgenden drei **Engineering-Verbindungsmodi** auswählen:

- **Vollständiger Zugriff**:

  Die Steuerung funktioniert wie in früheren Firmwareversionen. Sichere und nicht sichere Kommunikation werden akzeptiert.

  - Für die Control Expert-Kommunikation akzeptiert die Steuerung die nicht sicheren Treiber **Modbus TCP** und **Modbus TCP über USB** oder die sicheren Treiber **HTTPS** und **HTTPS über USB**.
  - Für die SCADA- oder Steuerung-zu-Steuerung-Kommunikation wird **Modbus TCP** (Port 502) akzeptiert.

- **Gefiltert** (Standard):

  Ein Hybridmodus, den Sie verwenden können, um Cybersicherheit auf die Engineering-Verbindung und nicht sichere Konnektivität auf Verbindungen zu SCADA oder anderen Steuerungen anzuwenden.

  - Für die Control Expert-Kommunikation akzeptiert die Steuerung die sicheren Treiber **HTTPS** und **HTTPS über USB**.
  - Für die SCADA- oder Steuerung-zu-Steuerung-Kommunikation werden **Modbus TCP** (Port 502) oder **UMAS** (OFS) akzeptiert.

    HINWEIS: Im Modus **Gefiltert** akzeptiert die Steuerung die nicht sicheren Treiber **Modbus TCP** und **Modbus TCP über USB**, jedoch nur, wenn der **Verbindungsmodus** in den Optionen des Projekts auf **Überwachung** eingestellt ist. Der Überwachungsmodus ist schreibgeschützt und es ist nicht möglich, eine Anwendung in die Steuerung herunterzuladen oder die Steuerung anzuhalten.

- **Erzwungen**:

  Dieser Modus bietet die höchste Sicherheitsebene. Nur sichere Protokolle werden von der Steuerung akzeptiert.

  - Für die Control Expert-Kommunikation akzeptiert die Steuerung nur die sicheren Treiber **HTTPS** und **HTTPS über USB**.
  - Für die SCADA- oder Steuerung-zu-Steuerung-Kommunikation werden **Modbus TCP** (Port 502) oder **UMAS** (OFS) **NICHT** akzeptiert.

HINWEIS: Die Zeit für den Download der Anwendung kann erheblich beeinflusst werden, wenn der Modus **Vollständiger Zugriff** konfiguriert ist und die sicheren Treiber **HTTPS** oder **HTTPS über USB** verwendet werden. Wenn Sie sichere Treiber verwenden möchten, sollten Sie den Modus **Gefiltert** oder **Erzwungen** in Betracht ziehen, um die Leistung nicht zu beeinträchtigen.

Zusammenfassung der Protokollverfügbarkeit

Jede Option für den **Engineering-Verbindungsmodus** unterstützt die folgenden Kombinationen aus logischem Port und Kommunikationsprotokoll:

Zweck der Verbindung:		**Sichere Engineering-Verbindung**	**Unsichere Engineering-Verbindung**		**HMI/SCADA**
Treiber:		**HTTPS** oder **HTTPS über USB**	**Modbus TCP** und **Modbus TCP über USB**		Modbus TCPIP oder UMAS
Logischer Kommunikationsport:		443	502		502
Verbindungsmodus:		**Überwachung** oder **Programmierung**	**Programmierung**	**Überwachung**	N/A
Engineering-Verbindungsmodus:	Erzwungen	✓	✗	✗	✗
	Gefilterte	✓	✗	✓	✓
	Vollständiger Zugriff	✓	✓	✓	✓

Zertifikat-Whitelist des Sicherheitseditors

Eine **Zertifikat-Whitelist** wird im **Sicherheitseditor** mit den folgenden Funktionen bereitgestellt:

- **Hinzufügen**: Verwenden Sie diesen Befehl, um die IP-Adresse der M580-Steuerung zu konfigurieren, auf der Sie eine sichere Engineering-Verbindung erstellen möchten.
- **Zertifikat abrufen**: Verwenden Sie diesen Befehl, um das HTTPS-Zertifikat aus dem Gerät abzurufen.
- Ein Dialogfeld, in dem Sie dem Zertifikat vertrauen und es dem Windows-Zertifikatspeicher hinzufügen können.
- **Zertifikat anzeigen**: Verwenden Sie diesen Befehl, um das Zertifikat anzuzeigen und zu überprüfen.
- **Entfernen**: Verwenden Sie diesen Befehl, um ein Zertifikat aus der Liste zu entfernen.

HINWEIS: In dieser Release werden nur selbstsignierte Zertifikate unterstützt.

Konfiguration einer sicheren Verbindung

Die Konfiguration der sicheren Engineering-Verbindung erfolgt mithilfe von Control Expert und dem Sicherheitseditor und anhand der nachfolgend beschriebenen Arbeitsschritte.

Vorab auszuführende Arbeitsschritte

1. Aktualisieren Sie Ihre Steuerung auf:
   a. V4.20 oder höher für Standardsteuerungen.
   b. V4.21 oder höher für Sicherheitssteuerungen.
2. Aktualisieren Sie Control Expert auf V16.0 oder höher.
3. Öffnen Sie ein vorhandenes Projekt und ändern Sie die Anwendungsebene in V4.20 oder höher, oder erstellen Sie ein neues Projekt mit der Anwendungsebene V4.20 oder höher.
4. Aktivieren Sie HTTPS, sofern deaktiviert, auf der Registerkarte „Sicherheit“ der Steuerung.
5. Wählen Sie eine Einstellung für den Engineering-Verbindungsmodus aus (siehe Engineering-Verbindungsmodi).
6. Konfigurieren Sie die endgültigen IP-Adresseinstellungen der M580-Ethernet-Steuerung, falls nicht bereits geschehen.

   HINWEIS: Da das Zertifikat einer M580-Steuerung ihre IP-Adresse enthält, erneuert die Steuerung jedes Mal ihr Zertifikat, wenn Sie die IP-Adresseinstellung ändern. Sie müssen dem Zertifikat im Sicherheitseditor jedes Mal erneut vertrauen.
7. Erstellen Sie ein Anwendungspasswort für das neue Projekt.
8. Erstellen Sie Firmware- und Webpasswörter für das neue Projekt.
9. Laden Sie die Anwendung über **Modbus TCP** oder **Modbus TCP über USB** in die Steuerung herunter.

Schritt 1: Festlegen des M580-Zertifikats als vertrauenswürdig im Sicherheitseditor

1. Öffnen Sie den Sicherheitseditor.
2. Konfigurieren Sie beim ersten Start des Sicherheitseditors ein Passwort für SecurityAdmin und warten Sie, bis der Sicherheitseditor die Installation abgeschlossen hat.
3. Melden Sie sich als SecurityAdmin mit dem konfigurierten Passwort an.

4. Wählen Sie **Zertifikat-Whitelist** aus.
5. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Verbindungskonfiguration hinzufügen** wird geöffnet.
6. Wählen Sie **HTTPS** oder **HTTPS über USB** als **Kommunikationsprotokoll** aus. Stellen Sie dann die **IP-Adresse** auf die konfigurierte IP-Adresse der Steuerung ein.
7. Klicken Sie auf **OK**.
8. Wählen Sie die Zeile aus, die der Steuerung entspricht.
9. Klicken Sie auf **Zertifikat vertrauen** und anschließend auf **Ja**, um es hinzuzufügen.

   Die Spalte mit dem Zertifikatstatus wird aktualisiert und zeigt Folgendes an:

   - Gültig: Das Zertifikat wurde erfolgreich hinzugefügt.
   - Unbekannt: Es wurde kein Zertifikat hinzugefügt. Verwenden Sie den Tooltip, um Details zu erkannten Fehlern anzuzeigen.
10. Wenn das Zertifikat gültig ist, klicken Sie auf das Auslassungszeichen (...), um den Gerätenamen und die Details anzuzeigen.

Schritt 2: Konfigurieren einer sicheren Verbindung

1. Wählen Sie **SPS > Adresse festlegen...** in Control Expert aus.
2. Geben Sie im SPS-Bereich entweder die IP-Adresse der M580-Steuerung oder SYS ein, wenn Sie ein USB-Kabel verwenden.
3. Wählen Sie im Bereich **Kommunikationsprotokoll** das Protokoll **HTTPS** oder **HTTPS über USB** aus.
4. Klicken Sie auf **OK**.
5. Wählen Sie in Control Expert **SPS > Verbinden** aus.
6. Geben Sie das Anwendungspasswort ein.

Hinweise zu Betriebsarten

Out-of-the-Box-Kommunikation

Beim ersten Start einer neuen M580-Steuerung „out-of-the-box“ gelten die folgenden Einschränkungen:

- Eine HTTPS-Verbindung zwischen Control Expert und der M580-Steuerung wird nicht unterstützt.

- Die Kommunikation ist nur über USB oder TCPIP möglich.

Zurücksetzen der M580-Steuerung auf NOCONF

Sie können Ihre M580-Steuerung wie folgt auf NOCONF (Keine Konfiguration) umschalten:

- Stellen Sie das Drehrad auf den Reset einer Hot Standby M580-Steuerung ein.
- Verwenden Sie eine SD-Karte wie folgt:
  1. Erstellen Sie eine Anwendung ohne Passwort.
  2. Laden Sie die Anwendung in eine andere M580-Steuerung mit derselben Referenz.
  3. Setzen Sie die SD-Karte in diese Steuerung ein.
  4. Setzen Sie %S66 auf TRUE, um die Anwendung auf der SD-Karte zu sichern.
  5. Setzen Sie die SD-Karte in die ursprüngliche M580-Steuerung ein und schalten Sie die Steuerung aus und wieder ein.

Zurücksetzen des Anwendungspassworts

Das Verfahren zum Zurücksetzen des Anwendungspassworts über den technischen Support ist weiterhin im **Engineering-Verbindungsmodus Gefiltert** und **Vollständiger Zugriff** verfügbar.

Eine Änderung des Passworts für Online-Änderungen wird unterstützt.

Kompatibilität und Einschränkungen der erzwungenen sicheren Programmierung

Kompatibilität

Siehe das Thema Konfigurieren einer sicheren Engineering-Verbindung zwischen Control Expert und einer M580-Ethernet-Steuerung, Seite 115.

Einschränkungen des Engineering-Verbindungsmodus

Für jede physische Verbindung gelten die folgenden Einschränkungen für die Option **Erzwungen** des **Engineering-Verbindungsmodus**:

- Die Datenwörterbuch-Funktion ist nicht funktionsfähig.
- BMENUA0100•• wird im erzwungenen Engineering-Verbindungsmodus nicht unterstützt.
- Führen Sie ein Upgrade auf M580 mit einer Produktversion (PV) ab 3 durch.
- Auf die Steuerung kann nicht über die folgenden Funktionsbausteine zugegriffen werden:
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH
  - READ_REMOTE
- Die Steuerung kann nicht von einem Modbus-Scanner abgefragt werden.
- Der Modbus-Scanner der M580-Steuerung kann Modbus-Geräte nicht abfragen.
- Je nach ausgewähltem Kommunikationsprotokoll (Modbus TCP oder EtherNet/IP) sind einige DTM-Diagnosedienste nicht verfügbar:

DTM-Dienste	Protokoll	Verfügbarkeit
EtherNet/IP-DTM-Verbindung	EtherNet/IP	✓
EtherNet/IP-DTM-Trennung	EtherNet/IP	✓
Modbus-DTM-Verbindung	Modbus TCP	✗
Modbus-DTM-Trennung	Modbus TCP	✗
Ethernet-Diagnose	EtherNet/IP	✓
Bandbreitendiagnose	Modbus TCP	✗
RSTP-Diagnose	Modbus TCP	✗
Netzwerkzeitdienst-Diagnose	EtherNet/IP	✓

Kompatibilität des Kommunikationsadapters

In der folgenden Tabelle sind die Dienste zusammengefasst, die je nach ausgewähltem Engineering-Modus mit einer Steuerung oder einem Kommunikationsadapter verfügbar sind.

Die Zeilen entsprechen den verfügbaren Diensten:

- Engineering-Verbindung: Die Verbindung zwischen Control Expert und Steuerung.
- Clientmodus-Kommunikation: Scanner, Modbus, EtherNet/IP (implizit oder explizit), OPC UA, DNP3, IEC 61850.
- Servermodus-Kommunikation: Modbus, EtherNet/IP, OPCUA, DNP3, IEC 61850.

Die Spalten entsprechen den verschiedenen möglichen Konfigurationen. Beispiel:

- Steuerung allein: Eine Steuerung wird ohne Kommunikationsadapter verwendet.
- Steuerung + NOC mit Baugruppenträger Ein: Eine Steuerung und ein BMENOC03•• sind im Hauptrack vorhanden; der Baugruppenträger-Port des BMENOC03•• ist aktiviert; Control Expert ist mit dem BMENOC03•• verbunden.
- Steuerung + NOC-Baugruppenträger Aus: Eine Steuerung und ein BMENOC03•• sind im Hauptrack vorhanden; der Baugruppenträger-Port des BMENOC03•• ist deaktiviert; Control Expert ist mit dem BMENOC03•• verbunden.

Wenn ein Kommunikationsadapter verwendet wird, sind einige Dienste auf dem Kommunikationsadapter selbst oder von der Steuerung über den Kommunikationsadapter verfügbar. Zur Unterscheidung dieser beiden Fälle werden die Buchstaben „S“ für Steuerung und „M“ für Modul verwendet. Beispiel:

- Wenn die Verbindung von Control Expert zur Steuerung über die IP-Adresse der Steuerung hergestellt werden kann, gilt der Buchstabe „S“.
- Wenn die Verbindung vom Control Expert über die IP-Adresse des BMENUA0100 hergestellt wird, gilt der Buchstabe „M“ in der Spalte, die sich auf das Modul bezieht.

