Modicon M580

Integriertes Modul BMENUA0100 OPC UA

Installations- und Konfigurationshandbuch

Übersetzung der Originalbetriebsanleitung

04/2025

PHA83352.04

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

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

Deckungsbereich

In diesem Handbuch werden Funktionen und Verwendung des Ethernet-Kommunikationsmoduls M580 BMENUA0100 mit integriertem OPC UA-Server beschrieben.

HINWEIS: Die in diesem Handbuch beschriebenen Einstellungen sind lediglich als Beispiel zu verstehen. Die für Ihre Konfiguration erforderlichen Einstellungen können von den in diesem Handbuch verwendeten Einstellungen abweichen.

Gültigkeitshinweis

Dieses Dokument ist gültig für ein M580-System bei Verwendung mit EcoStruxure™ Control Expert Version 16.2 oder einer nachfolgenden unterstützenden Version.

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

Produktbezogene Informationen

⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENS

- Trennen Sie alle Geräte, einschließlich der angeschlossenen Komponenten, vor der Entfernung von Abdeckungen oder Türen sowie vor der Installation oder Entfernung von Zubehörteilen, Hardware, Kabeln oder Drähten von der Spannungsversorgung, ausgenommen unter den im jeweiligen Hardwarehandbuch für diese Geräte angegebenen Bedingungen.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um sicherzustellen, dass an den betreffenden Stellen und zum jeweils angegebenen Zeitpunkt tatsächlich keine Spannung mehr anliegt.
- Bringen Sie alle Abdeckungen, Zubehörteile, Hardware, Kabel und Drähte wieder an, sichern Sie sie und vergewissern Sie sich, dass eine ordnungsgemäße Erdung vorhanden ist, bevor Sie die Spannungszufuhr zum Gerät einschalten.
- Verwenden Sie für den Betrieb dieses Geräts und jeglicher verbundener Produkte ausschließlich die vorgeschriebenen Spannungswerte.

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

⚠WARNUNG

KONTROLLVERLUST

- Führen Sie vor der Implementierung eine Fehlermodus- und Effektanalyse (FMEA, Failure Mode and Effects Analysis) oder eine gleichwertige Risikoanalyse Ihrer Anwendung durch und wenden Sie vorbeugende und detektive Kontrollen an.
- Stellen Sie einen Fallback-Zustand für den Fall unerwünschter Steuerungsereignisse oder -sequenzen bereit.
- Sorgen Sie für separate oder redundante Steuerungspfade, wann immer erforderlich.
- Stellen Sie geeignete Parameter bereit, insbesondere für Grenzwerte.
- 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 die Steuerungsfunktionen (z. B. Not-Aus, Zustände bei Grenzüberschreitung und Fehlern) in Übereinstimmung mit der Sicherheitsanalyse und geltenden Richtlinien und Vorschriften bereit.
- Wenden Sie vor Ort Maßnahmen zur Unfallverhütung sowie Sicherheitsvorkehrungen und -richtlinien an.
- 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.

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

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

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

Allgemeine Informationen zur Cybersicherheit

In den letzten Jahren hat sich durch die wachsende Anzahl an vernetzten Maschinen und Produktionsanlagen das Potenzial für Cyberbedrohungen wie unbefugter Zugriff, Datenverletzungen und Betriebsunterbrechungen entsprechend erhöht. Sie müssen daher alle möglichen Maßnahmen zur Cybersicherheit in Betracht ziehen, um Anlagen und Systeme vor solchen Bedrohungen zu schützen.

Um die Sicherheit und den Schutz Ihrer Schneider Electric-Produkte zu gewährleisten, ist es in Ihrem Interesse, die Best Practices für die Cybersicherheit umzusetzen, die im Dokument Cybersecurity Best Practices beschrieben sind.

Schneider Electric bietet zusätzliche Informationen und Unterstützung:

- Abonnieren Sie den Sicherheits-Newsletter von Schneider Electric.
- Besuchen Sie die Webseite Cybersecurity Support Portal, um:
  - Sicherheitshinweise zu suchen
  - Schwachstellen und Vorfälle zu melden
- Besuchen Sie die Webseite Schneider Electric Cybersecurity and Data Protection Posture, um:
  - auf den Cybersicherheitsstatus zuzugreifen
  - mehr über Cybersicherheit in der Cybersecurity Academy zu erfahren
  - die Cybersicherheits-Services von Schneider Electric zu entdecken

Umgebungsdaten

Informationen zu Produktkonformität und Umgebungsbedingungen finden Sie im Schneider Electric Environmental Data Program.

Weiterführende Dokumente

Titel der Dokumentation	Referenznummer
Modicon M580 Standalone, Systemplanungshandbuch für verwendete Architekturen	HRB62666 (Englisch), HRB65318 (Französisch), HRB65319 (Deutsch), HRB65320 (Italienisch), HRB65321 (Spanisch), HRB65322 (Chinesisch)
Modicon M580, Systemplanungshandbuch für komplexe Topologien	NHA58892 (Englisch), NHA58893 (Französisch), NHA58894 (Deutsch), NHA58895 (Italienisch), NHA58896 (Spanisch), NHA58897 (Chjnese)

Titel der Dokumentation	Referenznummer
Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen	NHA58880 (Englisch), NHA58881 (Französisch), NHA58882 (Deutsch), NHA58883 (Italienisch), NHA58884 (Spanisch), NHA58885 (Chinesisch)
Modicon M580, M340 und X80 I/O-Plattformen, Normen und Zertifizierungen	EIO0000002726 (Englisch), EIO0000002727 (Französisch), EIO0000002728 (Deutsch), EIO0000002730 (Italienisch), EIO0000002729 (Spanisch), EIO0000002731 (Chinesisch)
M580 BMENOS0300 Schaltmodul für Netzwerkoptionen, Installations- und Konfigurationshandbuch	NHA89117 (ENG) NHA89119 (FRE) NHA89120 (GER) NHA89121 (ITA) NHA89122 (SPA) NHA89123 (CHS)
Modicon M580, Hardware, Referenzhandbuch	EIO0000001578 (Englisch), EIO0000001579 (Französisch), EIO0000001580 (Deutsch), EIO0000001582 (Italienisch), EIO0000001581 (Spanisch), EIO0000001583 (Chinesisch)
Modicon M580, RIO-Module, Installations- und Konfigurationshandbuch	EIO0000001584 (Englisch), EIO0000001585 (Französisch), EIO0000001586 (Deutsch), EIO0000001587 (Italienisch), EIO0000001588 (Spanisch), EIO0000001589 (Chinesisch),
Modicon M580CCOTF (Change Configuration On The Fly), Benutzerhandbuch	EIO0000001590 (Englisch), EIO0000001591 (Französisch), EIO0000001592 (Deutsch), EIO0000001594 (Italienisch), EIO0000001593 (Spanisch), EIO0000001595 (Chinesisch)
Modicon X80, Digitale Ein-/Ausgangsmodule, Benutzerhandbuch	35012474 (Englisch), 35012475 (Deutsch), 35012476 (Französisch), 35012477 (Spanisch), 35012478 (Italienisch), 35012479 (Chinesisch)
Modicon X80, BMXEHC0200 Zählmodul, Benutzerhandbuch	35013355 (Englisch), 35013356 (Deutsch), 35013357 (Französisch), 35013358 (Spanisch), 35013359 (Italienisch), 35013360 (Chinesisch)
Erdung und Elektromagnetische Verträglichkeit von SPS-Systemen, Grundlagen und Maßnahmen - Benutzerhandbuch	33002439 (ENG) 33002440 (FRE) 33002441 (GER) 33002442 (SPA) 33003702 (ITA) 33003703 (CHS)
EcoStruxure™ Control ExpertProgrammiersprachen und -struktur, Referenzhandbuch	35006144(Englisch), 35006145(Französisch), 35006146(Deutsch), 35013361(Italienisch), 35006147 (Spanisch), 35013362(Chinesisch)
EcoStruxure™ Control ExpertSystembits und -wörter, Referenzhandbuch	EIO0000002135 (Englisch), EIO0000002136 (Französisch), EIO0000002137 (Deutsch), EIO0000002138 (Italienisch), EIO0000002139 (Spanisch), EIO0000002140 (Chinesisch)
EcoStruxure™ Control Expert, Betriebsarten	33003101 (Englisch), 33003102 (Französisch), 33003103 (Deutsch), 33003104 (Spanisch), 33003696 (Italienisch), 33003697 (Chinesisch)

Titel der Dokumentation	Referenznummer
EcoStruxure™ Control Expert, Installationshandbuch	35014792 (Englisch), 35014793 (Französisch), 35014794 (Deutsch), 35014795 (Spanisch), 35014796 (Italienisch), 35012191 (Chinesisch)
Web Designer für FactoryCast - Benutzerhandbuch	35016149 (Englisch), 35016150 (Französisch), 35016151 (Deutsch), 35016152 (Italienisch), 35016153 (Spanisch), 35016154 (Chinesisch)
Modicon-Steuerungsplattform Cybersicherheit, Referenzhandbuch	EIO0000001999 (ENG) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002003 (SPA) EIO0000002002 (ITA) EIO0000002004 (CHS)

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

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

Norm/Standard	Beschreibung
ISO 14119:2013	Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
ISO 13850:2015	Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
IEC 62061:2021	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Steuerungssysteme
IEC 61508-1:2010	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.

Marken

Windows ist eine eingetragene Marke der Microsoft Corporation.

Merkmale des Moduls BMENUA0100

Einführung

In diesem Kapitel wird das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA Server beschrieben.

Merkmale des Moduls

Einführung

Das OPC UA-Servermodul Modicon BMENUA0100 stattet Modicon M580-Steuerungssysteme mit leistungsstarken OPC UA-Funktionen aus.

OPC UA ist eine sichere und offene Kommunikationsplattform für die industrielle Kommunikation. Sie wurde im Hinblick auf Flexibilität und Skalierbarkeit entwickelt und eignet sich für den Einsatz mit ressourcenbeschränkten IoT-Sensoren vor Ort bis hin zu in Datacentern oder in der Cloud gehosteten Enterprise-Servern. Über die Verbindung und Verlagerung von Daten hinaus definiert OPC UA ein umfassendes Informationsmodell für die Veröffentlichung und Verwaltung von Metadaten und Systemkontexten, um die Automatisierungstechnik und Systemintegration zu vereinfachen.

Durch die Einführung eines Kommunikationsstandards für moderne, vernetzte industrielle Betriebsabläufe stellt OPC UA eine einheitliche Verbindung zwischen vernetzten Produkten in den Feld-Controllern und Unternehmensanwendungen und Analytik bereit. OPC UA wurde für die Kompatibilität mit IT- und Sicherheitsinfrastrukturen wie Firewalls, VPNs und Proxys ausgelegt. Die Skalierungskapazität ermöglicht eine Ausrichtung sowohl an funktionalen Anforderungen wie auch an der Bandbreite.

Merkmale

Das Modul BMENUA0100 umfasst einen OPC UA-Server und einen integrierten Ethernet-Switch. Es ist im **Hardwarekatalog** Control Expert in der Modulgruppe **Kommunikation** enthalten.

Mit dem Modul BMENUA0100 werden die folgenden Funktionen auf der Modicon M580-Plattform bereitgestellt:

Allgemeines:

- Direkter und optimierter Zugriff auf das Data Dictionary von Control Expert für die Zuordnung zwischen Control Expert- und OPC UA-Variablen, Seite 51.
- Unterstützung von Hot Standby-Konfigurationen über OPC UA-Redundanz, Seite 56.
- Kompatibilität mit M580-Sicherheitssystemen als nicht störendes Modul Typ 1 gemäß Definition des TÜV Rheinland.
- Nahtlose Ethernet-Baugruppenträger-Kommunikation.
- DHCP/FDR-Client für den Download von gespeicherten (nicht cybersicherheitsspezifischen) Konfigurationseinstellungen.
- NTP-Zeitserver, Seite 136 und Clientsynchronisation.
- Mehrere Diagnosemethoden, einschließlich LEDs, Seite 144, DDT, Seite 149, OPC_UA-Variablen und Datenelemente, Seite 161, Syslog, Seite 165, Modbus, Seite 169, SNMP, Seite 171 und sichere Webseiten, Seite 171.
- Firmware-Aktualisierung über das Tool EcoStruxure™ Automation Device Maintenance, Seite 181.
- Firmware-Integritätsprüfung.
- Hardware-gesicherter Speicher.

Cybersicherheit:

- Sichere Kommunikation über HTTPS, OPC UA (optional) und IPsec (optional).
- Über HTTPS konfigurierbare OPC UA-Sicherheit, Seite 100 auf Modulebene.
- Die Möglichkeit, den ein- und ausgehenden Kommunikationsstrom durch Aktivieren und Deaktivieren von Kommunikationsdiensten, Seite 102 zu steuern.
- IPsec, Seite 109 basierend auf einem vorinstallierten Schlüssel (PSK) zur Sicherung von Diensten wie SNMPv1, Modbus/TCP, Syslog und NTPv4.

  HINWEIS: BMENUA0100 unterstützt den Hauptmodus IPsec. Ein IPsec-Kanal kann entweder durch den BMENUA0100-Server oder einen dezentralen OPC UA-Client geöffnet werden. Auf einem PC-Client wird IPsec auf den Systemen Windows 7, 10 und Windows Server 2016 unterstützt und validiert.

Authentifizierungsmanagement:

- Rollenbasierte Zugriffsskontrolle (Role-Based Access Control, RBAC) und Benutzerauthentifizierung, Seite 122 für HTTPS- und OPC UA-Clients.
- Zertifikate, Seite 113 für OPC UA-Client-Anwendungseinheiten.

Das M580-Kommunikationsmodul bieten u. a. folgende Funktionen:

- Ethernet-Baugruppenträger-Port für die Ethernet-Kommunikation über das lokale Ethernet-Hauptrack.
- X-Bus-Baugruppenträger-Port für 24-VDC-Spannungsversorgung und Rack-Adressierung.
- NTP-Zeitserver, Seite 136 und Clientsynchronisation.

Modulbeschreibung

Einführung

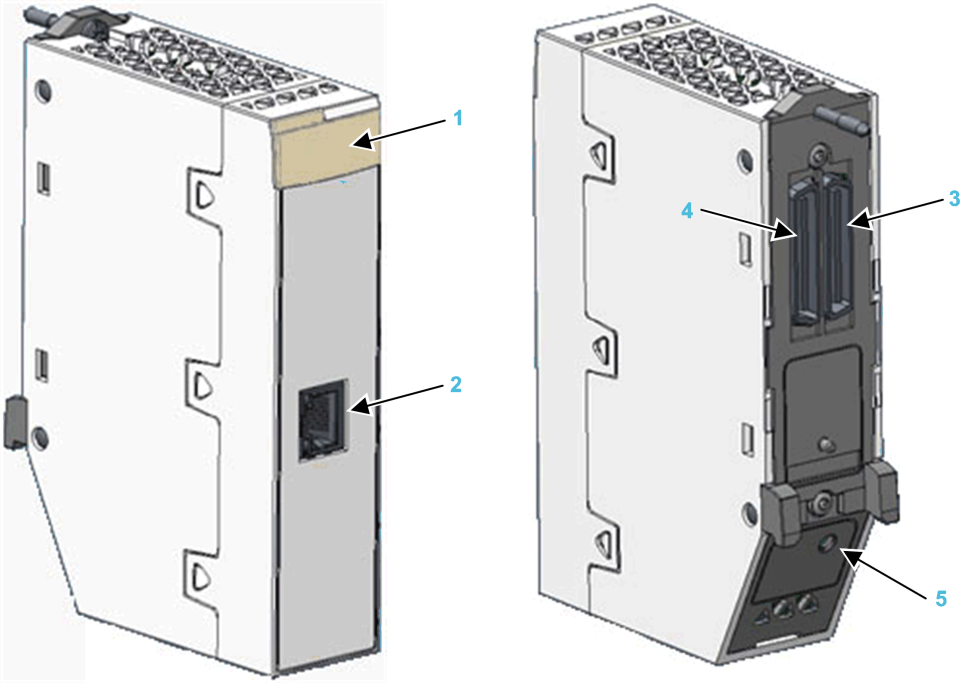
Schneider Electric bietet zwei Ethernet-Kommunikationsmodule mit integriertem OPC UA-Server für die Kommunikation mit OPC UA-Clients, einschließlich SCADA:

- BMENUA0100-Modul für Standardumgebungen
- BMENUA0100H-Modul für raue Umgebungsbedingungen

Das Modul kann nur in einem Ethernet-Steckplatz in einem zentralen, lokalen Ethernet-Rack installiert werden. Im Abschnitt *Unterstützte Konfigurationen des BMENUA0100-Moduls*, Seite 65 finden Sie eine Beschreibung der unterstützten Modulplatzierungen, einschließlich der maximalen Anzahl von BMENUA0100-Modulen, die in einem Rack platziert werden können.

Physische Beschreibung

Die nachstehende Abbildung zeigt die externen Merkmale des Moduls BMENUA0100:



1 LED-Bereich

2 Steuerungsport mit LEDs für Ethernet-Verbindung und -Aktivität

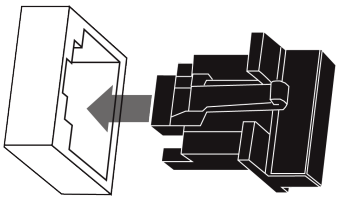
3 Ethernet-Baugruppenträger-Port

4 X Bus-Baugruppenträger-Port

5 Drehwahlschalter für den Cybersicherheits-Betriebsmodus

Informationen zum Lesen der Modul-LEDs finden Sie im Abschnitt LED-Diagnose, Seite 144.

Wenn der Ethernet-Steuerungsport nicht aktiviert ist, verwenden Sie den Verschlussstopfen, der mit jedem Modul geliefert wird, um zu verhindern, dass Schmutz in den Steuerungsport gelangt:



Externe Ports

Das BMENUA0100-Modul verfügt über die folgenden externen Ports:

Port	Beschreibung
Steuerungsport	Der Steuerungsport ist der einzelne Port, der sich an der Vorderseite des BMENUA0100-Moduls befindet. Er verfügt über die folgenden Funktionen: • Wenn der Steuerungsport aktiviert ist, handelt es sich hierbei um die Exklusivschnittstelle für die OPC UA-Kommunikation, es sei denn, IPv6 ist konfiguriert. ◦ Wenn IPv6 konfiguriert ist, können sowohl der Baugruppenträger-Port als auch der Steuerungsport für die OPC UA-Kommunikation verwendet werden. ◦ Wenn IPv6 nicht konfiguriert ist, können Sie OPC UA-Clients im Baugruppenträger-Netzwerk über den BMENUA0100-Steuerungsport verbinden, wenn auf dem Computer, der den OPC UA-Client hostet, ein Pfad definiert/deklariert wurde. • Betriebsgeschwindigkeit bis zu 1 Gbit/s. Bei Betrieb mit einer Geschwindigkeit von: ◦ 1 Gbit/s – Verwenden Sie nur geschirmte, verdrillte CAT6-Vierleiterkabel aus Kupfer. ◦ 10/100 Mbit/s – Verwenden Sie geschirmte, verdrillte CAT5- oder CAT6-Vierleiterkabel aus Kupfer. • Dualer IP-Stack, der sowohl die IPv4- (32-Bit) als auch die IPv6- (128-Bit) IP-Adressierung unterstützt: ◦ Für das Modul ist sowohl IPv4 als auch IPv6 konfiguriert. ◦ Die IPv6-Konfiguration kann statisch oder dynamisch sein (über SLAAC). ◦ Die IPv4-Standardeinstellung, Seite 127 wird basierend auf der MAC-Adresse des Moduls automatisch zugewiesen, wenn keine IP-Adresse konfiguriert ist. • Sicherer Zugriff auf den OPC UA-Server über IPv4- und IPv6-Protokolle. • Sicheres HTTPS-Protokoll (über IPv4) für die Firmware-Aktualisierung, Seite 181 und die Konfiguration der Cybersicherheit, Seite 92. • Unterstützung des sicheren NTPv4-Protokolls. • Von IPsec bereitgestellte Sicherheit für nicht sichere Dienste, einschließlich SNMPv1, Modbus TCP und Syslog.
Ethernet-Baugruppenträger-Port	Der Ethernet-Baugruppenträger-Port von BMENUA0100 unterstützt das IPv4-Protokoll (32 Bit). Wenn der Steuerungsport deaktiviert ist, kann der Baugruppenträger-Port die OPC UA-Kommunikation unterstützen. Der Baugruppenträger-Port weist folgende Merkmale auf: • Betriebsgeschwindigkeit bis zu 100 Mbit/s • Modbus TCP IPv4-Ethernet-Konnektivität mit der Steuerung: ◦ Der Ethernet-Baugruppenträger-Port ist der exklusive Port für die Modbus-Diagnose. • Exklusiver Port für eine andere als die Cybersicherheitskonfiguration (IP, NTPv4, SNMPv1) durch: ◦ Control Expert v14.1 und alle nachfolgenden unterstützenden Versionen ◦ FDR/DHCP-Server • Wenn der Steuerungsport deaktiviert ist, ermöglicht der Ethernet-Baugruppenträger-Port den sicheren Zugriff auf den OPC UA-Server über das IPv4-Protokoll und unterstützt die folgenden Dienste: ◦ Sicheres HTTPS-Protokoll für die Firmwareaktualisierung, Seite 181 und die Konfiguration der Cybersicherheit, Seite 92. ◦ NTPv4, SNMPv1/v3 und Syslog.
X Bus-Baugruppenträger-Port	Das BMENUA0100-Modul verwendet die X Bus-Baugruppenträger-Kommunikation für Folgendes: • Empfang von 24-VDC-Spannung.

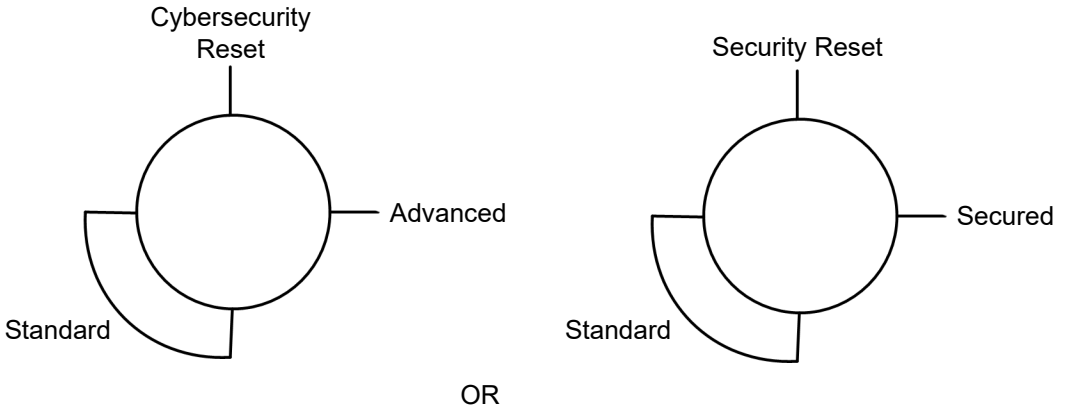
Port	Beschreibung
	• Erkennung der Rack- und der Steckplatzadresse des BMENUA0100-Moduls. **HINWEIS:** Es erfolgt keine weitere Kommunikation über den X Bus-Baugruppenträger-Port des BMENUA0100-Moduls.

Drehwahlschalter

Auf der Rückseite des Moduls befindet sich ein Drehwahlschalter mit vier Stellungen. Stellen Sie diesen Drehwahlschalter ein, um einen Modus für die Steuerung zu konfigurieren.

HINWEIS: Im Lieferumfang ist ein Kunststoffschraubendreher enthalten. Verwenden Sie diesen oder einen gleichwertigen, um die Stellung des Drehwahlschalters zu ändern. Verwenden Sie keine Metallschraubendreher.

Je nach Version des Moduls sind die Stellungen am Drehwahlschalter:



Die Einstellungen sind:

- „Advanced“ oder „Secured“: Erweiterter (RL 6 und höher) oder sicherer (vor RL 6) Modus, Seite 32
- „Standard“: Standardmodus, Seite 32
- „Cybersecurity/Security Reset“: Zurücksetzen der Cybersicherheit (RL 6 und höher) oder der Sicherheit (vor RL 6), Seite 33

HINWEIS:

- Der Drehwahlschalter ist nicht zugänglich, wenn das Modul im Rack platziert ist.
- Stellen Sie in einem Hot Standby-System sicher, dass die Stellungen des Drehwahlschalters des BMENUA0100-Moduls – sowohl im primären als auch im lokalen Standby-Hauptrack – identisch sind. Das System führt diese Überprüfung nicht automatisch für Sie durch.

Informationen zu jeder Position des Drehwahlschalters finden Sie in der Beschreibung des Betriebsmodus der Cybersicherheit, Seite 30.

Modul-LEDs

LED-Anzeige

Auf der Vorderseite des BMENUA0100-Moduls befindet sich ein Anzeigefeld mit 7 LEDs:

Die LEDs zeigen folgenden Informationen zum Modul an:

LED	Beschreibt den Status des Moduls
RUN	Betriebszustand
ERR	Erkannte Fehler
UACNX	OPC UA-Verbindungen
BS	Baugruppenträger-Port
NS	Steuerungsport
SEC	Zustand der Cybersicherheit
BUSY	Status des Datenwörterbuchs

Informationen zur Verwendung dieser LEDs für die Diagnose des Status des BMENUA0100-Moduls finden Sie im Abschnitt LED-Diagnose, Seite 144.

LEDs des Steuerungsports

Der Steuerungsport an der Vorderseite des Moduls verfügt über zwei LEDs, die den Status der Ethernet-Verbindung über den Port beschreiben:

- Die LED ACT weist auf das Vorhandensein von Ethernet-Aktivität am Port hin.
- Die LED LNK weist auf das Vorhandensein einer Ethernet-Verbindung und die Verbindungsgeschwindigkeit hin.

Informationen zur Verwendung der Steuerungsport-LEDs für die Diagnose des Status des Steuerungsports am BMENUA0100-Modul finden Sie im Abschnitt LED-Diagnose, Seite 148.

Normen und Zertifizierungen

Übersicht

In diesem Kapitel werden die Normen und Zertifizierungen beschrieben, die für das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server gelten.

Normen und Zertifizierungen

Download

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

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

BMENUA0100-Modulstandard

Behördliche Anforderungen

Das in das Modul BMENUA0100 integrierte OPC UA-Ethernet-Kommunikationsmodul entspricht den folgenden behördlichen Standards:

Kennzeichen	Anforderung
OPC Unified Architecture	OPC UA V1.03: Kommunikationsprotokoll OPC Unified Architecture Machine-to-Machine.

Kompatibilität der BMENUA0100-Firmware mit EcoStruxure™ Control Expert

Kompatibilität

Die mit der Software EcoStruxure™ Control Expert erstellten Anwendungen sind wie folgt mit der Firmware des BMENUA0100-Moduls kompatibel:

BMENUA0100-Firmwareversion	**EcoStruxure™ Control Expert-Softwareversion**	
	14.0	**ab 15.0**
1.01	Volle Kompatibilität	Nur Legacy-Funktionen der Firmwareversion 1.01 werden von der Software unterstützt[1, 2, 3].
1.10	Volle Kompatibilität	Volle Kompatibilität

1. Wenn ein BMENUA0100-Modul mit der Firmwareversion 1.01 eine mit EcoStruxure™ Control Expert V15 generierte Anwendung erhält, wobei:

- **Schnelle Abtastrate** (auf der Registerkarte „IP-Konfig.“, Seite 128) **Aktiviert** ist, wird diese Einstellung nicht implementiert.
- IPv4 für den Steuerungsport deaktiviert ist, wird der Steuerungsport des Moduls mit der IPv4-Adresse konfiguriert, die auf der Registerkarte **IP-Konfig.** für das Modul grau abgeblendet angezeigt wird.

  HINWEIS: Bei der grau abgeblendeten IPv4-Adresse kann es sich um die neueste, vom Benutzer eingegebene IPv4-Adresse oder um die automatisch von der Software EcoStruxure™ Control Expert vorgegebene IPv4-Adresse (172.16.12.1) handeln, wenn vorher keine IPv4-Adresse eingegeben wurde.
- NTP, Seite 138 wurde mit einer IPv6-Adresse konfiguriert. Die Webseiten des Moduls geben fälschlicherweise an, dass NTP betriebsbereit ist, wenn der NTP-Dienst tatsächlich nicht betriebsbereit ist.

2. Wenn zwei BMENUA0100-Module mit der Firmwareversion 1.01 in einem Hot Standby-Rack mit EcoStruxure™ Control Expert V15 konfiguriert sind, gelten die in den vorhergehenden Punkten aufgeführten Einschränkungen auch für diese Module.

3. Wenn SNMP in Control Expert aktiviert ist, müssen Sie die IPv4-Adresse des SNMP-Managers auf der SNMP-Registerkarte für das BMENUA0100-Modul, Seite 140 angeben, damit der SNMP-Manager auf die SNMP-MIB zugreifen kann.

HINWEIS: Die für das BMENUA0100-Modul angezeigten Webseiten ist von der Firmwareversion des Moduls abhängig (z. B. Version 1.01, 1.10 oder 2.01).

Funktionsbeschreibung des Moduls BMENUA0100

Einführung

In diesem Kapitel werden die unterstützten Funktionen des Ethernet-Kommunikationsmoduls BMENUA0100 mit integriertem OPC UA-Server beschrieben.

Einstellungen des Cybersicherheits-Betriebsmodus

Einführung

Das BMENUA0100-Modul kann für den Betrieb im erweiterten (oder sicheren) Modus oder im Standardmodus konfiguriert werden. Der Drehwahlschalter mit 4 Stellungen an der Rückseite des Moduls bestimmt den Betriebsmodus.

Die drei Drehschalterstellungen sind:

- Erweiterter (oder sicherer) Modus
- Standardmodus
- Zurücksetzen der Cybersicherheit (oder Sicherheit)

HINWEIS:

- Die Standardkonfiguration des Moduls ist der erweiterte (oder sichere) Modus.
- Sie können die Stellung des Drehwahlschalters auf der Startseite, Seite 97 der Webseiten des Moduls anzeigen.

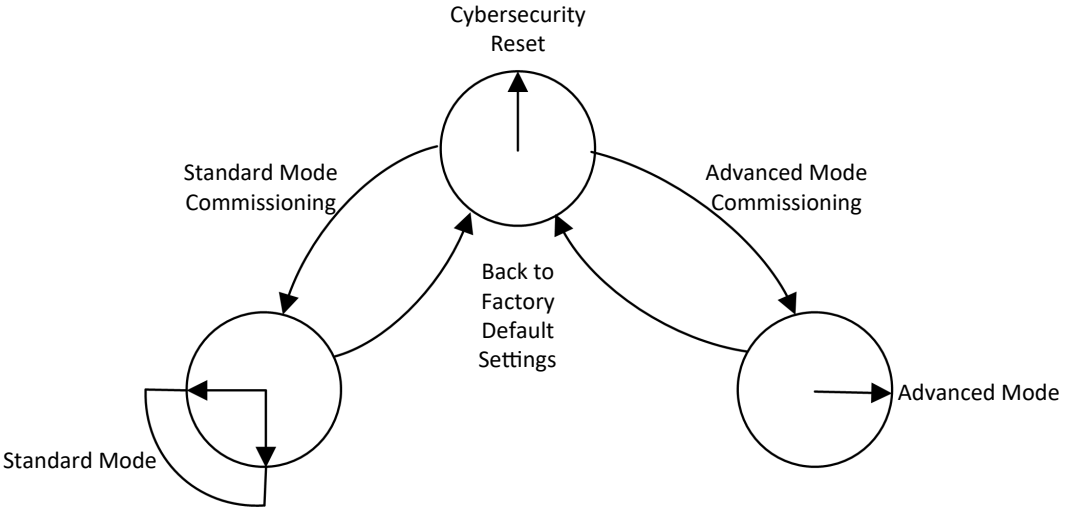
Da der Drehwahlschalter nicht zugänglich ist, während sich das Modul im Rack befindet, kann die Schalterstellung nur geändert werden, wenn das Modul ausgeschaltet und aus dem Rack entfernt wird. Nach der Auswahl einer neuen Schalterstellung kann das Modul wieder in das Rack eingeführt und mit Spannung versorgt werden.

HINWEIS: Verwenden Sie nur den kleinen Kunststoffschraubendreher, der im Lieferumfang des Moduls enthalten ist, Seite 25, um die Schalterstellung zu ändern und einen Betriebsmodus für die Cybersicherheit zu konfigurieren.

Änderung des Betriebsmodus

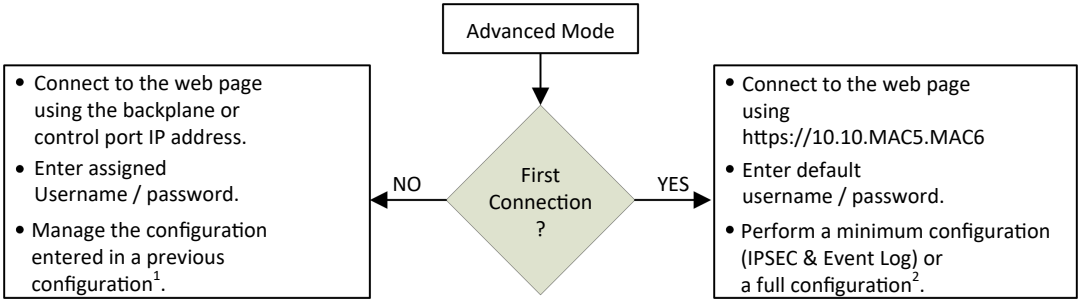
Jedes Mal, wenn Sie den Cybersicherheits-Betriebsmodus vom erweiterten (oder sicheren) Modus in den Standardmodus oder vom Standardmodus in den erweiterten (oder sicheren) Modus umschalten, führen Sie einen Vorgang Zurücksetzen der Cybersicherheit (oder Sicherheit), Seite 88 durch, bevor der neue Modus konfiguriert wird.

Die Stellung des Drehwahlschalters bestimmt den Betriebszustand des Moduls wie folgt:



Ein neues Standardmodul (vorkonfigurierte Werkseinstellung) oder ein Modul, für das ein **Zurücksetzen der Cybersicherheit (oder Sicherheit)** durchgeführt wurde, kann im Standardmodus, Seite 87 oder erweiterten (oder sicheren) Modus, Seite 85 in Betrieb genommen werden.

Der Prozess für die Konfiguration des Moduls für einen Betrieb im erweiterten (oder sicheren) Modus fällt unterschiedlich aus, je nachdem, ob Sie nach einem Cybersicherheits- (oder Sicherheits-) Reset zum ersten Mal eine Verbindung zu den Konfigurationseinstellungen des Moduls herstellen:



1 Informationen zur Verwaltung der Konfiguration finden Sie im Kapitel zur Konfiguration, Seite 92.

2 Informationen zur Durchführung einer Konfiguration bei der ersten Verbindung finden Sie im Abschnitt Inbetriebnahme im erweiterten (oder sicheren) Modus, Seite 85.

Erweiterter (oder sicherer) Modus

Im erweiterten (oder sicheren) Modus kommuniziert das Modul erst dann über den Steuerungsport oder den Baugruppenträger-Port mit dem Prozess, wenn gültige Einstellungen für die Cybersicherheit konfiguriert wurden. Nach der Konfiguration des erweiterten (oder sicheren) Modus können Sie die Cybersicherheitseinstellungen auf den Modul-Webseiten, Seite 92 konfigurieren, auf die mit dem HTTPS-Protokoll entweder über den Baugruppenträger- oder den Steuerungsport zugegriffen werden kann. Im erweiterten (oder sicheren) Modus unterstützt das Modul die Cybersicherheitsstufe, die in der Cybersicherheitskonfiguration angegeben ist. Erst nachdem die Cybersicherheitseinstellungen konfiguriert wurden, können die Einstellungen für IP-Adresse, NTP-Client und SNMP-Agent, Seite 126 mithilfe der Konfigurationssoftware Control Expert konfiguriert werden.

Standardmodus

Im Standardmodus kann die Modulkommunikation ohne Konfiguration der Cybersicherheit beginnen. Einstellungen für die Cybersicherheit sind nicht erforderlich und können nicht konfiguriert werden. Nur die IP-Adresse und andere in Control Expert verfügbare Einstellungen können konfiguriert werden.

Zurücksetzen der Cybersicherheit (oder Sicherheit)

Das **Zurücksetzen der Cybersicherheit (oder Sicherheit)** stellt die werkseitigen Standardkonfigurationseinstellungen wieder her. Es löscht alle vorhandenen Einstellungen für Cybersicherheit, Allowlist, Zertifikate und rollenbasierte Zugriffskontrolle. Um den Reset der Cybersicherheit (oder Sicherheit) abzuschließen, schalten Sie die Spannungsversorgung des BMENUA0100-Moduls aus und wieder ein oder entfernen Sie das Modul physisch aus dem Rack (wodurch die Spannungsversorgung abgeschaltet wird) und setzen Sie es dann wieder in das Rack ein (wodurch die Spannungsversorgung wieder eingeschaltet wird). Während die Werkseinstellungen wiederhergestellt werden, blinkt die **RUN**-LED grün. Nach Abschluss des Prozesses leuchtet die **RUN**-LED dauerhaft grün und die Dienste sind deaktiviert.

Diese Einstellung kann entweder über den Drehwahlschalter oder über die Webseiten (im erweiterten (oder sicheren) Modus) vorgenommen werden:

- Wenn über den Drehwahlschalter eingestellt: Das Modul funktioniert nicht mehr, bis das Modul aus dem Rack entfernt wird, der Drehwahlschalter entweder in die Stellung des erweiterten (oder sicheren) Modus („Advanced“ oder „Secured“) oder des Standardmodus („Standard“) zurückgesetzt und das Modul wieder in das Rack eingesetzt wird. Die erforderlichen Konfigurationen müssen angewendet werden.
- Wenn über die Webseiten festgelegt: Nach dem Aus- und Wiedereinschalten des Moduls - oder Hot-Swapping - im Standard- oder im erweiterten (oder sicheren) Modus. Sowohl die Cybersicherheits- als auch die IP-Adresseinstellungen müssen konfiguriert werden.

  HINWEIS: Nach einem Reset der Cybersicherheit (oder Sicherheit) des BMENUA0100-Moduls gelten die folgenden Bedingungen für das Modul:

  - Es werden keine Gerätezertifikate beibehalten.
  - Alle Dienste sind deaktiviert, mit Ausnahme von HTTPS, das zur Erstellung der Konfiguration der Cybersicherheit über den Steuerungsport verwendet wird.
  - Die Werkseinstellungen werden übernommen, einschließlich:
    - Standardeinstellungen, Seite 33 für Benutzername/Passwort.
    - Standardeinstellung für die IP-Adresse: 10.10.MAC5.MAC6, Seite 126.

  HINWEIS: Wenn die letzten beiden Bytes der MAC-Adresse (*MAC5.MAC6*) *0,0* in der Standardadresse entsprechen, stellen Sie eine Punkt-zu-Punkt-Kabelverbindung zwischen Ihrem Computer und dem Controller, dem Kommunikationsmodul oder einem anderen Modul her.

Standardkombination Benutzername/Passwort

Die standardmäßige Kombination aus Benutzername und Passwort ist von der Einstellung des Betriebsmodus der Cybersicherheit abhängig:

- Erweiterter (oder sicherer) Modus: admin / password
- Standardmodus: installer / Inst@ller1

HINWEIS: Sie werden bei der ersten Verwendung im erweiterten (oder sicheren) Modus aufgefordert, das Passwort zu ändern. Überprüfen Sie Ihre lokalen Gesetze und Vorschriften, ob dies erforderlich ist.