Modicon M580-System		Steuerung allein			Steuerung + NOCs (NOC301, NOC311, NOC321			Steuerung + NOCs (NOC301, NOC311, NOC321			Steuerung + NOC321			Steuerung + NUA (Sicherheitsmodus)			Steuerung + BMXNOR			Steuerung + BMENOR			Steuerung + NOP			Steuerung + NOP		
Parameter des Kommunikations-adapters					Baugruppenträger-Port aktiviert			Baugruppenträger-Port deaktiviert			Baugruppenträger-Port deaktiviert IP-Weiterleitung			IP-Weiterleitung			Baugruppenträger potentialgetrennt			Baugruppenträger-Port deaktiviert			Baugruppenträger-Port aktiviert ohne IP-Weiterleitung			Baugruppenträger-Port deaktiviert IP-Weiterleitung		
Topologie																												
Sicherheitsmodus		🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒	🔓	🔑	🔒
Engineering-Verbindung	HTTPS	S	S	S	S	S	S	X	X	X	S	S	S	S* M	S* M	X	X	X	X	X	X	X	S	S	S	X	X	X
	Modbus TCP - Überwachung	S	S	X	S M	S M	X	S	S	X	S	S	X	S* M	S* M	X	M	M	X	M**	M**	X	S M	S M	X	M	M	X
	Modbus TCP - Programmierung	S	X	X	S M	X	X	S	X	X	S	X	X	S* M	X	X	M	X	X	M**	X	X	S M	X	X	M	X	X

Modicon M580-System		**Steuerung allein**			**Steuerung + NOCs (NOC301, NOC311, NOC321**			**Steuerung + NOCs (NOC301, NOC311, NOC321**			**Steuerung + NOC321**			**Steuerung + NUA (Sicherheitsmodus)**			**Steuerung + BMXNOR**			**Steuerung + BMENOR**			**Steuerung + NOP**			**Steuerung + NOP**		
Parameter des Kommunikations-adapters					**Baugruppenträger-Port aktiviert**			**Baugruppenträger-Port deaktiviert**			**Baugruppenträger-Port deaktiviert IP-Weiterleitung**			**IP-Weiterleitung**			**Baugruppenträger potentialgetrennt**			**Baugruppenträger-Port deaktiviert**			**Baugruppenträger-Port aktiviert ohne IP-Weiterleitung**			**Baugruppenträger-Port deaktiviert IP-Weiterleitung**		
Topologie																												
Sicherheitsmodus																												
Clientmodus	E/A-Scanner Modbus	S	S	X	S M	S M	M	M	M	M	S M	S M	M	S*	S*	X	-	-	-	-	-	-	S	S	X	-	-	-
	EIP-Scanner	S	S	S	S M	S M	S M	M	M	M	S M	S M	S M	S*	S*	S*	-	-	-	-	-	-	S	S	S	-	-	-
	EFB Modbus	S	S	X	S	S	X	S	S	X	S	S	X	S*	S*	X	S	S	X	S	S	X	S	S	X	S	S	X
	EFB EIP	S	S	S	S	S	S	S	S	S	S	S	S	S*	S*	S*	S	S	S	S	S	S	S	S	S	S	S	S
	EFB OPCUA	S	S	S	-	-	-	-	-	-	S	S	S	S*	S*	S*	-	-	-	-	-	-	S	S	S	S	S	S
	DNP3 IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X
Servermodus	Modbus-Server / UMAS	S	S	X	M	M	X	M	M	X	S	S	X	S* M-*	S* M*	X	M	M	X	M**	M**	X	S M	S M	X	M	M	X

Modicon M580-System		**Steuerung allein**			**Steuerung + NOCs (NOC301, NOC311, NOC321**			**Steuerung + NOCs (NOC301, NOC311, NOC321**			**Steuerung + NOC321**			**Steuerung + NUA (Sicherheitsmodus)**			**Steuerung + BMXNOR**			**Steuerung + BMENOR**			**Steuerung + NOP**			**Steuerung + NOP**		
Parameter des Kommunikations-adapters			**Baugruppenträger-Port aktiviert**			**Baugruppenträger-Port deaktiviert**			**Baugruppenträger-Port deaktiviert IP-Weiterleitung**			**IP-Weiterleitung**			**Baugruppenträger potentialgetrennt**			**Baugruppenträger-Port deaktiviert**			**Baugruppenträger-Port aktiviert ohne IP-Weiterleitung**			**Baugruppenträger-Port deaktiviert IP-Weiterleitung**		
Topologie																										
Sicherheitsmodus																										
SCADA-Kommunikation	OPCUA-Server	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	-	-	-	-	-	-	-	-	-	-	-	-
	EtherNet/IP-Adapter (Lokaler Server)	S	S	S	M	M	M	M	M	M	S M	S M	S M	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	HTTPS-Webserver der Steuerung	S	S	S	S	S	S	-	-	-	S	S	S	S*	S*	S*	-	-	-	-	-	-	S	S	S	-	-	-
	DNP3 - IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X

Symbol	Beschreibung
	Engineering-Verbindungsmodus eingestellt auf **Vollständiger Zugriff**
	Engineering-Verbindungsmodus eingestellt auf **Gefiltert**
	Engineering-Verbindungsmodus eingestellt auf **Erzwungen**
S	• Im Clientmodus zeigt „S“ an, dass die Kommunikation von der Steuerung initiiert wurde. • Im Servermodus gibt „S“ an, dass die Ziel-IP-Adresse die Steuerung ist.
M	• Im Clientmodus zeigt „M“ an, dass die Kommunikation vom Kommunikationsadapter initiiert wurde. • Im Servermodus gibt „M“ an, dass die Ziel-IP-Adresse der Kommunikationsadapter ist. In beiden Fällen kommuniziert das Modul über XBUS mit der Steuerung.
X	Nicht unterstützt
*	Abhängig von den im BMENUA0100-Modul konfigurierten Weiterleitungsregeln.
**	Wenn der Modbus-Server im BMENOR00200 aktiviert ist.
-	Nicht zutreffend

M580-Ethernet-Dienste und -Ports

In diesem Abschnitt werden die verfügbaren M580-Ethernet-Dienste und deren Standardstatus in der Control Expert-Anwendung vorgestellt.

„Out-of-Box“ entspricht der Konfiguration einer Steuerung ab Werk, auf der keine Anwendung installiert ist. Sobald eine Anwendung auf der Steuerung installiert wird, kann diese „Out-of-Box“-Konfiguration nicht mehr realisiert werden.

„Standard“ entspricht der Konfiguration einer Control Expert-Standardanwendung.

M580-Steuerungen mit Firmwareversion ≥ 4.10

Dienst	Portnummer	Out-of-Box	Standard	Bemerkungen
HTTP	80/tcp	Geschlossen	Geschlossen	Webserver
Modbus TCP	502/tcp	Offen	Offen	-
EtherNet/IP	44818/tcp-udp	Geschlossen	Geschlossen	EtherNet/IP Explizit (Klasse 3)
DHCP	67/udp	Geschlossen	Geschlossen	-
FTP	21/tcp	Offen	Geschlossen	Firmware, Datenspeicherung, FDR
TFTP	69/udp	Geschlossen	Geschlossen	FDR (X80)
SNMP	161/udp	Geschlossen	Geschlossen	-
EtherNet/IP	2222/udp	Geschlossen	Geschlossen	EtherNet/IP Implizit (Klasse 1)
NTP/SNTP	123/udp	Geschlossen	Geschlossen	NTPV4 oder SNTP

M580-Steuerungen mit Firmwareversion < 4.10

Dienst	Portnummer	Out-of-Box	Standard	Bemerkungen
HTTPS	443/tcp	Offen	Offen	Web, Firmware, Datenspeicherung
Modbus TCP	502/tcp	Offen	Offen	HINWEIS(1)
EtherNet/IP	44818/tcp-udp	Geschlossen	Geschlossen	EtherNet/IP Explizit (Klasse 3)
DHCP	67/udp	Geschlossen	Geschlossen	-
FTP	21/tcp	Geschlossen	Geschlossen	FDR

Dienst	Portnummer	Out-of-Box	Standard	Bemerkungen
TFTP	69/udp	Geschlossen	Geschlossen	FDR (X80)
SNMP	161/udp	Geschlossen	Geschlossen	-
EtherNet/IP	2222/udp	Geschlossen	Geschlossen	EtherNet/IP Implizit (Klasse 1)
NTP/SNTP	123/udp	Geschlossen	Geschlossen	NTPV4 oder SNTP
DPWS	9867/tcp	Offen	Offen	Firmwareaktualisierung, HINWEIS(1)
WS-Erkennung	3702/udp	Geschlossen	Geschlossen	Statussynchr. über SNMP

HINWEIS(1): Der Port und die zugehörigen Dienste sind für den Kunden von zentraler Bedeutung, um sicherzustellen, dass grundlegende Funktionen in der gewünschten industriellen Umgebung funktionsfähig sind. Der Port bleibt zu Sicherheits- und Verfügbarkeitszwecken offen. Benutzer können den Port nicht deaktivieren.

Cybersicherheit-Dienste pro System

Einführung

In diesem Kapitel werden die wichtigsten Cybersicherheit-Dienste aufgeführt, die für jedes System verfügbar sind. Darüber hinaus wird angegeben, wo Sie detaillierte Informationen in der Hilfe von Control Expert finden.

Cybersicherheit-Dienste

Überblick

Software, DTM oder Geräte sind Elemente, die Cybersicherheit-Dienste in einem globalen System bereitstellen. Die verfügbaren Cybersicherheit-Dienste werden für die folgenden Elemente aufgelistet:

- Control Expert-Software, Seite 131
- Modicon M340-Steuerung, Seite 131
- Modicon M580-Steuerung, Seite 132
- Modicon Quantum-Steuerung und Kommunikationsmodule, Seite 133
- Modicon X80-Module, Seite 134
- Modicon Premium/Atrium-Steuerung und Kommunikationsmodule, Seite 135
- Modicon Momentum MDI, Seite 137
- Modicon MC80, Seite 137

Die nachstehend aufgeführten Cybersicherheit-Dienste werden im vorherigen Kapitel beschrieben:

- Deaktivierung nicht verwendeter Dienste, Seite 32
- Zugriffskontrolle, Seite 33
- Einrichtung der verschlüsselten Kommunikation, Seite 36
- Ereignisprotokollierung, Seite 53
- Authentifizierung, Seite 101
- Berechtigungen, Seite 107
- Integritätsprüfungen, Seite 112

Cybersicherheit-Dienste in der Unity Pro/Control Expert-Software

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

Verfügbarkeit der Cybersicherheit-Dienste

Software	**Cybersicherheit-Dienste**							
Referenz	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Verschlüsselte Kommunikation mit Datenschutz**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
Unity Pro v8.1	–	N.A.	–	–	–	X	X	X
Unity Pro ≥ v10.0	–	N.A.	X	–	X	X	X	X
Unity Pro ≥ v13.0	–	N.A.	X	X	X	X	X	X
Control Expert ≥ v14.0	X	X	X	X	X	X	X	X

X Verfügbar, mindestens ein Dienst implementiert

– Nicht verfügbar

N.A. Nicht zutreffend

Bei Verwendung einer Version von Control Expert ab v.15.1 für Anwendungen mit M580-Firmwareversionen ab v4.01 stehen robustere Mechanismen zur Passwortwiederherstellung zur Verfügung.

Cybersicherheit-Dienste in der Modicon M340-Steuerung

Erforderliche Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in der Modicon M340-Steuerung:

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–

X Verfügbar, mindestens ein Dienst implementiert

– Nicht verfügbar

Cybersicherheit-Dienste in der Modicon M580-Steuerung

Erforderliche Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in der Modicon M580-Steuerung:

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
BME P58 5040	2.10	X	X	–	X	X	X	X
BME P58 6040	2.10	X	X	–	X	X	X	X

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
BME H58 2040	2.10	X	X	–	X	X	X	X
BME H58 4040	2.10	X	X	–	X	X	X	X
BME H58 6040	2.10	X	X	–	X	X	X	X
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Cybersicherheit-Dienste in Modicon Quantum-Steuerung und -Modulen

Erforderliche Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in der Modicon Quantum-Steuerung:

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
140CPU31110	3.20	–	–	–	–	X	X	–
140CPU43412•	3.20	–	–	–	–	X	X	–
140CPU53414•	3.20	–	–	–	–	X	X	–
140CPU651•0	3.20	X	X	–	–	X	X	–
140CPU65260	3.20	X	X	–	–	X	X	–
140CPU65860	3.20	X	X	–	–	X	X	–
140CPU67060	3.20	X	X	–	–	X	X	–
140CPU67160	3.20	X	X	–	–	X	X	–
140CPU6726•	3.20	X	X	–	–	X	X	–

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
140CPU67861	3.20	X	X	–	–	X	X	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Modicon Quantum-Module, die Cybersicherheit-Dienste unterstützen:

Modul		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
140NOC7710•	1.00	–	X	–	–	X	–	–
140NOC78000	2.00	X	X	–	–	X	–	–
140NOC78100	2.00	X	X	–	–	X	–	–
140NOE771••	X	X	–	–	–	X	–	–
140NWM10000	–	X	–	–	–	–	–	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Cybersicherheit-Dienste in Modicon X80-Modulen

Modicon X80-Module, die Cybersicherheit-Dienste unterstützen:

Modul		Cybersicherheit-Dienste							
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Verschlüsselte Kommunikation mit Datenschutz**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
BMECXM0100	1.01	X	X	–	–	X	–	–	X
BMENOC0301	1.01	X	X	X	–	X	X	–	X
BMENOC0311	1.01	X	X	X	–	X	X	–	X
BMXNOC0401.2	2.05	X	X	–	–	–	–	–	–
BMXNOE0100.2	2.90	X	X	–	–	–	–	–	–
BMXNOE0110.2	6.00	X	X	–	–	–	–	–	–
BMXPRA0100	2.60	X	X	–	–	–	X	–	–
BMENOC0301	2.11	X	X	X	X	X	X	–	X
BMENOC0311	2.11	X	X	X	X	X	X	–	X

X Verfügbar, mindestens ein Dienst implementiert

– Nicht verfügbar

Cybersicherheit-Dienste in Modicon Premium/Atrium-Steuerung und -Modulen

Erforderliche Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in der Modicon Premium/Atrium-Steuerung:

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
TSXH57•4M	3.10	–	–	–	–	X	X	–
TSXP570244M	3.10	–	–	–	–	X	X	–
TSXP57•04M	3.10	–	–	–	–	X	X	–
TSXP57•54M	3.10	–	–	–	–	X	X	–

Steuerung		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
TSXP571634M TSXP572634M TSXP573634M (über den ETY-Port)	3.10	X	X	–	–	X	X	–
TSXP574634M TSXP575634M TSXP576634M (integrierter Ethernet-Port)	3.10	X	X	–	–	X	X	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Modicon Premium/Atrium-Module, die Cybersicherheit-Dienste unterstützen:

Modul		Cybersicherheit-Dienste						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–
TSXETY5103	5.90	X	X	–	–	–	–	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Cybersicherheits-Dienste in Modicon Momentum MDI-Steuerung und -Modulen

Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in Modicon Momentum MDI:

Steuerung		**Cybersicherheit-Dienste**						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
171CBU78090	1.0	X	X	–	–	X	X	–
171CBU98090	1.0	X	X	–	–	X	X	–
171CBU98091	1.0	X	X	–	–	X	X	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Cybersicherheits-Dienste in Modicon MC80-Steuerung und -Modulen

Firmware-Mindestversion und Verfügbarkeit der Cybersicherheit-Dienste in Modicon MC80:

Steuerung		**Cybersicherheit-Dienste**						
Referenz	**Minimale Firmware**	**Deaktivierung nicht verwendeter Dienste**	**Zugriffskontrolle**	**Verschlüsselte Kommunikation**	**Ereignisprotokollierung**	**Authentifizierung**	**Berechtigungen**	**Integritätsprüfungen**
BMKC8020301	1.2	X	X	–	–	X	X	–
BMKC8020310	1.0	X	X	–	–	X	X	–
BMKC8030311	1.2	X	X	–	–	X	X	–
X Verfügbar, mindestens ein Dienst implementiert **–** Nicht verfügbar								

Modicon M340-Sicherheitsdienste

Überblick

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die Modicon M340-Steuerung finden Sie in verschiedenen Handbüchern, wie im folgenden Abschnitt angegeben.

Modicon M340-Steuerung mit integrierten Ethernet-Ports

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfigurationsparameter für den Nachrichtenaustausch* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).

Modicon M580-Sicherheitsdienste

Modicon M580-Steuerung

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie im Abschnitt mit einer Beschreibung der *Registerkarte „Sicherheit“* (siehe Modicon M580, Hardware, Referenzhandbuch).

Modicon Quantum-Sicherheitsdienste

Überblick

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die Modicon Quantum-Steuerung und die Ethernet-Module finden Sie in verschiedenen Handbüchern, wie in den folgenden Abschnitten angegeben.

Modicon Quantum-Steuerung mit integrierten Ethernet-Ports

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit (Aktivieren/Deaktivieren von HTTP, FTP und TFTP)* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt zur *Konfiguration der Nachrichtenübertragung für Steuerungen der Baureihe Modicon Quantum mit Control Expert Ethernet* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modul 140 NOC 771 0x

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit (Aktivieren/Deaktivieren von HTTP, FTP und TFTP)* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der Zugriffskontrolle* (siehe Quantum mit EcoStruxure™ Control Expert, 140 NOC 771 01 Ethernet-Kommunikationsmodul, Benutzerhandbuch).

Modul 140 NOC 780 00

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Quantum EIO, Steuerungsnetzwerk, Installations- und Konfigurationshandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der Zugriffskontrolle* (siehe Quantum EIO, Steuerungsnetzwerk, Installations- und Konfigurationshandbuch).

Modul 140 NOC 781 00

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Quantum EIO, Steuerungsnetzwerk, Installations- und Konfigurationshandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der Zugriffskontrolle* (siehe Quantum EIO, Steuerungsnetzwerk, Installations- und Konfigurationshandbuch).

Modul 140 NOE 771 xx

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit (Aktivieren/Deaktivieren von HTTP, FTP und TFTP)* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch), den Abschnitt *Sicherheit* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch) und den Abschnitt *Erstellen von HTTP- und Schreib-Passwörtern* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modul 140 NWM 100 00

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit (Aktivieren/Deaktivieren von HTTP, FTP und TFTP)* (siehe Quantum mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modicon X80-Sicherheitsdienste

Überblick

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die Modicon X80-Ethernet-Module finden Sie in verschiedenen Handbüchern, wie in den folgenden Abschnitten angegeben.

Modul BMXNOC0401.2

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der Zugriffskontrolle* (siehe Modicon M340-Ethernet-Kommunikationsmodul BMX NOC 0401, Benutzerhandbuch).

Module BMXNOE0100.2 und BMXNOE0110.2

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfigurationsparameter für den Nachrichtenaustausch* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).

Modul BMXPRA0100

Das BMXPRA0100-Modul ist als Modicon M340-Steuerung konfiguriert. Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfigurationsparameter für den Nachrichtenaustausch* (siehe Modicon M340 für Ethernet, Kommunikationsmodule und Prozessoren, Benutzerhandbuch).

Modul BMXNOR0200H

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* (siehe Modicon X80, BMXNOR0200H RTU-Modul, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfigurationsparameter für den Nachrichtenaustausch*.

Modul BMENOR2200H

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit*.
Zugriffskontrolle:	Siehe den Abschnitt *Konfigurationsparameter für den Nachrichtenaustausch*.

Modul BMECXM0100

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie im Kapitel *Konfiguration der Ethernet-Dienste* (siehe Modicon M580, BMECXM CANopen Module, Benutzerhandbuch).

Module BMENOC0301 and BMENOC0311

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie im Abschnitt *Konfiguration der Sicherheitsdienste* (siehe Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Kommunikationsmodul, Installations- und Konfigurationshandbuch).

Modul BMENUA0100

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet- Kommunikation:	Siehe den Abschnitt zu den Einstellungen der Cybersicherheit (siehe M580, BMENUA0100 Integriertes OPC UA-Modul, Installations- und Konfigurationshandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Zugriffskontrolle*.

Modicon Premium/Atrium-Sicherheitsdienste

Überblick

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die Modicon Premium/Atrium-Steuerung und die Ethernet-Module finden Sie in verschiedenen Handbüchern, wie in den folgenden Abschnitten angegeben.

Modicon Premium/Atrium-Steuerung mit integrierten Ethernet-Ports

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Konfigurationsparameter für den Sicherheitsdienst* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der TCP/IP-Nachrichtenübertragung (TSX P57 6634/5634/4634)* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modicon Premium/Atrium-Steuerung über ETY-Ports

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Konfigurationsparameter für den Sicherheitsdienst* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der TCP/IP-Nachrichtenübertragung* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modul TSX ETC 101.2

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Sicherheit* Nachrichtenübertragung (siehe Premium mit EcoStruxure™ Control Expert, TSX ETC 101 Ethernet-Kommunikationsmodul, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der Zugriffskontrolle* (siehe Premium mit EcoStruxure™ Control Expert, TSX ETC 101 Ethernet-Kommunikationsmodul, Benutzerhandbuch).

Modul TSX ETY x103

Eine Beschreibung der Kommunikationsparameter für Cybersicherheit finden Sie in den angegebenen Abschnitten:

Ethernet-Kommunikation:	Siehe den Abschnitt *Konfigurationsparameter für den Sicherheitsdienst* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).
Zugriffskontrolle:	Siehe den Abschnitt *Konfiguration der TCP/IP-Nachrichtenübertragung* (siehe Premium und Atrium mit EcoStruxure™ Control Expert, Ethernet Netzwerkmodule, Benutzerhandbuch).

Modicon Momentum MDI-Sicherheitsdienste

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die Modicon Momentum MDI-Steuerung finden Sie im *Momentum für EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Prozessoren - Benutzerhandbuch*.

Modicon MC80-Sicherheitsdienste

Eine Beschreibung der Einstellungen für die Kommunikationssicherheitsdienste für die MC80-Steuerung finden Sie im Abschnitt *Modicon MC80 Program Logic Controller (SPS), Benutzerhandbuch*.

Schutz der M580-, M340-, Momentum MDI- und MC80-Architektur mit EAGLE40 über VPN

Einführung

In diesem Kapitel wird erläutert, wie Sie den Schutz von Steuerungen vor Cyberangriffen erhöhen können, indem Sie ein Firewall-Gerät wie das EAGLE40-07 von Belden einsetzen, das für den Aufbau von VPN-Verbindungen konfiguriert ist. Der Einsatz solcher Geräte in einer Architektur kann dazu beitragen, bestehende Schwachstellen in den Geräten zu mitigieren und die Angriffsfläche verschiedener Produkte zu reduzieren.

Es hat sich als vorteilhaft erwiesen, das Netzwerk, die Workstations und die Geräte zu härten, wie im *Modicon Steuerungssysteme, Cybersicherheit, Benutzerhandbuch* beschrieben. Das Handbuch ist zum Download verfügbar unter: https://www.se.com/us/en/download/document/EIO0000002000/

EAGLE40-Firewall

Warum eine Firewall verwenden?

Die Nutzung einer Firewall zur Stärkung der Cybersicherheit einer bestehenden Architektur bietet die folgenden Vorteile:

- Die Cybersicherheit von Steuerungsnetzwerken und -geräten wird verstärkt.
- Erhöhte Cybersicherheit beruht auf dem IPSEC-Protokoll.
- Auswirkungen auf die bestehende Architektur und die Leistung können minimiert werden.

Hauptmerkmale von EAGLE40

Die EAGLE40-Firewall ist eine Lösung zur Beseitigung bzw. Begrenzung von Cybersicherheits-Restproblemen.

- Über ein leistungsstarkes IPSEC-VPN gewährleistet die EAGLE40-Firewall die erwartete Vertraulichkeit für den Netzwerkverkehr und verhindert *Man-in-the-Middle*-Angriffe. Sie stellt die Authentifizierung des Senders sicher und verhindert dadurch Spoofing-Angriffe. Die Nachrichtenintegrität wird durch kryptografische Methoden gefestigt und kann nicht manipuliert werden.
- Übliche Filterfunktionen stehen zur Verfügung, mit denen Sie den Datenverkehr und die Protokolle basierend auf IP, Mac-Adresse und Port der Netzwerkgeräte kontrollieren können.
- Die EAGLE40-Firewall ist ein skalierbares Produkt, das in Mehrpunktarchitekturen integriert werden kann. Die Leistung in Bezug auf Baudrate und Bandbreite trägt zur Gewährleistung der Netzwerktransparenz bei.

Voraussetzungen

Softwareinstallation

Eine kompatible VPN-Client-Software ist erforderlich, um einen VPN-Tunnel auf der Grundlage des IPSEC-Protokolls zwischen Client und Firewall einzurichten.

Für die EAGLE40-Firewall muss der VPN-Client IPSEC/IKEV2 verwendet werden.

HINWEIS: Verwenden Sie die VPN-Client-Lösung von TheGreenBow.

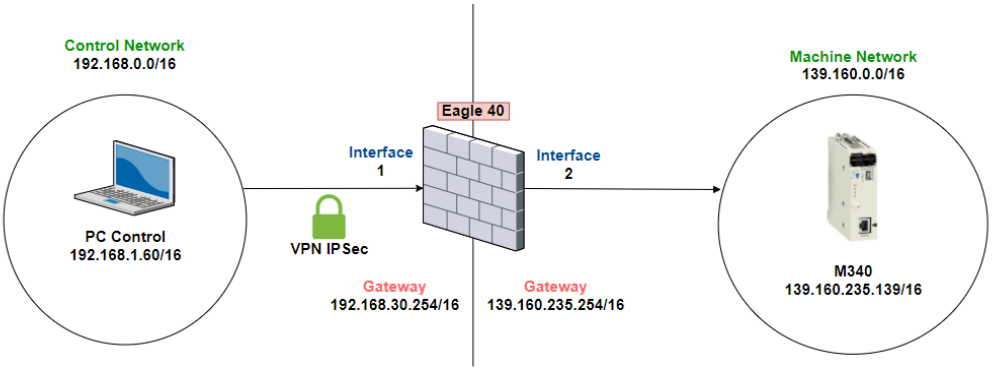
In den nachfolgend beschriebenen Konfigurationsverfahren wird diese Software verwendet, die Sie von folgender Adresse herunterladen können:

https://www.thegreenbow.com/en/

Maschinen und Betriebssysteme

Vor der Konfiguration der Firewall müssen Sie alle in den Architekturen verwendeten IP-Adressen vorbereiten.

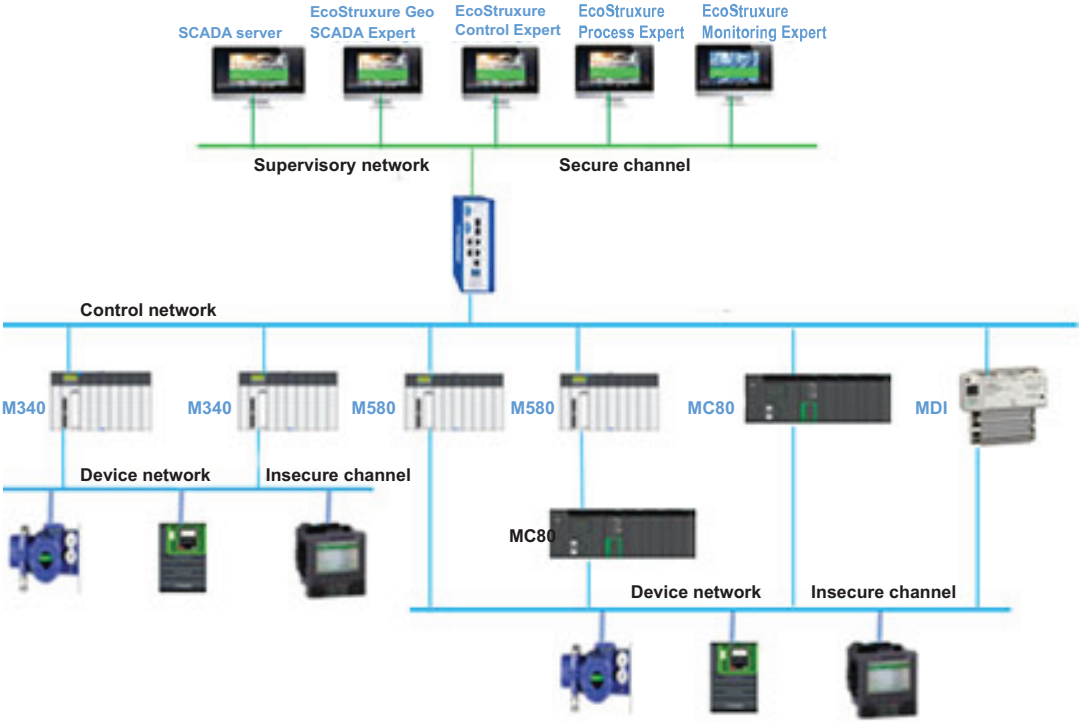
Die folgende Abbildung zeigt ein Beispiel:



Typische Architektur

Die Architektur- und Konfigurationsanweisungen in diesem Dokument dienen als Beispiele und können an verschiedene Architekturen und Systeme angepasst werden.

Die folgende gemischte Architektur, die Steuerungen der Baureihen Modicon M340, M580, Momentum MDI und MC80 kombiniert, ist ein typisches Beispiel für eine Architektur:



HINWEIS: Installieren Sie eine EAGLE40-Firewall in der Nähe der Steuerungen.