Im erweiterten (oder sicheren) Modus und im Standardmodus unterstützte Funktionen

Die folgenden Funktionen werden vom BMENUA0100-Modul im erweiterten (oder sicheren) Modus und im Standardmodus unterstützt:

Modus	**Standardmodus**			**Erweiterter (oder sicherer) Modus**		
Steuerungsport	**Deaktivieren**	**Aktivieren**		**Deaktivieren**	**Aktivieren**	
Ethernet-Port	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**
OPC UA-Komm.	Ja	Nein	Ja	Ja	Nein	Ja
Sicherheitseinstellungen (4)	Keine	–	Keine	Keine, Signieren, Signieren und Verschlüsseln (Standardwert)	–	Keine, Signieren, Signieren und Verschlüsseln (Standardwert)
Benutzerauthentifizierung	Keine Authentifizierung (anonym)	–	Keine Authentifizierung (anonym)	Bediener, Techniker, keine Authentifizierung (anonym)	–	Bediener, Techniker, keine Authentifizierung (anonym)
SNMP V1	Ja (1, 2)	Ja (1, 2)	Ja (1, 2)	Ja (1)	Ja (1)	Ja (1)
SNMP V3	Ja (1, 2)	Ja (1, 2)	Ja (1, 2)	Ja (1)	Ja (1)	Ja (1)
NTP V4	Nur Client (1)	Client (1), Server	Ja, nur Client (1)	Nur Client (1)	Client (1), Server	Ja, nur Client (1)
Ereignisprotokoll	Nein	Nein	Nein	Ja	Ja	Ja
IPsec	Nein	Nein	Nein	Nein	Nein	Ja für Modbus, SNMP V1/V3, NTP V4 (3) und Syslog (IPsec ist standardmäßig aktiviert)
Webbasierte CS-	Nein	Nein	Nein	Ja	Ja	Ja

Modus	**Standardmodus**			**Erweiterter (oder sicherer) Modus**		
Steuerungsport	**Deaktivieren**	**Aktivieren**		**Deaktivieren**	**Aktivieren**	
Ethernet-Port	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**
Konfigurationsänderung (HTTPS)						
Benutzerauthentifizierung	–	–	–	Admin	Admin	Admin
Netzwerkdienste-Kommunikationsserver aktivieren/deaktivieren	Falls unterstützt, immer aktiviert (siehe oben)	Falls unterstützt, immer aktiviert (siehe oben)	Falls unterstützt, immer aktiviert (siehe oben)	Alle Dienste sind konfigurierbar (standardmäßig deaktiviert)	Alle Dienste sind konfigurierbar (standardmäßig deaktiviert)	Alle Dienste sind konfigurierbar (standardmäßig deaktiviert)
Webdiagnose (nur Startseite und Diagnoseseite)	Ja	Ja	Ja	Ja	Ja	Ja
Benutzerauthentifizierung	Monteur (Standardanmeldeinformationen)	Monteur (Standardanmeldeinformationen)	Monteur (Standardanmeldeinformationen)	Administrator, Bediener, Techniker, Monteur	Administrator, Bediener, Techniker, Monteur	Administrator, Bediener, Techniker, Monteur
Firmwareaktualisierung (HTTPS)	Ja	Ja	Ja	Ja	Ja	Ja, wenn HTTPS aktiviert ist
Benutzerauthentifizierung	Monteur (Standardanmeldeinformationen)	Monteur (Standardanmeldeinformationen)	Monteur (Standardanmeldeinformationen)	Monteur	Monteur	Monteur
Filterung: Alle weiterleiten	–	–	(immer aktiviert)	–	–	Alle Protokolle weiterleiten
Filterung: Konfiguriertes Weiterleitungsprotokoll	–	–	–	–	–	Konfigurierte Protokolle weiterleiten

Modus	**Standardmodus**			**Erweiterter (oder sicherer) Modus**		
Steuerungsport	**Deaktivieren**	**Aktivieren**		**Deaktivieren**	**Aktivieren**	
Ethernet-Port	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**
Filterung: Control Expert-Datenflüsse zum Gerätenetzwerk (einschließlich Steuerung) (FTP, EIP, Explizit, Modbus, Ping) nur über IPv4[5]	–	–	Weiterleitung der Control Expert-Datenflüsse vom Steuerungsnetzwerk zum Gerätenetzwerk (immer aktiviert)	–	–	Weiterleitung der Control Expert-Datenflüsse vom Steuerungsnetzwerk zum Gerätenetzwerk (standardmäßig deaktiviert)

1. Konfigurierbar mit Control Expert.
2. Im Standardmodus wird die SNMP-Version des BMENUA0100-Moduls in Control Expert eingestellt. Wenn SNMP auf V3 eingestellt und das Modul wie folgt konfiguriert ist:
   - Firmwareversion 2 (BMENUA0100.2) verwendet SNMP V3 mit der Sicherheitsstufe ohne Autorisierung und ohne Datenschutz (NoAuthNoPriv).
   - Firmware vor Version 2 (BMENUA0100) verwendet SNMP V1.

   Weitere Informationen finden Sie unter SNMP-Agent-Konfiguration in Control Expert und auf den Webseiten, Seite 140.
3. NTP V4 kann so konfiguriert werden, dass der Transport außerhalb des IPsec-Tunnels erfolgt.
4. Für den Standard- und den erweiterten (oder sicheren) Cybersicherheits-Betriebmodus, wenn die Sicherheitseinstellungen auf *Keine* gesetzt sind, erfolgt keine Benutzerauthentifizierung (d. h. die OPC UA-Einstellung, Seite 111 **Benutzer-ID-Tokentypen** ist auf *Anonym* gesetzt).
5. Um Control Expert den Online-Zugriff auf die Steuerung oder das Gerätenetzwerk zu ermöglichen, konfigurieren Sie den PC (auf dem Control Expert installiert ist) mit einer IP-Adresse in demselben Subnetz wie der Steuerungsport des BMENUA0100-Moduls und verwenden Sie die IP-Adresse des BMENUA0100-Modulsteuerungsports als IP-Adresse des PC-Gateways. In diesem Fall darf sich keine IP-Adresse des PC im selben Subnetz befinden wie der Baugruppenträger-Port des BMENUA0100-Moduls.

OPC UA-Dienste

Einführung

In diesem Abschnitt werden die Dienste beschrieben, die von dem im Modul BMENUA0100 integrierten OPC UA-Server unterstützt werden.

BMENUA0100 - Betriebskenndaten des OPC UA-Servers

Einschränkungen

Maximal:

- können 100.000 Knoten im Adressraum für den Datenzugriff des BMENUA0100-OPC UA-Servers veröffentlicht werden.
- kann 192 MB Arbeitsspeicher dem OPC UA-Server des BMENUA0100-Moduls zugewiesen werden.

HINWEIS: Wenn einer der beiden Grenzwerte überschritten wird, wechselt der Server-Adressraum in den Zustand *LimitsExceeded*.

HINWEIS: Die zur Einrichtung eines Zeitabonnements erforderliche Zeit kann erheblich von der Anzahl der Elemente und der Anzahl der verbundenen Clients abhängen.

Weitere Einschränkungen, der Kontext, in dem die Überschreitung auftritt, und die Folgen, wenn die Grenzwerte überschritten werden, sind nachstehend aufgeführt:

Grenzwert	Wert	OPCUA-Dienst	Dienstparameter	Ergebnis
Kumulative Sitzungsanzahl	10	*CreateSession*	(Nicht zutreffend)	Ergebniscode des Dienstes *Bad_TooManySessions* (Fehler - Zu viele Sitzungen)
Minimales Sitzungs-Timeout	30 s	*CreateSession*	Angefordertes Sitzungs-Timeout	Geändertes Sitzungs-Timeout
Kumulatives Sitzungs-Timeout	3600 s	*CreateSubscription*	Angefordertes Sitzungs-Timeout	Geändertes Sitzungs-Timeout
Maximale kumulative Abonnementanzahl	40	*CreateSubscription*	(Nicht zutreffend)	Ergebniscode des Dienstes *Bad_TooManySubscriptions* (Fehler - Zu viele Abonnements)
Minimales Veröffentlichungsintervall	250 ms[1] 20 ms[2]	*CreateSubscription*	Angefordertes Veröffentlichungsintervall	Geändertes Veröffentlichungsintervall
Maximales Veröffentlichungsintervall	10 s	*CreateSubscription*	Angefordertes Veröffentlichungsintervall	Geändertes Veröffentlichungsintervall
Maximale Abonnementlaufzeit	300 s	*CreateSubscription*	Min. (Angefordertes Veröffentlichungsintervall, 3.600.000) * Angeforderte Lebensdauer	Geänderte Lebensdauer
Maximale Anzahl Benachrichtigungen pro	12500	*CreateSubscription*	Max. Anzahl Benachrichtigungen pro Veröffentlichung	Die maximale Benachrichtungskapazität beträgt daher (1000 / Geändertes

Grenzwert	Wert	OPCUA-Dienst	Dienstparameter	Ergebnis
Veröffentlichung				Veröffentlichungsintervall) * 1000 Benachrichtigungen pro Sekunde.
Minimales Abtastintervall	125 ms[1] 20 ms[2]	*CreateMonitoredtems*	Überwachungsparameter Abtastintervall	Geändertes Abtastintervall
Maximale Größe der Nachrichtenwarteschlange	3	*CreateMonitoredtems*	Überwachungsparameter Größe der Warteschlange	Geänderte Warteschlangengröße
Maximale kumulative Anzahl der überwachten Elemente	50010 oder 35010[3, 4] 2010[2]	*CreateMonitoredtems*	(Nicht zutreffend)	Ergebniscode des Dienstes *Bad_TooManyMonitoredItems* (Fehler - Zu viele überwachte Elemente)
Maximale Anzahl Abonnements pro Sitzung	4	–	–	–
Maximale Anzahl überwachter Elemente pro Abonnement	25000	–	–	–

1. Wenn Fast Sampling (schnelle Abtastung) deaktiviert ist.

2. Wenn Fast Sampling (schnelle Abtastung) aktiviert ist.

3. Wenn Fast Sampling deaktiviert und der Server wie folgt konfiguriert ist:

- ein Abtastintervall von mindestens 1 Sekunde und
- ein Veröffentlichungsintervall von mindestens 1 Sekunde

4. Wenn die Quellzeitstempelung aktiviert, Seite 130 ist, ist das Maximum 35010. Wenn nicht aktiviert, ist das Maximum 50010.

OPC UA-Server

Einführung

Der Hauptzweck des Ethernet-Kommunikationsmoduls BMENUA0100 ist die Bereitstellung eines OPC UA-Kommunikationskanals über Ethernet zwischen M580-Steuerungen und OPC UA-Clients. Die Daten der M580-Steuerung werden den Variablen im Modul BMENUA0100 zugeordnet und OPC UA-Clients über einen OPC UA-Kommunikations-

Stack, der in das Modul BMENUA0100 integriert ist, zur Verfügung gestellt. OPC-UA-Clients verbinden sich mit dem integrierten OPC-UA-Server-Stack über die IP-Adresse des Steuerungsports oder Baugruppenträger-Ports des BMENUA0100-Moduls, wodurch eine Client-Server-Verbindung hergestellt wird. Das BMENUA0100-Modul kann bis zu zehn (10) gleichzeitige OPC UA-Clientverbindungen für die Firmwareversion 1.1 (oder 3 (3) gleichzeitige OPC UA-Clientverbindungen für die Firmwareversion 1.0) verwalten.

HINWEIS: Die Bedingungen jeder Verbindung zwischen einem OPC UA-Client und dem in das Modul BMENUA0100 integrierten OPC UA-Server werden vom Client festgelegt, der die Attribute der Verbindung zwischen dem Client und dem Server bestimmt.

Der in das Modul BMENUA0100 integrierte OPC UA-Server-Stack besteht aus Funktionalitäten, die durch die folgenden Begriffe definiert sind:

- Profil: Eine Definition der Funktionalität, die weitere Profile, Facetten, Konformitätsgruppen und Konformitätseinheiten umfasst.
- Facet: Definiert eine Teilfunktionalität.
- Konformitätsgruppe: Eine Sammlung von Konformitätseinheiten.
- Konformitätseinheit: Ein bestimmter Dienst, z. B. Lesen, Schreiben usw.

Vom Modul BMENUA0100 unterstütztes Profil

Das Modul BMENUA0100 unterstützt das **Embedded 2017 UA Server-Profil**. Wie auf der Website der OPC Foundation angegeben, handelt es sich bei diesem Profil um ein „FullFeatured Profile“, das für Geräte mit mehr als 50 MB Arbeitsspeicher und einem leistungsstärkeren Prozessor konzipiert ist. Dieses Profil baut auf dem Micro Embedded Device Server-Profil auf. Die wichtigsten Ergänzungen sind: Sicherheitsunterstützung über die Sicherheitsrichtlinien und Unterstützung für das Standard DataChange Subscription Server Facet. Dieses Profil erfordert außerdem, dass Server alle OPC UA-Typen verfügbar machen, die vom Server verwendet werden, einschließlich ihrer Komponenten und derer Super-Typen.

Weitere Informationen finden Sie auf der Website der OPC Foundation unter: http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017.

Vom Modul BMENUA0100 unterstützte Facets

Das BMENUA0100-Modul unterstützt die folgenden Facets:

- **Server Category > Facets > Core Characteristics**:
  - **Core 2017 Server Facet** (http://opcfoundation.org/UA-Profile/Server/Core2017Facet)

- **Server Category > Facets > Data Access**:
  - **ComplexType 2017 Server Facet** (http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017)
  - **Data Access Server Facet** (http://opcfoundation.org/UA-Profile/Server/DataAccess)
  - **Embedded DataChange Subscription Server Facet** (http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription)
- **Server Category > Facets > Generic Features**:
  - **Method Server Facet** (http://opcfoundation.org/UA-Profile/Server/Methods)
- **Security Category > Facets > Security Policy**:
  - **Basic128RSA15** (http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15)
  - **Basic256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256)
  - **Basic256Sha256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256)
- **Transport Category > Facets > Client-Server**:
  - **UA-TCP- UA-SC UA-Binary** (http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary)

In den folgenden Abschnitten werden die Dienste erörtert, die sich auf die oben genannten Facets beziehen und die vom Modul BMENUA0100 unterstützt werden.

BMENUA0100 – OPC UA-Server-Stack – Dienste

Unterstützte OPC UA-Dienste

Der OPC UA-Server-Stack des BMENUA0100-Moduls unterstützt die folgenden Dienstgruppen (Service Sets) und Dienste:

Service Set (Dienstgruppe)	Services (Dienste)
Attribute (Attribut)	• Read (Lesen) • Write (Schreiben)
Discovery (Erkennung)	• FindServers (Server finden) • GetEndpoints (Endunkte abrufen)
MonitoredItem (Überwachtes Element)	• CreateMonitoredItems (Überwachte Elemente erstellen) • ModifyMonitoredItems (Überwachte Elemente ändern) • DeleteMonitoredItems (Überwachte Elemente löschen) • SetMonitoringMode (Überwachungsmodus einstellen)
SecureChannel (Sicherer Kanal)	• OpenSecureChannel (Sicheren Kanal öffnen) • CloseSecurechannel (Sicheren Kanal schließen)

Service Set (Dienstgruppe)	Services (Dienste)
Session (Sitzung)	• CreateSession (Sitzung erstellen) • ActivateSession (Sitzung aktivieren) • CloseSession (Sitzung schließen)
Subscription (Abonnement)	• CreateSubscription (Abonnement erstellen) • ModifySubscription (Abonnement ändern) • DeleteSubscription (Abonnement löschen) • SetPublishingMode (Veröffentlichungsmodus einstellen) • SetMonitoringMode (Überwachungsmodus einstellen) • Publish (Veröffentlichen) • Republish (Erneut veröffentlichen)
View (Anzeigen)	• Browse (Durchsuchen) • BrowseNext (Weiter durchsuchen) • TranslateBrowsePathToNodeIds (Suchpfad für Knoten-Ids übersetzen) • RegisterNodes (Knoten registrieren) • UnregisterNodes (Knotenregistrierung aufheben)

HINWEIS: Eine Beschreibung dieser Dienstgruppen und Dienste finden Sie im Dokument *OPC Unified Architecture Specification Part 4: Services (Release 1.04)*.

BMENUA0100 - OPC UA-Server-Stack - Datenzugriffsdienste

Unterstützte Datenzugriffsdienste

Der Datenzugriff über den in das BMENUA0100-Modul integrierten OPC UA-Server-Stack wird durch die Unterstützung der folgenden Facets und zugehörigen Dienste aktiviert:

- Data Access Server Facet
- ComplexType 2017 Server Facet
- Core 2017 Server Facet

HINWEIS: In den folgenden Beschreibungen der Facets verweist der kursiv formatierte Text auf ein direktes Zitat des Quellmaterials der OPC Foundation. Klicken Sie auf die folgenden Links und öffnen Sie die Beschreibungen der einzelnen Facets mit dem *OPC Foundation Unified Architecture Profile Reporting Visualization Tool*.

Core 2017 Server Facet

Wie auf der OPC Foundation-Website angegeben, definiert das Core 2017 Server Facet „die Kernfunktionen, die für eine UA Server-Implementierung erforderlich sind. Die Kernfunktionalität umfasst die Möglichkeit zur Erkennung von Endpunkten, zur Einrichtung sicherer Kommunikationskanäle, zur Erstellung von Sitzungen, zum Durchsuchen des Adressraums und zum Lesen und/oder Schreiben von Knotenattributen. Die Hauptanforderungen sind: Unterstützung für eine einzige Sitzung, Unterstützung für das Server- und Serverkapazitätsobjekt, alle Pflichtattribute für Teilnehmer im Adressraum und Authentifizierung mit Benutzernamen und Passwort. Für eine breite Anwendbarkeit wird empfohlen, dass Server mehrere Transport- und Sicherheitsprofile unterstützen.“

Eine vollständige Beschreibung dieses Facets finden Sie unter http://opcfoundation.org/UA-Profile/Server/Core2017Facet.

Der in das BMENUA0100-Modul integrierte OPC UA-Server-Stack unterstützt die folgenden Konformitätseinheiten im Core 2017 Server Facet:

- View Service Set, enthält die folgenden Gruppen und Dienste:
  - View Basic: Enthält den Browse- und den BrowseNext-Dienst.
  - View TranslateBrowsePath: Enthält den TranslateBrowsePathsToNodeIds-Dienst.
  - View Register Nodes: Enthält die Dienste RegisterNodes und UnregisterNodes, um den Zugriff auf wiederholt verwendete Knoten im OPC UA AddressSpace des Servers zu optimieren.
- Attribute Service Set, enthält die folgenden Gruppen und Dienste:
  - Attribute read: Enthält den Read-Dienst, der das Lesen eines oder mehrerer Attribute eines oder mehrerer Knoten unterstützt, einschließlich der Unterstützung des IndexRange-Parameters zum Lesen eines einzelnen Elements oder einer Reihe von Elementen, wenn der Attributwert ein Array ist.
  - Attribute Write values: Enthält den Write Value-Dienst, der das Schreiben eines oder mehrerer Werte in ein oder mehrere Attribute eines oder mehrerer Knoten unterstützt.
  - Attribute Write Index: Enthält den Write Index-Dienst, der den IndexRange für das Schreiben in ein einzelnes Element oder einen Bereich von Elementen unterstützt, wenn der Attributwert ein Array ist und partielle Aktualisierungen für dieses Array zulässig sind.

Data Access Server Facet

Wie auf der Website der OPC Foundation angegeben, gibt das Data Access Server Facet „die Unterstützung für ein Informationsmodell an, das zur Bereitstellung von industriellen Automatisierungsdaten verwendet wird. Dieses Modell definiert Standardstrukturen für analoge und digitale Datenelemente und deren Dienstqualität. Dieses Facet erweitert das

Core Server Facet, das die Unterstützung des grundlegenden AddressSpace-Verhaltens umfasst.“

Eine vollständige Beschreibung dieses Facets finden Sie unter http://opcfoundation.org/UA-Profile/Server/DataAccess.

ComplexType 2017 Server Facet

Wie auf der OPC Foundation-Website angegeben, erweitert das ComplexType 2017 Server Facet „das Core Server Facet um Variablen mit strukturierten Daten, d. h. Daten, die aus mehreren Elementen wie einer Struktur bestehen und in denen die einzelnen Elemente als Komponentenvariablen verfügbar gemacht werden. Die Unterstützung dieses Facets erfordert die Implementierung von strukturierten Datentypen und Variablen, die diese Datentypen nutzen. Das Service Set „Read“ (Lesen), „Write“ (Schreiben) und „Subscriptions“ (Abonnements) unterstützt die Kodierung und Dekodierung dieser strukturierten Datentypen. Optional kann der Server auch alternative Kodierungen unterstützen, z. B. eine XML-Kodierung, wenn das Binärprotokoll derzeit verwendet wird und umgekehrt.“

Eine vollständige Beschreibung dieses Facets finden Sie unter http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017.

BMENUA0100 - OPC UA-Server-Stack - Erkennungs- und Sicherheitsdienste

Einführung

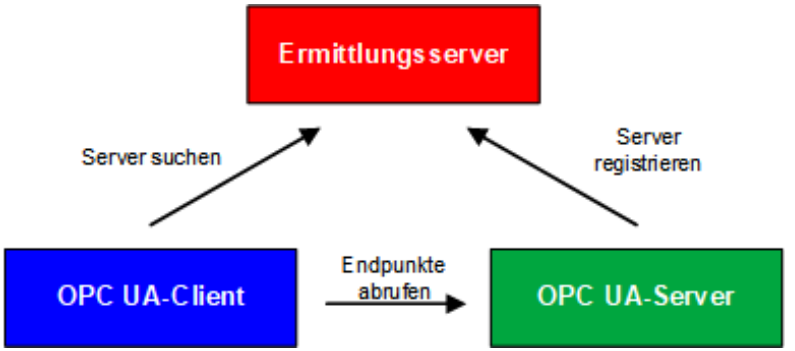
Der in das BMENUA0100-Modul integrierte OPC UA-Server-Stack unterstützt Erkennungs- und Sicherheitsdienste.

Um eine Verbindung zum OPC UA-Server im BMENUA0100-Modul herzustellen, benötigt ein OPC UA-Client Informationen, die den Server beschreiben, einschließlich seiner Netzwerkadresse, seines Protokolls und seiner Sicherheitseinstellungen. OPC UA definiert eine Reihe von Erkennungsfunktionen, die ein Client verwenden kann, um diese Informationen zu erhalten.

Die Informationen, die für den Verbindungsaufbau zwischen einem OPC UA-Client und einem OPC UA-Server benötigt werden, werden in einem Endpunkt gespeichert. Ein OPC UA-Server kann über mehrere Endpunkte verfügen, die jeweils Folgendes enthalten:

- Endpunkt-URL (Netzwerkadresse und Protokoll), zum Beispiel:
  - Für IPv4: opc.tcp://172.21.2.30:4840, wobei gilt:
    – opc.tcp = Protokolle
    – 172.21.2.30 = IPv4-Adresse
    – 4840 = opcua-tcp-Portnummer, konfiguriert in Control Expert
  - Für IPv6: opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, wobei gilt:
    – opc.tcp = Protokolle
    – [2a01:cb05:431:f00:200:aff:fe02:a0a] = IPv6-Adresse
    – 50000 = opcua-tcp-Portnummer, konfiguriert in Control Expert
- Sicherheitsrichtlinie (einschließlich einer Reihe von Sicherheitsalgorithmen und Schlüssellänge)
- Nachrichtensicherheitsmodus (Sicherheitsebene für ausgetauschte Nachrichten)
- Benutzer-Tokentyp (vom Server unterstützte Typen der Benutzerauthentifizierung)

Es können ein oder mehrere OPC UA-Server vorhanden sein. Bei mehreren Servern kann ein Erkennungsserver verwendet werden, um Informationen zu jedem Server zur Verfügung zu stellen. Einzelne Server können sich bei dem Erkennungsserver registrieren. Clients können eine Liste einiger oder aller verfügbaren Server beim Erkennungsserver anfordern und den GetEndpoints-Dienst nutzen, um Verbindungsinformationen von einem einzelnen Server zu erhalten.



Das BMENUA0100-Modul unterstützt verschiedene Erkennungs- und Sicherheitsdienste, u. a.:

- Dienstgruppe Erkennung (Discovery Service Set)
- Dienstgruppe Sichere Kanäle (SecureChannel Service Set)
- Dienstgruppe Sitzungen (Session Service Set)

Die Entscheidung, Dienste zu aktivieren oder zu deaktivieren, richtet sich nach den Cybersicherheitsrichtlinien, die Sie für den Server implementieren möchten.

Dienstgruppe Erkennung: Discovery Service Set

Der OPC UA-Server-Stack des BMENUA0100-Moduls unterstützt das „Discovery Service Set“, das im Core 2017 Server Facet, Seite 42 enthalten ist. Wie im BMENUA0100-Modul implementiert, werden u. a. folgende Dienste unterstützt:

- FindServers: Gemäß der Implementierung im OPC UA-Server-Stack des BMENUA0100-Moduls findet dieser Dienst die Server nur auf dem lokalen OPC UA-Server.
- GetEndpoints: Gibt die von einem Server unterstützten Endpunkte und die für die Einrichtung eines sicheren Kanals (SecureChannel) und einer Sitzung erforderlichen Konfigurationsinformationen zurück. Kann eine Rückgabeliste mit gefilterten Endpunkten bereitstellen, die auf Profilen basiert.

Dienstgruppe der sicheren Kanäle: SecureChannel Service Set

Der OPC UA-Server-Stack des BMENUA0100-Moduls unterstützt das „SecureChannel Service Set“, das die folgenden Dienste umfasst:

- OpenSecureChannel: Öffnet oder erneuert einen SecureChannel, der Vertraulichkeit und Integrität für den Austausch von Nachrichten während einer Sitzung bereitstellt. Dieser Dienst erfordert, dass der OPC UA-Server-Stack die verschiedenen Sicherheitsalgorithmen auf die Nachrichten anwendet, während sie gesendet und empfangen werden.
- CloseSecureChannel: Beendet einen SecureChannel.

Dienstgruppe der Sitzungen: Session Service Set

Der OPC UA-Server-Stack des BMENUA0100-Moduls unterstützt das „Session Service Set“, das im Core 2017 Server Facet, Seite 42 enthalten ist. Wie im BMENUA0100-Modul implementiert, werden u. a. folgende Dienste unterstützt:

- CreateSession: Nach dem Erstellen eines SecureChannel mit dem OpenSecureChannel-Dienst verwendet ein Client diesen Dienst, um eine Sitzung zu erstellen. Der Server gibt zwei Werte zurück, die die Sitzung eindeutig identifizieren:
  - Eine Sitzungs-ID, die verwendet wird, um die Sitzung in den Überwachungsprotokollen und im AddressSpace des Servers zu identifizieren.
  - Ein Authentifizierungstoken (authenticationToken), das verwendet wird, um einen eingehenden Request einer Sitzung zuzuordnen.
- ActivateSession: Wird vom Client verwendet, um die Identität des Benutzers anzugeben, der der Sitzung zugeordnet ist. Kann nicht verwendet werden, um den Benutzer der Sitzung zu ändern.
- CloseSession: Beendet eine Sitzung.

HINWEIS: Wenn „SecurityMode = None“, gilt für die Dienste CreateSession und ActivateSession Folgendes:

1. Das Anwendungszertifikat und Nonce sind optional.
2. Die Signaturen sind null/leer.

BMENUA0100 - OPC UA-Server-Stack - Veröffentlichungs- und Abonnementdienste

Abonnements

Statt Informationen per Abruf dauerhaft zu lesen, beinhaltet das OPC UA-Protokoll die Abonnementfunktion. Diese Funktion aktiviert den in das BMENUA0100-Modul integrierten OPC UA-Stack zur Bereitstellung von Publish-/Subscribe-Diensten, die verwendet werden, wenn das Modul eine Verbindung zu dezentralen Geräten herstellt.

Ein OPC UA-Client kann einen oder mehrere ausgewählte Knoten abonnieren und den Server diese Elemente überwachen lassen. Bei Auftreten eines Änderungsereignisses, z. B. einer Wertänderung, benachrichtigt der Server den Client über die Änderung. Dieser Mechanismus reduziert die Menge der übertragenen Daten erheblich und stellt somit eine bedeutende Reduzierung des Bandbreitenverbrauchs dar.

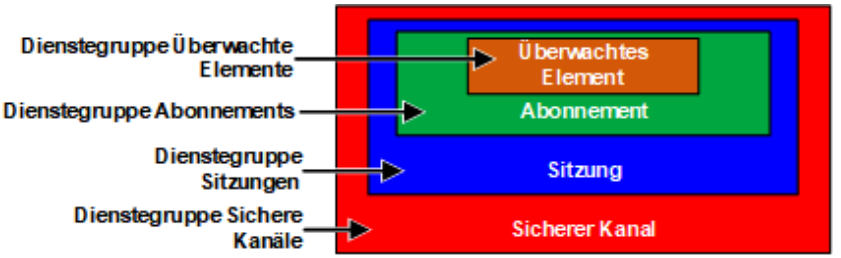
Ein OPC UA-Client kann die verschiedenen Arten von Informationen abonnieren, die ein OPC UA-Server bereitstellt. Das Abonnement fasst diese verschiedenen Arten von Daten (die überwachten Elemente) zu einer einzigen Datensammlung zusammen, die als Benachrichtigung bezeichnet wird.

Ein Abonnement muss:

- Aus mindestens einem überwachten Element bestehen.
- Im Kontext einer Sitzung erstellt werden, die im Kontext eines sicheren Kanals erstellt wird.

  HINWEIS: Das Abonnement kann in eine andere Sitzung übertragen werden.

Die an einem Clientabonnement beteiligten Dienstgruppen werden nachfolgend beschrieben:



Abonnements und Überläufe

In einigen Fällen, in denen eine große Anzahl an Abonnement-Requests vorhanden ist, versucht der OPC UA-Server, Daten von der Steuerung in einem Umfang zu erhalten, der größer ist, als die Steuerung oder das BMENUA0100-Modul im angegebenen Veröffentlichungsintervall verarbeiten kann. In diesem Fall wird die Ausführungszeit für Abonnement-Requests automatisch verlängert und die nächste Abonnementausführung verzögert, bis alle Requests abgeschlossen werden können.

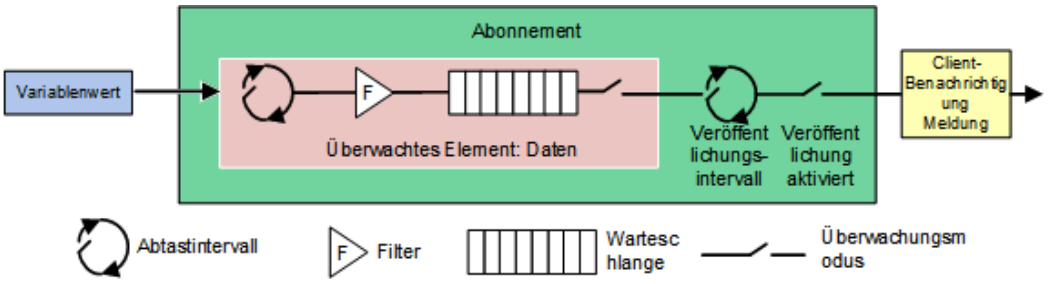
Berücksichtigen Sie bei der Einstellung eines Veröffentlichungsintervalls die Anzahl der Clients und Client-Requests, die der Server verarbeiten muss. Wenn Sie die Anzahl der Client-Requests ermitteln, müssen Sie sicherstellen, dass alle Clients online arbeiten. Beachten Sie in diesem Zusammenhang, dass es 2 Minuten oder länger dauern kann, bis einige Clients nach dem Einschalten online gehen.

HINWEIS: Stellen Sie das Veröffentlichungsintervall auf mindestens das Doppelte des Abtastintervalls ein, um das Fehlen von Datenänderungen zu vermeiden.

Änderungsereignisse

Ein Client kann ein Datenänderungsereignis, das durch die Änderung des Wertattributs einer Variablen ausgelöst wird, als überwachtes Element abonnieren.

Die konfigurierbaren Abonnementeinstellungen, ihre Reihenfolge und Rollen werden nachfolgend beschrieben:



Die folgenden drei Einstellungen bestimmen, wie überwachte Elemente einem Abonnement hinzugefügt werden:

- Abtastintervall: Das für jedes überwachte Element im Abonnement festgelegte Abtastintervall. Dies ist die Häufigkeit, mit der der Server die Datenquelle auf Änderungen überprüft. Für ein einzelnes Variablenelement kann das Abtastintervall kleiner (d. h. schneller) sein als der Zeitraum zwischen den Benachrichtigungen an den Client. In diesem Fall kann der OPC UA-Server die Abtastergebnisse in eine Warteschlange stellen und die komplette Warteschlange veröffentlichen. In extremen Fällen überarbeitet (d. h. verlangsamt) der Server das Abtastintervall, sodass die Datenquelle keine übermäßige Warteschlangenbelastung erfährt, die möglicherweise durch den Abtastvorgang selbst verursacht wird.

  HINWEIS: Wenn die OPC UA-Warteschlangeneinreihung von erfassten Datenwerten unterstützt wird, kann die Warteschlangengröße (d. h. die maximale Anzahl der Werte, die in eine Warteschlange gestellt werden können) für jedes überwachte Element konfiguriert werden. Sobald die Daten an den Client geliefert (veröffentlicht) werden, wird die Warteschlange geleert. Bei einem Warteschlangenüberlauf werden die ältesten Daten verworfen und durch neue Daten ersetzt.

- Filter: Eine Sammlung verschiedener Kriterien, die verwendet werden, um zu identifizieren, welche Datenänderungen oder Ereignisse gemeldet und welche blockiert werden.
- Überwachungsmodus: Wird zum Aktivieren oder Deaktivieren der Datenerfassung und Benachrichtigung verwendet.

Die folgenden beiden Einstellungen gelten für das Abonnement selbst:

- Veröffentlichungsintervall: Der Zeitraum, nach dem in den Warteschlangen gesammelte Benachrichtigungen in einer Benachrichtigung (Veröffentlichungsantwort) an den Client gesendet werden. Der OPC UA-Client muss bestätigten, dass der OPC UA-Server genügend Veröffentlichungs-Token (Veröffentlichungs-Requests) erhalten hat, sodass der Server, wenn das Veröffentlichungsintervall abgelaufen und eine Benachrichtigung versandbereit ist, ein solches Token verwendet und die Daten in einer Veröffentlichungsantwort sendet. Für den Fall, dass keine Benachrichtigung erforderlich ist (z. B. keine Werte geändert wurden), sendet der Server eine KeepAlive-Benachrichtigung an den Client, d. h. eine leere Veröffentlichung, um anzuzeigen, dass der Server weiterhin aktiv ist.
- Veröffentlichung aktiviert: Aktiviert und deaktiviert das Senden der Benachrichtigung.

Embedded DataChange Subscription Server Facet

Wie auf der OPC Foundation-Website angegeben, gibt das Embedded DataChange Subscription Server Facet die Mindestebene der Unterstützung für Datenänderungsbenachrichtigungen in Abonnements an. Es enthält Einschränkungen, die den Speicher- und Verarbeitungsaufwand für die Implementierung des Facets minimieren. Dieses Facet umfasst Funktionen zum Erstellen, Ändern und Löschen von Abonnements sowie zum Hinzufügen, Ändern und Entfernen von überwachten Elementen. Die Server unterstützen für jede Sitzung mindestens ein Abonnement mit bis zu zwei Elementen.

Darüber hinaus ist die Unterstützung für zwei parallele Veröffentlichungs-Requests erforderlich. Dieses Facet ist für eine Plattform konzipiert, wie die, die vom Micro Embedded Device Server-Profil bereitgestellt wird und in der der Speicher begrenzt und verwaltet werden muss.

Eine vollständige Beschreibung dieses Facets finden Sie unter http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription.

Dieses Facet unterstützt folgende Dienste:

- Dienstgruppe Überwachte Elemente (Monitored Item Service Set)
- Dienstgruppe Abonnements (Subscription Service Set)

Dienstgruppe Überwachte Elemente (Monitored Item Service Set)

Die Dienstgruppe „Monitored Item Service Set“ unterstützt die folgenden Dienste:

HINWEIS: Eine Beschreibung dieser Dienstgruppen und Dienste finden Sie im Dokument *OPC Unified Architecture Specification Part 4: Services (Release 1.04)*.

- CreateMonitoredItems: Ein asynchroner Aufruf zum Erstellen und Hinzufügen eines oder mehrerer überwachter Elemente (MonitoredItems) zu einem Abonnement.
- ModifyMonitoredItems: Ein asynchroner Aufruf zum Ändern überwachter Elemente. Dieser Dienst wird verwendet, um MonitoredItems eines Abonnements zu ändern. Änderungen an den MonitoredItem-Einstellungen werden sofort vom Server übernommen.
- DeleteMonitoredItems: Ein asynchroner Aufruf zum Löschen von überwachten Elementen. Dieser Dienst wird verwendet, um ein oder mehrere MonitoredItems eines Abonnements zu entfernen. Wenn ein MonitoredItem gelöscht wird, werden seine ausgelösten Elementverbindungen ebenfalls gelöscht.
- SetMonitoringMode: Ein asynchroner Aufruf zum Festlegen des Überwachungsmodus für eine Liste von MonitoredItems. Dieser Dienst wird verwendet, um den Überwachungsmodus für ein oder mehrere MonitoredItems eines Abonnements festzulegen. Durch das Festlegen des Modus auf DEAKTIVIERT werden alle Benachrichtigungen in der Warteschlange gelöscht.

Dienstgruppe Abonnements (Subscription Service Set)

Die Dienstgruppe „Subscription Service Set“ unterstützt die folgenden Dienste:

HINWEIS: Eine Beschreibung dieser Dienstgruppen und Dienste finden Sie im Dokument *OPC Unified Architecture Specification Part 4: Services (Release 1.04)*.

- CreateSubscription: Ein asynchroner Aufruf zum Erstellen eines Abonnements.
- ModifySubscription: Ein asynchroner Aufruf zum Ändern eines Abonnements. Der Server wendet Änderungen sofort auf das Abonnement an.

- DeleteSubscription: Ein asynchroner Aufruf zum Löschen von einem oder mehreren Abonnements, die zur Clientsitzung gehören. Bei erfolgreicher Ausführung dieses Dienstes werden alle dem Abonnement zugeordneten überwachten Elemente gelöscht.
- Publish: Dieser Dienst dient zwei Zwecken: Den Empfang von Benachrichtigungen (NotificationMessages) für ein oder mehrere Abonnements bestätigen und den Server zur Rückgabe einer NotificationMessage oder einer Keep-Alive-Nachricht auffordern.
- Republish: Ein asynchroner Aufruf zur erneuten Veröffentlichung, um verlorene Benachrichtigungen zu erhalten. Dieser Dienst fordert das Abonnement auf, eine NotificationMessage aus einer Wiederholungswarteschlange erneut zu veröffentlichen. Wenn der Server die angeforderte Nachricht nicht in seiner Wiederholungswarteschlange hat, gibt er eine Fehlerantwort zurück.
- SetPublishingMode: Ein asynchroner Aufruf, um das Senden von Benachrichtigungen über ein oder mehrere Abonnements zu ermöglichen.

BMENUA0100 – OPC UA-Server-Stack – Transportdienste

Unterstützung des UA-TCP UA-SC UA-Binary Facet

Das BMENUA0100-Modul unterstützt das UA-TCP UA-SC UA-Binary-Transport-Facet. (Weitere Informationen finden Sie in der Online-Beschreibung unter http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary.)