Konfiguration der Firewall

Webkonfiguration

Um die Firewall zu konfigurieren, öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

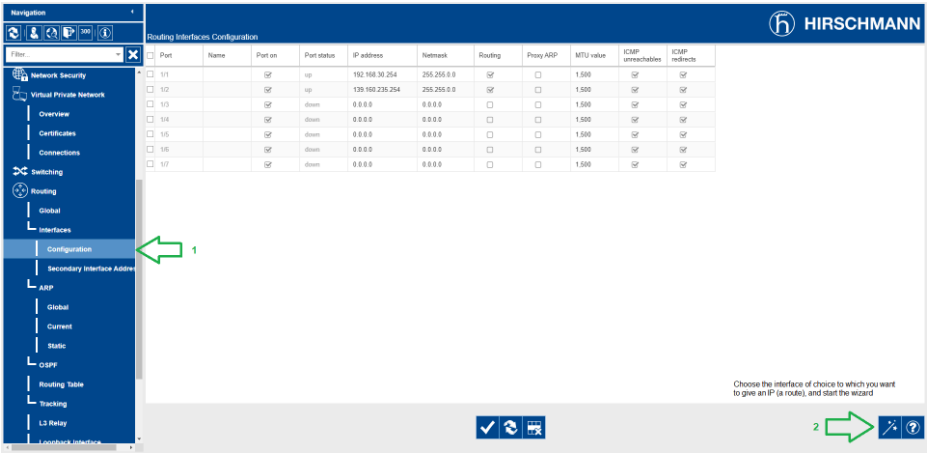
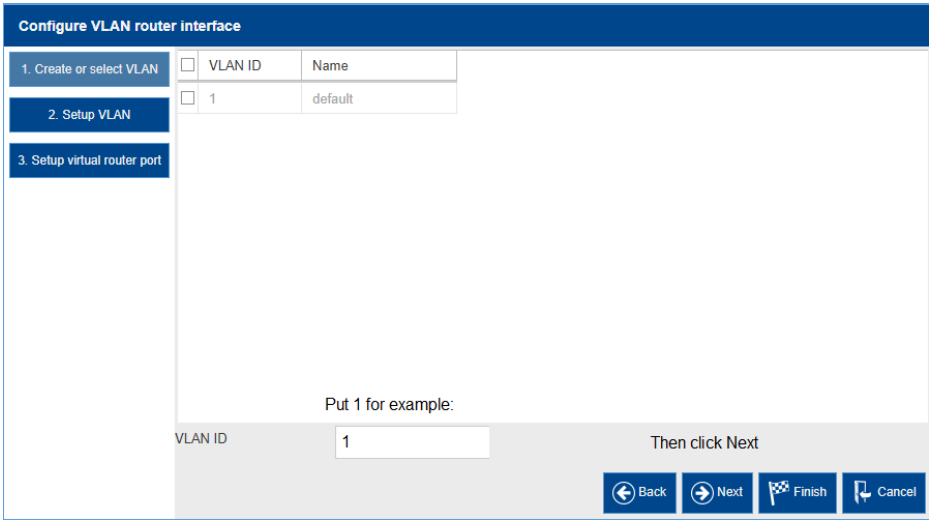
```
https://[IPFirewall]/admin
```

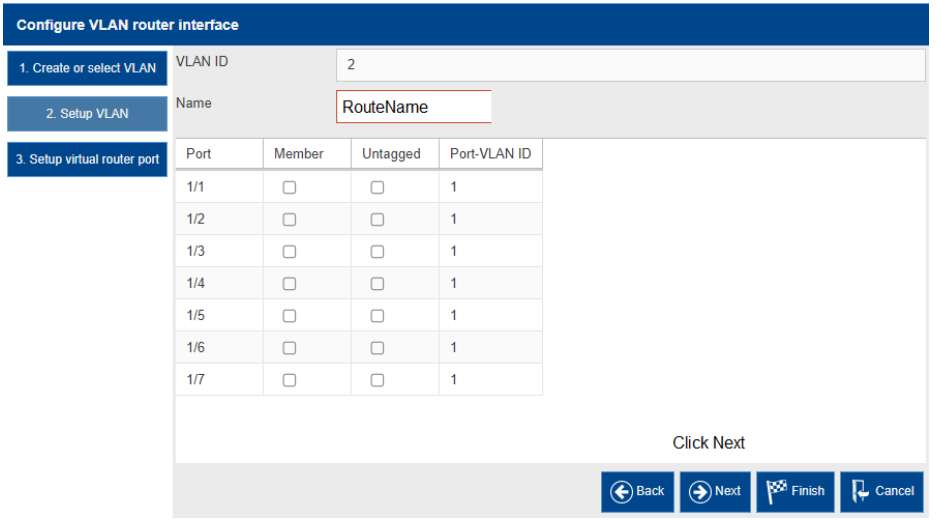
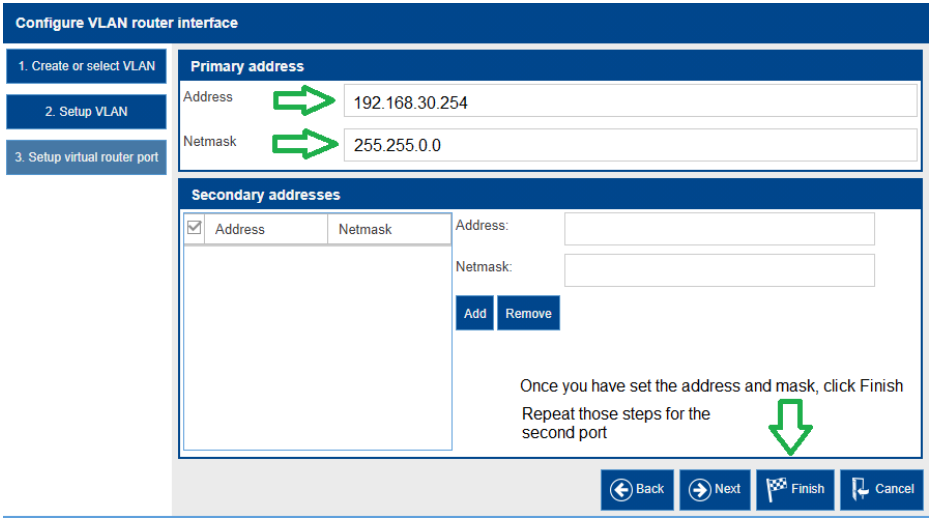
Drücken Sie die **Eingabetaste** und verwenden Sie die Standardkombination aus Benutzername und Passwort `admin/private`, um sich anzumelden.

HINWEIS: Bei der ersten Anmeldung müssen Sie das Passwort ändern.

Konfigurieren der Routen

Gehen Sie zur Konfiguration der Routen wie folgt vor:

Schritt	Aktion
1	 **1.** Öffnen Sie im linken Fensterbereich **Navigation** die Webseite **Routing > Interfaces > Configuration**. Wählen Sie die Ethernet-Schnittstelle aus, die Sie konfigurieren möchten. **2.** Klicken Sie auf das Symbol  , um das Fenster **Configure VLAN Router Interface** zu öffnen.
2	Legen Sie eine ID-Nummer für das VLAN fest, das Sie konfigurieren möchten (in diesem Beispiel 1), und klicken Sie dann auf **Next**. 

Schritt	Aktion
3	Legen Sie einen Routennamen für das VLAN fest, das Sie konfigurieren möchten (RouteName in diesem Beispiel), und klicken Sie dann auf **Next**. 
4	Legen Sie die IP-Adresse des Steuerungsnetzwerks und dessen Maske fest (`192.168.30.254/16` in diesem Beispiel), und klicken Sie dann auf **Finish**. 
5	Wiederholen Sie die Schritte 1 bis 4 für das Maschinennetzwerk mit der zweiten Ethernet-Schnittstelle.

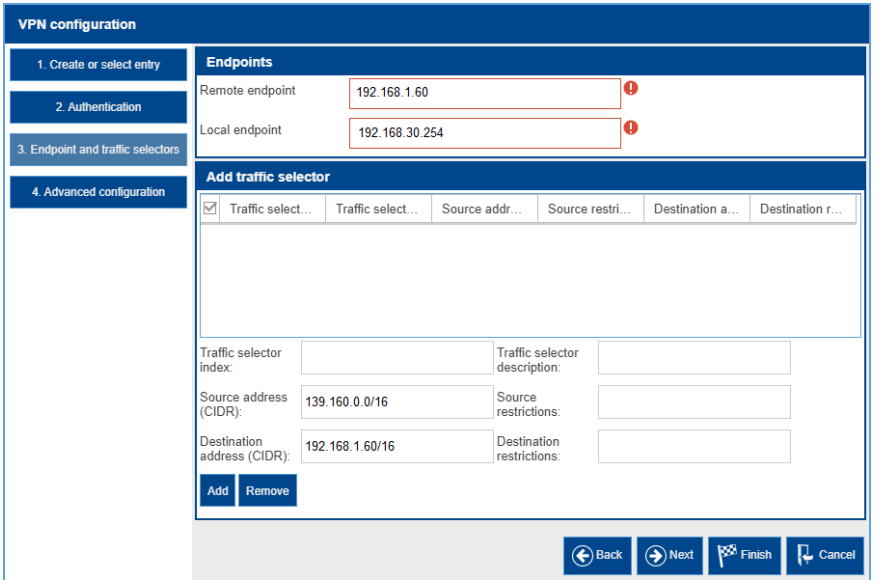
Im folgenden Beispiel wurde die Gateway-Schnittstelle für das Steuerungsnetzwerk der Firewall auf `192.168.30.254/16` am ersten physischen Port und für das Maschinennetzwerk auf `139.160.235.254/16` am zweiten physischen Port eingestellt.

Port	Name	Port on	Port status	IP address	Netmask	Routing	Proxy ARP	MTU value	ICMP unreachables	ICMP redirects
1/1		☑	up	192.168.30.254	255.255.0.0	☑	☐	1,500	☑	☑
1/2		☑	up	139.160.235.254	255.255.0.0	☑	☐	1,500	☑	☑
1/3		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/4		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/5		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/6		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/7		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑

Konfigurieren des VPN in der Firewall

Gehen Sie zur Konfiguration des VPN wie folgt vor:

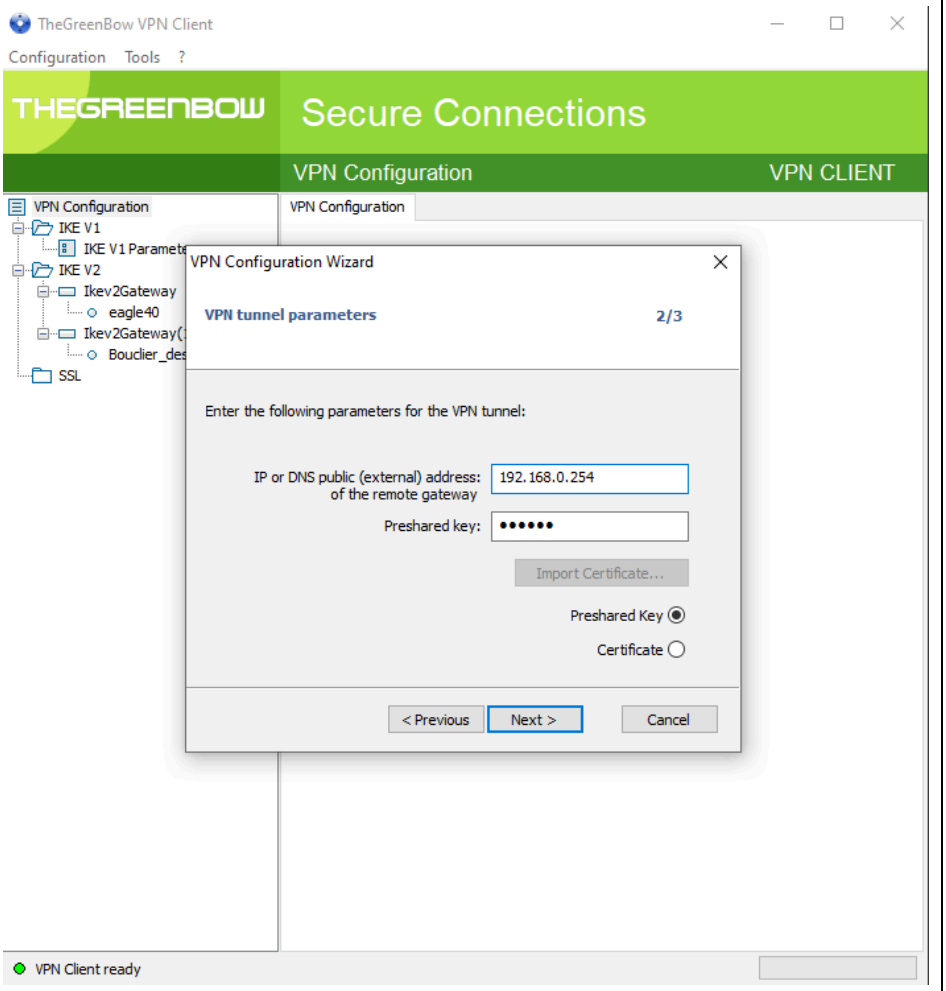
Schritt	Aktion
1	Klicken Sie am linken Rand der Webseite auf das Menü **Virtual Private Network > Connections**. Klicken Sie auf das Symbol  .
2	Wählen Sie eine Indexnummer und einen Namen aus und klicken Sie dann auf **Next**.
3	Wählen Sie ein Passwort (PSK) aus und klicken Sie dann auf **Next**.

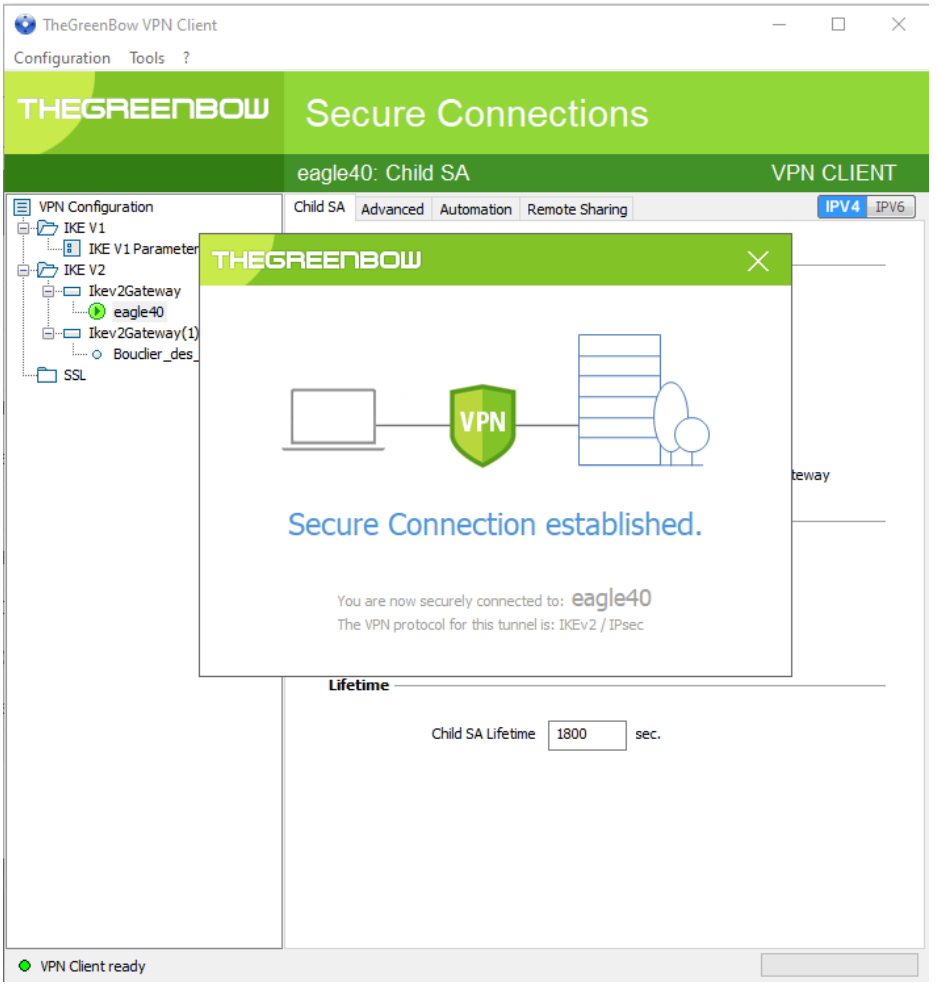
Schritt	Aktion
4	Füllen Sie die IP-Adressen und Masken entsprechend Ihrem Netzwerk aus. • **Remote endpoint**: Der Computer, der sich über ein VPN mit der Firewall verbindet. • **Local endpoint**: Das in den Routen konfigurierte Gateway. • **Source address (CIDR)**: Auf das geschützte Maschinennetzwerk kann nur zugegriffen werden, wenn eine Verbindung über ein VPN hergestellt wurde. • **Destination address (CIDR)**: Der Computer, der sich über ein VPN mit der Firewall verbindet.  Klicken Sie auf **Next**.
5	Legen Sie eine Zeitspanne fest. Der Standardwert ist 150. Stellen Sie **IKE Version** auf ikev2 ein und klicken Sie dann auf **Finish**.

Konfigurieren des VPN-Clients

HINWEIS: Im vorliegenden wird die VPN-Client-Lösung von TheGreenBow verwendet. Gehen Sie zur Konfiguration des VPN-Clients wie folgt vor:

Schritt	Aktion
1	Laden Sie die VPN-Client-Software herunter und installieren Sie sie.
2	Rechtsklicken Sie im linken Bereich des VPN-Client-Fensters auf **VPN Configuration** und wählen Sie **Wizard** aus.

Schritt	Aktion
3	Wählen Sie **IKEv2 Tunnel** aus und klicken Sie auf **Next**.
4	Legen Sie die IP-Adresse der Firewall fest, auf die über die Schnittstelle des Steuerungsnetzwerks zugegriffen werden kann (in diesem Beispiel 192.168.0.254). Geben Sie den zuvor ausgewählten PSK ein.  Klicken Sie auf **Next** und anschließend auf **Finish**.

Schritt	Aktion
5	Rechtsklicken Sie im linken Bereich des VPN-Client-Fensters auf den gerade erstellten Ikev2-Tunnel und benennen Sie ihn um.
6	Rechtsklicken Sie auf den gerade umbenannten Ikev2-Tunnel und wählen Sie **Open Tunnel** aus. Eine Benachrichtigung bestätigt, dass die sichere Verbindung hergestellt wurde. 

Glossar

802.1Q:

IEEE-Protokoll-Bezeichner für VLAN (Virtual Local Area Network). Dieser Standard ermöglicht die VLAN-Identifikation und stellt QoS-Ebenen (Quality of Service / Dienstgüte) bereit.

A

Adapter:

Ein Adapter ist das Ziel von E/A-Echtzeitdaten-Verbindungsrequests von Scannern. Er kann keine E/A-Echtzeitdaten senden oder empfangen, sofern er hierfür nicht von einem Scanner konfiguriert wurde. Zudem übernimmt er weder die Speicherung noch die Erstellung von Kommunikationsparametern, die zur Herstellung der Verbindung erforderlich sind. Ein Adapter akzeptiert Requests für explizite Nachrichten (verbunden und nicht verbunden) von anderen Geräten.

Anwendungsbasierte Zeitstempelung:

Verwenden Sie die anwendungsbasierte Zeitstempellösung, um mit einem SCADA-System, das die OPC DA-Schnittstelle nicht unterstützt, auf Zeitstempel-Ereignisspuffer zuzugreifen. In diesem Fall lesen die Funktionsbausteine in der Control Expert-Anwendung die Ereignisse im Puffer und formatieren diese Ereignisse zum Senden an das SCADA-System.

Architektur:

Die Architektur beschreibt ein Rahmenwerk für die Spezifikation eines Netzwerks, das aus folgenden Komponenten aufgebaut ist:

- Physische Komponenten und deren Organisation und Konfiguration
- Funktionsprinzipien und Verfahren
- Für den Betrieb verwendete Datenformate

ARRAY:

Unter `ARRAY` versteht man eine Tabelle mit Elementen, die denselben Typ aufweisen. Hierbei gilt folgende Syntax: `ARRAY [<Grenzwerte>] OF <Typ>`

Beispiel: `ARRAY [1..2] OF BOOL` ist eine eindimensionale Tabelle, die zwei Elemente vom Typ `BOOL` enthält.

`ARRAY [1..10, 1..20] OF INT` ist eine zweidimensionale Tabelle, die 10 x 20 Elemente vom Typ `INT` enthält.

ART:

(*Application Response Time*: Antwortzeit der Anwendung) Die Zeit, die eine Steuerungsanwendung benötigt, um auf einen bestimmten Eingang zu reagieren. Die ART entspricht dem Zeitraum, der zwischen der Aktivierung eines physischen Signals in der Steuerung und der Auslösung eines Schreibbefehls und der anschließenden Aktivierung des dezentralen Ausgangs liegt, die den Empfang der Daten signalisiert.

AUX:

Eine (AUX-) Task ist eine optionale, periodische Prozessortask, die über die Programmiersoftware des Prozessors gesteuert wird. Die AUX-Task dient der Ausführung eines Teils der Anwendung, für den eine niedrige Priorität ausreichend ist. Diese Task wird nur dann ausgeführt, wenn für die MAST- und FAST-Task keine Ausführung ansteht. Die AUX-Task besteht aus zwei Sections:

- IN: Vor der Ausführung der AUX-Task werden die Eingänge in den Abschnitt IN kopiert.
- OUT: Nach der Ausführung der AUX-Task werden die Ausgänge in die OUT-Section kopiert.

B

BCD:

(*Binary-Coded Decimal*) Binärkodierung von Dezimalzahlen.

Betriebsbereites Gerät:

Betriebsbereite Ethernet-Geräte stellen zusätzliche Dienste für EtherNet/IP- oder Modbus-Module bereit, z. B.: Einfache Parametereingabe, Bus-Editor-Deklaration, Systemübertragung, Warnmeldungen bei Änderungen und gemeinsam genutzte Benutzerrechte zwischen Control Expert und dem Geräte-DTM.

Betriebsnetzwerk:

Ein Ethernet-basiertes Netzwerk mit Bedienertools (SCADA, Client-PC, Drucker, Batch-Tools, EMS usw.). Die Steuerungen sind direkt oder per Routing über das steuerungsübergreifende Netzwerk miteinander verbunden. Dieses Netzwerk ist Teil des Steuerungsnetzwerks.

BOOL:

(*Boolean*) Der Typ Boolesch ist der Basisdatentyp bei der Datenverarbeitung. Eine Variable vom Typ `BOOL` besitzt einen der folgenden Werte: 0 (`FALSE`) oder 1 (`TRUE`).

Ein aus einem Wort extrahiertes Bit ist vom Typ `BOOL`. Beispiel: `%MW10.4`.

BOOTP:

(*bootstrap protocol*) Ein UDP-Netzwerkprotokoll, das von einem Netzwerk-Client verwendet werden kann, um von einem Server automatisch eine IP-Adresse zu erhalten. Der Client identifiziert sich beim Server mit seiner MAC-Adresse. Der Server, der eine vorkonfigurierte Tabelle der MAC-Adressen des Client-Geräts und der zugeordneten IP-Adressen speichert, sendet dem Client seine definierte IP-Adresse. Der BOOTP-Dienst nutzt die UDP-Ports 67 und 68.

Broadcast:

Eine an alle Geräte in einer Broadcast-Domain gesendet Nachricht.

C

CCOTF:

(*Change Configuration On The Fly*) CCOTF ist eine Control Expert-Funktion, die eine Änderung der Modulhardware in der Systemkonfiguration bei laufendem Systembetrieb ermöglicht, ohne andere aktive Vorgänge zu beeinträchtigen.

CIP™:

(*Common Industrial Protocol*) Eine umfassende Reihe von Meldungen und Diensten für die verschiedenen Anwendungen im Bereich der Fertigungsautomatisierung (Steuerung, Sicherheit, Synchronisation, Bewegung, Konfiguration und Information). CIP ermöglicht Benutzern die Integration dieser Produktionsanwendungen in die Ethernet-Netzwerke von Unternehmen und im Internet. CIP bezeichnet das Kernprotokoll von EtherNet/IP.

CPU:

(*Central Processing Unit*) Die CPU, auch als Prozessor oder Steuerung bezeichnet, ist das Gehirn eines industriellen Fertigungsprozesses. Im Gegensatz zu Relaisregelungssystemen automatisiert sie einen Prozess. PACs sind Computer, die rauen Betriebsbedingungen in industriellen Umgebungen standhalten.

D

DDT:

(*Derived Data Type*) Ein abgeleiteter Datentyp beinhaltet mehrere Elemente desselben Typs (`ARRAY`) oder verschiedener Typen (Struktur).

Determinismus:

Für eine vorgegebene Anwendung oder Architektur können Sie vorhersagen, dass es sich bei der Zeit zwischen einem Ereignis (Änderung des Werts einer Eingabe) und der entsprechenden Änderung eines Steuerungsausgangs um eine endliche Zeit *t* handelt, die die für den Prozess erforderliche Zeit nicht überschreitet.

Device DDT (DDDT):

Ein Geräte-DDT ist ein vom Hersteller vordefinierter DDT, der vom Benutzer nicht geändert werden kann. Er enthält die E/A-Sprachelemente eines E/A-Moduls.

DFB:

(*Derived Function Block*) DFB-Typen sind Funktionsbausteine, die vom Benutzer in den Sprachen ST, IL, LD oder FBD programmiert werden können.

Der Einsatz dieser DFB-Typen in Anwendungen ermöglicht Folgendes:

- den Entwurf und das Schreiben des Programms zu vereinfachen
- Verbesserung der Lesbarkeit des Programms
- Leichtere Ausführung der Debugging-Funktion
- Reduzierung der Menge des generierten Codes

DHCP:

(*Dynamic Host Configuration Protocol; dynamisches Hostkonfigurationsprotokoll*) Eine Erweiterung des BOOTP-Kommunikationsprotokolls, das die automatische Zuweisung von IP-Adresseinstellungen, wie IP-Adresse, Subnetzmaske, Gateway-IP-Adresse und DNS-Servernamen, ermöglicht. DHCP erfordert keine Tabelle zur Identifizierung aller Netzwerkgeräte. Der Client identifiziert sich gegenüber dem DHCP-Server entweder durch seine MAC-Adresse oder durch eine eindeutige zugewiesene Gerätekennung. Der DHCP-Dienst nutzt die UDP-Ports 67 und 68.

DIO-Cloud:

Eine Gruppe verteilter Geräte, die RSTP nicht unterstützen müssen. DIO-Clouds benötigen nur eine einzige (nicht ringförmige) Kupferdrahtverbindung. Sie können mit Kupferports an DRSs oder direkt mit der Steuerung oder mit Ethernet-Kommunikationsmodule im *lokalen Rack* verbunden werden. DIO-Clouds **können nicht** mit *Teilringen* verbunden werden.

DIO-Netzwerk:

Ein Netzwerk mit verteilten Geräten, in dem die E/A von einer Steuerung mit DIO-Abfragedienst im lokalen Rack abgefragt werden. Der DIO-Netzwerkverkehr erfolgt nach dem RIO-Datenverkehr, der in einem RIO-Netzwerk Priorität erhält.

DIO:

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

DNS:

(*Domain Name Server/Service*) Ein Dienst, der einen alphanumerischen Domänennamen in eine IP-Adresse überträgt, die eindeutige Kennung eines Geräts im Netzwerk.

Domänenname:

Eine alphanumerische Zeichenfolge, die ein Gerät im Internet identifiziert und als primäre Komponente der URL (Uniform Resource Locator) einer Website erscheint. So ist der Domänenname *schneider-electric.com* beispielsweise die primäre Komponente des URL *www.se.com*.

Jeder Domänenname wird als Teil des Domain Name System (DNS) zugewiesen und ist mit einer IP-Adresse verknüpft.

Auch als Hostname bezeichnet.

DRS:

(*Dual-Ring-Switch*) Erweiterter, verwalteter ConneXium-Switch, der für den Betrieb in einem Ethernet-Netzwerk konfiguriert wurde. Schneider Electric stellt vordefinierte Konfigurationsdateien bereit, die in einen DRS heruntergeladen werden können und Unterstützung für die spezifischen Funktionen einer Hauptring-/Teilring-Architektur bieten.

DSCP:

(*Differentiated Service Code Points*) 6-Bit-Feld, das als Header in einem IP-Datenpaket fungiert und eine Klassifizierung und Priorisierung des Verkehrs ermöglicht.

DT:

(*Date and Time*) Der `DT`-Typ für Datum und Uhrzeit wird in BCD im 64-Bit-Format kodiert und enthält die folgenden Informationen:

- Das Jahr in einem Feld von 16 Bits
- Den Monat in einem Feld von 8 Bits
- Den Tag in einem Feld von 8 Bits
- Die Uhrzeit in einem Feld von 8 Bits
- Die Minuten in einem Feld von 8 Bits
- Die Sekunden in einem Feld von 8 Bits

HINWEIS: Die acht niederwertigsten Bits (LSBs, Least Significant Bits) werden nicht verwendet.

Der `DT`-Typ wird in folgendem Format eingegeben:

`DT#``<Jahr>`**`-`**`<Monat>`**`-`**`<Tag>`**`-`**`<Stunden>`**`:`**`<Minuten>`**`:`**`<Sekunden>`

Die folgende Tabelle zeigt die Wertebereiche der einzelnen Felder:

Feld	Grenzwerte	Kommentar
Jahr	[1990,2099]	Jahr
Monat	[01,12]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.
Tag	[01,31]	Für die Monate 01/03/05/07/08/10/12
	[01,30]	Für die Monate 04/06/09/11
	[01,29]	Für den Monat 02 (Schaltjahr)
	[01,28]	Für den Monat 02 (kein Schaltjahr)
Stunde	[00,23]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.
Minute	[00,59]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.
Zweites	[00,59]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.

DTM:

(*Device Type Manager*) Ein DTM ist ein Gerätetreiber, der auf einem Host-PC ausgeführt wird . Er stellt eine vereinheitlichte Struktur für den Zugriff auf Geräteparameter, für die Konfiguration und den Betrieb der Geräte sowie für die Fehlerbehebung bereit. Bei DTMs kann es sich um einfache grafische Benutzeroberflächen zur Einstellung von Geräteparametern bis hin zu hoch entwickelten Anwendungen handeln, die komplexe Echtzeitberechnungen zu Diagnose- und Wartungszwecken durchführen können. Im Zusammenhang mit einem DTM kann ein Gerät ein Kommunikationsmodul oder ein dezentrales Gerät im Netzwerk sein.

Siehe FDT.

E

E/A-Abfragegerät:

Ethernet-Dienst, der kontinuierlich E/A-Module abfragt, um Daten, Status, Ereignisse und Diagnoseinformationen abzurufen. Bei diesem Vorgang werden Eingänge überwacht und Ausgänge gesteuert. Dieser Dienst unterstützt sowohl die RIO- als auch die DIO-Logikabfrage.

EDS:

(*Electronic Data Sheet; elektronisches Datenblatt*) Bei einem EDS handelt es sich um eine einfache Textdatei, in der die Konfigurationsmöglichkeiten eines Geräts beschrieben sind. EDS-Dateien werden vom Hersteller des Geräts erstellt und gepflegt.

EFB:

(*Elementarer Funktionsbaustein*) Es handelt sich um einen Baustein, der in einem Programm verwendet wird und dort eine vordefinierte Funktion ausführt.

Ein EFB verfügt über einen Status und interne Parameter. Folglich können die Ausgangswerte auch bei identischen Eingängen verschieden sein. Beispielsweise verfügt ein Zähler über einen Ausgang, der anzeigt, dass ein vorgegebener Wert erreicht wurde. Dieser Ausgang wird auf 1 gesetzt, sobald der Wert dem vordefinierten Wert entspricht.

EF:

Elementarfunktion) Es handelt sich um einen Baustein, der in einem Programm verwendet wird und dort eine vordefinierte Funktion ausführt.