Dieses Transport-Facet definiert eine Kombination aus Netzwerkprotokollen, Sicherheitsprotokollen und Nachrichtenverschlüsselung, die für geringen Ressourcenverbrauch und hohe Leistung optimiert ist. Es kombiniert das einfache TCP-basierte Netzwerkprotokoll UA-TCP 1.0 mit dem binären Sicherheitsprotokoll UA-SecureConversation 1.0 und der binären Nachrichtenverschlüsselung UA-Binary 1.0.

Daten, die zwischen einem OPC UA-Client und dem in das BMENUA0100-Modul eingebetteten OPC UA-Server übertragen werden, verwenden das TCP-Protokoll und sind binär codiert gemäß dem OPC UA-Binärdateiformat.

HINWEIS: Das OPC UA-Binärdateiformat ersetzt das XML UA-Nodeset-Schema der OPC Foundation. Es verbessert die Leistung und den Speicherverbrauch. Es erfordert keinen XML-Parser.

Erkennung von Steuerungsvariablen

Zuordnung von Control Expert-Steuerungsvariablen zu OPC UA-Datenlogikvariablen

Einführung

Der integrierte OPC UA-Server im BMENUA0100-Modul verwendet UMAS-Datenwörterbuch-Requests (Unified Messaging Application Services), um Anwendungsvariablen der M580-Steuerung zu suchen und zu erkennen. Sie müssen das Datenwörterbuch in den Control Expert-Projekteinstellungen aktivieren.

HINWEIS:

- Das BMENUA0100-Modul kann eine maximale Datenwörterbuchgröße von 100.000 Variablen unterstützen.
- Die für das Laden des Datenwörterbuchs in den OPC UA-Server erforderliche Zeit hängt von der Anzahl der Datenwörterbuch-Elemente und der MAST-Periodeneinstellung, Seite 178 ab.

Die erfassten Variablen werden mithilfe der entsprechenden OPC UA-Stack-Dienste von der Control Expert-Datenlogikmodellansicht in die OPC UA-Datenlogikmodellansicht übersetzt. Ein mit dem BMENUA0100-Modul verbundener OPC UA-Client - über seinen Steuerungsport, über seinen Baugruppenträger-Port über die Steuerung oder über ein BMENOC0301- oder BMENOC0311-Kommunikationsmodul - kann diese Datensammlung über die Dienste des vom Embedded 2017 UA Server Profile, Seite 39 unterstützten Data Access Server Facet, Seite 42 abrufen.

Vorladen des Datenwörterbuchs zur Vermeidung von Kommunikationsunterbrechungen

Eine Online-Anwendungsänderung mit Control Expert unterbricht vorübergehend die OPC UA-Server/Client-Kommunikation, während der Server ein aktualisiertes Datenwörterbuch erhält. Diese Unterbrechung wird durch eine inkonsistente Zuordnung der Steuerungsdaten verursacht, während das Datenwörterbuch aktualisiert wird. Während der Unterbrechung der Kommunikation befinden sich die überwachten Knoten, wie von UA Expert angegeben, im Fehlerzustand (**Ungültiger Kommunikationsfehler** oder **Ungültige Kommunikation** oder **Ungültiger Timeout**). Um diese Unterbrechung der Kommunikation und ihre Folgen zu vermeiden, kann ein Synchronisationsmechanismus zwischen dem BMENUA0100-Modul und der Control Expert-Konfigurationssoftware, basierend auf dem Vorladen des aktualisierten Datenwörterbuchs, eingerichtet werden.

HINWEIS: OPC UA-Befehle (READ/WRITE) werden nicht berücksichtigt, wenn sich der BMENUA0100 während der Erfassung des Datenwörterbuchs im Busy-Zustand befindet.

Diese Funktion wird in Control Expert im Fenster **Extras > Projekteinstellungen...** im Bereich **Allgemein > SPS Eingebettete Daten** über die Einstellungen (siehe EcoStruxure™ Control Expert, Betriebsarten) **Vorladen bei Generierungsänderungen** und **Timeout bei der Generierung von Änderungen** aktiviert. In der Online-Hilfe von Control Expert finden Sie Informationen zur Konfiguration dieser Funktion.

Aktivieren des Datenwörterbuchs

So aktivieren Sie das Datenwörterbuch in Control Expert:

Schritt	Aktion
1	Wählen Sie in Control Expert bei geöffnetem Projekt **Extras > Projekteinstellungen** aus.
2	Navigieren Sie im Fenster **Projekteinstellungen** zu **Allgemein > In SPS eingebettete Daten** und wählen Sie dann **Datenwörterbuch** aus. **HINWEIS:** Wenn das EcoStruxure™ Control Expert-Projekt ein BMENUA0100-Modul umfasst und diese Einstellung nicht aktiviert ist, wird bei der Anwendungsgenerierung ein Fehler ausgegeben.

Umwandlung variabler Datentypen

Das BMENUA0100-Modul kann die folgenden grundlegenden vom Control Expert-Datenlogikmodell unterstützten Variablentypen erkennen und in OPC UA-Datentypen konvertieren:

Elementarer Datentyp von Control Expert	OPC UA-Datentyp
BOOL	Boolesch
EBOOL	Boolesch
INT	Int16
DINT	Int32
UINT	UInt16
UDINT	UInt32
REAL	Float (Gleitkommawert)
BYTE	Byte
WORD	UInt16
DWORD	UInt32

Elementarer Datentyp von Control Expert	OPC UA-Datentyp
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double (Doppelwert)
STRING	ByteString (Byte-Zeichenfolge)
* In der folgenden Tabelle wird die datumsbezogene Datentypkonvertierung beschrieben.	

Für die Control Expert-Datentypen DATE, TIME, TOD, DT lauten die entsprechenden OPC UA-Datentypen wie folgt:

Elementarer Datentyp von Control Expert	In Control Expert angezeigter Beispielwert	OPC UA-Datentyp	Entsprechender Wert im OPC UA-Typ
DATE	D#2017-05-17	UInt32	20170517 hex.
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	07440100 hex.
DT[1]	DT#2017-05-17-07:44:01	Double (Doppelwert)	4.29E-154
1. Die zurückgegebenen Daten für Datums- und Uhrzeitwerte sind UATypeUInt64, d. h. die interne Kodierung des IEC 1131-DT in Control Expert - BCD-Kodierung (Binary Coded Decimal).			

Erkennbare Variablen

Bei Variablen greift der OPC UA-Client nicht direkt auf eine erkannte Datenlogikvariable der Steuerung zu. Stattdessen greift der Client auf die erkannte Steuerungsvariable über eine OPC UA-Datenlogikvariable zu, die im BMENUA0100-Modul vorhanden und der zugrunde liegenden Steuerungsvariablen zugeordnet ist. Aufgrund der Pass-Through-Natur des Datenvariablenzugriffs wird der Erfassungsanforderungsprozess nicht optimiert, und die Erfassungsleistung des Datenwörterbuchs ist nicht repräsentativ für die Steuerungsleistung.

HINWEIS: Verweise vom Typ REF_TO auf Anwendungsvariablen im OPC UA-Server sind für den OPC UA-Client nicht zugänglich.

Beispiele für Control Expert-Steuerungsvariablen, die vom OPC UA-Server im BMENUA0100-Modul erkannt werden können:

- Strukturierte Variablen mit Unterfeldern: DDT- und Array-Variablen.

- PU-Variablen (Program Unit: Programmeinheit) sind wie folgt auffindbar:
  - Ein-/Ausgabevariablen sind für den OPC UA-Client nur für den BOOL-Typ zugänglich.
  - Auf Ein- und Ausgangsvariablen kann durch den OPC UA-Client zugegriffen werden, mit Ausnahme der Typen REF_TO, ARRAY, String (Zeichenfolge) und Structure (Struktur).

Außerdem können die folgenden Variablen vom OPC UA-Server erkannt werden, indem sie Anwendungsvariablen zugeordnet und dann die zugeordneten Anwendungsvariablen erkannt werden:

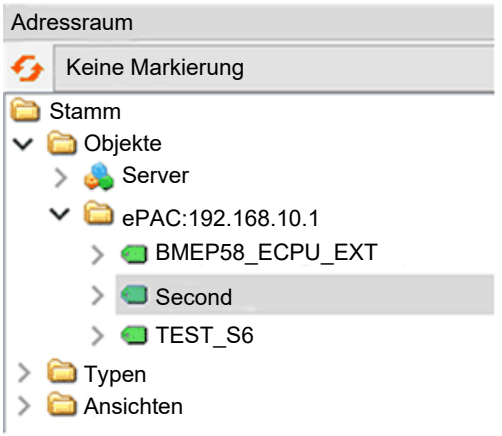
- Topologische E/A-Variablen:
  - Eingänge: %I, %IW, %ID, %IF.
  - Ausgänge: %Q, %QW, %QD, %QF.
- Lokalisierte Variablen: %M, %MW, %MD, %MF.
- Systemvariablen: %S, %SW, %SD.

  HINWEIS: Die Variablenerkennung beinhaltet eine Variable (oder ein Symbol) für ein extrahiertes Bit (z. B. MyBoolVar in %MW100.1).

Darstellung der erkannten Variablen im OPC UA-Client

Der OPC-UA-Server im BMENUA0100-Modul kann erkannte Steuerungsvariablen organisieren und grafisch darstellen. Ein OPC UA-Client-Tool kann eine Verbindung zum BMENUA0100-Modul herstellen und eine Knotenstrukturdarstellung der OPC UA-Server-Variablen anzeigen.

Im folgenden Beispiel kann ein OPC UA-Client (in diesem Beispiel das Client-Tool Unified Automation UaExpert), der mit dem BMENUA0100-Modul verbunden ist, Steuerungsvariablen in seinen Fenstern **Adressraum** anzeigen. Die IP-Adresse der M580-Steuerung wird durch den Knoten ePAC:192.168.10.1 dargestellt. Die untergeordneten Knoten entsprechen den Control Expert-Anwendungsvariablen:



Im obigen Beispiel stellt der erste Unterknoten, BMEP58_ECPU_EXT, den Geräte-DDT für die M580-Steuerung dar, der automatisch instanziiert wird, als die Steuerung der Control Expert-Anwendung hinzugefügt wurde. Die nachfolgenden Knoten stellen andere Objekte dar, die der Anwendung hinzugefügt wurden.

Mit dem OPC UA-Client-Tool wurde der Knoten TEST_S6 in das Fenster **Datenzugriffsansicht**, in dem die Details der Variablen angezeigt werden, gezogen und dort abgelegt:


Datenzugriffsansicht

Nr.	Server	Knoten-ID	Anzeigename	Wert	Datentyp	Zeitstempelung von Quellen	Serverzeitstempel	Statuscode
1	bmenua-server	NS2|String|0:Test_S6	TEST_S6:	false	Boolesch	10:43:54.830	10:43:54.830	Gut
2	bmenua-server	NS0|Numeric|2258	CurrentTime	2019-08-12T08:43:54.733Z	DateTime	10:43:54.733	10:43:54.830	Gut

In diesem Fall lautet der OPC UA-Datentyp der Variablen *Boolesch* (gibt an, dass der zugrunde liegende Steuerungsdatentyp BOOL ist). und sein Wert ist *False*.

> **HINWEIS:** Das Attribut **Serverzeitstempel** der OPC UA-Knoten wird vom OPC-UA-Server des BMENUA0100-Moduls in UTC (Universal Time Coordinated) empfangen. Es wird in der Ortszeit angezeigt.

Lesen und Schreiben erkannter Variablen im OPC UA-Client

Ein OPC UA-Tag in einem OPC UA-Client (z. B. einem SCADA), das sich auf eine Array-Variable bezieht, ermöglicht es dem Client, alle Elemente des Arrays zu lesen oder zu schreiben. Beispielsweise wird das Tag „MyArray“ als ARRAY[0...31] OF INT deklariert.

Damit der Client jedoch nur ein einzelnes Element eines Arrays lesen oder schreiben kann, ist es notwendig, ein bestimmtes Tag zu deklarieren, das auf das gewünschte einzelne Array-Element verweist. Beispielsweise wird „MyInt“ als INT deklariert, was sich auf MyArray[2] bezieht.

Hot Standby und Redundanz

OPC UA-Server - Redundanz

Zwei Redundanztypen

Das BMENUA0100-Modul unterstützt die folgenden Redundanztypen:

- Hot Standby-Architektur, die redundante Steuerungen beschreibt.
- OPC UA-Serverredundanz, in der die Verwendung redundanter BMENUA0100-Module beschrieben wird.

Die Redundanz der OPC UA-Server, die von den BMENUA0100-Modulen verwaltet wird, entspricht dem OPC UA-Standard der nicht-transparenten Serverredundanz im Warm-Failover-Modus, wie von der OPC Foundation definiert.

Diese beiden Redundanztypen können kombiniert werden. Folgende Designs werden unterstützt:

- Eine Standalone-Steuerung, die zwei BMENUA0100-Module enthält.
- Zwei Hot Standby-Steuerungen, die jeweils eines oder zwei BMENUA0100-Module enthalten.

OPC UA-Redundanz

In einer redundanten OPC UA-Serverarchitektur mit nicht-transparentem OPC UA-Server im Warm-Failover-Modus erstellt der OPC UA-Client Sitzungen und verwaltet die Kommunikation mit redundanten Servern. Zu den einzurichtenden Sitzungen gehören: eine aktive Sitzung mit dem primären Server und eine inaktive Sitzung mit dem sekundären (oder Standby-) Server. Der Client muss für diese beiden Sitzungen so konfiguriert werden, dass sie dieselben überwachten Elemente enthalten.

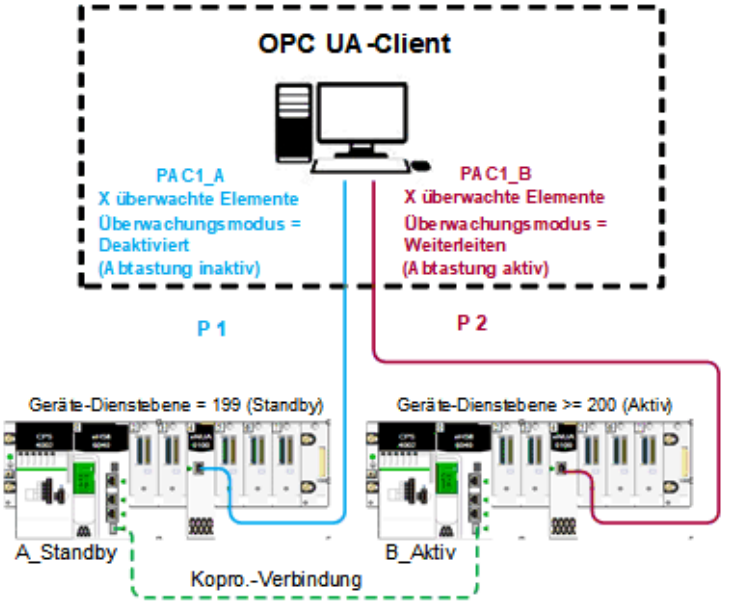
Der OPC UA-Client überprüft den Status der beiden Server über die Variable SERVICE_LEVEL und schaltet die Kommunikation zum funktionsfähigeren Server um, abhängig vom Wert dieser Variablen.

Der OPC UA-Standard besagt, dass die Aktivierung der Kommunikationsschnittstelle durch Anpassung des *Überwachungsmodus* der verschiedenen Sitzungen mit dem richtigen Wert

erfolgt. Der *Überwachungsmodus* der Server wird vom OPC UA-Client gesteuert, und die Vorgehensweise zur Änderung ist von der Implementierung des Clients abhängig. Für weitere Informationen zum Einstellen des *Überwachungsmodus* siehe die OPC UA-Client-Dokumentation.

Dieses Prinzip ist ein allgemeines Prinzip und gilt für jede Architektur, einschließlich einer Hot Standby-Architektur.

Die folgende Abbildung zeigt einen OPC UA-Client, der mit einem redundanten OPC UA-Server verbunden ist (jeder in ein BMENUA0100-Modul integriert). Der Client hat als aktiven Server denjenigen mit dem höheren SERVICE_LEVEL-Wert angegeben:



Hot Standby

In einer Hot Standby-Konfiguration können maximal zwei BMENUA0100-Module können in jedem lokalen Hot Standby-Hauptrack installiert werden. Jedes BMENUA0100-Modul ist mit einer eindeutigen, statischen IP-Adresse konfiguriert. Die BMENUA0100-Module behalten ihre jeweiligen IP-Adressen bei und tauschen bei einer Hot Standby-Umschaltung bzw. einem Hot Swapping keine IP-Adressen aus.

HINWEIS: Stellen Sie in einem Hot Standby-System sicher, dass für die BMENUA0100-Module in der primären Steuerung und in der Standby-Steuerung Folgendes zutrifft:

- Sie sind mit identischen Cybersicherheitseinstellungen, Seite 92 konfiguriert.
- Ihr Drehwahlschalter, Seite 25 (an der Rückseite des Moduls) ist auf dieselbe Stellung gesetzt.
- Sie sind in der gleichen Steckplatznummer, Seite 66 in ihren entsprechenden lokalen Hauptracks installiert.

Wenn diese Bedingungen nicht vorliegen, kann das Modul die von Control Expert festgelegte und in der Steuerung gespeicherte Konfiguration nicht abrufen und würde im Standalone-Modus starten. Das System führt diese Überprüfungen nicht automatisch durch.

Der BMENUA0100-Modul-DDT umfasst die SERVICE_LEVEL, Seite 161-Variable, die der Steuerung Informationen zur Funktionsfähigkeit des OPC UA-Servers im BMENUA0100-Modul bereitstellt. Der OPC UA-Client wird über die Variable SERVICE_LEVEL, die als OPC UA-Variable verfügbar ist, über den Serverstatus informiert.

HINWEIS: Fügen Sie die Elementarfunktion READ_DDT zum Zweck der Aktualisierung des DDT jedes BMENUA0100-Moduls ein. Fügen Sie in einer Hot Standby-Konfiguration den READ_DDT zu einer Code-Section hinzu, die ausgeführt wird, wenn sich die Steuerung im Standby-Modus befindet. Dieses Design gibt BMENUA0100-Diagnoseinformationen zurück, die zwischen der primären und der Standby-Steuerung ausgetauscht werden können. Die Anwendung kann diese Informationen verwenden, um eine Konsistenzprüfung der unterstützten Dienste und der Cybersicherheitskonfigurationen für die BMENUA0100-Module in der primären und der Standby-Steuerung durchzuführen.

Wenn der T_M_ECPU_HSBY DDT (siehe Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen) der Hot Standby-Steuerung und das zugehörige CMD_SWAP-Element als HMI-Variablen in einem SCADA-System verfügbar gemacht werden, kann die SCADA-Anwendung einen Austausch auslösen, indem sie in die entsprechende zugeordnete OPC UA-Variable im BMENUA0100 schreibt.

In einem Hot Standby-System kann das BMENUA0100-Modul, das die OPC UA-Kommunikation mit dem SCADA-System verwaltet, dasjenige sein, das sich im lokalen Standby-Rack befindet. Aus diesem Grund müssen Sie das Attribut **Austausch auf STBY** für alle abgefragten Anwendungsvariablen auswählen, um die Konsistenz der Variablenwerte zwischen der primären Steuerung und der Standby-Steuerung zu gewährleisten.

Um die Konsistenz zu gewährleisten, müssen außerdem die Anwendungen in den beiden Hot Standby-Steuerungen synchronisiert werden.

In seltenen Fällen (hauptsächlich, wenn das Bit ECPU_HSBY_1.PLCX_ONLINE manuell oder programmgesteuert auf FALSE gesetzt wird) kann sich eine der Steuerungen in einem Hot Standby-System im Wartemodus befinden. In diesem Modus ist diese Steuerung (die Standby-Steuerung) nicht mit der primären Steuerung synchronisiert und die aus dieser

Steuerung ausgelesenen Variablen sind ungenau. Der Status einer antwortenden Steuerung kann über die folgenden Felder des T_M_ECPU_HSBY-DDT überwacht werden:

- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.WAIT
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_PRIMARY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_STANDBY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.STOP

Außerdem ermöglicht das Hot Standby-System den Betrieb der beiden Steuerungen, während verschiedene Anwendungen ausgeführt werden. Um die Konsistenz der Variablen zwischen der primären Steuerung und der Standby-Steuerung zu gewährleisten, muss das Daten-Layout der 2 Steuerungen konsistent sein, wie das Feld des T_M_ECPU_HSBY-DDT zeigt:

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = FALSE

  HINWEIS: Wenn die OPC UA-Redundanz konfiguriert ist, müssen die Modul-DDTs programmgesteuert überprüft werden, um sicherzustellen, dass die unterstützten Dienste und die Cybersicherheitskonfigurationen für die BMENUA0100-Module konsistent sind.

OPC UA-Unterstützung für redundante Server, Clients und Netzwerke

Wie in OPC Unified Architecture Specification Part 4: Services, Release 1.04, angegeben: „OPC UA ermöglicht die Redundanz von Servern, Clients und Netzwerken. OPC UA stellt die Datenstrukturen und Dienste bereit, mit denen Redundanz auf standardisierte Weise erreicht werden kann.“

„Die Serverredundanz ermöglicht es den Clients, über mehrere Quellen zu verfügen, aus denen dieselben Daten abgerufen werden können. Die Serverredundanz kann auf vielfältige Weise erzielt werden, von denen einige eine Clientinteraktion erfordern, andere, die keine Interaktion mit einem Client erfordern. Redundante Server können in Systemen ohne redundante Netzwerke oder Clients vorhanden sein. Redundante Server können auch in Systemen mit Netzwerk- und Clientredundanz koexistieren...“

„Die Client-Redundanz ermöglicht identisch konfigurierten Clients, sich so zu verhalten, als wären sie einzelne Clients, aber nicht alle Clients empfangen Daten zu einem bestimmten Zeitpunkt. Idealerweise sollte es bei einem Client-Failover keinen Informationsverlust geben. Redundante Clients können in Systemen ohne redundante Netzwerke oder Server vorhanden sein. Redundante Clients können auch in Systemen mit Netzwerk- und Serverredundanz koexistieren...“

„Die Netzwerkredundanz ermöglicht es einem Client und einem Server, über mehrere Kommunikationspfade zu verfügen, um dieselben Daten zu erhalten. In Systemen ohne redundante Server oder Clients können redundante Netzwerke vorhanden sein.

Redundante Netzwerke können auch in Systemen mit Client- und Serverredundanz koexistieren...“ (OPC UA Part 4, Abschnitt 6.6.1.)

Serverredundanz

Wie in OPC Unified Architecture Specification Part 4: Services, Release 1.04, angegeben: „Es gibt zwei allgemeine Modi für die Serverredundanz: transparent und nicht transparent.“

„Bei transparenter Redundanz ist das Failover der Serverzuständigkeiten von einem Server auf einen anderen für den Client transparent. Der Client weiß nicht, dass ein Failover stattgefunden hat, und der Client hat keine Kontrolle über das Failover-Verhalten. Darüber hinaus muss der Client keine Aktionen durchführen, um weiterhin Daten zu senden oder zu empfangen.“

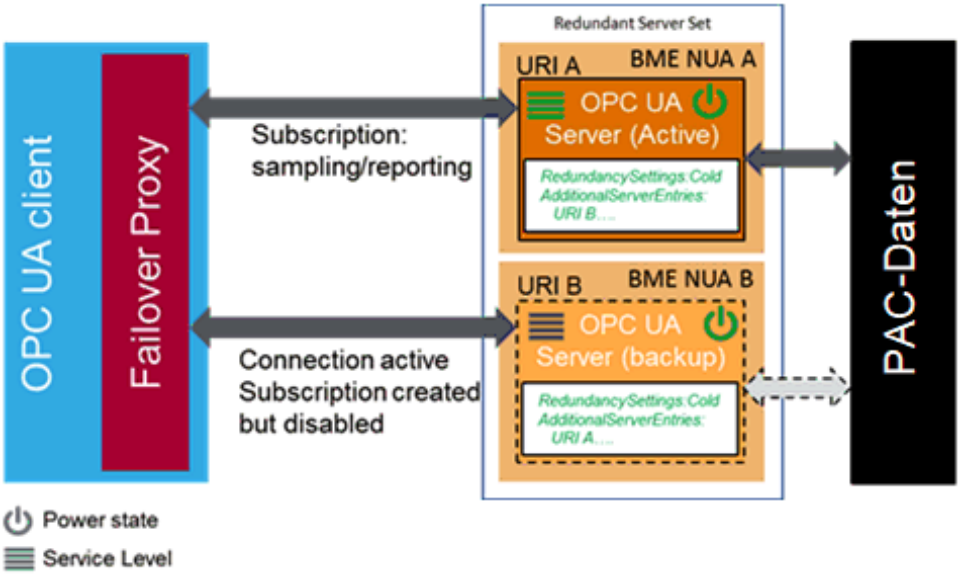
„Bei einer nicht transparenten Redundanz führt der Client das Failover von einem Server zu einem anderen Server und Aktionen zum weiteren Senden oder Empfangen von Daten durch. Der Client muss den redundanten Serversatz kennen und die erforderlichen Aktionen durchführen, um von der Serverredundanz zu profitieren.“

„Das ServerRedundancy-Objekt ... gibt den vom Server unterstützten Modus an. Der Objekttyp ServerRedundancyType und seine Untertypen TransparentRedundancyType und NonTransparentRedundancyType ... geben Informationen für den unterstützten Redundanzmodus an.“ (OPC UA Part 4, Abschnitt 6.6.2.)

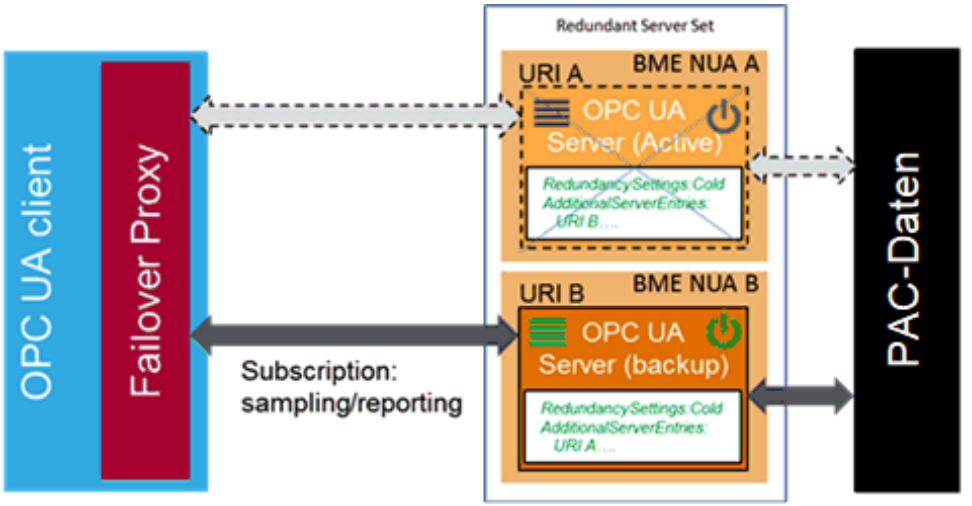
Der OPC UA-Server im BMENUA0100-Modul unterstützt die nicht transparente Serverredundanz im Warm-Failover-Modus.

OPC UA-Server - Warm-Failover-Modus

Wie in OPC Unified Architecture Specification Part 4: Services, Release 1.04, angegeben: Der Warm-Failover-Modus „ist der Bereich, in dem der/die Backup-Server aktiv sein können, aber keine Verbindung zu tatsächlichen Datenpunkten herstellen können.“ Daher kann nur ein einzelner Server Daten der Control Expert-Anwendung verbrauchen. „Die ServiceLevel-Variable ... gibt die Fähigkeit des Servers an, dem Client seine Daten zur Verfügung zu stellen.“ (OPC UA Part 4, Abschnitt 6.6.2.4.4.)



Bei einem Failover ist eine Aktion des OPC UA-Clients erforderlich. Der in das BMENUA0100-Modul integrierte Server wird inaktiv:



Failover-Verhalten des Clients

Wie in OPC Unified Architecture Specification Part 4: Services, Release 1.04, angegeben: „Jeder Server verwaltet eine Liste von ServerUris für alle redundanten Server im redundanten Serversatz.“

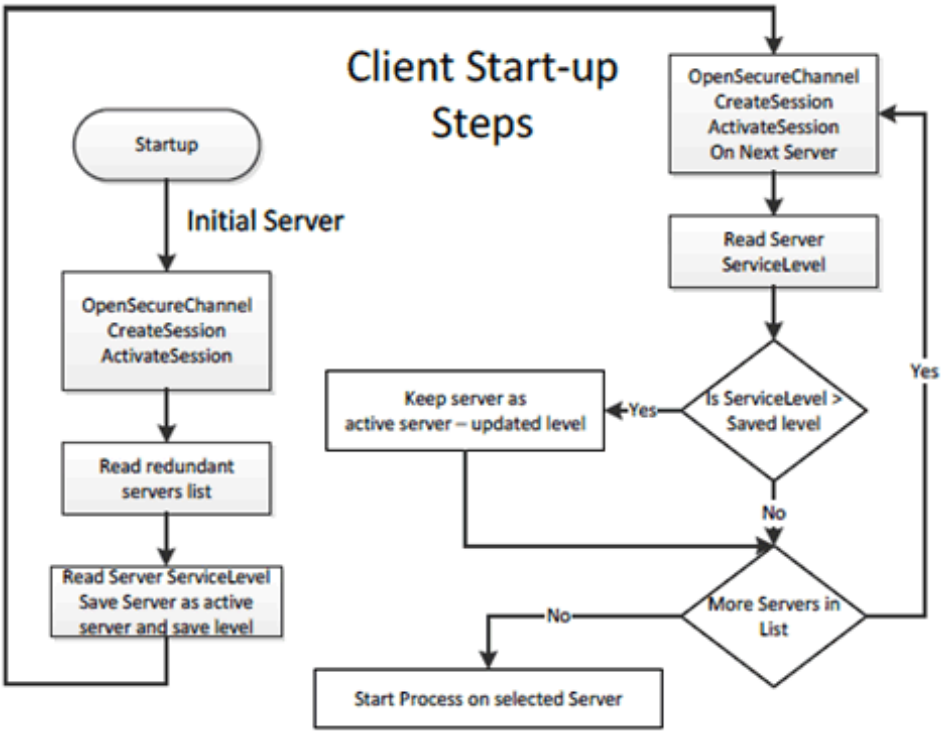
HINWEIS: Bei einem redundanten Serversatz handelt es sich um die Sammlung der OPC UA-Server in der Control Expert-Anwendung, die zur Bereitstellung von Redundanz konfiguriert sind.

„Die Liste wird zusammen mit dem Failover-Modus im ServerRedundancy-Objekt bereitgestellt. Damit Clients eine Verbindung zu allen Servern in der Liste herstellen können, muss jeder Server in der Liste die ApplicationDescription für alle Server im redundanten Serversatz über den FindServers-Dienst bereitstellen. Diese Informationen werden vom Client benötigt, um den ServerUri in Informationen zu übersetzen, die für die Verbindung mit den anderen Servern im redundanten Serversatz erforderlich sind. Daher muss ein Client nur mit einem der redundanten Server eine Verbindung herstellen, um die anderen Server auf der Grundlage der bereitgestellten Informationen zu finden. Ein Client sollte weiterhin Informationen über andere Server im redundanten Serversatz enthalten.“ (OPC UA Part 4, Abschnitt 6.6.2.4.5.1.)

Zu den Clientoptionen im Warm-Failover-Modus zählen:

- Bei der ersten Verbindung, zusätzlich zu den Aktionen auf dem aktiven Server:
  - Mit einem oder mehreren OPC UA-Servern verbinden.
  - Abonnements erstellen und überwachte Elemente hinzufügen.
- Beim Failover:
  - Abtastung für Abonnements aktivieren.
  - Veröffentlichung aktivieren.

„Clients, die mit einem nicht transparenten redundanten Serversatz kommunizieren, benötigen zusätzliche Logik, um Serverausfälle bewältigen und ein Failover auf einen anderen Server im redundanten Serversatz durchführen zu können. Die folgende Abbildung bietet einen Überblick über die Schritte, die ein Client normalerweise ausführt, wenn er sich zum ersten Mal mit einem redundanten Serversatz verbindet.“



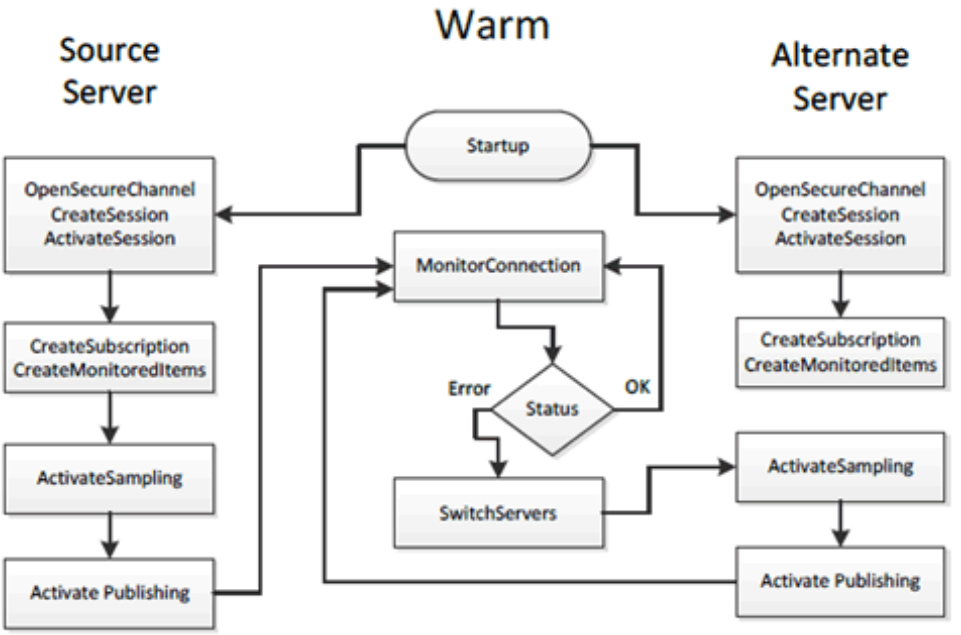
„Der ursprüngliche Server kann über die Standarderkennung oder über eine persistente Liste von Servern im redundanten Serversatz abgerufen werden. Der Client muss jedoch immer überprüfen, mit welchem Server im Serversatz er eine Verbindung herstellen soll. Die einzelnen Aktionen hängen vom Server-Failover-Modus ab, den der Server bereitstellt, und vom Failover-Modus, den der Client verwendet.“

„Clients, die einmal mit einem redundanten Server verbunden sind, müssen die von einem Server unterstützten Failover-Modi kennen, da diese Unterstützung die verfügbaren Optionen in Bezug auf das Client-Verhalten beeinflusst. Ein Client kann einen Server immer mit einem geringeren Failover-Modus handhaben, d. h. ein Client kann eine Verbindung zu einem Server herstellen, der Hot-Redundanz bereitstellt, und diesen so behandeln, als würde er mit Warmredundanz oder Kaltredundanz laufen. Diese Auswahl liegt in der Verantwortung des Clients. Im Failover-Modus „HotAndMirrored“ darf der Client den Hot- oder Warm-Failover-Modus nicht verwenden, da dies zu einer unnötigen Serverauslastung führen würde.“ (OPC UA Part 4, Abschnitt 6.6.2.4.5.1.)

OPC UA-Client - Warm-Failover-Modus

Wie in OPC Unified Architecture Specification Part 4: Services, Release 1.04, angegeben: Im Warm-Failover-Modus sollte sich der Client „mit einem oder mehreren Servern im redundanten Serversatz verbinden, hauptsächlich zur Überwachung des Service-Levels. Ein Client kann eine Verbindung zu mehreren Servern herstellen und Abonnements und MonitoredItems erstellen. Die Abtastung und Veröffentlichung kann jedoch nur auf einem Server ausgeführt werden. Der aktive Server sendet jedoch aktuelle Daten zurück, während die anderen Server im redundanten Serversatz einen entsprechenden Fehler für die MonitoredItems in der Veröffentlichungsantwort zurückgeben, wie z. B. Bad_ NoCommunication. Den einen aktiven Server finden Sie, indem Sie die ServiceLevel-Variable von allen Servern lesen.“

„Der Server mit der höchsten ServiceLevel ist der aktive Server. Für einen Failover aktiviert der Client die Abtastung und Veröffentlichung auf dem Server mit dem höchsten ServiceLevel. Abbildung 30 zeigt die Schritte, die ein Client bei der Kommunikation mit einem Server im Warm-Failover-Modus ausführen würde.“



(OPC UA Part 4, Abschnitt 6.6.2.4.5.3.)

Unterstützte Architekturen

Einführung

In diesem Kapitel werden die topologischen Architekturen beschrieben, die vom Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server unterstützt werden.

Unterstützte Konfigurationen des BMENUA0100-Moduls

Platzierung des BMENUA0100-Moduls

Das BMENUA0100-Modul kann in einem Ethernet-Steckplatz im lokalen Hauptrack (d. h. im gleichen Rack wie die Steuerung) in den folgenden Konfigurationen platziert werden:

- M580-Standalone-Konfiguration
- M580-Standalone-Sicherheitssteuerungskonfiguration
- M580-Hot Standby-Konfiguration
- M580-Hot Standby-Sicherheitssteuerungskonfiguration

HINWEIS:

- Das BMENUA0100-Modul kann mit allen M580-Steuerungen verwendet werden.
- Wenn eine Netzwerkschleife erstellt wird, wechselt das BMENUA0100-Modul in den Zustand NOCONF (Keine Konfiguration). Um Schleifen und damit zusammenhängende Ereignisse zu vermeiden, teilen Sie bei Verwendung des BMENUA0100-Steuerungsports das Steuerungsport-Netzwerk und das Steuerungsbaugruppenträger-Netzwerk physisch (über die Trennung der Verdrahtung) und nicht nur logisch (über die Einstellungen für Subnetz und Subnetzmaske).

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

Verbinden Sie den Steuerungsport des BMENUA0100-Moduls nicht mit dem Service-Port der Steuerung.

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

Verbindung über das HTTPS-Protokoll

Wenn bei Ihrer Anwendung Verbindungsprobleme auftreten, wenden Sie sich an Ihren lokalen IT-Support, um zu bestätigen, dass Ihre Netzwerkkonfiguration und Sicherheitsrichtlinien mit dem HTTPS-Zugriff (Port 443) auf die IP-Adresse des BMENUA0100-Moduls übereinstimmen.

Das BMENUA0100-Modul akzeptiert HTTPS-Verbindungen mit dem TLS-Protokoll (Transport Layer Security) ab v1.2. Beispiel: Windows 7 erfordert möglicherweise ein Update, damit TLS 1.2 die Firmware des BMENUA0100-Moduls aktualisieren oder auf dessen Website zugreifen kann.

Installation des BMENUA0100-Moduls in einem flachen Netzwerk

Bei mehreren M580-Racks, die mit einem einzigen Subnetz verbunden sind (d. h. einer flachen Netzwerkarchitektur), die BMENUA0100-Module mit deaktiviertem Steuerungsport umfassen, installieren Sie jedes BMENUA0100-Modul in einem anderen Steckplatz in seinem jeweiligen Rack (außer bei Hot Standby-Konfigurationen, bei denen die BMENUA0100-Module in derselben Steckplatznummer installiert sind). Alternativ können Sie einen Router verwenden, um die Racks zu isolieren und dadurch potenzielle Adresskonflikte mit den BMENUA0100-Modulen zu vermeiden.

Hinzufügen von Präfixen zu Gerätenamen (Funktionsnamen) in flachen Netzwerkdesigns

Wenn eine Architektur mehrere BMENUA0100-Module umfasst, die mit anderen Geräten kommunizieren, wie z. B. M580-Steuerungen, die im selben Subnetz konfiguriert sind, sollten Sie Präfixe für den Gerätenamen (oder Rollennamen) aller Geräte, einschließlich der M580-Steuerungen, verwenden. Diese Namenskonvention ermöglicht es den BMENUA0100-Modulen, zwischen den M580-Steuerungen zu unterscheiden und festzustellen, welche Steuerung in welchem Rack untergebracht ist. Diese Namenskonvention hilft, Unsicherheiten in Bezug auf ein flaches Netzwerkdesign zu beseitigen. Beispielsweise kann ein BMENUA0100-Modul ohne eindeutige Präfixe nicht bestimmen, mit welcher M580-Steuerung es nach einem Anwendungsdownload kommunizieren soll, um seine eigene Konfiguration abzurufen.

Das Präfix für den Gerätenamen kann in Control Expert auf der Registerkarte **Extras > Projekteinstellungen > Konfiguration** festgelegt werden.

Zugriff auf den integrierten OPC UA-Server des BMENUA0100

In den in diesem Kapitel beschriebenen topologischen Architekturen können der Ethernet-Baugruppenträger-Port des BMENUA0100-Kommunikationsmoduls und sein Steuerungsport verwendet werden, um den Zugriff auf den im Modul integrierten OPC UA-Server zu ermöglichen. Eine Beschreibung des Zeitpunkts, zu dem diese Ports für den Zugriff auf den integrierten OPC UA-Server verwendet werden können, finden Sie in den Beschreibungen des Steuerungsports und des Ethernet-Baugruppenträger-Ports im Abschnitt Externe Ports, Seite 23.

Maximale Anzahl an BMENUA0100-Modulen pro Konfiguration

In einer BMENUA0100-Konfiguration werden maximal folgende M580-Module unterstützt:

M580-Konfigurationstyp	**Maximale Anzahl BMENUA0100-Module**
Standalone	Zwei im lokalen Hauptrack für Standalone[1]- und Hot Standby[1,2]-Standard- und -Sicherheitskonfigurationen
Sicherheitssteuerung	
Hot Standby	
Hot Standby-Sicherheitssteuerung	

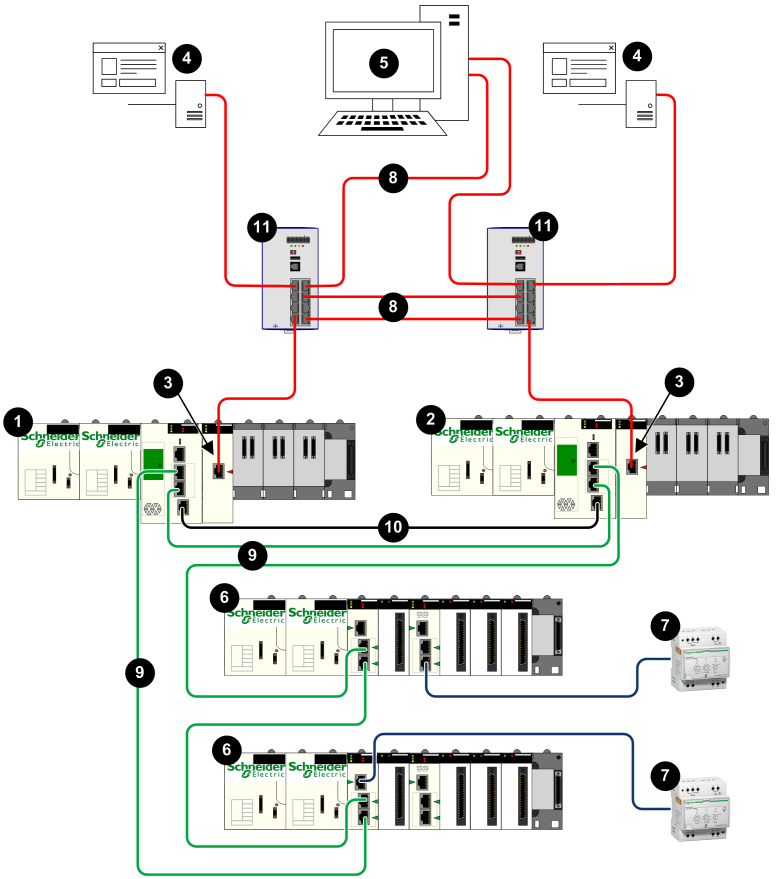
1. Wenn zwei BMENUA0100-Module in einem Hauptrack verwendet werden:
   - Die Leistung jedes Moduls ist geringer als bei Verwendung eines einzelnen Moduls.
   - Aktivieren Sie den Steuerungsport in der Konfiguration für beide Module.
2. Platzieren Sie in Hot Standby-Konfigurationen die BMENUA0100-Module in derselben Steckplatznummer in den entsprechenden lokalen Hauptracks.

CCOTF (Change Configuration on the Fly)

Das BMENUA0100-Modul unterstützt CCOTF nicht.

Isoliertes Steuerungsnetzwerk mit M580-Hot Standby-Steuerungen

Architektur



1 Primäre Hot Standby-Steuerung

2 Standby-Hot Standby-Steuerung

3 Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server

4 OPC UA-Client (SCADA-System)

5 Engineering-Workstation mit dualen Ethernet-Verbindungen

6 X80 Ethernet-RIO-Station

7 Verteiltes Gerät

8 Steuerungsnetzwerk

9 Ethernet-RIO-Hauptring

10 Hot Standby-Kommunikationsverbindung

11 Dual-Ring-Switch (DRS)

Beschreibung

Diese Architektur bietet redundante Verbindungen zu dualen OPC UA-Clients (SCADA-Systemen). Cybersicherheit kann in dieser Architektur entweder aktiviert oder deaktiviert werden. Das Steuerungsnetzwerk (8) ist sowohl von den Ethernet-Geräten, die sich im Ethernet-RIO-Hauptring (9) befinden, einschließlich der Steuerung, als auch von den verteilten Ethernet-Geräten (7) logisch isoliert. Dies wird auf der Netzwerkschicht des OSI-Modells über IP-Adressierung erreicht.

Der Steuerungsport (3) des Moduls BMENUA0100 mit seinen dualen IPv6/IPv4-Stacks ermöglicht eine Upstream-Konnektivität mit dem Steuerungsnetzwerk. Bei der Kommunikation über IPv6 unterstützt er sowohl die Autokonfiguration von zustandslosen Adressen (SLAAC) als auch die statische IP-Adressierung.

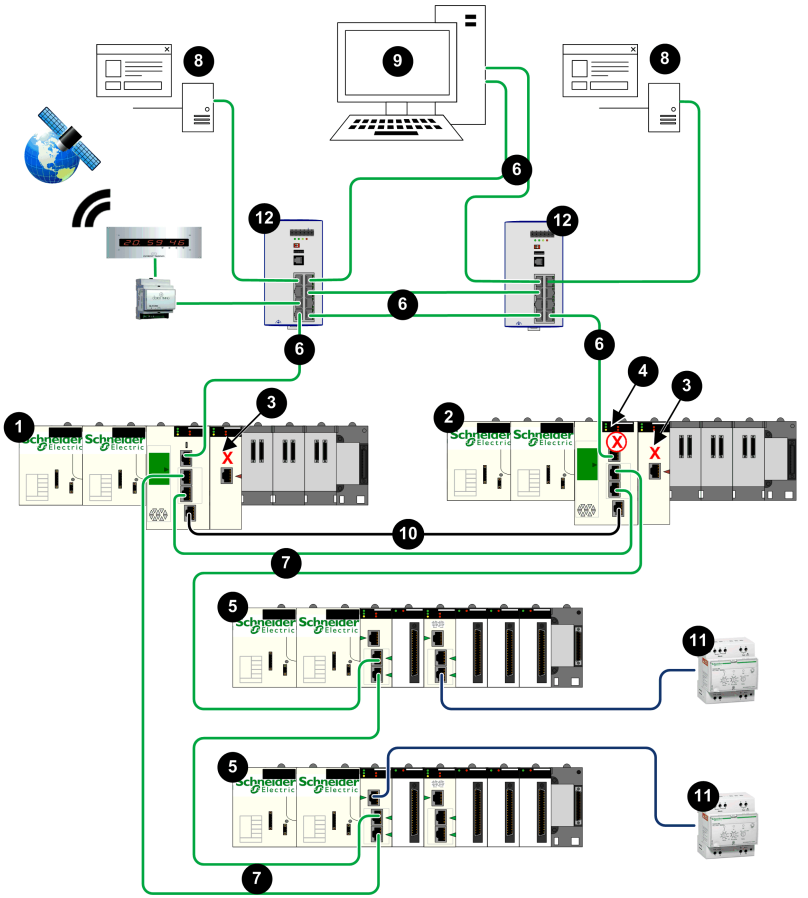
Das BMENUA0100-Modul bietet eine Modbus-Peer-to-Peer-Kommunikation zwischen den beiden Hot Standby-Steuerungen. Die Steuerungsports bieten Downstream-Konnektivität zu den Ethernet-Geräten im Ethernet-RIO-Hauptring.

Jedes BMENUA0100-Modul ist ein Client eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Die Verbindung wird über den BMENUA0100-Steuerungsport hergestellt. Die BMENUA0100-Module dienen auch als NTP-Server für andere Geräte im Ethernet-RIO-Hauptring. In diesem Hot Standby-Design ist das als „A“ konfigurierte Modul BMENUA0100 der primäre NTP-Server, das als „B“ konfigurierte Modul BMENUA0100 ist der Standby-NTP-Server. Auf diese Weise werden die Steuerungszeit und die BMENUA0100-Modulzeit synchronisiert.

Das Modul BMENUA0100 unterstützt die anwendungsbasierte Zeitstempelung. Dabei zeichnen Zeitstempelmodule Ereignisse in ihrem lokalen Puffer auf. Diese zeitgestempelten Ereignisse werden von der in der Steuerung ausgeführten Anwendung genutzt, die die Rohdaten konvertiert und in einem verwendbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Nicht isoliertes flaches Netzwerk mit M580 Hot Standby

Architektur



1 Primäre Hot Standby-Steuerung

2 Standby-Hot Standby-Steuerung

3 BMENUA0100 mit deaktiviertem Steuerungsport

4 Standby-Steuerung mit automatischer Sperre des Service-Ports

5 X80 Ethernet-RIO-Station

6 Steuerungsnetzwerk

7 Ethernet-RIO-Hauptring

8 OPC UA-Client (SCADA-System)

9 Engineering-Workstation mit dualen Ethernet-Verbindungen

10 Hot Standby-Kommunikationsverbindung

11 Verteiltes Gerät

12 Dual-Ring-Switch (DRS)

Beschreibung

Diese Architektur bietet redundante Verbindungen von M580-Hot Standby-Steuerungen zu dualen OPC-UA-Clients (SCADA-Systemen). Ihr Hauptzweck ist die Bereitstellung einer hohen Verfügbarkeit für die Hot Standby-Steuerungen. Aus diesem Grund bildet diese Architektur ein nicht isoliertes flaches Netzwerk, das das Steuerungsnetzwerk und den Ethernet-RIO-Hauptring in einem einzigen Subnetz vereint.

Der BMENUA0100-Steuerungsport ist deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt. Die Upstream-Kommunikation von den Hot Standby-Steuerungen zu den SCADA-Servern erfolgt über den Service-Port der primären Steuerung. Die Steuerungsports bieten Downstream-Konnektivität zu den Ethernet-Geräten im Ethernet-RIO-Hauptring.

Der Service-Port (4) der Standby-Steuerung wird deaktiviert. Verwenden Sie dazu die Control Expert-Konfigurationssoftware, um Folgendes auszuwählen: **Automatische Sperre des Service-Ports auf der Standby-CPU** auf der Registerkarte **ServicePort** der Konfiguration für die primäre und die Standby-Steuerung.

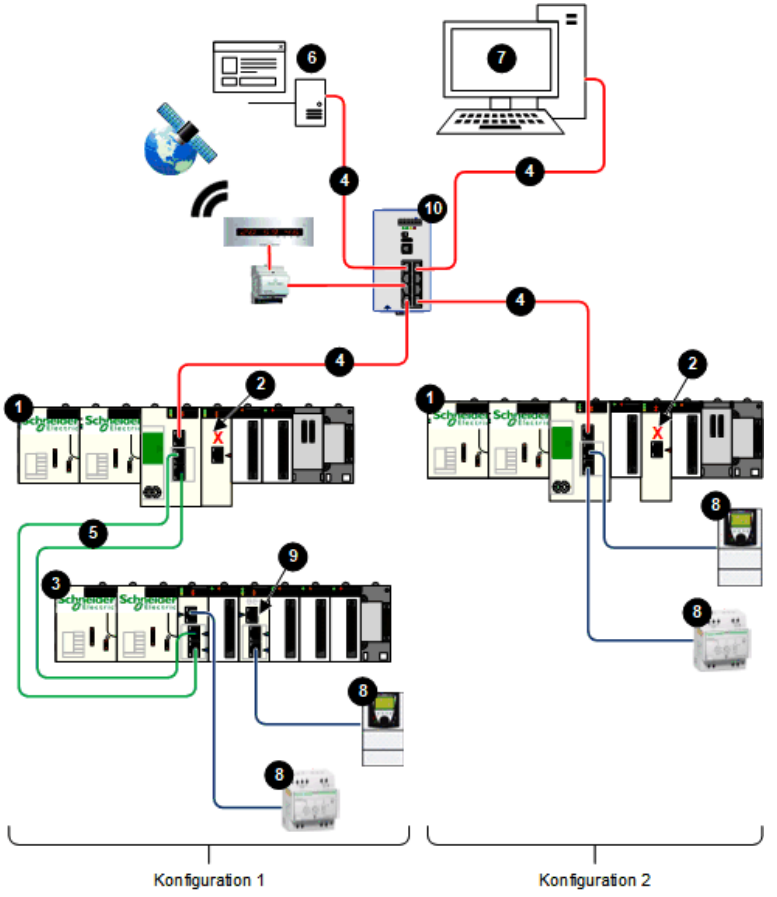
HINWEIS: Der Service-Port der Standby-Steuerung wird deaktiviert, um die unbeabsichtigte Bildung einer Ethernet-Kommunikationsschleife zu verhindern, bei der sowohl das Steuerungsnetzwerk als auch der Ethernet-RIO-Hauptring Teil desselben Subnetzes sind. Siehe *M580 Hot Standby Systemplanungshandbuch* und den Abschnitt Verwaltung von flachen Ethernet-Netzwerken mit M580 Hot Standby (für weitere Informationen siehe *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen*)).

In diesem flachen Netzwerkdesign können alle Geräte, einschließlich Steuerung, BMECRA31310-Module und BMENUA0100, Clients desselben NTP-Servers sein, der sich im Steuerungsnetzwerk befindet. Daher wird die Steuerungszeit mit dem BMENUA0100-Modul synchronisiert.

Das Modul BMENUA0100 unterstützt die anwendungsbasierte Zeitstempelung. Dabei zeichnen Zeitstempelmodule Ereignisse in ihrem lokalen Puffer auf. Diese zeitgestempelten Ereignisse werden von der in der Steuerung ausgeführten Anwendung genutzt, die die Rohdaten konvertiert und in einem verwendbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Flaches Netzwerk mit mehreren M580-Standalone-Steuerungen und einem einzelnen SCADA

Architektur



1 Standalone-Steuerung

2 BMENUA0100 mit deaktiviertem Steuerungsport

3 X80 Ethernet-RIO-Station

4 Steuerungsnetzwerk

5 Ethernet-RIO-Hauptring

6 OPC UA-Client (SCADA-System)

7 Engineering-Workstation mit einfacher Ethernet-Verbindung

8 Verteiltes Gerät

9 BMENOS0300-Switch

10 Dual-Ring-Switch (DRS)

Beschreibung

Diese Architektur bietet eine Verbindung zu einem einzelnen OPC UA-Client (einem SCADA-System) von mehreren M580-Standalone-Steuerungen. Es handelt sich um eine kostenoptimierte Architektur, die keine Hochverfügbarkeit erfordert. Diese Architektur stellt ein nicht isoliertes flaches Netzwerk dar, das das Steuerungsnetzwerk und den Ethernet-RIO-Hauptring in einem einzigen Subnetz vereint.

Der BMENUA0100-Steuerungsport ist für jede Standalone-Steuerung deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt. Die Upstream-Kommunikation von jeder Steuerung zum SCADA-Server erfolgt über den Service-Port der Steuerung.

In Konfiguration 1 wird die Downstream-Konnektivität von der Steuerung zur X80 Ethernet-RIO-Station (4) über die dualen Gerätenetzwerk-Ports der Steuerung bereitgestellt. Weitere Downstream-Verbindungen werden über den Service-Port des Moduls BMECRA31310 und einen BMENOS0300-Switch (9) für verteilte Ethernet-Geräte ermöglicht.

In Konfiguration 2 wird die Downstream-Konnektivität über die dualen Gerätenetzwerk-Ports an die verteilten Ethernet-Geräte geliefert.

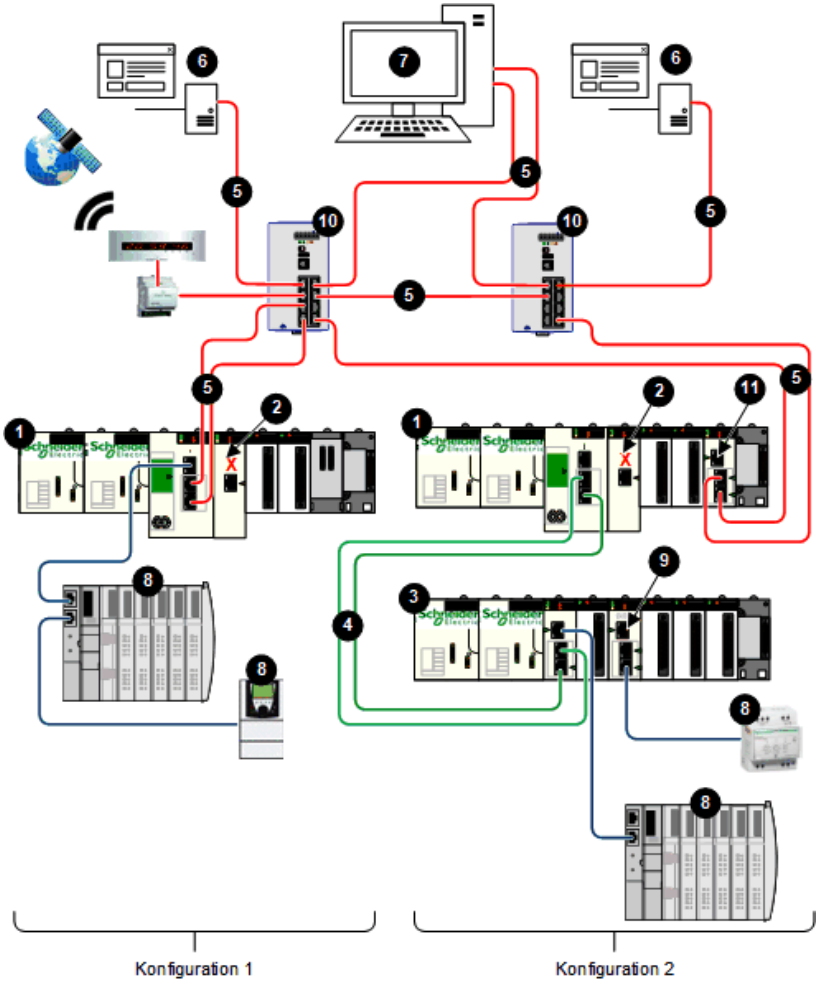
In diesem flachen Netzwerkdesign sind alle Netzwerkgeräte - einschließlich der Steuerung, der Module BMECRA31310 und der BMENUA0100 - NTP-Clients eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Demzufolge werden die Steuerungszeit und die BMENUA0100-Modulzeit synchronisiert.

Das Modul BMENUA0100 unterstützt die anwendungsbasierte Zeitstempelung. Dabei zeichnen Zeitstempelmodule Ereignisse in ihrem lokalen Puffer auf. Diese zeitgestempelten Ereignisse werden von der in der Steuerung ausgeführten Anwendung genutzt, die die

Rohdaten konvertiert und in einem verwendbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Flaches Netzwerk mit mehreren M580-Standalone-Steuerungen und redundantem SCADA

Architektur



1 Standalone-Steuerung

2 BMENUA0100 mit deaktiviertem Steuerungsport

3 X80 Ethernet-RIO-Station

4 Ethernet-RIO-Hauptring

5 Steuerungsnetzwerk

6 OPC UA-Client (SCADA-System)

7 Engineering-Workstation mit dualen Ethernet-Verbindungen

8 Verteiltes Gerät

9 BMENOS0300-Switch

10 Dual-Ring-Switch (DRS)

11 BMENOS0300-, BMENOC0301- oder BMENOC0311-Modul

Beschreibung

Diese Architektur bietet eine hohe Verfügbarkeit des Steuerungsnetzwerks über redundante Verbindungen zwischen OPC UA-Clients (SCADA-Systemen) und mehreren M580-Standalone-Steuerungen. Diese Architektur stellt ein nicht isoliertes flaches Netzwerk dar, das das Steuerungsnetzwerk und den Ethernet-RIO-Hauptring in einem einzigen Subnetz vereint.

Der BMENUA0100-Steuerungsport ist für jede Standalone-Steuerung deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

In Konfiguration 1 erfolgt die Upstream-Kommunikation mit den SCADA-Servern über die dualen Gerätenetzwerk-Ports der Steuerung. Dabei wird das RSTP-Redundanzprotokoll verwendet, um jedem Port Rollen zuzuweisen und logische Ethernet-Schleifen zu vermeiden. Die Downstream-Konnektivität zu den verteilten Ethernet-Geräten wird über den Service-Port der Steuerung bereitgestellt.

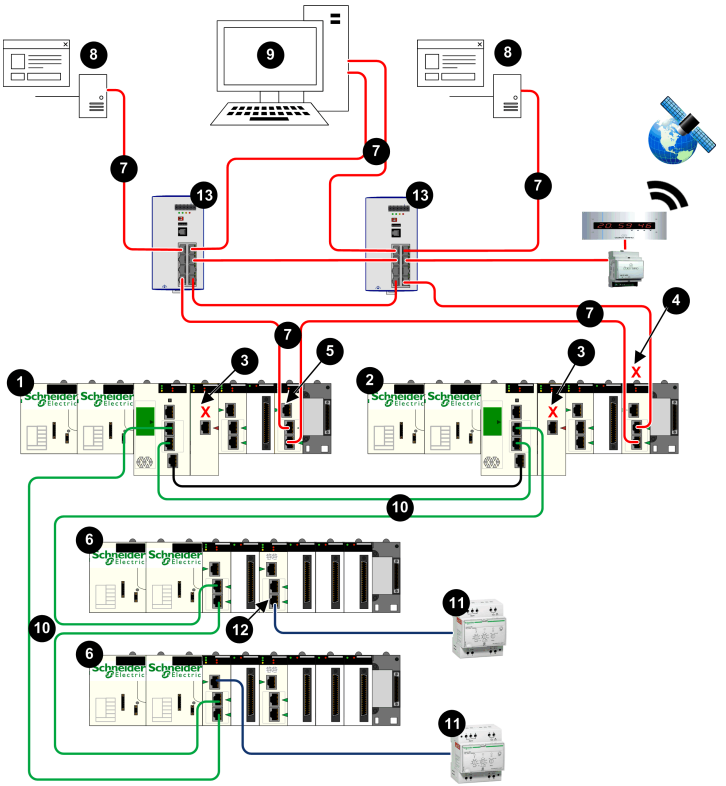
In Konfiguration 2 wird die Upstream-Konnektivität zu den SCADA-Servern über die Gerätenetzwerk-Ports eines BMENOS0300-, BMENOC0301- oder BMENOC0311-Moduls bereitgestellt. Das RSTP-Redundanzprotokoll wird verwendet, um zur Vermeidung von logischen Ethernet-Schleifen jedem Port Rollen zuzuweisen. Die Downstream-Konnektivität der Steuerung wird über die Gerätenetzwerk-Ports der Steuerung zur dezentralen X80 Ethernet-E/A-Station bereitgestellt. Weitere Downstream-Verbindungen werden sowohl über den Service-Port des Moduls BMECRA31310 als auch über einen BMENOS0300-Switch (9) für verteilte Ethernet-Geräte ermöglicht.

In diesem flachen Netzwerkdesign sind alle Netzwerkgeräte - einschließlich der Steuerung, der Module BMECRA31310 und der BMENUA0100 - NTP-Clients eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Demzufolge werden die Steuerungszeit und die BMENUA0100-Modulzeit synchronisiert.

Das Modul BMENUA0100 unterstützt die anwendungsbasierte Zeitstempelung. Dabei zeichnen Zeitstempelmodule Ereignisse in ihrem lokalen Puffer auf. Diese zeitgestempelten Ereignisse werden von der in der Steuerung ausgeführten Anwendung genutzt, die die Rohdaten konvertiert und in einem verwendbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Flaches Netzwerk mit M580-Hot Standby-Steuerungen und redundantem SCADA

Architektur



1 Primäre Hot Standby-Steuerung

2 Standby-Hot Standby-Steuerung

3 BMENUA0100 mit deaktiviertem Steuerungsport

4 BMENOS0300, BMENOC0301 oder BMENOC0311 mit deaktiviertem Baugruppenträger-Port

5 BMENOS0300, BMENOC0301 oder BMENOC0311 mit aktiviertem Baugruppenträger-Port

6 X80 Ethernet-RIO-Station

7 Steuerungsnetzwerk

8 OPC UA-Client (SCADA-System)

9 Engineering-Workstation mit dualen Ethernet-Verbindungen

10 Ethernet-RIO-Hauptring

11 Verteiltes Gerät

12 BMENOS0300-Switch

13 Dual-Ring-Switch (DRS)

Beschreibung

Diese Architektur bietet hohe Verfügbarkeit mit redundanten Verbindungen, die redundante OPC UA-Clients (SCADA-Systeme) mit redundanten Hot Standby-Steuerungen in einem einzigen Subnetz verbinden.

Jede Steuerung ist über ein BMENOS0300-, BMENOC0301- oder BMENOC0311-Modul mit SCADA verbunden. Um Ethernet-Schleifen zu vermeiden, muss der Baugruppenträger-Port eines der BMENOS0300-, BMENOC0301- oder BMENOC0311-Module deaktiviert sein. In diesem Beispiel hat das Modul in der Standby-Steuerung (4) einen deaktivierten Baugruppenträger-Port. Darüber hinaus wird das RSTP-Redundanzprotokoll verwendet, um jedem Port Rollen zuzuweisen, um logische Ethernet-Schleifen zu vermeiden.

Der BMENUA0100-Steuerungsport (3) ist für jede Standalone-Steuerung deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

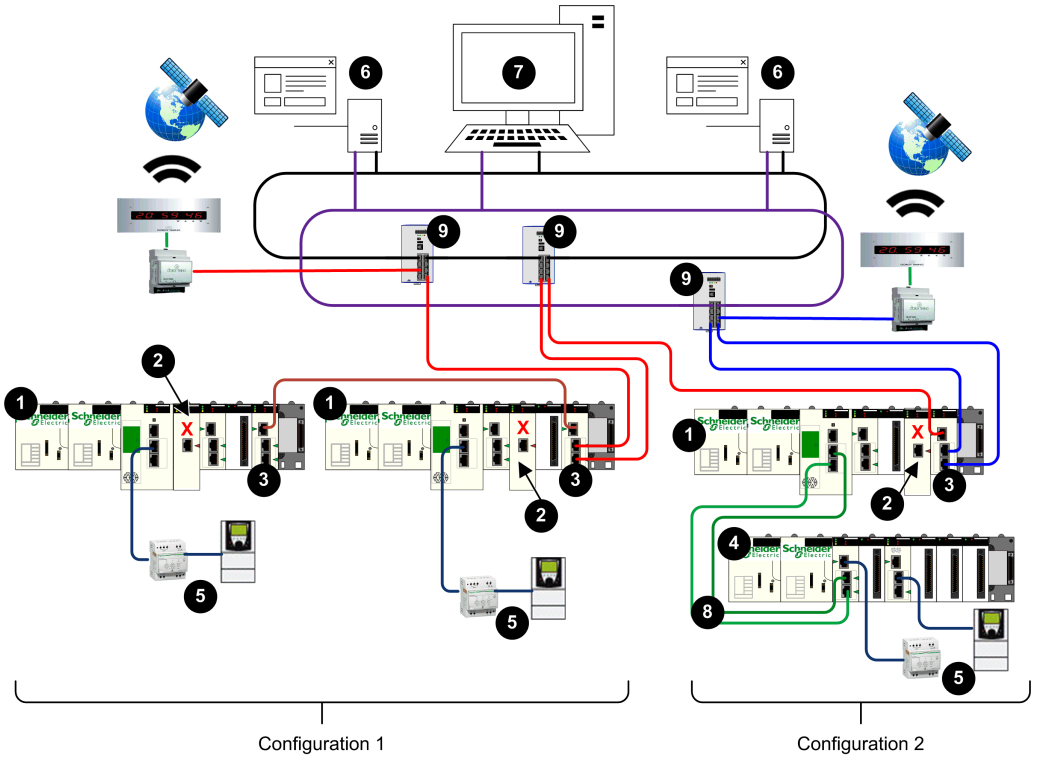
Die Downstream-Konnektivität zu den X80 Ethernet-RIO-Stationen wird über die Gerätenetzwerk-Ports der Steuerung bereitgestellt. Weitere Downstream-Konnektivität von den X80 Ethernet-RIO-Stationen wird sowohl vom CRA-Service-Port als auch von einem BMENOS0300-Switch (12) für verteilte Ethernet-Geräte ermöglicht.

In diesem flachen Netzwerkdesign sind alle Netzwerkgeräte - einschließlich jeder Hot Standby-Steuerung und des BMENUA0100-Moduls - NTP-Clients eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Demzufolge werden die Steuerungszeit und die BMENUA0100-Modulzeit synchronisiert.

Das Modul BMENUA0100 unterstützt die anwendungsbasierte Zeitstempelung. Dabei zeichnen Zeitstempelmodule Ereignisse in ihrem lokalen Puffer auf. Diese zeitgestempelten Ereignisse werden von der in der Steuerung ausgeführten Anwendung genutzt, die die Rohdaten konvertiert und in einem verwendbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Hierarchisches Netzwerk mit mehreren M580-Standalone-Steuerungen, verbunden mit dem Steuerungsnetzwerk und einem redundanten SCADA

Architektur



1 Standalone-Steuerung

2 BMENUA0100 mit deaktiviertem Steuerungsport

3 Ethernet-Kommunikationsmodul BMENOC0321

4 X80 Ethernet-RIO-Station

5 Verteiltes Gerät

6 OPC UA-Client (SCADA-System)

7 Engineering-Workstation mit dualen Ethernet-Verbindungen

8 Ethernet-RIO-Hauptring

9 Dual-Ring-Switch (DRS)

Beschreibung

Diese Architektur verfügt über ein hierarchisches Netzwerk, das auf BMENOC0321-Kommunikationsmodulen basiert, um den Netzwerkverkehr zwischen Subnetzen weiterzuleiten. Die Upstream-Kommunikation von den Steuerungen zu den OPC UA-Clients (SCADA-Systemen) erfolgt über die zwei Gerätenetzwerk-Ports des BMENOC0321-Moduls unter Verwendung des RSTP-Redundanzprotokolls zur Vermeidung logischer Ethernet-Schleifen

HINWEIS: Diese Architektur erfordert die Konfiguration statischer Routen in den Geräten des Steuerungsnetzwerks, um die verschiedenen Subnetze der Steuerungen umzuleiten.

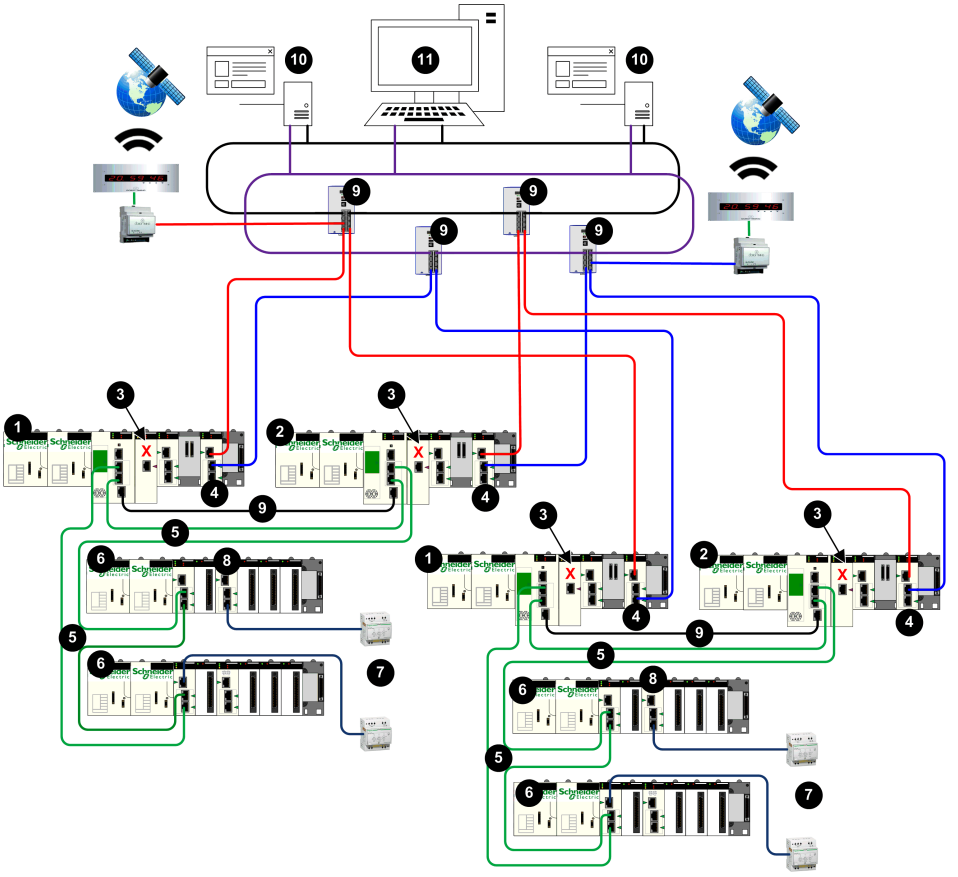
Der BMENUA0100-Steuerungsport (2) ist für jede Standalone-Steuerung deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

Konfiguration 1 umfasst zwei Steuerungen, die sich im gleichen Subnetz befinden. Bei dieser Konfiguration wird das Modul BMENOC0321 verwendet, um eine redundante Upstream-Kommunikation mit den redundanten SCADA-Servern bereitzustellen. Das Modul BMENOC0321 nutzt das RSTP-Redundanzprotokoll, um logische Ethernet-Schleifen zu vermeiden. Die dualen Gerätenetzwerk-Ports der beiden Steuerungen bieten eine Downstream-Kommunikation mit den verteilten Ethernet-Geräten.

Konfiguration 2 umfasst eine einzelne Steuerung mit X80 Ethernet-RIO-Station. Diese Steuerung verwendet das BMENOC0321-Modul für die Upstream-Kommunikation mit den redundanten SCADA-Servern. Das Modul BMENOC0321 erreicht dies durch die Verwendung von zwei unabhängigen Subnetzen. Die Downstream-Kommunikation von der X80 Ethernet-RIO-Station erfolgt über den Service-Port des Moduls BMECRA31310 und einen BMENOS0300-Switch zu verteilten Ethernet-Geräten.

Hierarchisches Netzwerk mit mehreren M580-Hot Standby-Steuerungen und redundanten SCADA-Verbindungen

Architektur



1 Primäre Hot Standby-Steuerung

2 Standby-Hot Standby-Steuerung

3 BMENUA0100 mit deaktiviertem Steuerungsport

4 Ethernet-Kommunikationsmodul BMENOC0321

5 Ethernet-RIO-Hauptring

6 X80 Ethernet-RIO-Station

7 Verteiltes Gerät

8 BMENOS0300-Switch

9 Dual-Ring-Switch (DRS)

10 OPC UA-Client (SCADA-System)

11 Engineering-Workstation mit dualen Ethernet-Verbindungen

Beschreibung

Diese Architektur verfügt über ein hierarchisches Netzwerk, das auf BMENOC0321-Kommunikationsmodulen (4) basiert, um den Netzwerkverkehr zwischen Subnetzen weiterzuleiten. Die Upstream-Kommunikation von den Hot Standby-Steuerungen zu den OPC UA-Clients (SCADA-Systemen) erfolgt über die dualen Gerätenetzwerk-Ports der BMENOC0321-Module, die das RSTP-Redundanzprotokoll verwenden, um logische Ethernet-Schleifen zu vermeiden.

> **HINWEIS:** Diese Architektur erfordert die Konfiguration statischer Routen in den Geräten des Steuerungsnetzwerks, um die verschiedenen Subnetze der Steuerungen umzuleiten.

Der BMENUA0100-Steuerungsport (3) ist für jede Steuerung deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

Bei dieser Konfiguration wird das BMENOC0321-Modul verwendet, um eine redundante Upstream-Kommunikation über redundante Verbindungen mit den redundanten SCADA-Servern bereitzustellen. Die dualen Gerätenetzwerk-Ports der Steuerungen bieten eine Downstream-Kommunikation mit den X80 Ethernet-RIO-Stationen. Eine weitere Downstream-Kommunikation von der X80 Ethernet-RIO-Station mit den verteilten Ethernet-Geräten erfolgt über den Service-Port BMECRA31310 und einen BMENOS0300-Switch (8).

Inbetriebnahme und Installation

Einführung

In diesem Kapitel wird beschrieben, wie eine Betriebsart ausgewählt das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server ausgewählt wird.

Inbetriebnahme-Checkliste für das BMENUA0100-Modul

Inbetriebnahme-Checkliste

In der folgenden Übersicht wird eine Reihe von Aufgaben beschrieben, die bei der Inbetriebnahme und Installation eines neuen BMENUA0100-Moduls zu befolgen sind. In diesem Beispiel wird das Modul so konfiguriert, dass es im PKI-Modus mit Selbstsignierung und Zertifizierungsstelle mit IPV6-SLAAC- und IPV4-Adressen betrieben wird:

1. Konfigurieren Sie die Control Expert-Anwendung, Seite 126.
2. Konfigurieren Sie den Router/SLAAC-Server (für IPV6 im SLAAC-Modus).
3. Wählen Sie den erweiterten (oder den sicheren) Modus für das Modul aus:

a.	Setzen Sie den Drehwahlschalter, Seite 25 auf der Rückseite des Moduls in die Stellung Erweiterter (oder sicherer) Modus, Seite 32.
b.	Installieren Sie das Modul, Seite 90 in einem Ethernet-Steckplatz im Rack.

4. Konfigurieren Sie die Cybersicherheitseinstellungen über die Webseiten, Seite 92 des Moduls:

a.	Erstellen Sie die Konfiguration der Cybersicherheit über die Webseite Einstellungen, Seite 100.
b.	Stellen Sie den **PKI-Modus** auf „Selbsigniert und CA“ ein.
c.	Erstellen Sie für Clientgeräte, die PKI nicht unterstützen, eine Liste, Seite 120 **Vertrauenswürdige Client-Zertifikate**.
d.	**Übernehmen** Sie die Konfigurationsdatei.

5. Führen Sie eine manuelle Zertifikatregistrierung, Seite 119 durch:

a.	Generieren Sie eine Zertifikatsignierungsanforderung (CSR).
b.	Übertragen Sie das Zertifizierungsstellenzertifikat per Push.
c.	Übertragen Sie das Gerätezertifikat per Push.