Eine Funktion besitzt keine Informationen zum internen Status. Mehrere Aufrufe der gleichen Funktion unter Verwendung der gleichen Eingangsparameter führen zur Rückgabe der gleichen Ausgangswerte. Informationen zur grafischen Form des Funktionsaufrufs finden Sie unter [*Funktionsbaustein (Instanz)*]. Im Gegensatz zum Aufruf eines Funktionsbausteins enthalten die Funktionsaufrufe lediglich einen unbenannten Ausgang, dessen Name mit dem Namen der Funktion identisch ist. In FBD wird jeder Aufruf mithilfe des Grafikbausteins anhand einer eindeutigen [Nummer] gekennzeichnet. Diese Nummer wird automatisch verwaltet und kann nicht geändert werden.

Positionieren und konfigurieren Sie diese Funktionen in Ihrem Programm für eine bedarfsgerechte Ausführung Ihrer Anwendung.

Mithilfe des Software Development Kits (SDKC) können auch andere Funktionen entwickelt werden.

Einfache Prioritätsverkettungsschleife:

Häufig auch als SDCL (Simple Daisy Chain Loop) bezeichnet. Eine einfache Prioritätsverkettungsschleife enthält ausschließlich RIO-Module (keine verteilten Geräte) Diese Topologie besteht aus einem lokalen Rack (mit einer Steuerung mit Ethernet-E/A-Abfragedienst) und einer oder mehreren RIO-Stationen (jede Station enthält ein RIO-Adaptermodul).

EIO-Netzwerk:

(Ethernet-E/A) Ein Ethernet-basiertes Netzwerk, das drei Gerätetypen umfasst:

- Lokales Rack
- Dezentrale X80-Station (mit einem BM•CRA312•0-Adaptermodul) oder BMENOS0300-Schaltmodul für Netzwerkoptionen
- Erweiterter ConneXium-Dual-Ring-Switch (DRS)

  HINWEIS: Auch verteilte Geräte können über eine Verbindung zu DRSs oder dem Service-Port dezentraler X80-Module an einem Ethernet-E/A-Netzwerk teilnehmen.

EN:

EN bedeutet **EN**able (aktivieren); es handelt sich um einen optionalen Bausteineingang. Wenn der Eingang des Typs EN aktiviert ist, wird automatisch ein Ausgang des Typs ENO bereitgestellt.

Wenn EN = 0, ist der Baustein nicht aktiviert, das bausteininterne Programm wird nicht ausgeführt und ENO wird auf "0" gesetzt.

Wenn EN = 1, wird das interne Programm des Bausteins ausgeführt und ENO auf "1" gesetzt. Wenn ein Laufzeitfehler auftritt, wird ENO auf "0" gesetzt.

Wenn der Eingang EN nicht angeschlossen ist, wird er automatisch auf "1" gesetzt.

ENO:

ENO bedeutet **E**rror **NO**tification (Fehlerbenachrichtigung); es handelt sich um einen Ausgang, der einem optionalen Eingang des Typs EN zugeordnet ist.

Wenn ENO auf "0" gesetzt wurde (weil EN = 0 oder im Fall eines Laufzeitfehlers bei der Ausführung),

- bleiben die Ausgänge der Funktionsbausteine in dem Status, in dem sie sich während des letzten fehlerfrei ausgeführten Abfragezyklus befunden haben.
- Die Ausgänge der Funktion sowie die Verfahren werden auf "0" gesetzt.

Erweiterter Modus:

In Control Expert wird unter „Erweitertem Modus“ eine Auswahl verstanden, die Konfigurationseigenschaften auf Expertenebene anzeigt, die bei der Definition von Ethernet-Verbindungen helfen. Da diese Eigenschaften nur von Personen mit soliden Kenntnissen über EtherNet/IP-Kommunikationsprotokolle bearbeitet werden sollten, können sie je nach Kompetenz des jeweiligen Benutzers ein- oder ausgeblendet werden.

Ethernet-DIO-Abfragedienst:

Dieser integrierte DIO-Abfragedienst von M580-Steuerungen verwaltet verteilte Geräte in einem M580-Gerätenetzwerk.

Ethernet-E/A-Abfragedienst:

Dieser integrierte Ethernet-E/A-Abfragedienst der M580-Steuerungen verwaltet verteilte Geräte **und** RIO-Stationen in einem M580-Gerätenetzwerk.

EtherNet/IP™:

Ein Netzwerkkommunikationsprotokoll für industrielle Automatisierungsanwendungen, das die standardmäßigen Internetübertragungsprotokolle TCP/IP und UDP mit dem Common Industrial Protocol (CIP) der Anwendungsschicht verbindet, um sowohl den Hochgeschwindigkeits-Datenaustausch als auch die industrielle Steuerung zu unterstützen. EtherNet/IP nutzt elektronische Datenblätter (EDS), um alle Netzwerkgeräte und ihre Funktionalität zu klassifizieren.

Ethernet:

Ein auf Frames basierendes CSMA/CD-LAN mit 10 oder 100 MBit/s oder 1 GBit/s, das über verdrillte Doppelkabel oder Glasfaserkabel betrieben werden kann. Der IEEE-Standard 802.3 legt die Regeln für die Konfiguration eines verdrahteten Ethernet-Netzwerks fest; der IEEE-Standard 802.11 legt die Regeln für die Konfiguration eines drahtlosen Ethernet-Netzwerks fest. Zu den gemeinsamen Formen zählen 10BASE-T, 100BASE-TX und 1000BASE-T, die verdrillte Doppelleitungen aus Kupfer der Kategorie 5 und modulare RJ45-Steckverbinder verwenden können.

Explicit Messaging Client:

(*Explicit Messaging Client Class*) Von der ODVA für EtherNet/IP-Knoten definierte Geräteklasse, die den expliziten Nachrichtenaustausch nur als Client unterstützen. HMI- und SCADA-Systeme sind die bekanntesten Beispiele für diese Geräteklasse.

Expliziter Nachrichtenaustausch:

TCP/IP-basierte Nachrichten für Modbus TCP und EtherNet/IP. Wird für Client/Server-Nachrichten mit Punkt-zu-Punkt-Übertragung verwendet, die sowohl Daten (in der Regel ungeplante Informationen zwischen einem Client und einem Server) als auch Routinginformationen enthalten. In EtherNet/IP gilt der explizite Nachrichtenaustausch als Nachrichtenaustausch der Klasse 3 und kann verbindungsbasiert oder verbindungslos sein.

F

FAST:

Optionale, periodische Prozessortask, die Requests mit hoher Priorität und mehreren Abfragen identifiziert und über die Programmiersoftware ausgeführt wird. Eine FAST-Task kann ausgewählte E/A-Module für eine mehrfache Auflösung ihrer Logik pro Abfragezyklus programmieren. Die FAST-Task besteht aus zwei Sections:

- IN: Vor der Ausführung der FAST-Task werden die Eingänge in die Section IN kopiert.
- OUT: Nach der Ausführung der FAST-Task werden die Ausgänge in die Section OUT kopiert.

FBD:

(*Funktionsbausteindiagramm*) Eine grafische Programmiersprache nach IEC 61131-3, die wie ein Ablaufdiagramm funktioniert. Durch Hinzufügen einfacher logischer Bausteine (z. B. `AND`, `OR`) wird jede Funktion bzw. jeder Funktionsbaustein im Programm in diesem grafischen Format dargestellt. Bei jedem Baustein befinden sich die Eingänge links und die Ausgänge rechts. Die Ausgänge der Bausteine können mit den Eingängen anderer Bausteine verbunden werden, um komplexe Ausdrücke zu bilden.

FDR:

(*Fast Device Replacement*) Dienst, der die Konfigurationssoftware zum Ersetzen eines funktionsunfähigen Produkts verwendet.

FDT:

(*Field Device Tool*) Eine Technologie, die die Kommunikation zwischen Feldgeräten und dem Hostsystem standardisiert.

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.

Funktionsbausteindiagramm:

Siehe FBD.

G

Gateway-:

Ein Gerät, das zwei verschiedene Netzwerke miteinander verbindet, manchmal über unterschiedliche Netzwerkprotokolle. Wenn ein Gateway zur Verbindung von Netzwerken eingesetzt wird, die auf unterschiedlichen Protokollen basieren, konvertiert es ein Datagramm von einem Protokollstapel zum anderen. Wird es zur Verbindung zweier IP-basierter Netzwerke verwendet, verfügt das Gateway (auch Router genannt) über zwei separate IP-Adressen –eine für jedes Netzwerk.

Gerät der Scannerklasse:

Ein Gerät der Scannerklasse ist gemäß ODVA als EtherNet/IP-Knoten definiert, der den Austausch von Eingängen/Ausgängen mit anderen Knoten im Netzwerk initiieren kann.

Gerätenetzwerk:

Ein Ethernet-basiertes Netzwerk innerhalb eines dezentralen E/A-Netzwerks, das sowohl dezentrale E/A- als auch verteilte E/A-Geräte einbindet. An dieses Netzwerk angeschlossene Geräte befolgen bestimmte Regeln, um Determinismus für dezentrale E/A zu ermöglichen.

GPS:

(*Global Positioning System*) Der GPS-Standard besteht aus weltraumgestützten Ortungs-, Navigations- und Zeitsignalen, die weltweit für zivile und militärische Zwecke bereitgestellt werden. Die Leistung des Standard Positioning Service (SPS) ist abhängig von den Rundfunksignalen von Satelliten, dem GPS-Konstellationsdesign, der Anzahl von Satelliten in Sichtweite sowie verschiedenen umweltspezifischen Parametern.

H

HART:

(*Highway Addressable Remote Transducer*) Bidirektionales Kommunikationsprotokoll für die Übertragung und den Empfang digitaler Informationen über analoge Leiter zwischen einem Steuerungs- und einem Überwachungssystem und intelligenten Geräten.

HART fungiert als globaler Standard bei der Bereitstellung eines Datenzugriffs zwischen Hostsystemen und intelligenten Feldgeräten. Bei einem Host kann es sich um eine beliebige Softwareanwendung handeln, vom Handgerät oder Laptop eines Technikers bis hin zu einer Prozesssteuerung, einem Anlagenmanagement oder jedem anderen System mit Steuerungsfunktion.

Hauptring:

Hauptring eines Ethernet-RIO-Netzwerks. Der Ring enthält RIO-Module, ein lokales Rack (mit einer Steuerung mit Ethernet-E/A-Abfragedienst) und ein Spannungsversorgungsmodul.

HMI:

(*Human Machine Interface*) System, dass eine Interaktion zwischen Mensch und Maschine ermöglicht.

Hot Standby:

Ein Hot Standby-System umfasst einen primären PAC (SPS) und einen Standby-PAC. Die zwei PAC-Racks weisen identische Hardware- und Softwarekonfigurationen auf. Der Standby-PAC überwacht den aktuellen Systemstatus des primären PAC. Sollte der primäre PAC betriebsunfähig werden, dann wird die Hochverfügbarkeit der Steuerung durch Übernahme der Systemsteuerung durch den Standby-PAC gewährleistet.

HTTP:

(*Hypertext Transfer Protocol*) Ein Netzwerkprotokoll für verteilte und kollaborative Informationssysteme. HTTP bildet die Grundlage der Datenkommunikation im Web.

I

%I:

In Übereinstimmung mit der IEC-Norm bezeichnet `%I` ein Sprachobjekt vom Typ "digitaler Eingang".

IEC 61131-3:

Internationaler Standard: Speicherprogrammierbare Steuerungen

Teil 3: Programmiersprachen

IGMP:

(Internet Group Management Protocol) Dieser Internet-Standard für Multicasting ermöglicht einem Host das Abonnieren einer bestimmten Multicast-Gruppe.

IL:

(*Instruction List / Anweisungsliste*) Eine Programmiersprache nach IEC 61131-3, die aus einer Reihe von Basisanweisungen besteht. Sie lehnt sich an die Assemblersprache an, mit der Prozessoren programmiert werden. Jede Anweisung besteht aus einem Anweisungscode und einem Operand.

Impliziter Nachrichtenaustausch:

Verbindungsorientierter, UDP/IP-basierter Nachrichtenaustausch der Klasse 1 für EtherNet/IP. Beim impliziten Nachrichtenaustausch wird eine offene Verbindung für die geplante Übertragung von Steuerdaten zwischen einem Producer und einem Consumer aufrechterhalten. Da eine offene Verbindung aufrecht erhalten wird, enthält jede Nachricht hauptsächlich Daten (ohne zusätzlich Objektinformationen) sowie eine Verbindungskennung.

INT:

(*INTeger*) (über 16 Bits kodiert) Gültiger Wertebereich: -(2 hoch 15) bis (2 hoch 15) - 1.

Beispiel: `-32768`, `32767`, `2#1111110001001001`, `16#9FA4`.

IODDT:

(*Input/Output Derived Data Type*: Abgeleiteter E/A-Datentyp) Strukturierter Datentyp, der ein Modul oder einen Kanal einer Steuerung darstellt. Jedes Anwendungs-Expertenmodul verfügt über eigene IODDTs.

IP-Adresse:

32-Bit-Bezeichner (bestehend aus einer Netzwerkadresse und einer Host-Adresse), der einem Gerät zugewiesen wird, das mit einem TCP/IP-Netzwerk verbunden ist.

IPsec:

(*Internet Protocol Security*) Eine offene Gruppe von Protokollstandards, die IP-Kommunikationssitzungen für den Datenverkehr zwischen Modulen mithilfe von IPsec, privat und verschlüsselt gestalten. IPsec wurde von der Internet Engineering Task Force (IETF) entwickelt. Für die IPsec-Authentifizierungs- und Verschlüsselungsalgorithmen sind benutzerdefinierte kryptografische Schlüssel erforderlich, die jedes Kommunikationspaket in einer IPsec-Sitzung verarbeiten.

Isoliertes DIO-Netzwerk:

Ein Ethernet-basiertes Netzwerk mit verteilten Geräten, das nicht an einem RIO-Netzwerk teilnimmt.

%IW:

In Übereinstimmung mit der IEC-Norm bezeichnet `%IW` ein Sprachobjekt vom Typ "analoger Eingang".

L

LD:

(*Ladder Diagram*: Kontaktplan (KOP)) Eine IEC 61131-3-Programmiersprache, die die auszuführenden Anweisungen in Form von grafischen Diagrammen wiedergibt, die in ihrer Darstellung an Stromlaufpläne angelehnt sind (z. B. Kontakte, Spulen).

Literalwert einer Ganzzahl:

Ganzzahlliterale werden verwendet, um Werte vom Typ "integer" im Dezimalsystem einzugeben. Diesen Werten können die Zeichen (+/-) vorangestellt werden. Unterstriche (_) zwischen den Ziffern sind nicht signifikant.

Beispiel:

```
-12, 0, 123_456, +986
```

Lokaler Slave:

Die Funktionalität von EtherNet/IP-Kommunikationsmodulen von Schneider Electric, die es einem Scanner ermöglichen, die Rolle eines Adapters zu übernehmen. Der lokale Slave ermöglicht dem Modul die Veröffentlichung von Daten über Verbindungen zur implizite Nachrichtenübertragung. Der lokale Slave wird in der Regel beim Peer-to-Peer-Datenaustausch zwischen PACs eingesetzt.