6. Fügen Sie das Zertifizierungsstellenzertifikat zu den OPC UA-Clientgeräten hinzu.
7. Testen Sie die Kommunikation zwischen OPC UA-Client und -Server.

Inbetriebnahme des BMENUA0100-Moduls

Einführung

Das BMENUA0100-Modul mit integriertem OPC UA-Server ist im Hardwarekatalog von Control Expert als Kommunikationsmodul aufgeführt. Es belegt einen E/A-Kanal.

Wenn ein BMENUA0100-Modul werkseitig geliefert wird, ist sein Cybersicherheit-Betriebsmodus standardmäßig auf „Erweitert“ (oder „Sicher“) eingestellt. Um das neue Modul für den erweiterten (oder sicheren) Modus zu konfigurieren, folgen Sie dem Szenario für Inbetriebnahme im erweiterten (oder gesicherten) Modus, Seite 32 wie unten beschrieben.

Um den Cybersicherheits-Betriebsmodus für ein Modul zu ändern, das zuvor konfiguriert wurde, einschließlich eines neuen Moduls, das Sie für einen Betrieb im Standardmodus konfigurieren möchten, führen Sie einen Vorgang „Zurücksetzen der Cybersicherheit“ (oder der Sicherheit)“, Seite 88 für das Modul durch. Nach dem Zurücksetzen der Cybersicherheit (oder der Sicherheit) können Sie eines der folgenden Szenarien befolgen: Inbetriebnahme im erweiterten (oder sicheren) Modus, Seite 32 oder Inbetriebnahme im Standardmodus, Seite 32.

Inbetriebnahme im erweiterten (oder sicheren) Modus

Die Inbetriebnahme eines BMENUA0100-Moduls für den Betrieb im erweiterten (oder sicheren) Modus erfordert die Durchführung von zwei Konfigurationsprozessen:

- Cybersicherheitskonfiguration über die Webseiten des Moduls
- Konfiguration von IP-Adresse, NTP-Client und SNMP-Agent über das Control Expert-Konfigurationstool

Nur ein Sicherheitsadministrator kann das Modul durch Eingabe der Standardkombination aus Benutzername und Passwort, Seite 33 für den erweiterten (oder sicheren) Modus in diesem Modus in Betrieb nehmen.

HINWEIS: Führen Sie die folgenden Konfigurationsschritte in der angegebenen Reihenfolge durch:

- Verwenden Sie Control Expert, um die IP-Adressen von Steuerung und Baugruppenträger zu konfigurieren.
- Verwenden Sie die Modulwebseiten, um die Cybersicherheitseinstellungen zu konfigurieren.
- Verwenden Sie Control Expert, um die Konfiguration des NTP-Clients und SNMP-Agents abzuschließen.

HINWEIS: Informationen zur Inbetriebnahme im erweiterten (oder sicheren) Modus mit manueller Registrierung finden Sie im Abschnitt Manuelle Registrierung, Seite 119.

Die folgende Vorgehensweise ist für ein neues Modul vorgesehen, das noch nicht konfiguriert wurde. Wenn Sie ein Modul verwenden, das bereits konfiguriert wurde, führen Sie einen Vorgang „Zurücksetzen der Cybersicherheit“ (oder „Zurücksetzen der Sicherheit“), Seite 88 durch, bevor Sie mit den folgenden Schritten fortfahren.

So nehmen Sie das Modul im erweiterten (oder sicheren) Modus in Betrieb:

1. Konfigurieren Sie die IP-Adresseinstellungen:

a.	Öffnen Sie das Konfigurationstool von Control Expert.
b.	Erstellen Sie in Control Expert ein **Neues Projekt**, fügen Sie dem Projekt ein BMENUA0100-Modul aus dem **Hardwarekatalog** hinzu und konfigurieren Sie die IP-Adresseinstellungen, Seite 126.

2. Konfigurieren Sie die Einstellungen für die Cybersicherheit:

a.	Wenn das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 25, um den Drehwahlschalter in die Stellung **Erweitert (oder Sicher)** zu setzen.
b.	Installieren, Seite 89 Sie das Modul in einem Ethernet-Steckplatz im lokalen Ethernet-Hauptrack und schalten Sie das Modul aus und wieder ein.
c.	Verwenden Sie Ihren Webbrowser, um Ihren Konfigurations-PC über den Steuerungsport oder den Baugruppenträger-Port mit dem Modul zu verbinden, und navigieren Sie zu den Modulwebseiten an der konfigurierten IP-Adresse.
d.	Wenn Ihr Webbrowser eine Meldung anzeigt, Seite 94, die auf ein potenzielles Sicherheitsrisiko verweist, lesen Sie sich die Meldung durch und stellen Sie die Verbindung her, wenn Sie damit einverstanden sind. Klicken Sie dazu auf **Das Risiko akzeptieren und fortfahren** (oder eine vergleichbare, browserspezifische Angabe).
e.	Geben Sie auf der Anmeldeseite des Benutzers die Standardkombination aus Benutzername/ Passwort, Seite 33 ein.
f.	Ändern und bestätigen Sie das Passwort. Informationen zu den Passwortanforderungen finden Sie im Abschnitt Benutzerverwaltung, Seite 122. Die **Startseite** „Startseite“, Seite 97des Moduls wird angezeigt.
g.	Navigieren Sie von der **Startseite** zu den Webseiten des Moduls und konfigurieren Sie dessen Einstellungen für die Cybersicherheit.

3. Konfigurieren Sie die Einstellungen für NTP-Client und SNMP-Agent:

a.	Öffnen Sie das Konfigurationstool von Control Expert.
b.	Konfigurieren Sie in Control Expert die Einstellungen für den NTP-Client und den SNMP-Agent, Seite 126.
c.	Sobald die Control Expert-Projektkonfiguration abgeschlossen ist, stellen Sie eine Verbindung zur Steuerung her und übertragen Sie das Projekt in die Steuerung.

HINWEIS: Wenn die Konfiguration in das BMENUA0100-Modul geladen wird, ändert sich der Modulstatus von NICHT KONFIGURIERT zu KONFIGURIERT. Die **SECURE**-LED, Seite 148 gibt an, ob das Modul nicht konfiguriert oder konfiguriert ist und ob der OPC UA-Server mit einem OPC UA-Client verbunden ist.

Inbetriebnahme im Standardmodus

Im Standardmodus ist keine Cybersicherheitskonfiguration erforderlich. Die Einstellungen für IP-Adresse, NTP-Client und SNMP-Agent werden mithilfe des Control Expert-Konfigurationstools konfiguriert. Im Standardmodus beginnt das Modul mit der Kommunikation, wenn es im Rack platziert ist, eingeschaltet wurde und eine gültige Konfiguration von Control Expert erhält.

Verwenden Sie die Standardkombination aus Benutzername und Passwort, Seite 33, um das Modul im Standardmodus in Betrieb zu nehmen.

So nehmen Sie das Modul im Standardmodus in Betrieb:

1. Wenn das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 25, um den Drehwahlschalter in die Stellung **Standard** zu setzen.
2. Setzen Sie das Modul in einen Ethernet-Steckplatz im lokalen Ethernet-Hauptrack ein und schalten Sie die Spannungsversorgung aus und wieder ein.
3. Öffnen Sie das Konfigurationstool von Control Expert.
4. Erstellen Sie in Control Expert ein **Neues Projekt**, fügen Sie ein BMENUA0100-Modul aus dem **Hardwarekatalog** im Projekt hinzu und konfigurieren Sie dann die Einstellungen für IP-Adresse, Seite 126, NTP-Client, Seite 136 und SNMP-Agent, Seite 139.
5. Sobald die Control Expert-Projektkonfiguration abgeschlossen ist, stellen Sie eine Verbindung zur Steuerung her und übertragen Sie das Projekt in die Steuerung.

   HINWEIS: Bei einem Betrieb im Standardmodus ist die **SECURE**-LED aus.

Zurücksetzen der Cybersicherheit (oder der Sicherheit)

Führen Sie für ein zuvor konfiguriertes Modul oder für ein neues Modul, das Sie für einen Betrieb im Cybersicherheitsmodus konfigurieren möchten, einen Cybersicherheits-Reset (oder Sicherheits-Reset) durch, bevor Sie mit der Konfiguration der Cybersicherheit fortfahren. Durch einen Reset-Vorgang werden die Cybersicherheitseinstellungen auf die werkseitigen Standardwerte zurückgesetzt. Einen Reset können Sie über die Webseiten des Moduls oder mithilfe des Drehwahlschalters an der Rückseite des Moduls vornehmen.

Webseiten: Für ein BMENUA0100-Modul, das zurzeit für den erweiterten (oder sicheren) Modus konfiguriert ist:

1. Navigieren Sie zur Webseite **Konfigurationsverwaltung > RESET**.
2. Klicken Sie auf **Zurücksetzen**.

   HINWEIS: Der Vorgang „Zurücksetzen der Cybersicherheit (oder der Sicherheit)“ ist abgeschlossen, wenn die **RUN**-LED dauerhaft grün leuchtet und die **NS**-Steuerungsport-LED und die **BS**-Port-LED am Baugruppenträger rot leuchten.

3. Schalten Sie die Spannungsversorgung des Moduls auf eine der folgenden Arten ein und wieder aus:
   - Schalten Sie die Spannungsversorgung des Modulracks aus und anschließend wieder ein.
   - Entfernen Sie das Modul physisch aus dem Rack und setzen Sie es dann wieder ein.

   Sie können jetzt mit der Inbetriebnahme im erweiterten (oder sicheren) Modus fortfahren.

Drehwahlschalter: Für jedes BMENUA0100-Modul:

1. Wenn das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 25, um den Drehwahlschalter in die Stellung **Zurücksetzen der Cybersicherheit** zu setzen.
2. Installieren, Seite 89 Sie das Modul in einem Ethernet-Steckplatz im lokalen Ethernet-Hauptrack und schalten Sie das Modul aus und wieder ein.

   HINWEIS: Dadurch werden die werkseitigen Standardeinstellungen des Moduls wiederhergestellt, einschließlich der Standard-IP-Adresse des Steuerungsports, Seite 127: 10.10.MAC5.MAC6. Wenn die letzten beiden Bytes der MAC-Adresse (*MAC5.MAC6*) *0,0* in der Standardadresse entsprechen, stellen Sie eine Punkt-zu-Punkt-Kabelverbindung zwischen Ihrem Computer und dem Controller, dem Kommunikationsmodul oder einem anderen Modul her.

   Nach Abschluss des Vorgangs leuchtet die **RUN**-LED leuchtet dauerhaft grün und die **NS**-Steuerungsport-LED und die **BS**-Port-LED am Baugruppenträger leuchten rot. Sie können die Spannungsversorgung abschalten, das Modul aus dem Rack entfernen und entweder mit der Inbetriebnahme im erweiterten (oder sicheren) Modus, Seite 32 oder mit der Inbetriebnahme im Standardmodus, Seite 32 fortfahren.

Installation der Software BMENUA0100

Einführung

Sie können das BMENUA0100-Modul nur in einem lokalen Ethernet-Hauptrack installieren, indem Sie es in einem Ethernet-Steckplatz positionieren, der nicht der Spannungsversorgung oder der Steuerung vorbehalten ist.

HINWEIS: Wenn Ihre Anwendung auf einer EcoStruxure Control Expert-Version unter 15.3 basiert und Ihre Anwendung mehrere Steuerungen (die keine Hot Standby-Steuerungen sind) mit jeweils einem BMENUA0100-Modul umfasst, installieren Sie die Module so, dass die Steckplatznummer jedes BMENUA0100-Moduls eindeutig ist. Beispiel: Für eine Anwendung mit zwei Steuerungen gilt Folgendes: BMENUA0100-Modul im Rack von Steuerung 1 wird in Steckplatz 4 platziert. Platzieren Sie ein BMENUA0100-Modul im Rack von Steuerung 2 in einen anderen Steckplatz als Steckplatz 4.

Sicherheitshinweise zur Erdung

Es sind alle geltenden lokalen und nationalen Sicherheitsvorschriften und -standards zu beachten.

⚠⚠ GEFAHR

ELEKTRISCHER SCHLAG

Tragen Sie bei der Arbeit mit geschirmten Kabeln persönliche Schutzausrüstung (PSA).

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

Der Baugruppenträger für Ihr Modul fungiert gleichzeitig als Funktionserde-Masseplatte (FE) und muss an einen geerdeten, leitenden Baugruppenträger montiert und angeschlossen werden.

⚠ WARNUNG

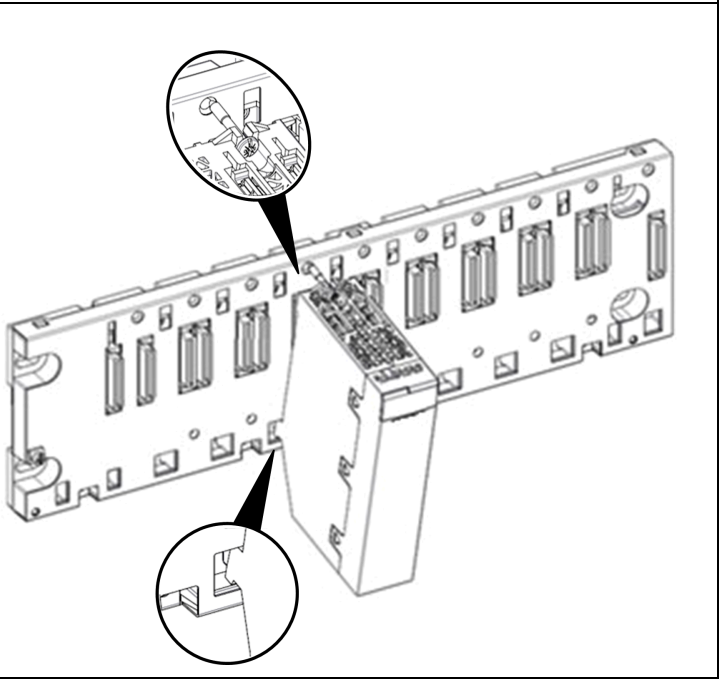
UNBEABSICHTIGTER GERÄTEBETRIEB

Verbinden Sie den Baugruppenträger mit der Funktionserde (FE) Ihrer Installation.

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

Installation eines BMENUA0100-Moduls im Rack

Ein BMENUA0100-Modul benötigt einen einzigen Rack-Ethernet-Steckplatz. Sie können das Modul in jedem Ethernet-Steckplatz installieren, der nicht für die Spannungsversorgung oder Steuerung reserviert ist. Gehen Sie vor wie folgt, um ein BMENUA0100-Modul in einem Rack zu installieren:

Schr-itt	Aktion	
1	Positionieren Sie die Führungsnasen an der Modulrückseite unten in den entsprechenden Steckplätzen im Rack.	
2	Drehen Sie das Modul gegen den oberen Rand des Racks, sodass das Modul bündig an die Rack-Rückseite anschließt. Das Modul befindet sich jetzt in der richtigen Position.	
3	Ziehen Sie die Schraube an der Moduloberseite fest, um das Modul in seiner Position im Rack zu sichern. Anzugsmoment: 0,4 bis 1,5 N•m (0.30 bis 1.10 lbf-ft).	

Erdung der E/A-Module

Informationen zur Erdung finden Sie im Abschnitt *Erdung des Racks und des Spannungsversorgungsmoduls* im Dokument *Modicon X80-Racks und Spannungsversorgungen - Hardware-Referenzhandbuch*.

Konfiguration

Einführung

In diesem Kapitel wird die Konfiguration des Ethernet-Kommunikationsmoduls BMENUA0100 mit integriertem OPC UA-Server beschrieben.

Konfiguration der Cybersicherheitseinstellungen des BMENUA0100-Moduls

Einführung

In diesem Abschnitt wird beschrieben, wie die Webseiten des Ethernet-Kommunikationsmoduls BMENUA0100 mit OPC UA-Server verwendet werden. Verwenden Sie die Webseiten, um eine Cybersicherheitskonfiguration für das Modul zu erstellen und um Diagnosedaten anzuzeigen.

Einführung in die Webseiten des BMENUA0100-Moduls

Einführung

Verwenden Sie die BMENUA0100-Webseiten, um eine Cybersicherheitskonfiguration für das Modul zu erstellen, zu verwalten und zu diagnostizieren und um Ereignis- und OPC UA-Diagnosedaten anzuzeigen.

HINWEIS:

- Die Webseiten des BMENUA0100-Moduls unterstützen die HTTPS-Kommunikation über das IPv4- und das IPv6-Protokoll, Seite 128.
- Verwenden Sie für den Zugriff auf die Webseiten nur die neuesten Versionen von Webbrowsern. Einige ältere Browser, z. B. Internet Explorer bis v7, werden nicht unterstützt.

  HINWEIS: Der Chrome-Webbrowser, Version 123.0.6312.123 (Build offiziell) (64 Bit), wurde mit den BMENUA0100-Webseiten getestet.

Für den Betrieb des BMENUA0100-Moduls im erweiterten (oder sicheren) Modus ist eine Cybersicherheitskonfiguration erforderlich, die durchgeführt werden muss, bevor die Einstellungen für IP-Adresse, NTP-Client und SNMP mit Control Expert konfiguriert, Seite

126 werden können. Eine Cybersicherheitskonfiguration kann nur lokal für jedes BMENUA0100-Modul erfolgen, indem ein Konfigurations-PC mit einem HTTPS-Browser mit dem BMENUA0100-Modul verbunden wird:

- über den Steuerungsport, wenn der Steuerungsport aktiviert ist.
- über den Baugruppenträger-Port (über ein BMENOC0301- oder BMENOC0311-Modul oder die Steuerung), wenn der Steuerungsport deaktiviert ist.

HINWEIS: Bevor das BMENUA0100-Modul die Gültigkeit der auf den Webseiten eingegebenen Cybersicherheitseinstellungen überprüft, werden die in Control Expert konfigurierten, Seite 126 IP-Adresseinstellungen für den Steuerungsport und Baugruppenträger-Port festgelegt.

Um das BMENUA0100-Modul im Standardmodus zu betreiben, sind keine Cybersicherheitseinstellungen erforderlich und diese können nicht konfiguriert werden.

HINWEIS:

- Wenn Sie ein selbstsigniertes Zertifikat verwenden, melden einige Browser die Verbindung zwischen dem PC und dem Modul möglicherweise als „Unsicher“.
- Für BMENUA0100-Module, die im erweiterten (oder sicheren) Modus in einem Hot Standby-System eingesetzt werden, überprüfen Sie, ob die Cybersicherheitseinstellungen für das BMENUA0100-Modul in der primären Steuerung den Cybersicherheitseinstellungen für das BMENUA0100-Modul in der Standby-Steuerung entsprechen. Das System führt diese Überprüfung nicht automatisch für Sie durch.

Die Zugänglichkeit der Webseiten richtet sich nach dem Cybersicherheitsmodus:

Webseite oder Gruppe	**Erweiterter (oder sicherer) Modus**	**Standardmodus**
Startseite, Seite 97	✓	✓
Einstellungen (Gerätesicherheit), Seite 100	✓	–
Zertifikatverwaltung, Seite 113	✓	–
Zugriffskontrolle, Seite 122	✓	–
Konfigurationsverwaltung, Seite 124	✓	–
Diagnose, Seite 171	✓	✓
✓: Zugriff auf Webseiten ist möglich. –: Zugriff auf Webseiten ist nicht möglich.		

Ursprüngliche Konfiguration der Cybersicherheitseinstellungen

Sie können die Cybersicherheitseinstellungen für ein BMENUA0100-Modul konfigurieren, auf das Folgendes zutrifft:

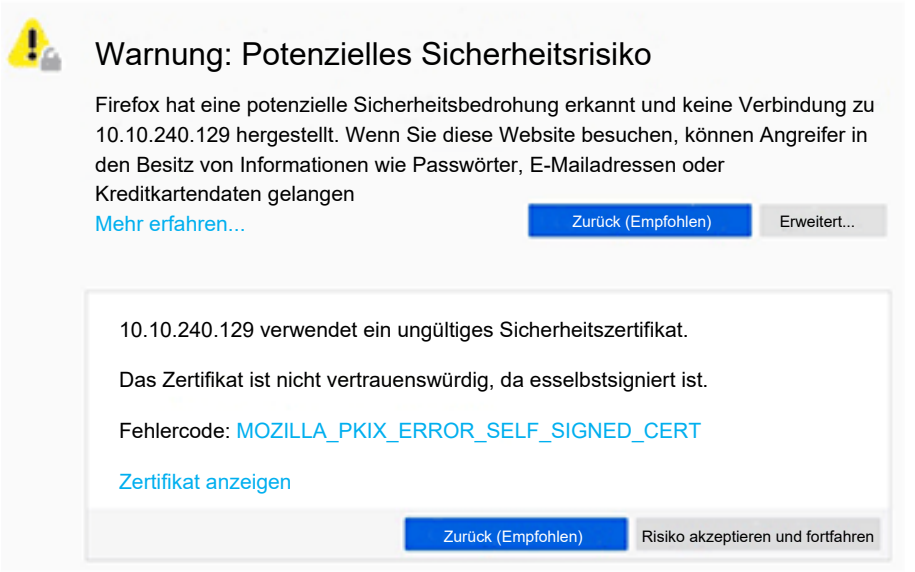
- Es wurde nie konfiguriert und behält seine ursprüngliche werkseitige Standardkonfiguration bei.
- Es wurde zuvor konfiguriert, aber die werksseitige Standardkonfiguration wurde wiederhergestellt, indem der Befehl zum Zurücksetzen der Cybersicherheit (oder Sicherheit), Seite 33 ausgeführt wurde.

Sobald ein Modul mit Cybersicherheitseinstellungen konfiguriert wurde und im erweiterten (oder sicheren) Modus betrieben wird, können Sie die Cybersicherheitseinstellungen auch über die Webseiten ändern.

Anweisungen zur Anwendung einer Anfangskonfiguration auf das Modul finden Sie im Abschnitt Inbetriebnahme, Seite 85.

Erste Anmeldung bei den Webseiten

Wenn Sie sich bei einem nicht konfigurierten BMENUA0100-Modul anmelden, wird das folgende Fenster (oder ein ähnliches Fenster, je nach verwendetem Browser) angezeigt:



Trotz der in der Meldung verwendeten Begriffe ist die Verbindung über HTTPS gesichert. Lesen Sie sich die Meldung durch und fahren Sie mit der Erstanmeldung fort, wenn Sie

damit einverstanden sind, indem Sie auf **[Risiko akzeptieren und fortfahren]** (oder eine ähnliche browserspezifische Meldung) klicken.

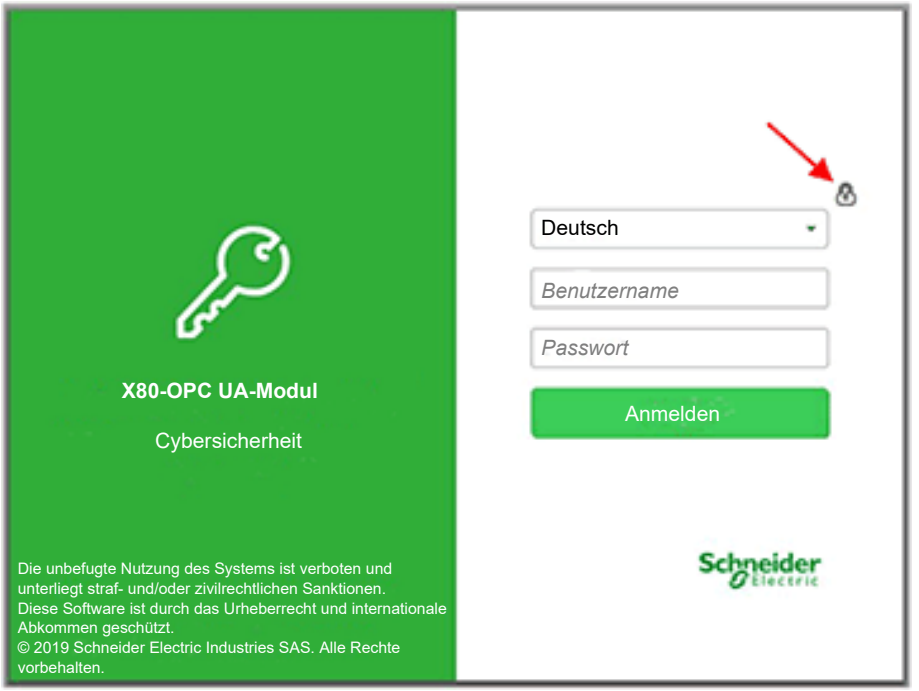
HINWEIS: Die obige Meldung wird angezeigt, da das Modul noch nicht über eine gültige Konfiguration verfügt und ein selbstsigniertes Zertifikat verwendet.

Anmelden bei den Webseiten

Bei der ersten Anmeldung gibt der Sicherheitsadministrator die Standardkombination aus Benutzername und Passwort, Seite 33 ein. Unmittelbar danach muss der Administrator das Standardpasswort ändern.

Sie müssen sich jedes Mal anmelden, wenn Sie die Webseiten für das BMENUA0100-Modul öffnen. Nur Personen, denen ein gültiges Benutzerkonto zugewiesen wurde – mit einer gültigen Kombination aus Benutzername und Passwort, die von einem Sicherheitsadministrator auf der Webseite, Seite 122 **Zugriffskontrolle > Benutzerverwaltung** erstellt wurde – können auf die Webseiten des Moduls zugreifen.

Wählen Sie auf der Anmeldeseite eine Sprache in der Dropdown-Liste aus und geben Sie dann **Benutzername** und **Passwort** ein.

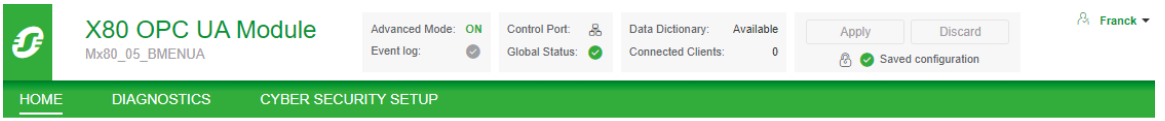


HINWEIS: Der Cybersicherheitsbetriebsmodus des Moduls wird durch das Schlosssymbol oben rechts im Dialogfeld angezeigt (durch den roten Pfeil oben gekennzeichnet). Das Schloss befindet sich in folgendem Zustand:

- Geschlossen (wie oben gezeigt): Das Modul wird im erweiterten (oder sicheren) Modus, Seite 32 ausgeführt.
- Geöffnet: Das Modul wird im Standardmodus, Seite 32 ausgeführt.

Webseiten-Banner

Jede Webseite verfügt über ein Banner oben auf der Seite:



Das Banner enthält die folgenden Informationen zum BMENUA0100-Modul:

- Erweiterter (oder sicherer) Modus:
  - EIN: Das Modul wird im erweiterten (oder sicheren) Modus, Seite 32 ausgeführt.
  - AUS: Das Modul wird im Standardmodus, Seite 32 ausgeführt.
- Ereignisprotokoll:
  - Der Ereignisprotokollierungsdienst ist deaktiviert.
  - Der Ereignisprotokollierungsdienst ist aktiviert, der Protokollserver ist erreichbar.
  - Der Ereignisprotokollierungsdienst ist aktiviert, aber der Protokollserver ist nicht erreichbar.
  - Der Ereignisprotokollierungsdienst ist aktiviert, aber es wurde ein Fehler erkannt.
- Steuerungsport:
  - Der Steuerungsport ist aktiviert.
  - Der Steuerungsport ist deaktiviert.
- Globaler Status:
  - Alle Dienste sind betriebsbereit.
  - Mindestens ein Dienst ist nicht betriebsbereit.

- Datenwörterbuch:
  - Verfügbar: Die Datenwörterbuch-Funktion ist verfügbar.
  - Nicht verfügbar: Die Datenwörterbuch-Funktion ist nicht verfügbar oder nicht aktiviert.
- Verbundene Clients: Die Anzahl der verbundenen OPC UA-Clients.
- Konfiguration übernehmen/verwerfen: Gibt den Status der Konfiguration der Cybersicherheits-Webseite des Moduls an:
  - Unveränderte Konfiguration: Die Cybersicherheitskonfiguration enthält keine ausstehenden oder ungültigen Änderungen. Die Schaltflächen **Übernehmen** und **Verwerfen** sind deaktiviert.
  - Ausstehende Konfiguration: Eine oder mehrere Änderungen an der Cybersicherheitskonfiguration wurden noch nicht angewendet. Beide Schaltflächen **Übernehmen** und **Verwerfen** sind aktiviert.
  - Unzulässige Konfiguration: Die Cybersicherheitskonfiguration ist unvollständig oder ungültig. Die Schaltfläche **Übernehmen** ist deaktiviert, die Schaltfläche **Verwerfen** ist aktiviert. In diesem Zustand wird auf der Webseite neben jedem betroffenen Menüpunkt ein roter Kreis angezeigt, der die Anzahl der ungültigen Konfigurationseinstellungen enthält, die über diesen Menüpfad erreicht werden können. Wenn Sie zu einer Seite mit einer ungültigen Konfigurationseinstellung navigieren, zeigt die Seite die ungültige Konfigurationseinstellung an.

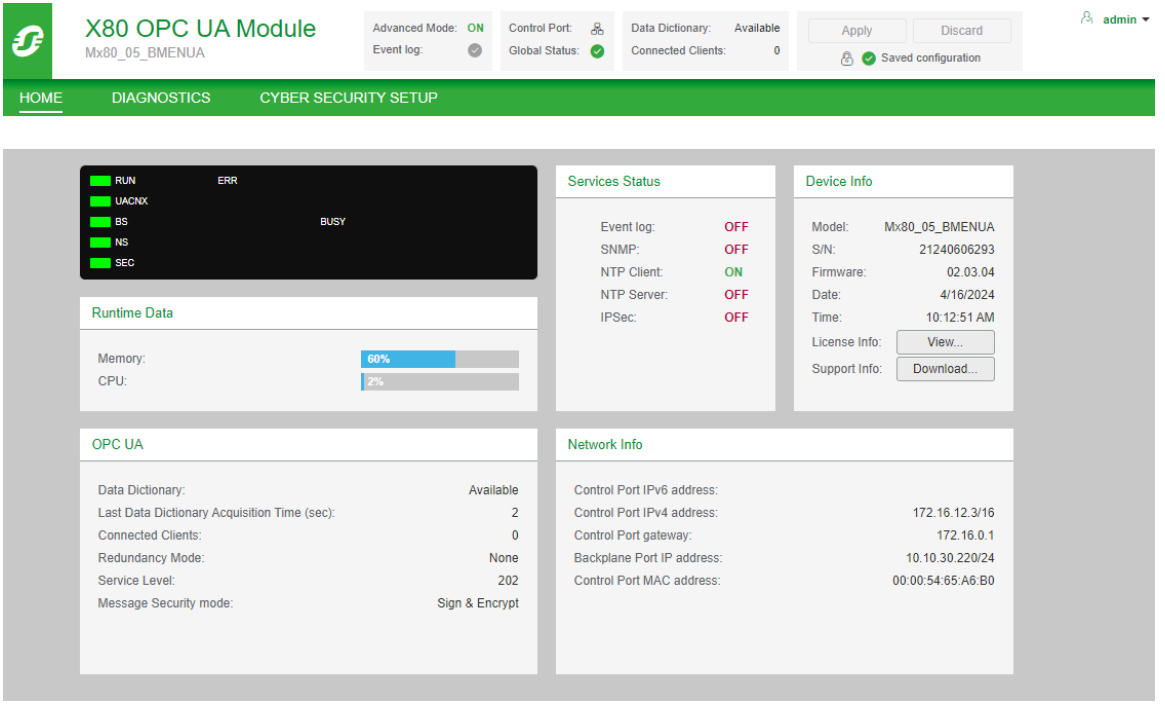
Webseiten-Hilfe

Viele Webseiten bieten kontextbezogene Hilfe auf Parameterebene. Um Hilfe für einen bestimmten Parameter oder ein bestimmtes Feld zu erhalten, platzieren Sie den Cursor auf das Symbol .

„Startseite“

Einführung in die Startseite

Wenn Sie sich bei den BMENUA0100-Webseiten anmelden, wird standardmäßig die **Startseite** geöffnet. Wenn das Modul über eine gültige Konfiguration verfügt, wird die folgende Seite angezeigt:



Verwenden Sie die Seite Home, um folgende Vorgänge durchzuführen:

- Zugriff auf die Navigationsstruktur, die Links zu den Webseiten des BMENUA0100-Moduls enthält. Wenn das Modul im folgenden Modus ausgeführt wird:
  - Erweiterter (oder sicherer) Modus, Seite 32 - Die Menüs DIAGNOSE und KONFIGURIEREN DER CYBERSICHERHEIT-EINSTELLUNGEN werden angezeigt und können vom Sicherheitsadministrator verwendet werden.
  - Standardmodus, Seite 32 - Nur das Menü DIAGNOSE ist zugänglich.
- Anzeigen des Status, Seite 144 der Modul-LEDs, Seite 26.
- Anzeigen von Datensammlungen für das Modul, einschließlich:
  - Laufzeitdaten, Seite 99
  - OPC UA, Seite 99
  - Dienststatus, Seite 99
  - Netzwerkinfo, Seite 100
  - Geräteinfo, Seite 100

  HINWEIS: Wenn der Drehwahlschalter auf der Rückseite des Moduls auf Zurücksetzen der Cybersicherheit (oder Sicherheit), Seite 33 steht, erfolgt keine Kommunikation mit dem Modul. Daher ist auch kein Zugriff auf die Webseiten - einschließlich der **Startseite** - möglich.

Laufzeitdaten

Der **OPC UA**-Bereich zeigt Folgendes an:

- **Speicher**: Der Prozentsatz des internen RAM, der vom OPC UA-Server (MEM_USED_PERCENT) verwendet wird.
- **CPU**: Der Prozentsatz der aktuell verwendeten CPU-Verarbeitungskapazität (CPU_USED_PERCENT).

  HINWEIS: Die oben beschriebenen Elemente basieren auf Elementen im T_BMENUA0100-DDT, Seite 149.

OPC UA

Der Bereich **Laufzeitdaten** zeigt Folgendes an:

- **Datenwörterbuch**: Der Verfügbarkeitsstatus des Datenwörterbuchs (DATA_DICT).
- **Erfassungszeit des letzten Datenwörterbuchs (Sek.)**: Die Dauer der letzten Erfassung des Datenwörterbuchs (DATA_DICT_ACQ_DURATION).
- **Verbundene Clients**: Die Anzahl der verbundenen OPC UA-Clients (CONNECTED_CLIENTS).
- **Redundanzmodus**: Der für ein Hot Standby-System (REDUNDANCY_MODE) unterstützte Failover-Modus.
- **Dienstebene**: Die Funktionsfähigkeit des OPC UA-Servers, basierend auf Daten und Dienstqualität (SERVICE_LEVEL).

  HINWEIS: Die oben beschriebenen fünf Elemente basieren auf Elementen im T_BMENUA0100-DDT, Seite 149.
- **Nachrichtensicherheitsmodus**: Die auf der OPC UA-Webseite, Seite 111 konfigurierte Einstellung: Keine, Signieren oder Signieren und Verschlüsseln.

Dienststatus

Der Bereich **Dienststatus** zeigt den Status - Aktiviert (EIN) oder Deaktiviert (AUS) - der folgenden Dienste an, wie im T_BMENUA0100-DDT, Seite 149 ausgewiesen:

- **Ereignisprotokoll** (EVENT_LOG_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **NTP-Client** (NTP_CLIENT_SERVICE)
- **NTP-Server** (NTP_SERVER_SERVICE)
- **IPSec** (IPSEC)

Für Module vor Version BMENUA0100.2.

- **Control Expert-Datenflüsse** (CONTROIL_EXPERT_IP_FORWARDING)
- **CPU-zu-CPU-Datenfluss** (CPU_TO_CPU_IP_FORWARDING)

Netzwerkinfo

In diesem Bereich werden die Konfigurationseinstellungen für das BMENUA0100-Modul angezeigt, die in Control Expert, Seite 126 eingegeben und im T_BMENUA0100-DDT, Seite 149 ausgewiesen werden. Dazu gehören:

- Steuerungsport (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4 und CONTROL_PORT_GTW)
- Baugruppenträger-Port (ETH_BKP_PORT_IPV4)
- MAC-Adresse des Moduls, ein eindeutiger Hexadezimalwert, der jedem Modul werkseitig zugewiesen wird.

Geräteinfo

In diesem Bereich werden die Referenz, die Seriennummer und die Firmwareversion (FW_VERSION im T_BMENUA0100-DDT, Seite 149), Datum und Uhrzeit für das BMENUA0100-Modul angezeigt.

Klicken Sie auf **Ansicht...**, um Lizenzinformationen anzuzeigen.

Klicken Sie auf **Herunterladen...** zur Anzeige des Dialogfelds **Supportinformationen herunterladen**. Siehe den Abschnitt Zugriffskontrolle, Seite 122 für weitere Informationen.

Einstellungen

Einstellungen

Wählen Sie auf den Webseiten des BMENUA0100-Moduls, beginnend mit der **Startseite**, die Option **Einstellungen** aus, um Links zu den folgenden Konfigurationsseiten anzuzeigen, auf denen Sie Einstellungen für die Gerätesicherheit eingeben können:

- Benutzerkontenrichtlinie, Seite 101
- Ereignisprotokolle, Seite 102
- Netzwerkdienste, Seite 102
- Dienstweiterleitung, Seite 105
- IPsec, Seite 109
- SNMP, Seite 111

- OPC UA, Seite 111
- Sicherheitsbanner, Seite 113

Nachfolgend sind die konfigurierbaren Parameter für jeden Netzknoten beschrieben.

Verwenden Sie diese Einstellungen, um die Gerätesicherheit für das BMENUA0100-Modul zu konfigurieren. Nach der Änderung der Einstellungen wählen Sie **Senden** oder **Abbrechen** aus.

Benutzerkontenrichtlinie

Verwenden Sie diese Einstellungen, um die Benutzerkontorichtlinie zu konfigurieren:

Parameter	Beschreibung
Maximale Inaktivität der Sitzung (Minuten)	Die Timeout-Dauer für Leerlaufsitzungen bei HTTPS-Verbindungen. Wenn während dieser Zeit keine Verbindung aufgebaut wird, wird die Benutzersitzung automatisch beendet. Standardwert = 15 Minuten. **HINWEIS:** Für OPC UA-Verbindungen besteht kein Inaktivitäts-Timeout.
Maximale Anzahl an Anmeldeversuchen	Die Anzahl der zulässigen erfolglosen Anmeldeversuche. Standard = 5 Versuche. Wenn der konfigurierte Höchstwert erreicht ist, wird das Benutzerkonto gesperrt.
Anmeldeversuch-Timer (Minuten)	Die maximale Dauer der Anmeldung. Standardwert = 3 Minuten.
Kontosperrdauer (Minuten)	Zeitraum, in dem keine weiteren Anmeldungen versucht werden dürfen, nachdem die maximale Anzahl an Anmeldeversuchen erreicht wurde. Nach Ablauf dieses Zeitraums wird die Sperre eines Benutzerkontos automatisch aufgehoben. Standardwert = 4 Minuten.

HINWEIS: Diese Benutzerkonto-Richtlinieneinstellungen gelten für OPC UA-Clients, Seite 179, denen ein Benutzername zugewiesen wurde.

Ereignisprotokolle

Verwenden Sie diese Einstellungen, um den Syslog-Client zu konfigurieren, der sich im BMENUA0100-Modul befindet. Die Protokolle werden lokal im Modul gespeichert und mit einem dezentralen Syslog-Server, Seite 165 ausgetauscht:

Parameter	Beschreibung
Dienstaktivierung	Schaltet den Syslog-Clientdienst ein und aus. Standard = AUS.
IP-Adresse des Syslog-Servers	IPv4- oder IPv6-Adresse des dezentralen Syslog-Servers. **HINWEIS:** IPv6 ist für Firmwareversionen ab 1.10 des BMENUA0100-Moduls verfügbar.
Syslog-Serverport	Die vom Syslog-Clientdienst verwendete Portnummer. Standardwert = 601.

Aktivierung der Netzwerkdienste

Diese Dienste bilden eine Firewall, die die Weiterleitung von Kommunikationssignalen über das BMENUA0100-Modul erlaubt oder verweigert. Verwenden Sie diese Einstellungen, um die folgenden Dienste zu aktivieren oder zu deaktivieren:

GLOBALE RICHTLINIEN:

Dienst	Beschreibung
Sicherheit verstärken	Deaktiviert die Netzwerkdienste außer IPsec.
Sicherheit freigeben	Aktiviert die Netzwerkdienste außer IPsec.

AKTIVIERUNG DER NETZWERKDIENSTE: Die Standardeinstellung für die folgenden Dienste ist vom Cybersicherheitmodus (CS Op Mode) wie folgt abhängig:

Dienst	Beschreibung	CS Op Mode - Standard	
		Norm/ Standard	Erweitert (oder Sicher)
SNMP-Agent	Ermöglicht die Aktivierung und Deaktivierung der Kommunikation mit dem SNMP-Agent.	Aktiviert	Deaktiviert
NTP-Server	Ermöglicht die Aktivierung und Deaktivierung der NTP-Serverkommunikation.	Aktiviert	Deaktiviert
IPsec	Aktiviert und deaktiviert die IPsec-Kommunikation.	Deaktiviert	Aktiviert[1]

Dienst	Beschreibung	CS Op Mode - Standard	
		Norm/ Standard	Erweitert (oder Sicher)
Datenflüsse von Steuerung zu Steuerung[2, 3]	Ermöglicht die Aktivierung bzw. Deaktivierung der Modbus-Kommunikation über das BMENUA0100-Modul zwischen M580-Steuerungen. Siehe *Konfiguration der Kommunikation für Datenflüsse von Steuerung zu Steuerung*, Seite 105.	Aktiviert	Deaktiviert
Nur Datenflüsse von Control Expert zur Steuerung[2, 3]	Ermöglicht die Aktivierung bzw. Deaktivierung der Modbus-, EtherNet/IP-, Ping-, expliziten Nachrichtenaustausch- und FTP-Kommunikation über das BMENUA0100-Modul zwischen der Control Expert-Konfigurationssoftware und der Steuerung. Siehe *Konfiguration der Kommunikation für Control Expert-Datenflüsse*, Seite 104.	Aktiviert	Deaktiviert
Datenflüsse von Control Expert zum Gerätenetzwerk[2, 3]	Ermöglicht die Aktivierung bzw. Deaktivierung der Modbus-, EtherNet/IP-, Ping-, expliziten Nachrichtenaustausch- und FTP-Kommunikation über das BMENUA0100-Modul zwischen der Control Expert-Konfigurationssoftware und den Netzwerkgeräten, einschließlich der Steuerung. Siehe *Konfiguration der Kommunikation für Control Expert-Datenflüsse*, Seite 104.	Aktiviert	Deaktiviert
HTTPS am Steuerungsport	Ermöglicht die Aktivierung und Deaktivierung der HTTPS-Kommunikation über den Steuerungsport. **HINWEIS:** Wenn HTTPS deaktiviert ist und die Änderung angewendet wird, kann über den Steuerungsport nicht auf die Webseiten zugegriffen werden. Um vom Steuerungsport wieder auf die Webseiten zugreifen zu können, können Sie die Cybersicherheitskonfiguration zurücksetzen.	Deaktiviert	Aktiviert

1. IPsec ist aktiviert, ohne dass Regeln definiert sind. Der Dienst muss konfiguriert werden.

2. Informationen zu diesem Konfigurationsentwurf finden Sie im Abschnitt zur Fehlerbehebung Aktivierung von Netzwerkdiensten nur über eine IPv6-Verbindung, Seite 180.

3. Wird nur von Modulen unterstützt, die älter sind als die Version BMENUA0100.2, wie in EcoStruxure Control Expert angegeben.

HINWEIS: SNMP-, NTP-, Syslog- und Modbus-Dienste sind nicht von Natur aus sichere Protokolle. Sie werden gesichert, wenn sie in IPsec gekapselt werden. Deaktivieren Sie IPsec nicht, wenn einer der SNMP-, NTP-, Modbus- oder Syslog-Dienste aktiviert ist.

Konfiguration der Kommunikation für dezentrale, auf PCs ausgeführte Software (ohne NAT-Weiterleitung)

Die Software adressiert das Zielgerät (z. B. die M580-Steuerung) über die IP-Adresse des Zielgeräts. Um diese Kommunikation zu unterstützen, richten Sie zwei Standard-Gateways wie folgt ein:

- Richten Sie auf dem Host-PC, auf dem die Software ausgeführt wird, mithilfe von IPv4 ein PC-Standard-Gateway zur IP-Adresse des Steuerungsports des BMENUA0100-Moduls ein.
- Richten Sie auf dem Zielgerät (z. B. der M580-Steuerung) mithilfe von IPv4 ein Geräte-Standard-Gateway zur IP-Adresse des Steuerungsports des BMENUA0100-Moduls ein.
- Fügen Sie auf dem Host-PC einen Pfad mit folgendem Befehl hinzu:

  ```
  route ADD <<destination=subnet of the target device>> MASK <<subnet mask of the target device>> <<gateway=BMENUA0100 module backplane port IP address>>
  ```

Für IPv4 in allen Firmwareversionen und für IPv6 in Firmwareversionen ab 1.10 richtet sich die Modbus-Kommunikation vom Control Expert Connect-Fenster an die IP-Adresse des BMENUA0100-Steuerungsports. Gateways sind für diese Kommunikation nicht erforderlich.

Konfiguration der Kommunikation für Datenflüsse von Steuerung zu Steuerung

Für die Modbus-TCP/IP-Kommunikation von Steuerung zu Steuerung über das BMENUA0100-Modul kann die IPv4- oder die IPv6-Steuerungsport-Adresse des BMENUA0100-Moduls verwendet werden, nicht die Adresse der Zielsteuerung.

HINWEIS:

- Für den BMENUA0100 ist die Weiterleitung von Steuerung zu Steuerung auf das Modbus TCP/IP-Protokoll beschränkt.
- Das Modbus-Protokoll ist das einzige Protokoll, das die Kommunikation zwischen Geräten unterstützt.
- Die IPv4-Adressierung unterstützt Modbus TCP/IP-Datenflüsse von Steuerung zu Steuerung sowohl im erweiterten/sicheren Modus als auch im Standardmodus.
- Die IPv6-Adressierung unterstützt Modbus TCP/IP-Datenflüsse von Steuerung zu Steuerung für den BMENUA0100 im erweiterten/sicheren Modus wie folgt:
  - Für Firmwareversionen ab 2.04, wenn eine Weiterleitungsregel auf der Webseite der Dienstweiterleitung (IP-Weiterleitung), Seite 105 definiert wurde oder wenn **Alle weiterleiten** auf **EIN** eingestellt ist.
  - Für Firmwareversionen 2.0x vor 2.04, wenn eine Weiterleitungsregel definiert wurde.

  Weitere Informationen finden Sie im Abschnitt Von erweiterten (oder sicheren) und Standardbetriebsarten unterstützte Funktionen, Seite 34.

Dienstweiterleitung (IP-Weiterleitung)

Ein BMENUA0100-Modul mit einer Firmwareversion ab 2.01 enthält diese Webseite. Verwenden Sie diese Option, um die Weiterleitung von Unicast-Datenflüssen zu konfigurieren, die das Modul zwischen dem Steuerungsnetzwerk und dem Gerätenetzwerk durchlaufen. Auf dieser Webseite können Sie eine Liste der IP-Weiterleitungsregeln für das Modul erstellen, bearbeiten oder entfernen.

HINWEIS: Die Funktion der Dienstweiterleitung (IP-Weiterleitung) bietet keine Unterstützung für die folgenden Funktionen:

- Multicast-Datenflüsse.
- Impliziter EtherNet/IP-Nachrichtenaustausch.

Folglich werden die folgenden Aufgaben von diesem Dienst nicht unterstützt:

- Geräteerkennung durch das Tool EcoStruxure Automation Device Maintenance (EADM), das im automatischen Erkennungsmodus arbeitet. Die EADM-Geräteerkennung im manuellen Erkennungsmodus wird unterstützt (Multicast).
- Nachrichtenweiterleitung an die lokalen EtherNet/IP-Kommunikationsmodule der Steuerung (impliziter EtherNet/IP-Nachrichtenaustausch).

Merkmale:

Die Hauptmerkmale der Funktion „Dienst-/IP-Weiterleitung“ sind:

- Möglichkeit, alle Datenflüsse weiterzuleiten („Alle weiterleiten“).
- IP-Weiterleitung der gängigsten Protokolle, die in der Architektur verwendet werden, über vordefinierte Vorlagen (z. B.: Modbus, HTTPS, SNMP usw.).
- Erstellung und Anwendung von benutzerdefinierten IP-Weiterleitungsvorlagen.
- NAT-Weiterleitung (Network Address Translation) einiger Protokolle an die lokale Steuerung, wenn die @dezentrale IP-Adresse dem BMENUA0100-IPv4-Steuerungsport entspricht.

  HINWEIS: Die NAT-Weiterleitung gilt für die folgenden Protokolle: Modbus, Modbus über TLS, EtherNet/IP explizit, EIP explizit über TLS, EIP implizit, OPC UA-Client.
- Die Option, IPsec für über NAT weitergeleitete Protokolle zu verwenden bzw. nicht zu verwenden. Beachten Sie die Richtlinien in den Hinweisen am Ende des IPsec-Abschnitts unten, Seite 109.

HINWEIS:

- Wenn sich mehrere BMENUA0100-Module im gleichen Rack befinden, konfigurieren Sie nur ein BMENUA0100-Modul mit der Weiterleitungsfunktion.
- Multicast-Datenflüsse werden nicht weitergeleitet.
- Eine Online-Aktualisierung der Regeln für die IP-Weiterleitung kann dazu führen, dass einige laufende Kommunikationen gestoppt werden.
- Damit die Dienstweiterleitung (IP-Weiterleitung) erfolgreich ist, muss sich das Ziel-IP-Netzwerk vom Quell-IP-Netzwerk unterscheiden. So ist es beispielsweise nicht möglich, eine IP-Weiterleitung zwischen folgenden Komponenten auszuführen:
  - Quell-IP-Netzwerk 192.168.x.x (Maske 255.255.0.0) und
  - Ziel-IP-Netzwerk 192.168.x.x (Maske 255.255.0.0).
- Der Wert für den OPC UA-Listening-Port muss für alle BMENUA0100-Kommunikationsmodule identisch sein (z. B. bei der OPC UA-NAT-Weiterleitung zwischen mehreren BMENUA0100-Modulen).
- Durch die Aktivierung des FTP-Protokolls wird ein Bereich von TCP-Ports zwischen 1024 und 65535 geöffnet. Das bedeutet, dass auch andere Protokolle mit TCP-Ports in diesem Bereich weitergeleitet werden können. Aktivieren Sie die Weiterleitung des FTP-Protokolls nur vorübergehend und wenn erforderlich.
  - Die Aktivierung des TFTP-Protokolls als benutzerdefinierte Regel führt zu demselben Ergebnis wie die Aktivierung des FTP-Protokolls. Aktivieren Sie die Weiterleitung des TFTP-Protokolls nur vorübergehend und wenn erforderlich.

Weitere Informationen zur Architektur der Dienstweiterleitung (IP) finden Sie in den folgenden Abschnitten:

- Unterstützte Architekturen für die Dienstweiterleitung (IP), Seite 186
- Nicht unterstützte Architekturen für die Dienstweiterleitung (IP), Seite 189

IP-Weiterleitung und OPC UA-Kommunikation

Sowohl die IP-Weiterleitung als auch OPC UA beanspruchen die verfügbare Kommunikationsbandbreite des BMENUA0100-Moduls. Eine Beschreibung der Auswirkungen der IP-Weiterleitung, der OPC UA-Kommunikation, der Vertraulichkeitseinstellungen und der benutzerdefinierten Bandbreitenregeln finden Sie im Kapitel IP-Weiterleitung und OPC UA-Kommunikation, Seite 190.

Erstellen von Regeln:

- Um sowohl vordefinierte als auch benutzerdefinierte Regeln zu dokumentieren, klicken Sie auf **Neue Weiterleitung** und vervollständigen Sie die Einstellungen, die diese Regel definieren.

  HINWEIS: Wenn Sie einen Dienstnamen auswählen, werden für Portnummer und Protokoll automatisch die Standardeinstellungen zugewiesen. Diese können nach Bedarf bearbeitet werden.

- Um eine bereits vorhandene Regel zu bearbeiten, klicken Sie auf das Stiftsymbol und bearbeiten Sie die zugehörigen Einstellungen.
- Um eine bereits vorhandene Regel zu entfernen, klicken Sie auf das Papierkorb-Container-Symbol.

Setzen Sie **Alle weiterleiten** auf **AUS**, um die aufgeführten Regeln anzuwenden. Wenn Sie **Alle weiterleiten** auf **EIN** setzen:

- Die Regeln werden aufgehoben und das Modul leitet alle Protokolle weiter.
- Sie können die Weiterleitung nicht für individuelle Dienste konfigurieren.
- Alle Dienste werden über IPsec weitergeleitet, wenn IPsec aktiviert ist.

Jede Regel wird in den folgenden Feldern definiert:

Einstellung	Beschreibung
Dienstname	Folgende Dienste sind vordefiniert: • Modbus • FTP • EIP Explizit • ICMP • NTP / SNTP • SNMP • SNMP-Trap • HTTPS • Modbus über TLS • EIP Explizit über TLS • LDAP für TLS-Start • Syslog • HTTP • DPWS-Metadaten • OPC UA (für OPC UA-Client) • DNP3 • DNP3 über TLS • IEC 60870 • IEC 60870 über TLS • EIP Implizit **HINWEIS:** Für OPC UA entspricht die Portnummer dem OPC UA-Port, der in Control Expert für das BMENUA0100-Modul festgelegt wurde.
Portnummer[1]	Der dem Dienst zugeordnete Port.
Protokoll[1]	Das dem Dienst zugeordnete Protokoll.

Einstellung	Beschreibung
IPsec-Verwendung	• **TRUE**: Das Protokoll wird über IPsec übertragen. • **FALSE**: Das Protokoll wird nicht über IPsec übertragen, selbst wenn IPsec in der Konfiguration aktiviert ist. Diese Auswahl ist nur verfügbar, wenn IPsec aktiviert ist. **HINWEIS:** • **Verwenden Sie IPsec nicht** für nativ sichere Protokolle (z.B. Modbus über TLS, EIP Explizit über TLS, DNP3 über TLS, EIP 60870 über TLS). • **Verwenden Sie IPsec** für nativ nicht sichere Protokolle (z. B. Modbus, EIP Explizit, OPC UA-Client, EIP IO).
Eingehende Schnittstelle	• **Steuerungsport**: Wenn der dezentrale Client-Request am Steuerungsport empfangen wird (Beispiel: Modbus TCP/IP-Request von Control Expert). • **Baugruppenträger-Port**: Wenn der dezentrale Client-Request am Baugruppenträger-Port empfangen wird (z. B. Modbus TCP-Request von einem Funktionsbaustein der Steuerung). • **Beide**: Wenn der dezentrale Client-Request sowohl am Steuerungs- als auch am Baugruppenträger-Port empfangen werden kann (Beispiel: Modbus-TCP/IP-Request von Control Expert und Modbus-TCP-Request von einem Funktionsbaustein der Steuerung).
1. Automatisch angegeben, kann jedoch bearbeitet werden, um einen vordefinierten Dienstnamen zu verwenden.	

IPsec

Verwenden Sie IPsec, um die IPv4-Ethernet-Kommunikation zu sichern.

HINWEIS: IPsec unterstützt keine IPv6-Adressierung.

Verwenden Sie diese Einstellungen, um maximal 8 IKE/IPsec-Kanäle über IPv4 für das BMENUA0100-Modul zu konfigurieren. Wenn mehr als 4 IPsec-Verbindungen konfiguriert sind, ist die automatische Verbindung zur Steuerung nach der Übertragung über das BMENUA0100-Modul möglicherweise nicht erfolgreich. Stellen Sie in diesem Fall manuell eine Verbindung zur Steuerung her.

Parameter	Beschreibung
IPsec-DIENST	• EIN: Aktiviert den IPsec-Dienst. **HINWEIS:** Voraussetzung für die Aktivierung des IPsec-Dienstes ist auch die Aktivierung des Steuerungsports in den IP-Konfig.-Einstellungen, Seite 128. • AUS: Deaktiviert den IPsec-Dienst.
NTP außerhalb von IPsec autorisiert	• Nicht ausgewählt (Deaktiviert): NTP wird nur über IPsec ausgetauscht. • Ausgewählt (Aktiviert): NTP wird über IPsec ausgetauscht, wenn der IPsec-Kanal geöffnet ist, und außerhalb von IPsec, wenn der IPsec-Kanal nicht geöffnet ist.

Parameter	Beschreibung
Neuer Link	Erstellt einen neuen IKE/IPsec-Kanal und fügt ihn in der Liste zur Bearbeitung hinzu. **HINWEIS:** Es werden maximal 8 IKE/IPsec-Kanäle unterstützt.
Konfigurieren Sie für jeden IKE/IPsec-Kanal die folgenden Einstellungen:	
Dezentrale IP-Adresse	IPv4-Adresse des dezentralen IPsec-Endpunkts. **HINWEIS:** Das dezentrale Gerät muss über den BMENUA0100-Steuerungsport zugänglich sein (und nicht über den BMENUA0100-Baugruppenträger-Port).
Vertraulichkeit	• Ausgewählt: Die Kommunikation wird verschlüsselt. • Nicht ausgewählt: Keine Verschlüsselung. **HINWEIS:** Vertraulichkeit ist deaktiviert, wenn *NTP ohne IPsec* aktiviert ist.
Clienttyp	Typ des dezentralen IPsec-Endpunkts: Windows oder Gerät. **HINWEIS:** Die Standardeinstellung ist Windows. Stellen Sie sicher, dass der konfigurierte Endpunkttyp mit dem Client übereinstimmt.
PSK	Vorinstallierter Schlüssel (Pre-Shared Key) mit einer Länge von 32 Hexadezimalzeichen - das Ergebnis einer vom BMENUA0100-Modul generierten Zufallszahl. Er kann auf dieser Webseite kopiert und bearbeitet werden. **HINWEIS:** PSK ist deaktiviert, wenn *NTP ohne IPsec* aktiviert ist.

HINWEIS: Konfigurieren Sie die Windows-Firewalleinstellungen, Seite 193, indem Sie das „Windows-Skript“ von BMENUA0100 herunterladen. Verwenden Sie dazu den Befehl **Skript herunterladen** für jede dezentrale IP-Adresse. Wenn **IPsec-Verwendung** für einige Protokolle geändert wurde, muss das Windows-Skript erneut aus dem BMENUA0100-Modul heruntergeladen und unter Windows ausgeführt werden. Ein Beispiel für ein Windows-Skript finden Sie im Abschnitt IPsec-Windows-Skripte, Seite 193.

HINWEIS: Wenn 8 IPsec-Tunnel konfiguriert sind, ist es unter Umständen nicht möglich, nach dem Download einer Anwendung die Verbindung zur Steuerung automatisch wiederherzustellen. Stellen Sie in diesem Fall nach dem Download manuell eine Verbindung zur Steuerung her.

HINWEIS: Wenn der IPsec-Dienst aktiviert ist (d. h. auf EIN gesetzt ist):

- Der lokale HTTPS-Server-Datenfluss verläuft außerhalb von IPsec.
- Der lokale OPC UA-Datenfluss wird standardmäßig in IPsec übertragen. Um den lokalen OPC UA-Datenfluss außerhalb von IPsec zu übertragen, muss eine OPC UA-Weiterleitungsregel mit „IPsec-Verwendung = FALSE“ festgelegt werden, auch wenn kein OPC UA-Datenfluss weitergeleitet werden muss.

SNMP

Verwenden Sie diese Einstellungen, um die SNMP-Version und die zugehörigen Einstellungen zu konfigurieren.

HINWEIS: Im erweiterten (oder sicheren) Modus muss die SNMP-Version in Control Expert, Seite 141 und auf der SNMP-Webseite identisch konfiguriert werden. Wenn diese Einstellungen nicht übereinstimmen, wird der SNMP-Dienst nicht gestartet.

Parameter	Beschreibung
SNMP-Version	• v1 • v3
Sicherheitsstufe	Für SNMP v1 und v3: • Keine Authentifizierung und kein Datenschutz: Kommunikation ohne Authentifizierung oder Datenschutz. **HINWEIS:** Für SNMP v1 ist dies die einzige verfügbare Einstellung. Nur für SNMP v3: • Authentifizierung und kein Datenschutz: Kommunikation mit Authentifizierung, aber ohne Datenschutz. Das Authentifizierungsprotokoll lautet SHA (Secure Hash Algorithm). • Authentifizierung und Datenschutz: Kommunikation mit Authentifizierung und Datenschutz. Folgende Protokolle werden verwendet: ◦ Authentifizierung: SHA ◦ Datenschutz: AES (Advanced Encryption Standard).
Authentifizierungspasswort	Wenn die Authentifizierung aktiviert ist, geben Sie ein Authentifizierungspasswort ein, bei dem die Groß-/Kleinschreibung beachtet werden muss. Es muss 8 bis 12 Zeichen umfassen und kann alphanumerische Zeichen (Großbuchstaben, Kleinbuchstaben und Ziffern) enthalten, wie im Tooltipp der Webseite angegeben.
Datenschutzpasswort	Wenn der Datenschutz aktiviert ist, geben Sie ein Passwort ein, bei dem die Groß-/Kleinschreibung beachtet werden muss. Es muss 8 Zeichen umfassen und kann alphanumerische Zeichen (Großbuchstaben, Kleinbuchstaben und Ziffern) enthalten, wie im Tooltipp der Webseite angegeben.

OPC UA

Verwenden Sie diese Einstellungen, um die Verbindung für den in das BMENUA0100-Modul integrierten OPC UA-Server zu konfigurieren:

Parameter	Beschreibung
Nachrichtensicherheitsmodus	• Signieren und Verschlüsseln (Standard): Jede Nachricht wird mit einer Signatur versehen und verschlüsselt. • Vorzeichen: Jede Nachricht wird mit einer Signatur versehen. • Keine: Es wird keine Sicherheitsrichtlinie angewendet. In diesem Fall sind die beiden folgenden Felder nicht verfügbar. **HINWEIS:** Wenn **Keine** ausgewählt ist, wird **Benutzer-ID-Tokentypen** im BMENUA0100-Modul als **Anonym** definiert. In diesem Fall müssen Sie auch die Benutzer-ID-Tokentypen im OPC UA-Client mit **Anonym** konfigurieren.
Sicherheitsrichtlinien	• Basic256Sha256 (Standard): Definiert eine Sicherheitsrichtlinie für Konfigurationen mit gültiger Verschlüsselungssuite. • Basic256: Definiert eine Sicherheitsrichtlinie für Konfigurationen mit veralteter Verschlüsselungssuite. **HINWEIS:** Diese Auswahl wird nur dann verwendet, wenn sie für die Interoperabilität mit einem dezentralen Client erforderlich ist. • Basic128Rsa15: Definiert eine Sicherheitsrichtlinie für Konfigurationen mit veralteter Verschlüsselungssuite. **HINWEIS:** Diese Auswahl wird nur dann verwendet, wenn sie für die Interoperabilität mit einem dezentralen Client erforderlich ist.
Benutzer-ID-Tokentypen	• Anonym: Es sind keine Benutzerinformationen verfügbar. • Benutzername (Standard): Der Benutzer wird anhand des Benutzernamens und des Passworts identifiziert.

HINWEIS: Änderungen an den OPC UA-Servereinstellungen zur Cybersicherheit führen dazu, dass der Server neu startet und die neuen Einstellungen übernommen werden. Wenn folglich eine oder mehrere OPC UA-Sitzungen vorhanden sind, während Konfigurationsänderungen vorgenommen werden, werden diese Sitzungen ausgesetzt. Sobald die *SessionTimeout*-Periode (Sitzungs-Timeout) abgelaufen ist, werden diese Sitzungen geschlossen. Das *SessionTimeout* ist Bestandteil der OPC UA-SCADA-Clientkonfiguration.

HINWEIS: Wenn die Einstellung **Nachrichtensicherheitsmodus** des OPC UA-Servers zunächst mit **Signieren und Verschlüsseln** oder **Signieren** konfiguriert wird, ein OPC UA-Client eine Verbindung herstellt und Sie anschließend die OPC UA-Servereinstellung **Nachrichtensicherheitsmodus** auf **Keine** einstellen, kann ein OPC UA-Client (mit der Einstellung **Nachrichtensicherheitsmodus** ebenfalls auf **Keine** gesetzt) keine Verbindung zum Server herstellen.

So stellen Sie erneut eine Verbindung her:

1. Trennen Sie Ihre OPC UA-Clients.
2. Ändern Sie die OPC UA-Konfiguration auf der BMENUA0100-Webseite.
3. Warten Sie, während die **BUSY**-LED leuchtet (gelb), bis sie erlischt (nicht leuchtet).
4. Ändern Sie für die OPC UA-Clients deren Konfiguration (**Nachrichtensicherheitsmodus**) zu der Einstellung, die für den OPC UA-Server verwendet wird.
5. Verbinden Sie die OPC UA-Clients erneut mit dem Server.

Sicherheitsbanner

Diese Seite enthält bearbeitbaren Text, der angezeigt wird, wenn der Benutzer auf die Webseiten des BMENUA0100-Moduls zugreift:

Parameter	Beschreibung
Bannertext	Eine Zeichenfolge mit bis zu 128 Zeichen, die einem Benutzer auf der Anmeldeseite angezeigt wird. Standardmäßig wird der folgende bearbeitbare Text angezeigt: „Die unbefugte Nutzung der Anlage ist untersagt und unterliegt Strafen und/oder Strafgebühren.“

Zertifikatverwaltung

Zertifikatverwaltung mit und ohne PKI

Das BMENUA0100-Modul benötigt für die Authentifizierung Zertifikate. Um Cybersicherheit zu gewährleisten, muss jede Einheit (einschließlich der OPC UA-Clients und des in das BMENUA0100-Modul integrierten OPC UA-Servers) eine Vertrauensliste aller Zertifikate von Geräten/Anwendungen verwalten, die mit ihr kommunizieren.

Die Methode der Zertifikatverwaltung hängt vom Systemdesign ab, das ggf. eine Public-Key-Infrastruktur (PKI) mit einer Zertifizierungsstelle (Certification Authority, CA) anwendet (oder nicht).

Zertifikatverwaltung ohne PKI:

Verwenden Sie diese Methode, wenn das System keine Zertifizierungsstelle hat. Diese Verwaltungsmethode wird von BMENUA0100-Modulen mit einer Firmware ab V1.0 unterstützt. Gehen Sie zur Verwaltung von Zertifikaten auf den Webseiten **Zertifikatverwaltung** vor wie folgt:

- Setzen Sie **PKI-Modus** auf **Nur Selbstsignatur**.
- Verwalten Sie die **Zertifikatvertrauensliste** unter Verwendung der Funktionen **Hinzufügen** und **Löschen** zur Erstellung einer Liste für OPC UA-Clients, die zur Kommunikation mit dem BMENUA0100-Modul berechtigt sind.
- Exportieren Sie das BMENUA0100-Modulzertifikat für OPC UA-Clientgeräte unter Verwendung des Befehls **Herunterladen** auf der Seite **PKI Configuration > Gerätezertifikat**.

Zertifikatverwaltung mit PKI:

Verwenden Sie diese Zertifikatverwaltungsmethode, wenn Ihr System eine Zertifizierungsstelle enthält. Diese Verwaltungsmethode wird von BMENUA0100-Modulen mit einer Firmware ab V1.1 unterstützt. Gehen Sie zur Verwaltung von Zertifikaten auf den Webseiten **Zertifikatverwaltung** vor wie folgt:

- Stellen Sie den **PKI-Modus** auf einen der folgenden Werte ein:
  - **Nur CA**: Wenn alle installierten OPC UA-Clientgeräte PKI unterstützen.
  - **Selbstsigniert & Zertifizierungsstelle**: Wenn einige der installierten OPC UA-Clientgeräte PKI nicht unterstützen.
- Wenn der **PKI-Modus** auf **Nur CA** eingestellt ist:
  - Registrieren, Seite 119 Sie jedes BMENUA0100-Modul manuell bei der Zertifizierungsstelle.
- Wenn der **PKI-Modus** auf **Selbstsigniert & Zertifizierungsstelle** eingestellt ist:
  - Registrieren, Seite 119 Sie jedes BMENUA0100-Modul manuell bei der Zertifizierungsstelle.
  - Verwalten Sie die **Zertifikatvertrauensliste** unter Verwendung der Funktionen **Hinzufügen** und **Löschen** zur Erstellung einer Liste für OPC UA-Clients, die zur Kommunikation mit dem BMENUA0100-Modul berechtigt sind.

Aktualisieren der Zertifikatvertrauensliste

Nach der ersten Installation von BMENUA0100 mit einer Firmwareversion ab 2.0 (BMENUA0100.2) müssen Sie die vom Benutzer hinzugefügten Zertifikate aus der **Zertifikatvertrauensliste** auf der Webseite **Zertifikatverwaltung** entfernen. Dies können Sie folgendermaßen tun:

- Manuelles Entfernen dieser Zertifikate mithilfe des Befehls **Löschen** oder

- Setzen des Cybersicherheits-Drehwahlschalters in die Stellung **Zurücksetzen der Cybersicherheit**.

Nachdem die **Zertifikatsvertrauensliste** gelöscht wurde, können Sie sie mit selbstsignierten oder von der Zertifizierungsstelle ausgestellten Zertifikaten erneut auffüllen.

Diese Aufgabe muss nur bei der Erstinstallation einer Firmware ab Version 2.0 ausgeführt werden. Sie müssen das Verfahren bei nachfolgenden Installationen späterer Firmwareversionen nicht wiederholen.

HINWEIS: Wenn Sie die **Zertifikatvertrauensliste** nicht wie oben beschrieben löschen, können keine Verbindungen zu OPC UA-Clients hergestellt werden oder diese werden, wenn sie hergestellt wurden, verworfen.

Authentifizierung im Überblick

Ein OPC UA-Client oder ein BMENUA0100-Modul kann auf drei Arten authentifiziert werden:

- Für eine Firmwareversion ab 1.0:
  - (Nur) Selbstsigniertes Zertifikat
- Für eine Firmwareversion ab 1.10:
  - PKI-Zertifikat, nur von einer Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters ausgestellt
  - PKI-Zertifikat, ausgestellt von einer Zertifizierungsstelle, und selbstsigniertes Zertifikat

Um die erforderliche Cybersicherheit zu gewährleisten, muss jede Einheit (OPC UA-Client, BMENUA0100) eine Vertrauensliste aller Zertifikate von Geräten/Anwendungen verwalten, die mit ihr kommunizieren.

Für eine Firmwareversion ab 1.10 erstellt das BMENUA0100-Modul ein selbstsigniertes Zertifikat für:

- Konfiguration der Cybersicherheitseinstellungen über die Webseiten des Moduls
- Diagnose des Moduls über seine Webseiten
- Firmwareaktualisierung
- OPC UA-Anwendungsinstanzzertifikate, die es OPC UA-Clients ermöglichen, auf den integrierten OPC UA-Server im BMENUA0100-Modul zuzugreifen.

Für die Firmwareversion 1.0 erstellt das Modul zwei Zertifikate: ein HTTPS-Zertifikat und ein OPC UA-Zertifikat.

HINWEIS:

- Die Ablaufdaten der vertrauenswürdigen Zertifikate werden anhand der internen Datums- und Uhrzeiteinstellungen des BMENUA0100-Moduls festgelegt. Um Inkonsistenzen zu vermeiden, verwenden Sie den NTP-Dienst, um die Datums- und Uhrzeiteinstellungen des BMENUA0100-Moduls zu aktualisieren, und überprüfen Sie, ob der Zugriff auf den NTP-Server möglich ist und ob er über aktualisierte Einstellungen für Datum und Uhrzeit verfügt.
- Wenn Sie bei dem Versuch, den OPC UA-Client mit dem BMENUA0100-Server in IPv6 zu verbinden, einen *BadCertificateHostnameInvalid*-Fehler empfangen, kann dies durch eine komprimierte IPv6-Adresse (d. h. eine gekürzte IPv6-Adresse) verursacht werden. Überprüfen Sie in diesem Fall die verwendete IPv6-Adresse und ersetzen Sie sie ggf. durch ein unkomprimiertes Format.
- Das BMENUA0100-Modul verwaltet nicht automatisch das Ablaufdatum von Zertifikaten. Sie müssen das Ablaufdatum des Zertifikats manuell verwalten.

Verwalten der Zertifikate

Wählen Sie auf den Webseiten des BMENUA0100-Moduls, beginnend mit der **Startseite**, **Zertifikatverwaltung** aus, um Links zu den folgenden Seiten zur Zertifikatverwaltung für Anwendungsinstanzen anzuzeigen:

- PKI-Konfiguration, Seite 118
- Verwaltung der Client-Vertrauensliste, Seite 120
- Exportieren von Gerätezertifikaten, Seite 121
- Manuelle Registrierung, Seite 119
- CA-Zertifikate, Seite 121

In den Abschnitten *Verwenden von GPOs/LGPOs*, Seite 179 und *Anwenden der MMC-Gruppenrichtlinienverwaltung*, Seite 179 finden Sie Informationen zu den Windows™-Tools, die Sie zum Verwalten von Zertifikaten verwenden können.

Zertifikatserweiterungen

Um die Kommunikation mit dem BMENUA0100-Modul zu unterstützen, müssen selbstsignierte Zertifikate und Zertifikate von Zertifizierungsstellen spezifische Erweiterungen umfassen:

Selbstsignierte Zertifikate:

- KeyUsage (als kritisch markiert):
  - DigitalSignature
  - KeyEncipherment (Keine Verwendung für die TLS-Suite, die auf kurzlebigen Schlüsseln (ephemeral) wie TLS_ECDHE_xxxx basiert - Verwendung für TLS_RSA_xxxx).
  - KeyCertSign: Wenn der Subject-Public-Key zum Überprüfen von Signaturen in öffentlichen Schlüsselzertifikaten verwendet wird (Wert TRUE).
  - nonRepudiation (erforderlich nach OPC UA-Standard)
  - dataEncipherment (erforderlich nach OPC UA-Standard)
- Subject Alt Name: Im SAN-Feld können die folgenden Werte angegeben werden: IPAddress V4/V6, URI
- Basic Constraints:
  - cA-Feld: Ob der zertifizierte öffentliche Schlüssel zum Überprüfen von Zertifikatsignaturen (Wert TRUE) und pathLenConstraint=0 verwendet werden kann.
- Subject Key Identifier:
  - Methoden zur Identifizierung von Zertifikaten, die einen bestimmten öffentlichen 160-Bit-SHA-1-Hash des Werts von BIT STRING subjectPublicKey enthalten (ausgenommen Tag, Länge und Anzahl nicht verwendeter Bits).
- Extended Key Usage extension:
  - id-kp-serverAuth, wenn TLS-Webserver-Authentifizierung
  - id-kp-clientAuth, wenn TLS-Webclient-Authentifizierung

CA-Zertifikate:

- KeyUsage (als kritisch markiert):
  - DigitalSignature
  - KeyEncipherment (Keine Verwendung für die TLS-Suite, die auf kurzlebigen Schlüsseln (ephemeral) wie TLS_ECDHE_xxxx basiert - Verwendung für TLS_RSA_xxxx).
  - KeyCertSign: Wenn der Subject-Public-Key zum Überprüfen von Signaturen in öffentlichen Schlüsselzertifikaten verwendet wird (Wert FALSE).
  - nonRepudiation (erforderlich nach OPC UA-Standard)
  - dataEncipherment (erforderlich nach OPC UA-Standard)
- Subject Alt Name: Im SAN-Feld können die folgenden Werte angegeben werden: IPAddress V4/V6, URI
- Basic Constraints:
  - cA-Feld: Ob der zertifizierte öffentliche Schlüssel zum Überprüfen von Zertifikatsignaturen (Wert FALSE) verwendet werden kann.

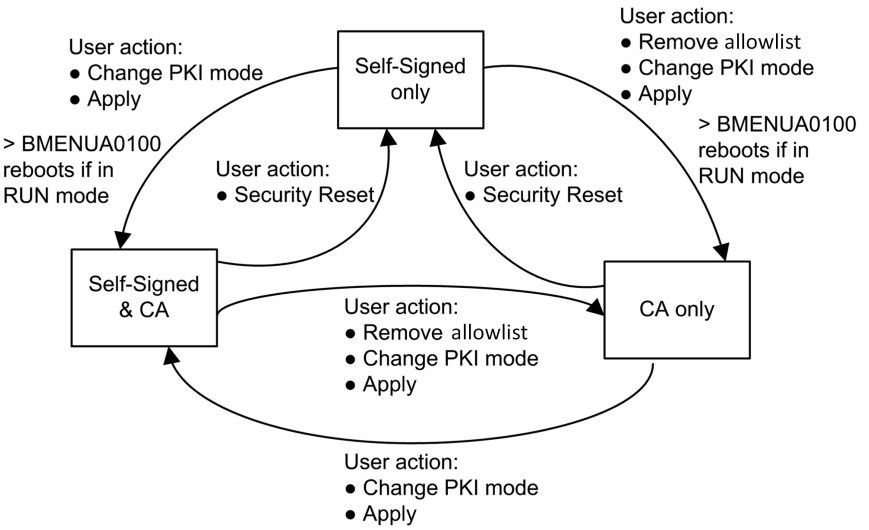
- Extended Key Usage extension:
  - id-kp-serverAuth, wenn TLS-Webserver-Authentifizierung
  - id-kp-clientAuth, wenn TLS-Webclient-Authentifizierung
- CRL Distribution points
- Authority Key Identifier:
  - Kennung des öffentlichen Schlüssels, der dem privaten Schlüssel entspricht, der zum Signieren eines Zertifikats verwendet wird.

PKI-Konfiguration

Verwenden Sie die Seite **PKI-Konfiguration**, um die Typen von Zertifikaten anzugeben, die von dem in das Modul integrierten OPC UA-Server akzeptiert werden, einschließlich:

PKI-Modus	Beschreibung
Nur selbstsigniert	Nur Zertifikate in der Liste **Vertrauenswürdiges Clientzertifikat** müssen verwaltet werden.
Nur CA	Alle Systemgeräte benötigen Zertifikate, die von einer Zertifizierungsstelle signiert wurden.
Selbstsigniert und CA	Zertifikate werden wie folgt verwaltet: • Das Zertifikat für das BMENUA0100-Modul mit einer Firmwareversion ab 1.10 wird von einer Zertifizierungsstelle ausgestellt. • Zertifikate für Clientgeräte, die PKI unterstützen, werden von einer Zertifizierungsstelle ausgestellt. • Zertifikate für Clientgeräte, die PKI nicht unterstützen, sind selbstsigniert.