Lokales Rack:

Ein M580-Rack mit der Steuerung und einer Stromversorgung. Ein lokales Rack besteht aus einem oder zwei Racks: einem Hauptrack und einem Erweiterungsrack, das derselben Familie angehört wie das Hauptrack. Das Erweiterungsrack ist optional.

M

%M:

In Übereinstimmung mit der IEC-Norm bezeichnet `%M` ein Sprachobjekt vom Typ "Speicherbit".

M580 Ethernet-E/A-Gerät:

Ein Ethernet-Gerät, das automatische Netzwerkwiederherstellung und deterministische RIO-Leistung bietet. Die Zeit, die für die Auflösung einer logischen RIO-Abfrage benötigt wird, kann berechnet werden, und das System kann nach einer Unterbrechung der Kommunikation schnell wiederhergestellt werden. M580 Ethernet Zu den E/A-Geräten gehören:

- Lokales Rack (einschließlich einer Steuerung mit Ethernet-E/A-Abfragedienst)
- RIO-Station (einschließlich eines X80-Adaptermoduls)
- DRS-Switch mit vordefinierter Konfiguration

MAST:

Eine Master-Task (MAST) ist eine Prozessortask, die über die Programmiersoftware ausgeführt wird. Die MAST-Task programmiert die Auflösung der RIO-Modullogik in jedem E/A-Abfragezyklus. Die MAST-Task besteht aus zwei Sections:

- IN: Vor der Ausführung der MAST-Task werden die Eingänge in die IN-Section kopiert.
- OUT: Nach der Ausführung der MAST-Task werden die Ausgänge in die OUT-Section kopiert.

MB/TCP:

(*Modbus über TCP-Protokoll*) Dies ist eine Modbus-Variante, die für die Kommunikation über TCP/IP-Netzwerke verwendet wird.

MIB:

(*Management Information Base*) Eine virtuelle Datenbank, die zur Verwaltung von Objekten in einem Kommunikationsnetzwerk verwendet wird. Siehe SNMP.

Modbus:

Modbus ist ein Nachrichtenaustauschprotokoll der Anwendungsschicht. Modbus bietet Client- und Server-Kommunikationen zwischen Geräten, die an verschiedene Bus- oder Netzwerktypen angeschlossen sind. Modbus stellt zahlreiche durch Funktionscodes spezifizierte Dienste bereit.

Multicast:

Eine besondere Form von Broadcast, bei dem Kopien des Pakets nur an eine bestimmte Untergruppe von Netzwerkzielen gesendet wird. Beim impliziten Nachrichtenaustausch wird in der Regel das Multicast-Format für die Kommunikation in einem EtherNet/IP-Netzwerk verwendet.

%MW:

In Übereinstimmung mit der IEC-Norm bezeichnet `%MW` ein Sprachobjekt vom Typ "Speicherwort".

N

Netzwerkkonvergenz:

Aktivität der Neukonfiguration des Netzwerks bei Netzwerkverlust, um die Systemverfügbarkeit zu gewährleisten.

Netzwerk:

Netzwerk hat zwei verschiedene Bedeutungen:

- In einem Kontaktplan (LD):

  Ein Netzwerk ist eine Gruppe von untereinander verknüpften Grafikelementen. Die Reichweite eines Netzes bzw. Netzwerks gilt in Bezug auf die organisatorische Einheit (Section) des Programms, in dem sich das Netz befindet, als lokal.

- Für Expertenkommunikationsmodule:

  Hier stehen die Begriffe Netz bzw. Netzwerk für eine Gruppe von Stationen, die miteinander kommunizieren. Außerdem werden die Begriffe *Netz und Netzwerk* auch hier verwendet, um eine Gruppe von miteinander verbundenen grafischen Elementen zu bezeichnen. Eine solche Gruppe bildet dann einen Teil eines Programms, das aus einer Netzgruppe bestehen kann.

Netzwerkzeitdienst (NTS):

Verwenden Sie den NTS-Dienst (Network Time Service) zur Synchronisation von Computeruhren über das Internet für die Aufzeichnung von Ereignissen (Sequenzierung von Ereignissen), die Synchronisation von Ereignissen (gleichzeitige Auslösung von Ereignissen) oder die Synchronisation von Alarmen und E/A (Zeitstempelung von Alarmen).

NIM:

(*Network Interface Module*) Ein NIM befindet sich auf einer STB-Insel in der ersten Position (ganz links in der physischen Konfiguration). Das NIM bietet eine Schnittstelle zwischen den E/A-Modulen und dem Feldbus-Master. Es ist das einzige feldbusabhängige Modul auf der Insel: für jeden Feldbus steht ein anderes NIM zur Verfügung.

NTP:

(*Network Time Protocol*) Protokoll für die Synchronisierung der Uhren von Computersystemen. Das Protokoll nutzt ein Jitter-Buffer, um die Auswirkungen der variablen Latenz zu kompensieren.

O

O -> T:

(*Originator To Target*) Siehe Ziel an Ursprung.

ODVA:

(*Open DeviceNet Vendors Association*) Die ODVA unterstützt auf CIP basierende Netzwerktechnologien.

OFS:

(*OPC Factory Server*) OFS ermöglicht die Echtzeitkommunikation zwischen SCADA-Systemen und Steuerungen der SPS-Baureihe Control Expert. OFS verwendet das Standard-OFS-Datenzugriffsprotokoll.

OPC DA:

(*OLE for Process Control Data Access*) Die Data Access-Spezifikation ist der am häufigsten implementierte OPC-Standard und stellt Kenndaten für die Echtzeitkommunikation zwischen Clients und Servern bereit.

P

PAC:

(*Programmable Automation Controller*) Programmierbare Automationssteuerung. Der PAC ist das Gehirn eines industriellen Fertigungsverfahrens. Im Gegensatz zu Relaisregelungssystemen automatisiert der PAC einen Prozess. PACs sind Computer, die rauen Betriebsbedingungen in industriellen Umgebungen standhalten.

Port 502:

Der Port 502 des TCP/IP-Stacks ist ein wohlbekannter Port, der der Modbus TCP-Kommunikation vorbehalten ist.

Port-Spiegelung:

In diesem Modus wird der Datenverkehr, der über den Quellport eines Netzwerkschalters abgewickelt wird, auf einen Zielport kopiert. Dieser ermöglicht einem angeschlossenen Verwaltungstool das Überwachen und Analysieren des Datenverkehrs.

Prioritätsverkettungsschleife mit hoher Kapazität:

Häufig kurz als HCDL (High-Capacity Daisy Chain Loop) bezeichnet. Hochleistungsfähige Prioritätsverkettungsschleifen verwenden Dual-Ring-Switches (DRSs), um Geräte-Teilringe (mit RIO-Stationen oder verteilten Geräten) und/oder DIO-Clouds mit dem Ethernet-RIO-Netzwerk zu verbinden.

PTP:

(*Precision Time Protocol*) Verwenden Sie dieses Protokoll zur Synchronisation aller Uhren in einem Computernetzwerk. In einem LAN-Netzwerk wird mit dem PTP eine höhere Zeitgenauigkeit als im Mikrosekundenbereich erzielt. Damit ist das Protokoll für Mess- und Steuersysteme geeignet.

Q

%Q:

In Übereinstimmung mit der IEC-Norm bezeichnet `%Q` ein Sprachobjekt vom Typ "digitaler Ausgang".

QoS:

(*Quality of Service* Die Regulierung des Datenflusses im Netzwerk, indem Datenverkehrstypen verschiedene Prioritäten zugewiesen werden. In einem industriellen Netzwerk kann QoS dabei helfen, eine vorhersehbare Netzwerkleistung aufrechtzuerhalten.

%QW:

In Übereinstimmung mit der IEC-Norm bezeichnet `%QW` ein Sprachobjekt vom Typ "analoger Ausgang".

R

Rackoptimierte Verbindung:

Die Daten mehrerer E/A-Module werden in einem einzelnen Datenpaket zusammengefasst, das dem Scanner in einem EtherNet/IP-Netzwerk in einer impliziten Nachricht präsentiert wird.

Raue Umgebungsbedingungen:

Beständigkeit gegenüber Kohlenwasserstoffen, Industrieölen, Reinigungsmitteln und Lötchips. Relative Luftfeuchtigkeit bis zu 100 %, salzhaltige Atmosphäre, bedeutende Temperaturschwankungen, Betriebstemperaturen zwischen -10 °C und +70 °C oder mobile Installationen. Bei Hardened-Geräten (H) kann die relative Luftfeuchtigkeit 95 % erreichen und die Betriebstemperatur zwischen -25 °C und +70 °C liegen.

RIO-Netzwerk:

Ein Ethernet-basiertes Netzwerk, das 3 Typen von RIO-Geräten umfasst: ein lokales Rack, eine RIO-Station und einen erweiterter ConneXium-Dual-Ring-Switch (DRS). Auch verteilte Geräte können über eine Verbindung mit DRSs- oder BMENOS0300-Schaltmodulen für Netzwerkoptionen an einem RIO-Netzwerk teilnehmen.

RIO-Station:

Einer der drei Typen von RIO-Modulen in einem Ethernet-RIO-Netzwerk. Eine RIO-Station besteht aus einem M580-Rack mit E/A-Modulen, die mit einem Ethernet-RIO-Netzwerk verbunden sind und von einem dezentralen Ethernet-RIOAdaptermodul verwaltet werden. Eine Station kann einem einzelnen Rack oder einem Hauptrack mit Erweiterungsracks entsprechen.

RPI:

(Requested Packet Interval) Der Zeitraum zwischen den vom Scanner angeforderten zyklischen Datenübertragungen. EtherNet/IP-Geräte veröffentlichen Daten in den Abständen, die über das vom Scanner zugewiesene RPI festgelegt werden, und sie erhalten in jedem RPI Nachrichtenrequests vom Scanner.

RSTP:

(*Rapid Spanning Tree Protocol*) Ermöglicht die Aufnahme redundanter (Reserve-) Verbindungen in ein Netzwerk-Design, damit automatische Ersatzpfade bereitgestellt werden, wenn eine aktive Verbindung fehlschlägt, ohne dass die Gefahr von Schleifen oder die Notwendigkeit einer manuellen Aktivierung/Deaktivierung der Ersatzverbindungen besteht.

S

S908 RIO:

Ein Quantum-RIO-System mit Koaxialkabeln und Abschlusswiderständen.

SCADA:

(*Supervisory Control And Data Acquisition*) SCADA-Systeme sind Computersysteme, die industrielle, infrastruktur- und funktionsbasierte Prozesse steuern und überwachen (Beispiele: Übertragung von Strom, Beförderung von Gas und Öl in Pipelines und Wasserverteilung).

Scanner:

Ein Scanner fungiert als Urheber von E/A-Verbindungsrequests für den impliziten Nachrichtenaustausch in EtherNet/IP bzw. von Nachrichtenrequests für Modbus TCP.

Service-Port:

Ein dedizierter Ethernet-Port an M580-RIO-Modulen. Der Port kann folgende Hauptfunktionen (je nach Modultyp) unterstützen:

- Port-Spiegelung: Zu Diagnosezwecken
- Zugriff: Zur Verbindung von HMI/Control Expert/ConneXview mit der Steuerung
- Erweitert: Zur Erweiterung des Gerätenetzwerks auf ein anderes Teilnetz
- Deaktiviert: Zur Deaktivierung des Ports. In diesem Modus erfolgt kein Datenverkehr.

SFC:

(*Sequential Function Chart*: Ablaufsprache) Eine IEC 61131-3-Programmiersprache, die eine strukturierte grafische Darstellung des Betriebs einer Ablaufsteuerung ermöglicht. Diese grafische Beschreibung des sequenziellen Verhaltens der Steuerung und der verschiedenen daraus resultierenden Situationen wird mithilfe einfacher grafischer Symbole erstellt.

SFP:

(*Small Form-Factor Pluggable*) Der SFP-Transceiver fungiert als Schnittstelle zwischen einem Modul und Glasfaserkabeln.

SMTP:

(*Simple Mail Transfer Protocol*) E-Mail-Benachrichtigungsdienst, der steuerungsbasierten Projekten die Ausgabe von Alarmen bzw. die Signalisierung von Ereignissen ermöglicht. Die Steuerung überwacht das System und kann automatisch eine E-Mail-Warnung mit Daten, Alarmen und/oder Ereignissen erstellten. Bei den Mail-Empfängern kann es sich um lokale oder dezentrale Geräte handeln.

SNMP:

(*Simple Network Management Protocol*) Protokoll, das in Netzwerkmanagementsystemen zur Überwachung der mit dem Netzwerk verbundenen Geräte eingesetzt wird. Das Protokoll zählt zu den von der Internet Engineering Task Force (IP) definierten Internetprotokollen (IETF), die bei der Verwaltung von Netzwerken als Richtlinie dienen. Diese Richtlinien umfassen darüber hinaus ein Anwendungsprotokoll, ein Datenbankschema und einen Satz von Datenobjekten.

SNTP:

(*Simple Network Time Protocol*) Siehe NTP.

SOE:

(*Sequence of Events*) SOE-Software hilft den Benutzern, die Kette von Vorkommnissen zu verstehen, die zu unsicheren Prozessbedingungen und möglichen Stillstandszeiten führen können. SOEs können für die Lösung und Vermeidung derartiger Situationen von entscheidender Bedeutung sein.

Sommerzeit:

Im Englischen auch als DST (*Daylight Saving Time*) bezeichnet. Die Umstellung auf die *Sommer-/Winterzeit* besteht in einer Vorstellung der Uhrzeit im Frühling und einer Rückstellung der Uhrzeit im Herbst.

Steuerungsnetzwerk:

An Ethernet-basiertes Netzwerk, das PACs, SCADA-Systeme, einen NTP-Server, PCs, AMS, Switches und andere Komponenten umfasst. Es werden zwei Arten von Topologien unterstützt:

- Flach: Alle Module und Geräte in diesem Netzwerk gehören demselben Subnetz an.
- 2-stufig: Das Netzwerk ist in ein Betriebsnetzwerk und ein steuerungsübergreifendes Netzwerk unterteilt. Diese beiden Netzwerke sind zwar physisch voneinander unabhängig, in der Regel jedoch über ein Routing-Gerät miteinander verbunden.

Steuerungsübergreifendes Netzwerk:

Ein Ethernet-basiertes Netzwerk, das Teil des Steuerungsnetzwerks ist und einen Datenaustausch zwischen den Steuerungen und den technischen Tools (Programmierung, Asset Management System (AMS)) ermöglicht.

ST:

(*Structured Text / Strukturierter Text*) Eine Programmiersprache nach IEC 61131-3, die in strukturierten Literalen geschrieben wird. Es handelt sich um eine höhere Programmiersprache, ähnlich denjenigen, die zur Abfassung von Computerprogrammen verwendet werden. Sie ermöglicht die Strukturierung einer Folge von Anweisungen.

Subnetzmaske:

Der 32-Bit-Wert, mit dem der Netzwerkabschnitt der IP-Adresse ausgeblendet (oder maskiert) wird, wodurch wiederum die Host-Adresse eines Geräts in einem Netzwerk gezeigt wird, das das IP-Protokoll verwendet.