Die folgende Abbildung zeigt die Benutzeraktionen und -ereignisse im Zusammenhang mit der Änderung der PKI-Moduseinstellung:



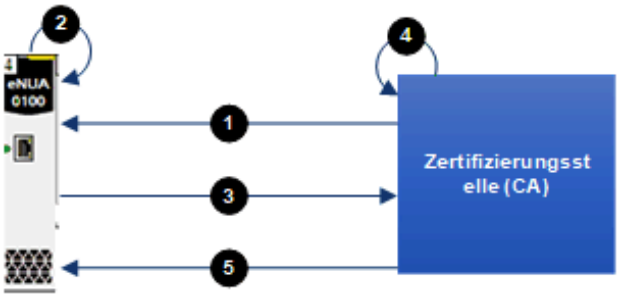
Manuelle Registrierung

Nach der Konfiguration des BMENUA0100-Moduls in Control Expert können Sie die Seite **Manuelle Registrierung** Seite zum Abrufen (**Get**) einer CSR-Datei verwenden, die an eine Zertifizierungsstelle gesendet werden soll. Nachdem Sie die CSR-Datei übermittelt haben, können Sie das entsprechende CA-Zertifikat extrahieren. Danach können Sie dieses CA-Zertifikat per **Push** an das BMENUA0100-Modul übertragen. Über die kombinierten **Get**- und **Push**-Vorgänge wird ein von einer Drittanbieter-Zertifizierungsstelle ausgestelltes Zertifikat manuell registriert. Nachdem das Zertifikat per Push übertragen wurde, wendet der OPC UA-Server dieses Zertifikat zum Signieren und Verschlüsseln seiner Kommunikation mit dem OPC UA-Client an.

HINWEIS: Voraussetzung für die manuelle Registrierung:

- Vergewissern Sie sich, dass der NTP-Client aktiviert, Seite 137 ist.
- Stellen Sie sicher, dass die Zeiteinstellung für das BMENUA0100-Modul korrekt ist.

Nachfolgend finden Sie eine Übersicht über den Prozess der manuellen Zertifikatregistrierung:



1 Das BMENUA0100-Modul importiert ein CA-Zertifikat von der Zertifizierungsstelle (CA).

2 Das BMENUA0100-Modul generiert eine Zertifikatssignierungsanforderung (CSR).

3 Das BMENUA0100-Modul exportiert die CSR in die Zertifizierungsstelle.

4 Die Zertifizierungsstelle führt die CSR aus und generiert ein Zertifikat.

5 Das BMENUA0100-Modul importiert das Zertifikat aus der Zertifizierungsstelle.

Siehe das Schneider Electric-Video „How to work with PKI mode „Self-Signed & CA“ on BMENUA0100 module?“ (Verwenden des PKI-Modus „Selbstsigniert und CA“ im BMENUA0100-Modul) unter https://www.se.com/us/en/faqs/FAQ000191153/.

Verwaltung der Client-Vertrauensliste

Nur OPC UA-Clients, die dem BMENUA0100-Modul ein Anwendungsinstanzzertifikat bereitgestellt haben, können mit dem im Modul integrierten OPC UA-Server kommunizieren. Das Modul implementiert die lokale (modulbasierte) Verwaltung von OPC UA-Anwendungsinstanzzertifikaten, die in einer Vertrauensliste gespeichert sind. Verwenden Sie die Befehle auf den Webseiten **Zertifikatverwaltung** zum **Hinzufügen**, **Herunterladen** oder **Löschen** eines Zertifikats.

HINWEIS: Zertifikate der OPC UA-Anwendungsinstanzvertrauensliste werden in ANSI-CRT codiert.

So fügen Sie der Liste ein Zertifikat hinzu:

Schritt	Aktion
1	Klicken Sie im Menü der Vertrauenslistenverwaltung auf **Hinzufügen**.
2	Klicken Sie auf **Durchsuchen**, navigieren Sie dann zu dem Zertifikat, das Sie in der Liste hinzufügen möchten, und wählen Sie es aus.

Schritt	Aktion
3	Klicken Sie auf **Senden**, um das Zertifikat hinzuzufügen.
4	Klicken Sie auf **Übernehmen**, um die Änderung in der Konfiguration zu speichern.

So entfernen Sie ein Zertifikat aus der Liste:

Schritt	Aktion
1	Klicken Sie in der Vertrauensliste auf das Zertifikat, das Sie entfernen möchten.
2	Wählen Sie **Löschen** aus.
3	Klicken Sie auf **Ja**, um das Zertifikat aus der Liste zu entfernen.
4	Klicken Sie auf **Übernehmen**, um die Änderung in der Konfiguration zu speichern.

Exportieren von Gerätezertifikaten

Sie können das BMENUA0100-Modulzertifikat für HTTPS und OPC UA auf der Seite **ZERTIFIKATVERWALTUNG > PKI-KONFIGURATION** durch Klicken auf die Schaltfläche **Herunterladen** exportieren.

CA-Zertifikate

Das CA-Zertifikat ist ein Public-Key-Zertifikat, das die Zertifizierungsstelle (CA) in einer Public-Key-Infrastruktur (PKI) identifiziert. Verwenden Sie die Seite **CA-Zertifikate**, um das bzw. die CA-Zertifikate zum Gerät hinzuzufügen.

So fügen Sie der Liste der Zertifizierungsstellenzertifikate ein Zertifikat aus der Zertifizierungsstelle hinzu:

Schritt	Aktion
1	Öffnen Sie die Webseiten für das Modul und geben Sie im Dialogfeld **Anmelden** Folgendes ein: • Benutzername • Passwort Klicken Sie auf **Anmelden**.
2	Navigieren Sie zu **KONFIGURIEREN DER CYBERSICHERHEIT-EINSTELLUNGEN > ZERTIFIKATVERWALTUNG**, um auf die Registerkarte der Zertifikatverwaltung zuzugreifen, und wählen Sie dann **CA-Zertifikate** aus.
3	Klicken Sie in der Liste **VERTRAUENSWÜRDIGE ZERTIFIKATE** auf **HINZUFÜGEN**, um das CA-Zertifikat in der Liste hinzuzufügen.
4	Wenden Sie die Änderungen auf die Konfiguration der Cybersicherheit an.

HINWEIS: Es können maximal zehn CA-Zertifikate hinzugefügt werden.

Zugriffskontrolle

Einführung

Das BMENUA0100-Modul unterstützt die lokale Authentifizierung von Benutzern basierend auf der Verwendung von Kombinationen aus Benutzername/Passwort für:

- Konfiguration der Cybersicherheitseinstellungen des Moduls über HTTPS
- Firmware-Download über HTTPS
- Diagnose über die Modulwebseiten per HTTPS

  HINWEIS: Nur ein Benutzer mit der Sicherheitsadministrator-Rolle kann Benutzerkonten erstellen, bearbeiten oder löschen.

Die BMENUA0100-Webseiten stellen Tools für die Verwaltung von Benutzerkonten bereit. Klicken Sie auf der **Startseite** auf **Zugriffskontrolle**, um eine Liste der vorhandenen OPC UA-Benutzerkonten anzuzeigen, einschließlich ihrer Rollen und Berechtigungen. Auf dieser Seite können Sie Folgendes durchführen:

- Benutzerkonto erstellen, Seite 123.
- Profil aktualisieren, Seite 124 für ein vorhandenes Benutzerkonto.
- Löschen, Seite 124 eines Benutzerkontos.

Benutzerverwaltung

Das BMENUA0100-Modul ermöglicht die rollenbasierte Zugriffskontrolle (RBAC: Role-Based Access Control). Alle Benutzerkonten erhalten eine Rolle und können nur die Aufgaben ausführen, die dieser Rolle zugeordnet sind.

Die folgenden Rollen und Berechtigungen werden unterstützt:

Rolle	Berechtigungen			
	Cybersicherheitskonfiguration	Firmwareaktualisierung	Zugriff auf Diagnose-Webseiten	OPC UA-Protokollzugriff
SECADM (SICHERHEITSADMINISTRATOR)	Aktualisieren, Lesen, Löschen	–	Lesen	–
OPERATOR (BEDIENER)	–	–	Lesen	Verbinden

Rolle	Berechtigungen			
	Cybersicherheitskonfiguration	**Firmwareaktualisierung**	**Zugriff auf Diagnose-Webseiten**	**OPC UA-Protokollzugriff**
ENGINEER (TECHNIKER)	–	–	Lesen	Verbinden
INSTALLER (MONTEUR)	–	Aktualisieren	Lesen	–

Jedes BMENUA0100-Modul unterstützt maximal 15 gleichzeitige Benutzer.

Es können keine benutzerdefinierten Rollen oder Berechtigungsgruppen konfiguriert werden. Es kann keine Liste der zulässigen IP-Adressen für die Zugriffskontrolle konfiguriert werden.

Erstellen eines Benutzerkontos

Ein Sicherheitsadministrator kann auf **Neuer Benutzer** klicken und dann die folgenden Parameter ausfüllen, um ein neues Benutzerkonto zu erstellen:

Parameter	Beschreibung
Benutzername	Die Benutzer-ID. Der Benutzer gibt diese ID zusammen mit dem Passwort ein, um Zugang zu den zulässigen Funktionen zu erhalten.
Passwort Passwort bestätigen	Das Benutzerpasswort. Das Passwort wird nicht als Klartext angezeigt. Geben Sie diesen Wert zweimal ein, um seine Genauigkeit zu bestätigen. **HINWEIS:** Jedes Passwort muss mindestens 8 Zeichen lang sein und mindestens eines der folgenden Zeichen enthalten: • einen Großbuchstaben (A bis Z) • einen Kleinbuchstaben (a bis z) • eine Zahl auf Basis 10 (0 bis 9) • ein Sonderzeichen ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : " < >
Rollen	Wählen Sie die Rolle aus, die die Berechtigungen definiert, die dem Benutzer gewährt werden sollen: • SEDADM (Sicherheitsadministrator) • Operator (Bediener) • Engineer (Techniker) • Installer (Monteur)

Klicken Sie auf **Änderungen übernehmen**, nachdem diese Parameter für die Erstellung des Benutzerkontos konfiguriert wurden.

Aktualisieren eines Benutzerkontos

Um die Einstellungen eines Benutzerkontos zu bearbeiten, kann ein Sicherheitsadministrator auf das Bearbeitungssymbol (Bleistift) für das Profil klicken, das bearbeitet werden soll. Klicken Sie auf **Änderungen übernehmen**, um Ihre Änderungen zu speichern. Es wird dasselbe Dialogfeld geöffnet, das auch zum Erstellen eines Benutzerkontos verwendet wird. Hier können Sie einige oder alle der ausgewählten Benutzerkontoparameter aktualisieren.

Löschen eines Benutzerkontos

Um ein vorhandenes Benutzerkonto zu löschen, kann ein Sicherheitsadministrator in der Liste mit der rechten Maustaste auf das Benutzerkonto und dann unter **Benutzer löschen** auf **OK** klicken.

Konfigurationsverwaltung

Einführung

Um die Systemkonfiguration zu erleichtern, können Sie die Cybersicherheitseinstellungen eines konfigurierten BMENUA0100-Moduls exportieren und diese Konfiguration in ein anderes Modul importieren. Wählen Sie auf den Webseiten des BMENUA0100-Moduls auf der **Startseite** die Option **Konfigurationsverwaltung** aus, um Links zu den folgenden Verwaltungsseiten für die Konfiguration der Cybersicherheit anzuzeigen:

- EXPORTIEREN, Seite 124
- IMPORTIEREN, Seite 125
- ZURÜCKSETZEN, Seite 126

HINWEIS: Nur ein Sicherheitsadministrator mit der Rolle SECADM kann die in diesem Abschnitt beschriebenen Konfigurationsverwaltungsaufgaben durchführen.

Exportieren einer Konfiguration

Auf der Seite **EXPORTIEREN** können Sie die Konfigurationsdatei für die Cybersicherheit des lokalen BMENUA0100-Moduls exportieren. Die exportierte Konfigurationsdatei wird mit dem auf dieser Seite zugewiesenen Passwort verschlüsselt. Eine exportierte Konfigurationsdatei kann gespeichert und wiederverwendet werden.

So exportieren Sie die Cybersicherheitskonfigurationsdatei des lokalen BMENUA0100-Moduls:

Schritt	Beschreibung
1	Weisen Sie auf der Seite **EXPORTIEREN** der Konfigurationsdatei ein **Passwort** zu. **HINWEIS:** Das Passwort muss aus mindestens 16 Zeichen bestehen. Es gelten die gleichen Regeln wie beim Erstellen von Benutzerpasswörtern, Seite 123.
2	Geben Sie das zugewiesene Passwort erneut in das Feld **Passwort bestätigen** ein.
3	Klicken Sie auf **Herunterladen**.

HINWEIS: Die Konfigurationsdatei wird mit folgendem Namen erstellt: Mx80_xx_ BMENUA.cfg, wobei „xx“ die Steckplatznummer angibt, die vom Modul im Rack belegt wird.

Importieren einer Konfiguration

Auf der Seite **IMPORTIEREN** können Sie eine Cybersicherheitskonfigurationsdatei importieren und auf das lokale BMENUA0100-Modul anwenden. Die mit diesem Befehl angewendeten Cybersicherheitseinstellungen überschreiben die vorhandenen Cybersicherheitseinstellungen des Moduls.

So importieren Sie eine Cybersicherheitskonfigurationsdatei und wenden diese auf das lokale BMENUA0100-Modul an:

Schritt	Beschreibung
1	Klicken Sie auf der Seite **IMPORTIEREN** auf das Dateisymbol, um ein Fenster zu öffnen, in dem Sie ein **Konfigurationsarchiv** auswählen können.
2	Navigieren Sie zu der Konfigurationsdatei, die Sie importieren möchten, wählen Sie sie aus und klicken Sie auf **OK**.
3	Geben Sie auf der Seite **IMPORTIEREN** die das **Passwort** der Konfigurationsdatei ein, das der Datei beim Export zugewiesen wurde. **HINWEIS:** Optional können Sie **Speichern** auswählen, um die importierte Konfiguration anzuwenden, unmittelbar nachdem sie hochgeladen wurde.
4	Klicken Sie auf **Hochladen**. Es wird ein Dialogfeld geöffnet, das Sie darüber informiert, dass Ihre Sitzung geschlossen wurde. Die Konfiguration wurde in den Server geladen.
5	Klicken Sie auf **Neu verbinden**, um das Dialogfeld zu schließen und das Anmeldefenster, Seite 95 zu öffnen.

Schritt	Beschreibung
6	Geben Sie Ihren Benutzernamen und Ihr Passwort für den Sicherheitsadministrator ein und klicken Sie auf **Anmelden**. Die Startseite wird angezeigt. Wenn **Speichern** in Schritt 3 nicht ausgewählt wurde, zeigt das Banner an, dass eine Konfiguration ausstehend ist.
7	Klicken Sie im Banner auf **Übernehmen** und dann auf **Ja**, um zu bestätigen, dass Sie die ausstehende Konfiguration anwenden möchten. Die neue Konfiguration wird angewendet. **HINWEIS:** Wenn Sie zuvor **Speichern** auf der Seite **IMPORTIEREN** ausgewählt haben (wie in Schritt 3 oben angegeben), wird die Konfiguration automatisch übernommen und dieser Schritt 7 wird automatisch durchgeführt.

Zurücksetzen einer Konfiguration

Klicken Sie auf der Seite **ZURÜCKSETZEN** auf **Zurücksetzen**, um die bei Auslieferung eingestellten werkseitigen Standardeinstellungen für die Cybersicherheit im lokalen BMENUA0100-Modul wiederherzustellen. Diese Aktion hat die gleiche Wirkung wie das Setzen des Drehwahlschalters in die Stellung Zurücksetzen der Cybersicherheit (oder Sicherheit), Seite 33. Nach Abschluss des Resets müssen Sie das Modul neu starten.

Konfiguration des BMENUA0100-Moduls in Control Expert

Einführung

In diesem Kapitel wird die Konfiguration der IP-Adresseinstellungen, des NTPv4-Clients und des SNMPv1-Agenten für das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server beschrieben.

Konfiguration der IP-Adresseinstellungen

Einführung

Das BMENUA0100-Ethernet-Kommunikationsmodul mit integriertem OPC UA-Server verfügt über zwei Ethernet-Ports:

- den Steuerungsport an der Vorderseite des Moduls

- einen Baugruppenträger-Port, der das Modul mit dem Ethernet-Baugruppenträger des lokalen Hauptracks verbindet.

Der Steuerungsport kann aktiviert oder deaktiviert werden und ist standardmäßig deaktiviert. Der Baugruppenträger-Port ist immer aktiviert.

Die statischen IP-Adresseinstellungen für den Steuerungsport und den Baugruppenträger-Port können auf der Registerkarte **IP-Konfig.** des Dialogfelds zur BMENUA0100-Konfiguration vorgenommen werden. Darüber hinaus können die IP-Adresseinstellungen dem Steuerungsport dynamisch über die SLAAC-Methode (Stateless Address Auto-configuration) zugewiesen werden.

Wenn das BMENUA0100-Modul mit einer Standalone-Steuerung verwendet wird, werden die IP-Adresseinstellungen für ein Modul konfiguriert. Wenn zwei Instanzen des BMENUA0100-Moduls in einer Hot Standby-Steuerungsarchitektur verwendet werden (ein BMENUA0100-Modul in jeder Steuerung), enthält die Control Expert-Registerkarte **IP-Konfig.** Einstellungen für zwei Module (A und B). In einer Hot Standby-Steuerungsarchitektur kann sich die IP-Adresse für jedes Modul in verschiedenen Subnetzen befinden.

IPv4- und IPv6-Stack-Unterstützung

Der Steuerungsport kann wie folgt zur Unterstützung von IP-Stacks (von denen jeder aus einer Gruppe von internetfähigen Protokollen besteht) konfiguriert werden:

- IPv4-Stack: Unterstützt nur die 32-Bit-Adressierung. Ein Beispiel für eine IPv4-IP-Adresse: 192.168.1.2.
- IPv4/IPv6-Dual-Stack: Unterstützt sowohl die 32-Bit- als auch die 128-Bit-Adressierung. Wenn sowohl die IPv4- als auch die IPv6-Stacks konfiguriert sind, kann der Steuerungsport sowohl IPv4- als auch IPv6-Ethernet-Pakete empfangen und verarbeiten. Nachfolgend ein Beispiel für eine IPv6-128-Bit-IP-Adresse: 2001:0578:0123:4567:89AB:CDEF:0123:4567.

  HINWEIS:

  Beim ersten Einschalten (oder nachdem der Drehwahlschalter des Moduls auf **Zurücksetzen der Cybersicherheit (oder der Sicherheit)** gesetzt, eingeschaltet und anschließend auf **Erweiterter (oder Sicherer) Modus** zurückgesetzt und erneut eingeschaltet wurde) wird dem Steuerungsport die Standard-IPv4-Adresse 10.10. MAC5.MAC6 zugewiesen, wobei MAC5 dem Dezimalwert des 5. Oktetts der MAC-Adresse des Moduls und MAC6 dem Dezimalwert des 6. Oktetts entspricht.

  Wenn die letzten beiden Bytes der MAC-Adresse (*MAC5.MAC6*) *0,0* in der Standardadresse entsprechen, stellen Sie eine Punkt-zu-Punkt-Kabelverbindung zwischen Ihrem Computer und dem Controller, dem Kommunikationsmodul oder einem anderen Modul her.

  Die MAC-Adresse des Moduls wird an der Vorderseite angezeigt.

IPv6 über den Steuerungsport

Die IPv6-Kommunikation wird nur über den Steuerungsport unterstützt.

HINWEIS: Der Control Expert-Datenfluss kann so konfiguriert werden, dass er an eine M580-Steuerung weitergeleitet wird. Control Expert ab V15 kann über die BMENUA0100-IPv6-Adresse mit einer M580-Steuerung verbunden werden.

Konfiguration der IP-Adressen

Konfigurieren Sie die IP-Adressen in Control Expert wie folgt:

Schr-itt	Aktion
1	Erweitern Sie im **Projekt-Browser** den Knoten **SPS-Bus** und öffnen Sie das Dialogfeld zur BMENUA0100-Modulkonfiguration.
2	Klicken Sie auf die Registerkarte **IP-Konfig.**.
3	Nehmen Sie die erforderlichen Änderungen in den entsprechenden Feldern auf der Konfigurationsseite **IP-Konfig.** vor. (In der nachstehenden Tabelle werden die Parameter der Konfigurationsseite beschrieben.)

Konfigurierbare Parameter

Konfigurieren Sie die folgenden IP-Parameter für jedes BMENUA0100-Kommunikationsmodul in Ihrem Projekt:

Parameter	Beschreibung
Steuerungsport	Aktiviert/deaktiviert den Steuerungsport des BMENUA0100-Moduls. Bei einer Einstellung auf: • Aktiviert: Der Steuerungsport ist die exklusive Schnittstelle für die IPv4- oder IPv6-Kommunikation mit dem integrierten OPC UA-Server. • Deaktiviert (Standard): Der Ethernet-Baugruppenträger-Port unterstützt die IPv4-Kommunikation mit dem OPC UA-Server.
Konfiguration des IPv6-Steuerungsports	

Parameter		Beschreibung
	IPv6	Aktiviert/deaktiviert die IPv6-IP-Adressierung für den Steuerungsport, wenn der Steuerungsport aktiviert ist. Standard = Deaktiviert.
	Modus	Identifiziert die Quelle der IPv6-Adresse: • SLAAC: Gibt an, dass die IPv6-IP-Adresse von einem DHCP-Server über das SLAAC-Verfahren an den Steuerungsport übermittelt wird. • Statisch (Standard): Aktiviert das Feld „IPv6 @“ zur Eingabe einer statischen IPv6-IP-Adresse.
	IPv6 @	Wenn **Statisch** als **Modus** ausgewählt wird, geben Sie eine gültige IPv6-Adresse für den Steuerungsport ein. **HINWEIS:** • Das BMENUA0100-Modul kann keine doppelten IPv6-Adressen erkennen. Wenden Sie sich an Ihren Netzwerkadministrator, um sicherzustellen, dass keine doppelten IPv6-Adressen innerhalb desselben Netzwerksegments vorhanden sind. • Das BMENUA0100-Modul akzeptiert ungültige IPv6-Adressen, kann sie aber nicht verwenden.
	Länge des Subnetz-Präfixes	Wird automatisch für eine statische IPv6-Adresse festgelegt und entspricht der Anzahl an Bits der SLAAC-zugewiesenen IPv6-Adresse, die das Subnetz-Netzwerkpräfix definieren (Standard = 64).
Konfiguration des IPv4-Steuerungsports		
	IPv4	Aktiviert/deaktiviert die IPv4-IP-Adressierung für den Steuerungsport, wenn der Steuerungsport aktiviert ist. Standard = Aktiviert.
	Modus	Identifiziert die Quelle der IPv4-Adresse: • Standard: Die Zuweisung einer IP-Adresse erfolgt automatisch durch die Software. • Statisch (Standard): Aktiviert die Felder **IPv4 @**, **Subnetzmaske** und **Standard-Gateway** zur Eingabe einer statischen IPv4-IP-Adresse für den Steuerungsport.
	IPv4 @	Wenn folgender Modus ausgewählt ist: • **Standard**: Die IP-Adresse wird automatisch zugewiesen. Die Felder **IPv4 @**, **Subnetzmaske** und **Standard-Gateway** sind deaktiviert. • **Statisch**: Geben Sie eine gültige IPv4-Adresse für den Steuerungsport ein.
	Subnetzmaske	Wenn **Statisch** als **Modus** ausgewählt ist, geben Sie eine gültige IPv4-Subnetzmaske für den Steuerungsport ein, die den Netzwerkteil der IPv4-Adresse bestimmt.
	Standard-Gateway	Wenn **Statisch** als **Modus** ausgewählt ist, geben Sie eine gültige IPv4-Adresse für das Standard-Gateway ein.

Parameter		Beschreibung
Baugruppenträger-Port		
	IPv4 @	Geben Sie eine gültige IPv4-Adresse für den Baugruppenträger-Port ein.
Quelle Zeitstempelung		Weitere Informationen finden Sie im Abschnitt Konfiguration der Quellzeitstempelung, Seite 130.
Schnelle Abtastrate		Bei ausgewählter Option können Sie den OPC UA-Client mit einem Mindestabtastintervall von 20 ms konfigurieren, was die Überwachung von 2.000 Elementen ermöglicht. Standardmäßig ist die Option nicht ausgewählt. Die Standardabtastperiode ist 250 ms, was die Überwachung von entsprechenden 20.000 Elementen des Typs INT ermöglicht. **HINWEIS:** Eine Änderung dieser Einstellung wird erst nach dem vollständigen Download der Anwendung wirksam.
OPCUA-TCP-Überwachungsport		Der TCP-Port für die OPC UA-Kommunikation: • Standardmäßig: Voreinstellung auf Port 4840 • Anderer Wert: Benutzerdefiniert **HINWEIS:** Der Wert für diesen Port muss für alle BMENUA0100-Kommunikationsmodule gleich sein (z. B. bei der OPC UA-NAT-Weiterleitung zwischen mehreren BMENUA0100-Modulen).

HINWEIS: Gehen Sie bei der Konfiguration Ihrer Anwendung in Control Expert wie folgt vor:

- Im Fenster **Ethernet-Netzwerk** (geöffnet über **Extras > Ethernet-Netzwerkmanager...**) werden die Einstellungen für den Baugruppenträger-Port und den Steuerungsport für das BMENUA0100-Modul angezeigt, einschließlich Informationen zum NTP-Server, SNMP-Manager und - für ein Hot Standby-System - zum Standby-BMENUA0100-Modul (B).
- Auf der Seite **Adress-Server** der Steuerung (geöffnet im **DTM-Browser** durch einen Doppelklick auf die Steuerung und Auswahl von **Services > Adress-Server**) wird die IP-Adresse des Baugruppenträger-Ports des BMENUA0100-Moduls angezeigt. In einer Hot Standby-Konfiguration wird auf der Seite **Adress-Server** die IP-Adresse des Baugruppenträger-Ports für beide BMENUA0100-Module angezeigt.

Konfiguration der Quellzeitstempelung

Die Quellzeitstempelung wird von der Firmwareversion 2.01 (oder höher) des BMENUA0100-Moduls (BMENUA0100.2) in Control Expert unterstützt.

Um die Quellzeitstempelung in einer Anwendung verwenden zu können, müssen Sie sie aktivieren.

Nachdem die Quellzeitstempelung sowohl aktiviert als auch ausgelöst wurde, beginnt das BMENUA0100-Modul mit dem Abruf von Geräten, wenn mindestens ein überwachtes Element vorhanden ist, wobei der **Überwachungsmodus** im OPC UA-Client auf **Weiterleiten** oder **Berichterstellung** eingestellt ist.

HINWEIS: Die Werte werden von einem Quellzeitstempelgerät nur für die Variablen BOOL und EBOOL abgerufen, die:

- in Control Expert als an der Quelle zeitgestempelt (ASTS: At-Source-Time-Stamped) konfiguriert sind.
- von einem OPC UA-Client als Teil des OPC UA-Abonnements überwacht werden.

Wenn der OPC UA-Knoten nicht zu einem Abonnement hinzugefügt wurde und nicht als Teil eines Abonnements überwacht wird, erkennt der synchrone OPC UA-Lesedienst einen Fehler und meldet ihn.

Aktivieren der Quellzeitstempelung

Die Quellzeitstempelung wird im Fenster der Projekteinstellungen aktiviert. Navigieren Sie zu **Allgemein > Zeit > Zeitstempel-Modus** und wählen Sie dann **System** aus.

HINWEIS: Die Standardeinstellung für den **Zeitstempelmodus** lautet **Anwendung**. Wenn Sie die Standardeinstellung nicht zu **System** ändern, wird beim Erstellen der Anwendung ein Fehler angezeigt.

Auslösen der Quellzeitstempelung

Verwenden Sie die Registerkarte **IP-Konfig.** des BMENUA0100-Konfigurationsfensters zur Aktivierung und Konfiguration der Zeitstempelung.

Konfigurieren Sie im Bereich **Quellzeitstempelung** die folgenden Einstellungen:

Einstellung	Beschreibung
Aktiviert	Aktiviert die Quellzeitstempelung für die Anwendung.
Pufferabfrage (ms)	Die Abfragerate für vom BMENUA0100 verarbeitete Ereignis-Leserequests. Der gültige Einstellungsbereich reicht von mindestens 250 ms bis maximal 5000 ms in Schritten von 250 ms. **HINWEIS:** Die maximale Anzahl quellzeitgestempelter Variablen in Control Expert ist 5000.

HINWEIS: Wenn das lokale M580-Rack zwei BMENUA0100-Module enthält, kann die Quellzeitstempelung nur von einem Modul verwendet werden. Informationen zur Verwaltung zeitgestempelter Variablen finden Sie unter Angabe des BMENUA0100-Moduls zur Verwaltung zeitgestempelter Variablen, Seite 134.

Verwaltung von Variablen mit Zeitstempelung an der Quelle

Verwendung der OPC UA-Datenelemente #TSEventItemsReady und #TSEventSynchro

Sie können die OPC UA-spezifischen Datenelemente `#TSEventItemsReady` und `#TSEventSynchro` zum Durchsuchen und Festlegen des Status von an der Quelle zeitgestempelten Variablen verwenden.

HINWEIS: Beide Datenelemente sind nur dann von Bedeutung, wenn die Zeitstempelung in Control Expert aktiviert und für das spezifische BMENUA0100-Modul aktiviert ist.

Das BMENUA0100-Modul behandelt das `#TSEventSynchro`-Datenelement als boolescher OPC UA-Knoten.

Durch die Einstellung des `#TSEventSynchro`-Elements wird ein Synchronisierungsbefehl an alle an der Quelle mit Zeitstempel versehenen Geräte der M580-Steuerung gesendet. Die von den Geräten an den OPC UA-Client zurückgegebenen Werte initialisieren die an der Quelle mit Zeitstempel versehenen Variablen mit ihren aktuellen Werten.

Das BMENUA0100-Modul antwortet auf die Clienteinstellung des `#TSEventSynchro`-Elements mit einer der folgenden Meldungen:

- `UA_EGOOD`: Der Synchronisations-Request wurde ordnungsgemäß an alle Zeitstempel-Geräte gesendet.
- `UA_EBAD`: Der Synchronisations-Request war nicht erfolgreich, da die Zeitstempelung im Control Expert-Projekt deaktiviert ist.
- `UA_EBADINVALIDSTATE`: Der Synchronisations-Request war nicht erfolgreich, da die Zeitstempelung für das BMENUA0100-Modul über die Funktion %MW400, Seite 134 ausgeschaltet wurde.
- `UA_EBADINUSE`: Der Synchronisations-Request war nicht erfolgreich, da das BMENUA0100-Modul den Zeitstempelpuffer nicht reservieren konnte.
- `UA_EBADDISCONNECT`: Timeout des Synchronisations-Requests. Die Werte konnten nicht im angegebenen Zeitrahmen geschrieben werden.

Verwenden Sie für diese Initialisierung einen OPC UA-Client - z. B. UaExpert -, um die folgende Tasksequenz auszuführen:

1. Überwachen Sie das `#TSEventItemsReady`-Element, das angibt, dass das BMENUA0100-Modul bereit ist zur Verwaltung der zeitgestempelten Variablen der Steuerungspuffer (einschließlich M580-Steuerung, BMECRA31310, BMXERT1604), und warten Sie, bis der Wert zu 1 (TRUE) wechselt.
2. Fügen Sie überwachte Datenelemente, die als an der Quelle mit Zeitstempel versehene Variablen konfiguriert sind, zu einem oder mehreren Abonnements hinzu.

3. Stellen Sie den `#TSEventSynchro`-Schreibbefehl zum Aktualisieren des Werts und des Zeitstempels an der Quelle jedes Elements ein.

   HINWEIS:

   - Das BMENUA0100-Modul liest alle konfigurierten Variablen mit Zeitstempel in der Steuerung. Wenn ein Ereignis (Änderung des Elementstatus) bei einem überwachten Element mit Zeitstempel auftritt, wird dieses Element aktualisiert. Wenn ein Element nicht überwacht wird, wird es verworfen.
   - Setzen Sie den Datenänderungsfilter auf **Status/Wert/Zeitstempel**. Andernfalls ist es möglich, dass verschiedene OPC UA-Clients - z. B. Clients, die Werte nur bei Status-/Wertänderungen aktualisieren - einen unterschiedlichen Status und Wert für dieselbe Variable anzeigen.
   - Da das BMENUA0100-Modul Werte regelmäßig aktualisiert, kann es vorkommen, dass seit der vorherigen Aktualisierung mehrere Ereignisse auftreten. In diesem Fall zeigt das BMENUA0100-Modul nur den neuesten Wert an.
   - Weil `#TSEventSynchro` an mehrere Zeitstempelgeräte gesendet wird, gibt die Einstellung `#TSEventSynchro`, wenn ein einzelnes Gerät nicht innerhalb des erwarteten Zeitrahmens antwortet, die Antwort `UA_EBADDISCONNECT` zurück, was darauf verweist, dass der Befehl wegen Zeitüberschreitung nicht erfolgreich war. Dies gilt auch dann, wenn andere Geräte erfolgreich reagieren.
   - Wenn das Abonnement so bearbeitet wird, dass es z. B. nur eine Variable für ein Gerät enthält, bewirkt die Ausführung von `#TSEventSynchro` den Verlust zuvor zurückgegebener Werte für zuvor abonnierte Geräte und Variablen.

Ermitteln der für die Zeitstempelung reservierten Kanäle der M580-Steuerung

Für die Kommunikation zwischen BMENUA0100 und einer M580-Steuerung, bei der die Zeitstempelung in Control Expert aktiviert ist, sind 25 % der Steuerungskanäle für die Unterstützung der Zeitstempelfunktion reserviert. Maximal 75 % der Steuerungskanäle bleiben für andere Kommunikationsrequests verfügbar.

Beispiel: Für die BMEP584040-Steuerung:

- Maximale Anzahl der Kanäle 13
- Für die Zeitstempelung verwendete Kanäle: 3
- Für andere Zwecke als die Zeitstempelung verwendete Kanäle: 10

Ermitteln der Kapazität des BMENUA0100-Moduls zum Lesen zeitgestempelter Variablen

Die Anzahl der zeitgestempelten Variablen, die das BMENUA0100-Modul pro Zyklus lesen kann, ist von folgenden Faktoren abhängig:

- Die Einstellung **Abfrage des Puffers** auf der Registerkarte **IP-Konfig.** des Moduls und:
- Die Kapazität des Quellgeräts, einschließlich:
  - Die maximale Anzahl von TCP-Verbindungen und:
  - Die maximale Anzahl unterstützter an der Quelle zeitgestempelter Variablen.

Die Formel für die Ermittlung der maximalen Anzahl der an der Quelle zeitgestempelten Variablen für ein Gerät lautet:

((Max. Anzahl der TCP-Verbindungen) / (Anzahl der Kanäle)) x (Max. Anzahl der zeitgestempelten Variablen pro Zyklus)

Beispiel:

- BMEP586040(C): 16 max. Verbindungen, 4 Kanäle, 82 max. Variablen:

  ((16 / 4) x 82 = 328 Gesamtvariablen

  Wenn **Abfrage des Puffers** = 500 ms: 656 Variablen pro Sekunde
- BMECRA31310: 1 Verbindung, 1 Kanal, 82 max. Variablen:

  1 x 82 = 82 Gesamtvariablen

  Wenn **Abfrage des Puffers** = 500 ms: 164 Variablen pro Sekunde
- BMXERT1604: 1 Verbindung, 1 Kanal, 20 max. Variablen:

  1 x 20 = 20 Gesamtvariablen

  Wenn **Abfrage des Puffers** = 500 ms: 40 Variablen pro Sekunde

Angabe des BMENUA0100-Moduls zur Verwaltung zeitgestempelter Variablen

Ein M580-Hauptrack kann zwei BMENUA0100-Module enthalten. Variablen mit Zeitstempel in den M580-Steuerungen, BMECRA31310- und BMXERT1604-Modulen können nur von jeweils einem BMENUA0100-Modul gelesen und verwaltet werden. Beim Start versucht jedes BMENUA0100-Modul standardmäßig, den Zugriff auf zeitgestempelte Variablen zu reservieren und zu sperren.

In einem Rack mit zwei BMENUA0100-Modulen müssen Sie das Modul angeben, das Variablen mit Zeitstempel liest und verwaltet. Gehen Sie wie folgt vor, um das BMENUA0100-Modul anzugeben, das Variablen liest und verwaltet:

1. Wählen Sie auf der Registerkarte **IP-Konfig.** für die beiden BMENUA0100-Module, für die Sie eine Zeitstempelung wünschen, die Option **Aktiviert** aus.
2. Verwenden Sie für das BMENUA0100-Modul, für das Sie den Zeitstempelpuffer reservieren möchten, den `WRITE_VAR`-Baustein, um das Wort %MW400 auf 2 zu setzen, wodurch das Lesen und Verwalten der zeitgestempelten Variablen für dieses Modul eingeschaltet wird.

   HINWEIS: Durch die Einstellung %MW400 = 2 wird das BMENUA0100-Modul identifiziert, das Variablen liest und verwaltet, wenn für zwei BMENUA0100-Module die Einstellung **Aktiviert** ausgewählt ist.
3. Für das andere BMENUA0100-Modul, für das Sie den Zeitstempelpuffer nicht reservieren möchten, verwenden Sie den `WRITE_VAR`-Baustein, um das Wort %MW400 auf 1 zu setzen, wodurch das Lesen und die Verwaltung zeitgestempelter Variablen für dieses Modul ausgeschaltet wird.

   HINWEIS: Sie müssen diese Schritte nach jeder Änderung des Betriebsmodus ausführen, einschließlich Aus- und Wiedereinschalten, Laden der Anwendung oder Durchführen einer Initialisierung.

Das von Ihnen angegebene BMENUA0100-Modul behält die Kontrolle über das Lesen und die Verwaltung zeitgestempelter Variablen, solange beide der folgenden Bedingungen weiterhin bestehen:

- Es wird mindestens eine zeitgestempelte Variable überwacht.
- Der BMENUA0100-**Überwachungsmodus** wird entweder auf **Weiterleiten** oder auf **Abtasten** eingestellt.

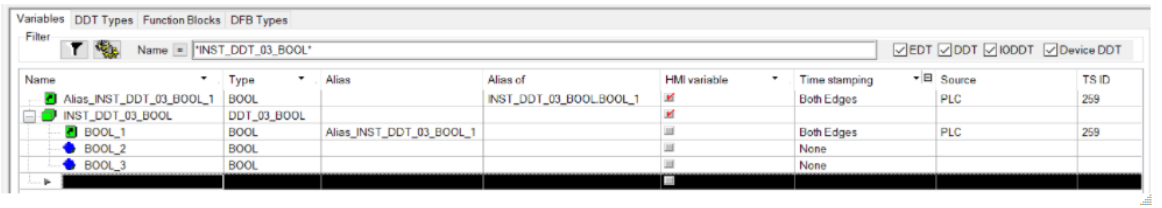
HINWEIS:

Wenn die Einstellung **Aktiviert** nicht ausgewählt wird, entsprechen die vom BMENUA0100 gelesenen Variablenwerte den Werten im Speicher der Steuerung.

Wenn die Einstellung **Aktiviert** ausgewählt und %MW400 auf 1 gesetzt ist, behalten die vom BMENUA0100-Modul gelesenen Variablenwerte den zuletzt gelesenen Wert bei, als der Zeitstempelpuffer reserviert wurde.

Überwachen zeitgestempelter Alias-Variablen

Das BMENUA0100-Modul erkennt zeitgestempelte BOOL- oder EBOOL-**Alias**-Variablen, die in Control Expert erstellt wurden, jedoch keine entsprechenden **Alias von**-Variablen. Nachfolgend ein Beispiel für **Alias**- und **Alias von**-Variablen:



Um vom BMENUA0100 erkannt zu werden, müssen die **Alias**-Variablen in das Datenwörterbuch integriert sein.