Switch:

Ein Gerät mit mehreren Ports, das zur Segmentierung des Netzwerks sowie zur Verringerung der Wahrscheinlichkeit von Kollisionen eingesetzt wird. Pakete werden anhand ihrer Quell- und Zieladresse gefiltert oder weitergeleitet. Switches sind für den Vollduplex-Betrieb geeignet und können für jeden Port die volle Netzwerkbandbreite bereitstellen. Ein Switch kann über unterschiedliche Eingangs-/Ausgangsgeschwindigkeiten verfügen (z.B. 10, 100 oder 1000 MBit/s). Switches arbeiten auf der OSI-Schicht 2 (Sicherungsschicht).

%SW:

In Übereinstimmung mit der IEC-Norm bezeichnet `%SW` ein Sprachobjekt vom Typ "Speicherwort".

T

T -> O:

(*Target to Originator*) Siehe Ziel an Ursprung.

TCP/IP:

Bei dem auch als *Internet Protocol Suite* bezeichneten TCP/IP handelt es sich um eine Sammlung von Protokollen, die dazu verwendet werden, Transaktionen in einem Netzwerk auszuführen. Der Name dieser Sammlung leitet sich aus zwei allgemein verwendeten Protokollen ab: Transmission Control Protocol und Internet Protocol. TCP/IP ist ein verbindungsorientiertes Protokoll, das von Modbus Modbus TCP und EtherNet/IP für den expliziten Nachrichtenaustausch verwendet wird.

TCP:

(*Transmission Control Protocol*) Ein grundlegendes Protokoll der Internetprotokoll-Familie, das die verbindungsorientierte Kommunikation unterstützt, indem es die Verbindung herstellt, die zur Übertragung einer geordneten Sequenz von Daten über denselben Kommunikationspfad erforderlich ist.

Teilring:

Ein Ethernet-basiertes Netzwerk mit einer Schleife, das über einen Dual-Ring-Switch (DRS) oder ein BMENOS0300-Schaltmodul für Netzwerkoptionen mit dem Hauptring verbunden ist. Dieses Netzwerk enthält RIO oder verteilte Geräte.

TFTP:

(*Trivial File Transfer Protocol*) Eine vereinfachte Version des *File Transfer Protocol* (FTP). TFTP verwendet eine Client/Server-Architektur für die Herstellung einer Verbindung zwischen zwei Geräten. Ein TFTP-Client kann unter Verwendung des UDP-Protokolls (User Datagram Protocol) für den Datentransport einzelne Dateien vom Server herunterladen bzw. auf den Server hochladen.

TIME_OF_DAY:

Siehe `TOD`.

TOD:

(*Time Of Day*) Der Typ `TOD` für die Tageszeit wird in BCD über 32 Bits kodiert und enthält die folgenden Informationen:

- Die Stunde in einem Feld von 8 Bits
- Die Minuten in einem Feld von 8 Bits
- Die Sekunden in einem Feld von 8 Bits

  HINWEIS: Die acht niederwertigsten Bits (LSBs, Least Significant Bits) werden nicht verwendet.

Der TOD-Typ wird in folgendem Format eingegeben: **`TOD#`**`<Stunden>`**`:`**`<Minuten>`**`:`** `<Sekunden>`

Die folgende Tabelle zeigt die Wertebereiche der einzelnen Felder:

Feld	Grenzwerte	Kommentar
Stunde	[00,23]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.
Minute	[00,59]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.
Zweites	[00,59]	Die führende Null wird immer angezeigt, kann bei der Dateneingabe aber ausgelassen werden.

Beispiel: `TOD#23:59:45`.

Trap:

Ein Trap ist ein von einem SNMP-Agent gesteuertes Ereignis, das auf eines der folgenden Ereignisse verweist:

- Der Status eines Agents hat sich geändert.
- Ein nicht autorisiertes SNMP-Managergerät hat versucht, Daten von einem SNMP-Agent abzurufen oder Daten auf einem SNMP-Agent zu ändern.

TR:

(*Transparent Ready*) Internetfähiges Gerät zur Verteilung von Strom, einschließlich Mittel- und Niederspannungsschaltanlagen, Schalttafeln, Schaltpults, Motorsteuerungszentralen und Unterstationen. Transparent Ready-Geräte ermöglichen Ihnen den Zugriff auf den Mess- und Gerätestatus von jedem beliebigen PC im Netzwerk aus mit einem standardmäßigen Webbrowser.

U

UDP:

(*User Datagram Protocol*) UDP ist ein Transportschichtprotokoll, das die verbindungslose Kommunikation unterstützt. Anwendungen, die auf Netzwerkknoten ausgeführt werden, können sich mithilfe von UDP gegenseitig Datagramme senden. Im Gegensatz zu TCP beinhaltet UDP keine vorbereitende Kommunikation zur Erstellung eines Datenpfads bzw. der Bereitstellung der Datenbestellung und -prüfung. Durch die Vermeidung des für die Bereitstellung dieser Funktionen erforderlichen Overhead ist UDP jedoch schneller als TCP. UDP kann als bevorzugtes Protokoll für zeitkritische Anwendungen eingesetzt werden, wenn verworfene Datagramme verspäteten Datagrammen vorzuziehen sind. UDP ist das primäre Transportprinzip für den impliziten Nachrichtenaustausch in EtherNet/IP.

UMAS:

(*Unified Messaging Application Services*) Proprietäres Systemprotokoll, das die Kommunikation zwischen Control Expert und einer Steuerung verwaltet.

Urheber:

In EtherNet/IP wird ein Gerät als Urheber bezeichnet, wenn es eine CIP-Verbindung für den impliziten oder expliziten Nachrichtenaustausch herstellt oder einen Nachrichtenrequest für den verbindungslosen expliziten Nachrichtenaustausch initiiert.

UTC:

(*Coordinated Universal Time*) Vorrangiger Zeitstandard, der weltweit zur Einstellung der Uhrzeit verwendet wird (mit dem früheren GMT-Zeitstandard vergleichbar).

V

Variable:

Speichereinheit vom Typ `BOOL`, `WORD`, `DWORD` und ähnlichen Typen, mit Inhalten, die vom aktuell ausgeführten Programm geändert werden können.

Verbindung der Klasse 1:

Eine CIP-Verbindung der Transportklasse 1 zur Übertragung von E/A-Daten über den impliziten Nachrichtenaustausch zwischen EtherNet/IP-Geräten.

Verbindung der Klasse 3:

Eine CIP-Verbindung der Transportklasse 3 zum expliziten Nachrichtenaustausch zwischen EtherNet/IP-Geräten.

Verbindungslos:

Beschreibt die Kommunikation zwischen zwei Netzwerkgeräten, bei der die Daten ohne vorherigen Verbindungsaufbau zwischen den beiden Geräten gesendet werden. Jede übertragene Dateneinheit enthält auch Routing-Informationen, einschließlich der Quell- und Zieladresse.

Verbindungsorientierter Nachrichtenaustausch:

In EtherNet/IP wird beim verbindungsorientierten Nachrichtenaustausch eine CIP-Verbindung für die Kommunikation verwendet. Eine verbindungsorientierte Nachricht ist eine logische Beziehung zwischen zwei oder mehr Anwendungsobjekten auf unterschiedlichen Knoten. Die Verbindung erstellt im Vorhinein einen virtuellen Schaltkreis für einen bestimmten Zweck, zum Beispiel häufige explizite Nachrichten oder E/A-Echtzeitdatenübertragungen.

Verbindungsurheber:

Der EtherNet/IP-Netzwerkknoten, der einen Verbindungsrequest für die E/A-Datenübertragung oder den expliziten Nachrichtenaustausch initiiert.

Verbindung:

Ein virtueller Schaltkreis zwischen zwei oder mehr Netzwerkgeräten, der vor der Datenübertragung hergestellt wird. Nach dem Aufbau einer Verbindung werden eine Reihe von Daten über denselben Kommunikationspfad übertragen, ohne dass für jede Dateneinheit Routing-Informationen (wie die Quell- und Zieladresse) angegeben werden müssen.

Verteilte Geräte:

Alle Ethernet-Geräte (Schneider Electric-Geräte, PCs, Server oder Dritthersteller-Geräte), die den Austausch mit einer Steuerung oder einem anderen Ethernet-E/A-Abfragedienst unterstützten.

VLAN:

(*Virtual Local Area Network*) Lokales Netzwerk (LAN), das sich über ein einzelnes LAN hinaus auf eine Gruppe von LAN-Segmenten erstreckt. Ein VLAN ist eine logische Einheit, die mithilfe einer Anwendungssoftware erstellt und eindeutig konfiguriert wird.

Vollduplex:

Die Fähigkeit zweier in einem Netzwerk miteinander verbundener Geräte, unabhängig und gleichzeitig in beide Richtungen miteinander zu kommunizieren.

Z

Ziel:

In EtherNet/IP wird ein Gerät als Ziel bezeichnet, wenn es Empfänger eines Verbindungsrequests für den impliziten bzw. expliziten Nachrichtenaustausch oder eines Nachrichtenrequests für den verbindungslosen expliziten Nachrichtenaustausch ist.

Index

A

ACL
Sicherheit....33
Administrationsschnittstelle
CSPN....51
Änderung der Datenflüsse
CSPN....51
Änderung der Firmware
CSPN....51
Änderung des Ausführungsmodus
CSPN....51
Änderung des Speicherprogramms
CSPN....51
Architektur....19
Audit-Trail
Sicherheit....53
Ausführungsmodus der Steuerung
CSPN....51
Ausführungsmodus, Steuerung
CSPN....51
Authentifizierung
Cybersicherheit....130

B

Benachrichtigungen
Cybersicherheit....18
Benutzerprofile
Sicherheit, M580 Control Expert-Sicherheitseditor....46
Berechtigung
Sicherheit....107
Berechtigungen
Cybersicherheit....130
Betriebsarten
CSPN, M580....48

C

Control Expert
password....106
CSPN....43
Kritische Komponenten, Steuerung....49
Kritische Komponenten, Umgebung....49
M580-Betriebsarten....48
M580-Cybersicherheitsparameter....48
M580, Änderung der Datenflüsse....51
M580, Änderung der Firmware....51
M580, Änderung des Ausführungsmodus....51
M580, Änderung des Speicherprogramms....51
M580, Denial of Service....51
M580, Firmwaresignatur....51
M580, Integrität des Steuerungsausführungsmodus....51
M580, Integrität und Authentizität des Steuerungsspeichers....51
M580, Richtlinien für die Zugriffskontrolle....51
M580, Sichere Speicherung von Geheimnissen....51
M580, Verschlüsselte Authentifizierung über die Administrationsschnittstelle....51
M580, Verschlüsselte Kommunikation....51
M580, Verwaltung fehlerhafter Eingänge....51
Cybersicherheit....17
Authentifizierung....130
Benachrichtigungen....18
Berechtigungen....130
CSPN....43
CSPN, M580....43
CSPN, M580-Betriebsarten....48
Deaktivierung nicht verwendeter Dienste....130
Dienste....130
Dokumentation....17
Ereignisprotokollierung....130
Firmware....130
FTP....104
Gesicherte Kommunikation....130
HTTP....103
Integritätsprüfungen....130
Konten....101
LAN-Verbindung....29
LANMAN / NTLM....28
M340....138
M580....138
M580 Control Expert-Sicherheitseditor....46
M580 CSPN-Parameter....48

Netzwerkschnittstellenkarten 28
Passwörter 102
Premium/Atrium 143
Quantum 138
Remote Desktop 28
Richtlinien 17
Schwachstellen 18
SNMP 105
X80 140
Zugriffskontrolle 130

D

Deaktivieren
Kommunikationsdienste 32
Deaktivierung nicht verwendeter Dienste
Cybersicherheit 130
Denial of Service
CSPN 51
Dienste
Cybersicherheit 130
Sicherheit 130
Dokumentation
Cybersicherheit 17

E

Ereignisprotokollierung
Cybersicherheit 130
Ereignisprotokollmeldungen
BMENOR2200H 84
BMENUA0100 84
M580-Steuerung (Firmware vor V4.10) 84
Ereignisprotokollnachrichten 69
Control Expert 63
M580-Steuerung (für Firmware V4.10 und alle nachfolgenden unterstützenden Versionen) 69

F

Firmware
Cybersicherheit 130
Sicherheit 130
Firmwaresignatur
CSPN 51
FTP
cybersecurity 104

G

Gesicherte Kommunikation
Cybersicherheit 130

H

Härten
PC 23
HTTP
cybersecurity 103

I

Integritätsprüfung
Sicherheit 112
Integritätsprüfungen
Cybersicherheit 130

K

Kommunikation, sicher
CSPN 51
Kommunikationsdienste
Deaktivieren 32
Komponenten
Kritisch, M580 CSPN-Steuerung 49
Kritisch, M580 CSPN-Umgebung 49
Konten
Cybersicherheit 101
Kritische Komponenten
PAC, M580 CSPN 49
Umgebung, M580 CSPN 49

L

LAN
Cybersicherheit 29
LANMAN / NTLM
Cybersicherheit 28

M

M340
cybersecurity 138
M580
cybersecurity 138

N

Netzwerkschnittstellenkarten
Cybersicherheit 28

O

Operate (Betrieb)
M580 Control Expert-Sicherheitseditor-Profil 46

P

Passwort
Control Expert 106
Passwörter
Cybersicherheit 102
PC
Härten 23
Premium/Atrium
cybersecurity 143
Profil
M580 Control Expert-Sicherheitseditor 46
Program (Programm)
M580 Control Expert-Sicherheitseditor-Profil 46
Protokollierung
Sicherheit 53

Q

Quantum
cybersecurity 138

R

ReadOnly (Nur Lesen)
M580 Control Expert-Sicherheitseditor-Profil 46
Remote Desktop
Cybersicherheit 28
Richtlinien für die Zugriffskontrolle
CSPN 51
Run/Stop
Sicherheit 109

S

Schnittstelle, administrativ
CSPN 51
Schutz
Section 108
Speicher 109
Schwachstellen
Cybersicherheit 18
Section
Schutz 108
Sichere Kommunikation
CSPN 51
Sicherheit
ACL 33
Audit-Trail 53
Berechtigung 107
CSPN 43
CSPN, M580-Betriebsarten 48
Dienste 130
Firmware 130
Integritätsprüfung 112
M580 Control Expert-Sicherheitseditor 46
M580 CSPN-Parameter 48
Protokollierung 53
Run/Stop 109
Speicherschutz 112
Syslog 53
Zugriffskontrolle 33
Sicherheitseditor von Control Expert 46
Signatur, Firmware
CSPN 51
SNMP
cybersecurity 105
Speicher
Schutz 109
Speicher, Steuerung
CSPN 51

Speicherschutz
Sicherheit 112
Speicherung von Geheimnissen
CSPN 51
Steuerungsspeicher
CSPN 51
Syslog
BMENOR2200H 84
BMENUA0100 84
Control Expert 63
M580-Steuerung (Firmware V4.10 und alle nachfolgenden unterstützenden Versionen) 69
M580-Steuerung (Firmware vor V4.10) 84
security 53

U

USB
Zugriff 20

V

Verwaltung der Eingänge, fehlerhaft
CSPN 51

X

X80
cybersecurity 140

Z

Zertifizierung
CSPN 43
Zugriff
USB 20
Zugriffskontrolle
Cybersicherheit 130
Sicherheit 33

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.

EIO0000002000.10