BOOL- oder EBOOL-**Alias**-Variablen und die entsprechenden **Alias von**-Variablen nutzen dieselbe logische Adresse im M580-Speicher und dieselbe EventID im M580-Zeitstempelpuffer. Die Quellzeitstempelung wird nur für **Alias**- und nicht für **Alias von**-Variablen verwaltet. Mit anderen Worten: Sie müssen die **Alias**-Variable (OPC UA-Knoten) im OPC UA-Client abonnieren, um die Quellzeitstempelung vom Gerät anstatt vom BMENUA0100-Modul empfangen zu können.

Da weder die BOOL- noch die EBOOL-**Alias von**-Variable von der BMENUA0100-Firmware als an der Quelle zeitgestempelt angesehen wird, muss das **Alias** in das Datenwörterbuch integriert sein. In diesem Fall müssen Sie die **Alias**-Variable als überwachtes Element in einem OPC UA-Abonnement hinzufügen, um die vom Gerät festgelegte Quellzeitstempelung zu erreichen.

Konfiguration des Netzwerkzeitdienstes

Einführung

Das BMENUA0100-Ethernet-Kommunikationsmodul mit integriertem OPC UA-Server unterstützt Version 4 des Netzwerkzeitprotokolls (NTP). Der NTP-Dienst synchronisiert die Uhrzeit im BMENUA0100-Modul mit der Uhrzeit eines Zeitservers. Der synchronisierte Wert wird dann zur Aktualisierung der Uhrzeit im Modul herangezogen.

Sowohl das IPv4- als auch das IPv6-Protokoll werden unterstützt.

HINWEIS:

- Wenn sich der NTP-Server in der Steuerung befindet, kann das BMENUA0100-Modul seine Zeiteinstellungen ohne Verzögerung aktualisieren.
- Wenn ein neuer NTP-Server erreicht wird oder wenn es einen Zeitverschiebung auf einem NTP-Server gibt, kann es bis zu 5 Minuten dauern, bis das BMENUA0100-Modul aktualisiert wird. Die **ERR**-LED, Seite 144 bleibt EIN, bis die BMENUA0100-Zeit mit dem NTP-Server synchronisiert wird.
- Wenn Sie eine Zeitänderung manuell konfigurieren, indem Sie eine zukünftige Uhrzeit eingeben, werden möglicherweise die bestehenden OPC UA-Kanäle getrennt. Wenn der OPC UA-Client eine automatische Neuverbindung zum OPC UA-Server durchführt, werden neue Kanäle erstellt und die Verbindung wird wiederhergestellt.

Aktivieren und Deaktivieren des NTP-Clients und des NTP-Servers

Das BMENUA0100-Modul enthält einen NTP-Server und einen NTP-Client.

NTP-Client:

Wenn die IP-Adresse des primären oder des sekundären NTP-Servers auf einen anderen Wert als 0.0.0.0 festgelegt ist, wird der NTP-Client aktiviert. Wenn sowohl die IP-Adresseinstellungen des primären als auch des sekundären NTP-Servers leer sind oder auf 0.0.0.0 (IPv4) oder 0000:0000:0000:0000:000:000:000:000:000 (IP 6) stehen, wird der NTP-Client deaktiviert.

HINWEIS: Wenn die IP-Adresseinstellungen von **Primärer NTP-Server** und **Sekundärer NTP-Server** auf 0.0.0.0 gesetzt sind, kann das BMENUA0100-Modul weder als NTP-Client noch als NTP-Server betrieben werden.

NTP-Server:

Je nach Cybersicherheitsmodus wird der NTP-Server wie folgt aktiviert:

- Im erweiterten (oder sicheren) Modus ist der NTP-Server aktiviert, wenn:
  - Die IP-Adresse des primären oder des sekundären NTP-Servers auf einen Wert festgelegt ist, der nicht null ist (d. h. auf einen anderen Wert als 0.0.0.0), und
  - der NTP-Server in den Konfigurationseinstellungen der Webseite, Seite 102 **Netzwerkdienste** aktiviert ist.
- Im Standardmodus ist der NTP-Server aktiviert, wenn die IP-Adresseinstellung von **Primärer NTP-Server** oder **Sekundärer NTP-Server** auf einen Wert ungleich null gesetzt ist (d. h. auf einen anderen Wert als 0.0.0.0).

  HINWEIS: Wenn BMENUA0100 als NTP-Client im Baugruppenträger-Netzwerk konfiguriert ist (**Primärer NTP-Server** oder **Sekundärer NTP-Server**), kann der BMENUA0100-NTP-Server nicht für ein anderes Gerät aktiviert werden.

Wenn sowohl der NTP-Server als auch der NTP-Client im BMENUA0100-Modul aktiviert sind, erhält der NTP-Client des Moduls die Zeiteinstellungen über seinen Steuerungsport von einem dezentralen NTP-Server. Der NTP-Server des Moduls leitet diese Zeiteinstellungen über seinen Baugruppenträger-Port an die NTP-Clients weiter.

HINWEIS: Das BMENUA0100-Modul kann nicht als NTP-Server über seinen Steuerungsport betrieben werden.

NTP-Abfrage

Das BMENUA0100-Modul verwaltet den NTP-Abfragezeitraum optimal und dynamisch in Verbindung mit dem NTP-Server. Eine Konfiguration ist nicht erforderlich.

Einschalten

Um die genaue Ethernet-Systemnetzwerkzeit festzulegen, führt das System beim Start folgende Aufgaben aus:

- Das BMENUA0100-Kommunikationsmodul wird gestartet.
- Die BMENUA0100-Kommunikationsmodul erhält die Uhrzeit vom NTP-Server.
- Für den Dienst muss die Uhrzeit regelmäßig abgerufen werden, damit kontinuierlich der richtige Uhrzeitwert abgefragt und die Zeit auf dem aktuellen Stand gehalten werden kann. Die Konfiguration des **Abfragezeitraums** beeinflusst die Genauigkeit der Uhrzeit.

Sobald eine genaue Zeit ermittelt ist, legt der Dienst den Status in der zugeordneten Zeitdienstdiagnose fest.

HINWEIS: Das BMENUA0100-Kommunikationsmodul führt keine Uhrzeiteinstellung durch. Nach dem Einschalten oder einem Aus- und Wiedereinschalten ist der Uhrwert des Moduls 0, was dem 1. Januar 1980 00:00:00:00 entspricht.

Konfigurieren des Dienstes

Gehen Sie wie folgt vor, um den Dienst für die Netzwerkzeitsynchronisation in Control Expert zu konfigurieren:

Schritt	Aktion
1	Erweitern Sie im **Projekt-Browser** den Knoten **SPS-Bus** und öffnen Sie das Dialogfeld zur BMENUA0100-Modulkonfiguration.
2	Klicken Sie auf die Registerkarte **NTP**.
3	Geben Sie die Änderungen in die entsprechenden Felder auf der Konfigurationsseite **Netzwerkzeitdienst** ein. (In der nachstehenden Tabelle werden die Parameter der Konfigurationsseite beschrieben.)

Konfigurierbare Parameter

Konfigurieren Sie diese Zeitsynchronisationsparameter für jedes BMENUA0100-Kommunikationsmodul in Ihrem Projekt:

Parameter		Beschreibung
IPv4-NTP-Serverkonfiguration		
	Primärer NTP-Server (siehe Hinweis)	Geben Sie eine gültige IPv4- oder IPv6-Adresse für den primären NTPv4-Server ein. **HINWEIS:** Stellen Sie standardmäßig die Haupt-IP-Adresse der Steuerung ein.

Parameter		Beschreibung
	Sekundärer NTP-Server (siehe Hinweis)	Geben Sie eine gültige IPv4- oder IPv6-Adresse für den sekundären NTPv4-Server ein.

HINWEIS:

- Konfigurieren Sie die NTP-Serveradresse, die vom BMENUA0100-Modul erreicht werden kann. Ist der Steuerungsport deaktiviert, geben Sie die IP-Adressen des NTP-Servers ein, die sich im gleichen Subnetz wie der Baugruppenträger-Port befinden.
- Sie können eine IPV4-Adresse für den primären NTP-Server und eine IPV6-Adresse für den sekundären NTP-Server (und umgekehrt) konfigurieren, wenn sich beide Adressen in derselben Domäne befinden.
- Bei Hot Standby-Konfigurationen müssen sich die NTP-Adressen für **NUA(A)** und **NUA(B)** im selben Netzwerk befinden, z. B. in dem Netzwerk, auf das über den Baugruppenträger-Port oder über den Steuerungsport zugegriffen werden kann.

HINWEIS: Vergewissern Sie sich beim Betrieb im erweiterten (oder sicheren) Modus, dass der NTP-Dienst im Bereich Aktivierung der Netzwerkdienste, Seite 102 auf der Webseite **Einstellungen** aktiviert ist.

SNMP-Agent-Konfiguration

Über SNMP

Alle Firmwareversionen des BMENUA0100-Moduls unterstützen den SNMP-Agent der Version 1 (V1). Firmwareversion 2 (und höher) des Moduls (BMENUA0100.2) unterstützt auch Version 3 (V3) des SNMP-Agent.

HINWEIS: Beide SNMP-Versionen, V1 und V3, werden nicht gleichzeitig unterstützt.

Ein SNMP-Agent ist eine Softwarekomponente des SNMP-Dienstes, die auf dem BMENUA0100-Modul ausgeführt wird und Zugriff auf Diagnose- und Verwaltungsinformationen für das Modul bietet. Sie können SNMP-Browser, Netzwerkverwaltungssoftware und andere Funktionen für den Zugriff auf diese Daten verwenden.

Darüber hinaus kann der SNMP-Agent mit den IP-Adressen von 1 oder 2 Geräten konfiguriert werden, wobei es sich im Allgemeinen um die PCs handelt, auf denen die Netzwerkverwaltungssoftware ausgeführt wird, um als Ziel ereignisgesteuerter Trap-Nachrichten zu dienen. Solche Nachrichten informieren das Verwaltungsgerät über Ereignisse wie Kaltstarts und die Unfähigkeit, ein Gerät zu authentifizieren.

HINWEIS: Die Kommunikation mit dem SNMP-Agent, der auf dem BMENUA0100-Modul ausgeführt wird, kann entweder über eine IPv4- oder eine IPv6-Adressierung erfolgen.

Beendigung des SNMP-Dienstes

Der im BMENUA0100-Modul ausgeführte SNMP-Dienst wird beendet, wenn Folgendes zutrifft:

- Das Modul befindet sich im Zustand ERROR.
- Der SNMP-Dienst befindet sich im Zustand FAULT.

Zugriff auf die Registerkarte „SNMP“

Doppelklicken Sie auf das BMENUA0100-Modul in der Control Expert-Konfiguration, um auf die Registerkarte **SNMP** zuzugreifen.

Der SNMP-Agent kann zu 1 oder 2 SNMP-Managern eine Verbindung herstellen und mit ihnen kommunizieren. Der SNMP-Dienst umfasst Folgendes:

- Authentifizierungsprüfung durch das BMENUA0100-Modul hinsichtlich aller SNMP-Manager, die SNMP-Requests senden.
- Verwaltung von Ereignissen oder Traps.

Konfiguration des SNMP-Agenten in Control Expert und auf den Webseiten

Allgemeine SNMP-Parameter werden in Control Expert konfiguriert. Die Cybersicherheit betreffenden SNMP-Parameter werden auf den Webseiten des Moduls konfiguriert.

Wenn der Drehwahlschalter für die Cybersicherheit auf folgenden Wert eingestellt ist:

- Erweiterter (oder sicherer) Modus: Sie können den SNMP-Agent in Control Expert und auf den Webseiten des BMENUA0100-Moduls konfigurieren.

  HINWEIS: Im erweiterten (oder sicheren) Modus muss die SNMP-Version in Control Expert und auf der SNMP-Webseite, Seite 111 identisch konfiguriert werden. Wenn diese Einstellungen nicht übereinstimmen, wird der SNMP-Dienst nicht gestartet.

- Standardmodus: Sie können den SNMP-Agent nur in Control Expert konfigurieren.

  HINWEIS: Wenn das Modul in Control Expert für SNMP V3 konfiguriert ist:

  - Das BMENUA0100.2-Modul, ausgestattet mit einer Firmwareversion ab 2, betreibt SNMP V3 mit der Sicherheitsstufe NoAuthNoPriv.
  - Das BMENUA0100-Modul mit einer älteren Firmware als Version 2 betreibt SNMP V1.

SNMP-Parameter

Die Control Expert-Registerkarte **SNMP** enthält die folgenden Parameter. Sofern nicht anders angegeben, gelten die Parameter sowohl für SNMP V1 als auch für V3.

HINWEIS: Im erweiterten (oder sicheren) Modus muss die SNMP-Version in Control Expert und auf der SNMP-Webseite, Seite 111 identisch konfiguriert werden. Wenn diese Einstellungen nicht übereinstimmen, wird der SNMP-Dienst nicht gestartet.

Bereich	Parameter	Beschreibung	Wert
SNMP-Version	SNMP V1	Wählen Sie dies aus, um SNMP V1 zu verwenden.	Ausgewählt/Abgewählt
	SNMP V3	Wählen Sie dies aus, um SNMP V3 zu verwenden.	
IP-Adressmanager	IP-Adressmanager 1	Die IP-Adresse des ersten SNMP-Managers, an den der SNMP-Agent Benachrichtigungen aufgrund von Traps sendet.	Protokollabhängig (IPv4)
	IP-Adressmanager 2	Die IPv4-Adresse des zweiten SNMP-Managers, an den der SNMP-Agent Trap-Nachrichten sendet.	
Agent	Standort (SysLocation)	Position des betroffenen Geräts	31 Zeichen (maximal)
	Kontakt (SysContact)	Informationen zur Kontaktperson für die Gerätewartung	
	SNMP-Manager aktivieren	*Abgewählt* (Standard): Sie können die Parameter für den **Standort** und den **Kontakt** ändern. *Ausgewählt*: Sie können die Parameter für den **Standort** und den **Kontakt** nicht ändern.	Ausgewählt/Abgewählt
Community-Namen (nur SNMP V1)	Set	Passwort, das der SNMP-Agent zum Lesen von Befehlen von einem SNMP-Manager benötigt **HINWEIS:** Es gibt keine Standardeinstellung. Wenn ein SNMP-Manager verwendet wird, geben Sie denselben Community-Namen ein, der vom SNMP-Manager verwendet wird.	15 Zeichen (maximal)
	Get		
	Trap		

Bereich	Parameter	Beschreibung	Wert
Sicherheit (nur SNMP V1)	**Authentifizierungsfehler**-Trap aktivieren	*Abgewählt* (Standard): Nicht aktiviert. *Ausgewählt*: Aktiviert. Der SNMP-Agent sendet eine Trap-Nachricht an den SNMP-Manager, wenn ein nicht autorisierter Manager einen **Get**- oder **Set**-Befehl an den Agent sendet.	Ausgewählt/Abgewählt
SNMP-Benutzername (nur SNMP V3)		Der vom SNMP-Server erkannte Benutzername.	Zeichenfolge mit max. 32 Zeichen ASCII / UTF8 im Codierungsbereich [33-122]

Unterstützte Traps

Standardmäßig unterstützt der SNMP V1-Agent des BMENUA0100-Moduls folgende Traps:

- Linkup
- Linkdown

Der **Authentifizierungsfehler**-Trap wird ebenfalls unterstützt, wenn aktiviert.

SNMP MIB-II-Objektbezeichner

Unter dem **Anbieternamen** Schneider Electric weist das BMENUA0100-Modul die folgenden OID-Werte (Objektbezeichner) auf:

Objektname	OID	Wert
SysDesc	1.3.6.1.2.1.1.1	Produkt: BMENUA0100 - OPC UA-Kommunikationsmodul Firmware-ID: xx.yy
SysObjectID	1.3.6.1.2.1.1.2	1.3.6.1.4.1.3833.1.7.255.53
SysName	1.3.6.1.2.1.1.5	BMENUA0100
SysServices	1.3.6.1.2.1.1.7	74, was der Summe von (2_{7-1} + $_{24-1}$ + 2_{2-1}) entspricht und die Unterstützung von Protokollen in den folgenden OSI-Schichten anzeigt: • 7: Anwendungsschicht • 4: Transportschicht • 2: Datenverbindungsschicht
ifDesc	1.3.6.1.2.1.2.2.1.2	Diese OID enthält Informationen, die die Schnittstelle beschreiben, einschließlich Produktname und Portname.

Konfiguration der M580-Steuerungseinstellungen für OPC UA-Client-Server-Verbindungen

Einführung

In diesem Abschnitt werden die Einstellungen für die M580-Steuerungskonfiguration zur Unterstützung der Verbindungen zwischen dem OPC UA-Server im BMENUA0100-Modul und einen OPC UA-Client beschrieben.

Konfiguration der Sicherheitseinstellungen für die M580-Steuerung

Konfiguration der Steuerungsdienste

Aktivieren Sie zur Unterstützung der Kommunikation zwischen dem OPC UA-Server im BMENUA0100-Modul und einem OPC UA-Client die folgenden Einstellungen auf der Registerkarte „Sicherheit“ der M580-Steuerung:

- **TFTP**
- **DHCP / BOOTP**

Wenn diese beiden Dienste in der Steuerung nicht aktiviert sind, funktioniert die OPC UA-Kommunikation nicht ordnungsgemäß.

Diagnose

Übersicht

In diesem Kapitel werden die Diagnosetools beschrieben, die für das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server verfügbar sind.

Diagnose-LEDs

Diagnose über die LEDs auf dem Anzeigefeld

Nachfolgend ist der Status der LEDs auf dem Anzeigefeld, Seite 26 des BMENUA0100-Moduls für die verschiedenen Betriebszustände des Moduls aufgeführt.

HINWEIS: Der Status der **SECURE**-LED für den konfigurierten und den nicht konfigurierten Zustand des Moduls wird nachfolgend separat nach der ersten Beschreibung angezeigt.

Betriebszustand		**LED-Anzeigen**						
		RUN (Grün)	**UACNX (Grün/Rot)**	**ERR (Rot)**	**BS (Grün/Rot)**	**NS LED (Grün/Rot)**	**BUSY (Gelb)**	**SEC (Grün/Rot)**
Einschalt-sequenz	1	AUS	EIN	EIN	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Grün AUS Rot EIN
	2 (Alle LEDs EIN)	EIN	EIN	EIN	Grün EIN Rot EIN	Grün EIN Rot EIN	EIN	Grün EIN Rot EIN
	3 (Alle LEDs AUS)	AUS	AUS	AUS	Grün AUS Rot AUS	Grün AUS Rot AUS	AUS	Grün AUS Rot AUS
	4	EIN	AUS	EIN	Grün AUS Rot AUS	Grün AUS Rot AUS	AUS	Grün AUS Rot AUS
	5 (Autotest[1])	Blin-ken	Blinkt	Blinken	Grün Blinken Rot AUS	Grün Blinken Rot AUS	Blinken	Grün Blinken Rot AUS
Nicht konfiguriert		AUS	AUS	Blinken	Rot blinkend, wenn keine Verbindung zu einem Ethernet-Baugrup-penträger-Port besteht. Andernfalls blinkt die LED grün.	AUS, wenn kein Kabel angeschlos-sen ist und keine Verbindung zu einem anderen mit Spannung versorgten Gerät besteht. Andernfalls blinkt die LED grün.	AUS	Siehe LEDs für die Cybersi-cherheit unten, Seite 148.

Betriebszustand		**LED-Anzeigen**						
		RUN (Grün)	**UACNX (Grün/Rot)**	**ERR (Rot)**	**BS (Grün/Rot)**	**NS LED (Grün/ Rot)**	**BUSY (Gelb)**	**SEC (Grün/Rot)**
Konfiguriert	Nach der Erkennung einer doppelten IPv4-Adresse am Baugruppenträger-Port	Blinken	Siehe die Beschreibung der **UACNX**-LED unten, Seite 147.	/	Grün AUS Rot EIN	/	/	Siehe die Beschreibung der LED „Sicherer Kommunikationsstatus“ unten, Seite 148.
	Nach der Erkennung einer doppelten IPv4-Adresse am Steuerungsport	Blinken		/	/	Grün AUS Rot EIN	/	
	RUN-Zustand	EIN		AUS	Grün EIN Rot AUS	Leuchtet grün, wenn verbunden; Aus, wenn getrennt.	EIN, wenn eine Erfassung des Datenwörterbuchs läuft; Blinken bei Überlauf des Datenwörterbuchs; Andernfalls AUS.	
Spannungsversorgung aus		AUS	AUS	AUS	Grün AUS Rot AUS	Grün AUS Rot AUS	AUS	Grün AUS Rot AUS
Behebbarer Fehler oder inkonsistente Konfiguration[2]		/	/	EIN	/	/	/	/
Nicht behebbarer Fehler (Das Modul wird neu gestartet)		AUS	AUS	EIN	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Grün AUS Rot EIN

Betriebszustand		LED-Anzeigen						
		RUN (Grün)	**UACNX (Grün/Rot)**	**ERR (Rot)**	**BS (Grün/Rot)**	**NS LED (Grün/ Rot)**	**BUSY (Gelb)**	**SEC (Grün/Rot)**
Zurücksetzen der Cybersicherheit (oder Sicherheit)	Verarbeitung läuft	Blinken	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rot EIN	EIN	Grün AUS Rot AUS
	Abgeschlossen	EIN	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Grün AUS Rot AUS
Zurücksetzen der Cybersicherheit (oder Sicherheit) fehlt[3]		AUS	AUS	EIN	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Blinken Rot
Betriebssystemaktualisierung		Blinken	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rot EIN	EIN	Grün AUS Rot AUS

1. Der Autotest wird schnell durchgeführt und das Blinken der LED ist visuell nicht erfassbar.

   HINWEIS: Wenn sich das Modul weiterhin im Autotest-Zustand befindet, überprüfen Sie den Drehwahlschalter, um sicherzustellen, dass sich das Modul in einer gültigen Stellung befindet.

2. Siehe erkannte Fehlercodes von SERVICES_STATUS im T_BMENUA0100-DDT, Seite 149.

3. Dieser Zustand ergibt sich aus dem Wechsel des Drehwahlschalters vom Standard- in den erweiterten (oder sicheren) Modus oder vom erweiterten (oder sicheren) in den Standardmodus ohne Durchführung eines Resets der Cybersicherheit (oder Sicherheit), Seite 31 als Zwischenschritt.

   HINWEIS: In dieser Tabelle verweist „/“ auf einen beliebigen Zustand.

UACNX-LED, wenn sich das Modul im konfigurierten Zustand befindet

Die Farbe (rot oder grün) und der Status (blinkend oder leuchtend) beschreiben den Status der OPC UA-Verbindungen:

Datenwörterbuch-Status	OPC UA-Client-Verbindungsstatus	
	Kein OPC UA-Client verbunden	**Mindestens 1 OPC UA-Client verbunden**
Datenwörterbuch nicht verfügbar	Blinken Rot	Leuchten Rot
Datenwörterbuch verfügbar	Blinken Grün	Leuchten Grün

LED für sicheren Kommunikationsstatus, wenn Modul im konfigurierten/nicht konfigurierten Zustand

Nachfolgend wird der Status der **SECURE**-LED beschrieben, wenn sich das Modul im konfigurierten oder nicht konfigurierten Zustand befindet:

LED-Status	Beschreibung
AUS	Das Modul befindet sich nicht im sicheren Modus (d. h. der Drehwahlschalter befindet sich nicht in der Stellung „Secure“).
ROT	Es wurde ein sicherer Kommunikationsfehler erkannt. Beispielsweise ist keine Sicherheitskonfiguration vorhanden, ein Zertifikat ist ungültig, ein Zertifikat ist abgelaufen, die Kommunikation wurde angehalten usw.
GRÜN	Sichere Kommunikation ist aktiviert und läuft fehlerfrei. Ein Client ist mit dem Modul verbunden und das Modul hat eine gültige Cybersicherheitskonfiguration erhalten. Die Sitzung wird geöffnet und das Modul ist bereit, auf Client-Requests zu antworten.
ROT BLINKEN	Sichere Kommunikation ist aktiviert und läuft, es wurde jedoch ein Fehler erkannt. Ein Zertifikat ist beispielsweise abgelaufen, aber die Konfiguration autorisiert die Fortsetzung der Kommunikation.
GRÜN BLINKEN	Das Modul hat eine gültige Cybersicherheitskonfiguration erhalten und ist bereit, mit einem Client zu kommunizieren, der eine Kommunikation initiiert.

Diagnose über die LEDs des Steuerungsports

Die Steuerungsport-LEDs, Seite 27 können zur Diagnose des Status der Ethernet-Kommunikation über den Steuerungsport verwendet werden:

LED	Status	Beschreibung
ACT	Aus	Keine Verbindung aufgebaut.
	Grün	Verbindung aufgebaut, keine Aktivität.
	Blinken Grün	Verbindung hergestellt, Aktivität erkannt.
LNK	Aus	Keine Verbindung aufgebaut.
	Gelb	Verbindung aufgebaut mit einer Geschwindigkeit, die unter der max. Modulkapazität liegt (10/100 Mbit/s).
	Grün	Verbindung aufgebaut mit einer Geschwindigkeit, die der maximalen Modulkapazität entspricht (1.000 Mbit/s).

DDT BMENUA0100 (Derived Data Type: Abgeleiteter Datentyp)

Einführung

Jedes Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server, das Sie Ihrer Anwendung hinzufügen, instanziiert eine gemeinsame Gruppe von Datenelementen. Sie können die in der Control Expert-Software enthaltenen Tools verwenden, um auf diese Datenelemente zuzugreifen und eine Moduldiagnose durchzuführen.

HINWEIS:

- Die als Antwort auf einen Modbus-Request zurückgegebenen DDT-Daten dürfen 256 Byte nicht überschreiten.
- Angesichts der Struktur des Datenwörterbuchs von Control Expert müssen Requests für in Wortbits gespeicherte Daten vom anfordernden Client extrahiert werden.

Der Zugriff auf den DDT-Inhalt erfolgt über die Elementarfunktion READ_DDT, Seite 154 (EF) in der Control Expert-Software.
s

HINWEIS: Wenn der Modul-DDT aus einem beliebigen Grund nicht gelesen werden kann - z. B. wenn die IP-Adresse des Baugruppenträgers nicht ordnungsgemäß konfiguriert ist -, können Sie eine Moduldiagnose über die Modul-LEDs, Seite 144 durchführen.

Struktur des DDT T_BMENUA0100

Der DDT BMENUA0100 umfasst folgende Elemente:

Element	Typ	Adresse	Beschreibung
DEVICE_NAME	STRING [16]	MW1...8	Name des Moduls.
CONTROL_PORT_IPV6	STRING [44]	MW9...30	Steuerungsport IPv6 / Länge des Subnetz-Präfixes.
CONTROL_PORT_IPV4	STRING [18]	MW31...39	Steuerungsport IPv4 / Länge des Subnetz-Präfixes.
CONTROL_PORT_GTW	STRING [16]	MW40...47	Standard-Gateway des Steuerungsports.
ETH_BKP_PORT_IPV4	STRING [18]	MW48...56	Baugruppenträger-Port IPv4 / Länge des Subnetz-Präfixes.

Element	Typ	Adresse	Beschreibung
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	• 0: Die Steuerungsport-Verbindung ist nicht betriebsbereit. • 1: Die Steuerungsport-Verbindung ist betriebsbereit.
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0: Die Verbindung zum Baugruppenträger-Port ist nicht betriebsbereit. • 1: Die Verbindung zum Baugruppenträger-Port ist betriebsbereit.
GLOBAL_STATUS	BOOL	MW57.2	• 0: Das Modul ist nicht betriebsbereit. • 1: Das Modul ist betriebsbereit.
NETWORK_HEALTH	BOOL	MW57.3	• 0: Netzwerküberlast erkannt. • 1: Das Netzwerk funktioniert normal.
Reserviert	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	Siehe nachstehende Details.
DATA_DICT	BYTE	MW58[0]	• 1: Nicht verfügbar. Mögliche Ursachen: ◦ Die Datenwörterbuch-Funktion ist in der Control Expert-Anwendung nicht verfügbar oder aktiviert und kann nicht in die Steuerung integriert werden. ◦ Das Datenwörterbuch wird im OPC UA-Server geladen/durchsucht. • 2: Verfügbar, z. B.: ◦ Das Laden/Durchsuchen des Datenwörterbuchs durch den OPC UA-Server wurde erfolgreich abgeschlossen. ◦ Es wird ggf. gerade ein Vorladevorgang (gemäß den Projekteinstellungen des Control Expert-Datenwörterbuchs) ausgeführt. • 4: Bereits aktiv. • 8: Überlauf des Datenwörterbuchs.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Dauer der letzten Erfassung (0 bis 255 Sekunden). **HINWEIS:** Der Wert 255 gibt eine Zeitdauer von mindestens 255 Sekunden an.
CONNECTED_CLIENTS	BYTE	MW59[0]	Anzahl der verbundenen OPC UA-Clients.

Element	Typ	Adresse	Beschreibung
DATA_DICT_PRELOAD_ DURATION	BYTE	MW59[1]	Dauer des letzten Vorladevorgangs des Datenwörterbuchs (0 bis 255 Sekunden). **HINWEIS:** Sie können die in diesem Element enthaltenen Informationen verwenden, um die Einstellung **Timeout bei der Generierung von Änderungen** im Konfigurationsfenster **Extras > Projekteinstellungen > Allgemein > In SPS eingebettete Daten** anzupassen und zu optimieren. Informationen zur Konfiguration dieser Einstellung finden Sie in der Online-Hilfe von Control Expert.
SERVICE_LEVEL	BYTE	MW60[0]	• 0: Keine • 2: Nicht-transparenter („Warm“-) Redundanzmodus • 3: Nicht transparenter („Hot") Redundanzmodus
SERVICE_LEVEL	BYTE	MW60[1]	OPC UA-Serverfunktionsfähigkeit, Seite 161, abhängig von der Daten- und Dienstqualität.
Reserviert	WORD	MW61	–
SERVICES_STATUS	T_ SERVICES _STATUS	MW62...68	Siehe nachstehende Details.
NTP_CLIENT_SERVICE	BYTE	MW62[0]	NTP-Clientstatus: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode: ◦ 1 = Ungültige Zeit (Uhrzeit nie aktualisiert). ◦ 2 = Zeiteinholung (Die Serverzeit hat sich um ein Offset von mindestens 1000 Sekunden erhöht oder verringert. Die Neusynchronisation des BMENUA0100-Moduls kann bis zu 5 Minuten dauern.). ◦ 4 = Der NTP-Server ist nach wie vor erreichbar, synchronisiert den Client jedoch nicht. Wenn der NTP-Server den Betrieb wieder aufnimmt, wird der erkannte Fehler automatisch behoben. Dies kann bis zu 1024 Sekunden dauern.
NTP_SERVER_SERVICE	BYTE	MW62[1]	NTP-Serverstatus • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode - nur erweiterter (oder sicherer) Modus: ◦ 1 = Steuerungsport nicht konfiguriert ◦ 2 = NTP-Client des Baugruppenträgers und Servers aktiviert auf den Webseiten

Element	Typ	Adresse	Beschreibung
SNMP_SERVICE	BYTE	MW63[0]	SNMP-Serverstatus: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bit 1 (SNMP V1): 0 = SNMP nicht konfiguriert / 1 = SNMP konfiguriert • Bits 1 und 2: (SNMP V3): 00 = SNMP nicht konfiguriert / 11 = SNMP konfiguriert • Bits 4 bis 7: Fehlercode: ◦ 1 = SNMP ist im erweiterten (oder sicheren) Modus aktiviert, und in Control Expert (0.0.0.0) ist keine SNMP-IP-Adresse definiert.
Reserviert	BYTE	MW63[1]	–
WEB_SERVER	BYTE	MW64[0]	Status des Webservers: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode: ◦ 1 = Nicht behebbarer Fehler
FW_UPGRADE	BYTE	MW64[1]	Status der Firmwareaktualisierung: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode: ◦ 1 = Ungültiges Firmwarepaket ◦ 2 = Letzte Firmwareaktualisierung fehlgeschlagen (wird als nicht behebbarer Fehler verwaltet)
Reserviert	BYTE	MW65[0]	–
Reserviert	BYTE	MW65[1]	–
CONTROL_EXPERT_IP_ FORWARDING	BYTE	MW66[0]	Status der IP-Weiterleitung in Control Expert: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur erweiterter (oder sicherer) Modus): ◦ 1 = Steuerungsport nicht konfiguriert **HINWEIS:** Bei Modulen ab Firmwareversion 2.01 wird der Wert dieses Elements auf 0 forciert.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Status der Weiterleitung von Steuerung zu Steuerung: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur erweiterter (oder sicherer) Modus): ◦ 1 = Steuerungsport nicht konfiguriert **HINWEIS:** Bei Modulen ab Firmwareversion 2.01 wird der Wert dieses Elements auf 0 forciert.

Element	Typ	Adresse	Beschreibung
IPSEC	BYTE	MW67[0]	IPsec-Status: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur erweiterter (oder sicherer) Modus): ◦ 1 = Steuerungsport nicht konfiguriert
Reserviert	BYTE	MW67[1]	–
EVENT_LOG_SERVICE	BYTE	MW68[0]	Status des Ereignisprotokollierungsdienstes: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur erweiterter (oder sicherer) Modus): ◦ 1 = Fehler im Dienstereignisprotokoll ◦ 2 = Fehler in der Ereignisprotokollkonfiguration
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Status des Protokollservers: • Bit 0: 0 = Bestätigung vom Syslog-Server empfangen / 1 = Keine Bestätigung vom Syslog-Server empfangen
FW_VERSION	T_FW_ VERSION	MW69...72	Firmwareversion des Moduls. Siehe nachstehende Details.
MAJOR_VERSION	WORD	MW69	Firmware-Hauptversion.
MINOR_VERSION	WORD	MW70	Firmware-Nebenversion.
INTERNAL_REVISION	WORD	MW71	Interne Firmware-Revision.
Reserviert	WORD	MW72	–
CONTROL_PORT_STATUS	BYTE	MW73[0]	IPv4-Status des Steuerungsports: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur erweiterter (oder sicherer) Modus): ◦ 1 = Ungültige IP ◦ 2 = Doppelte IP
Reserviert	BYTE	MW73[1]	–
IN_PACKETS_RATE	UINT	MW74	Anzahl der Pakete, die pro Sekunde an allen Ethernet-Schnittstellen empfangen werden.
IN_ERROR_COUNT	UINT	MW75	Anzahl der eingehenden Pakete mit Fehlern seit dem letzten Reset (Modulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Anzahl der pro Sekunde an allen Ethernet-Schnittstellen ausgegebenen Pakete.
OUT_ERROR_COUNT	UINT	MW77	Anzahl der ausgehenden Pakete mit Fehlern seit dem letzten Reset (Modulo 65535).

Element	Typ	Adresse	Beschreibung
MEM_USED_PERCENT	BYTE	MW78[0]	Vom OPC UA-Server verwendeter Prozentsatz des internen RAM.
CPU_USED_PERCENT	BYTE	MW78[1]	Verwendeter Prozentsatz des internen Prozessors.
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Cybersicherheitsstatus. Siehe nachstehende Details.
SECURE_MODE	BYTE	MW79[0]	• 0: Das Modul läuft im Standardmodus. • 1: Das Modul läuft im erweiterten (oder sicheren) Modus.
CYBERSECURITY_STATE	BYTE	MW79[1]	Cybersicherheitsstatus: • 0: Erweiterter (oder sicherer) Modus AUS. (**SECURE**-LED AUS) • 1: Eine sichere Kommunikation ist aktiviert und verläuft fehlerfrei. (**SECURE**-LED GRÜN) • 2: Kommunikationsbereit. (**SECURE**-LED BLINKT GRÜN) • 3: Sichere Kommunikation verläuft mit geringfügigen Fehlern. (**SECURE**-LED BLINKT ROT) • 4: Sichere Kommunikation wurde aufgrund eines kritischen Fehlers angehalten. (**SECURE**-LED ROT)
IPSEC_CHANNELS	BYTE	MW80[0]	Anzahl der geöffneten IPsec-Kanäle.
Reserviert	BYTE	MW80[1]	–

Konfiguration der Elementarfunktion READ_DDT

Überblick

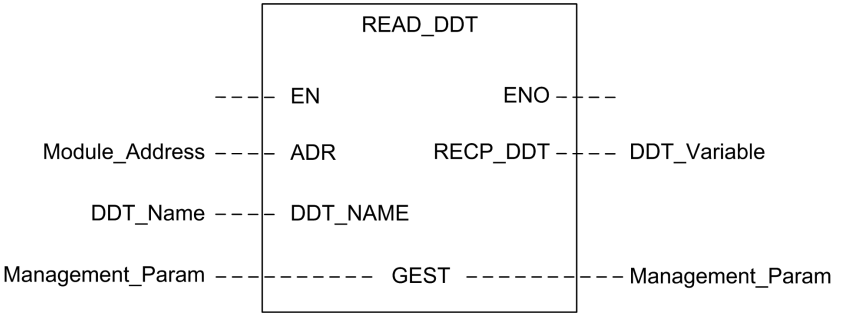
Verwenden Sie den Funktionsbaustein `READ_DDT` zur Konfiguration des Lesens von Nachrichten für das BMENUA0100-Kommunikationsmodul.

Die `ADR`-, `DDT_NAME`- und `GEST`-Parameter definieren den Vorgang.

`EN` und `ENO` können als zusätzliche Parameter konfiguriert werden.

HINWEIS: Informationen zur Verwendung dieses Funktionsbausteins in einem Hot Standby-System finden Sie im Abschnitt Asynchrone Kommunikationsfunktionsbausteine (siehe *Modicon M580 Hot Standby - Häufig verwendete Architekturen - Systemhandbuch*).

Darstellung in FBD



Eingangsparameter

Parameter	Datentyp	Beschreibung
EN	BOOL	Dieser Parameter ist optional. Wenn dieser Eingang auf 1 gesetzt wird, ist der Funktionsbaustein aktiviert und kann den Algorithmus des Funktionsbausteins auflösen. Wenn dieser Eingang auf Null gesetzt wird, wird der Baustein deaktiviert und löst den Funktionsbausteinalgorithmus nicht auf.
ADR	Beliebiges Array von INT	Array, das die Adresse der Zieleinheit des Austauschvorgangs enthält. Die Adresse ist das Ergebnis der ADDMX-Funktion. (Beispiel: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) zeigt das Modul an der IP-Adresse 192.168.10.2 mit UnitId 100 (lokaler Server des Moduls), verbunden mit dem integrierten Ethernet-Port.
DDT_NAME	STRING	Der Name des zu lesenden DDT: T_BMENUA0100

Eingangs-/Ausgangsparameter

Das GEST-Array ist lokal:

<table>
<tr><th>Parame-ter</th><th>Datentyp</th><th colspan="3">Beschreibung</th></tr>
<tr><td rowspan="2">GEST</td><td rowspan="2">Array [0...3] of INT</td><td colspan="3">Die Verwaltungsparameter bestehen aus vier Wörtern. Siehe das Hilfethema in Control Expert Struktur der Verwaltungsparameter (siehe EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek) für weitere Informationen zu diesen Parametern.</td></tr>
<tr><td>Wort-nr.</td><td>Höherwertiges BYTE</td><td>Niederwertiges BYTE</td></tr>
</table>

Parame-ter	Datentyp	Beschreibung		
		0	Austauschnummer	Aktivitätsbit: Rang 0 Abbruchbit: Rang 1 Bit für Sofortquittierung: Rang 2
		1	Betriebsrückmeldung (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*)	Kommunikationsrückmeldung (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*)
		2	Timeout (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*)	
		3	Länge (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*)	

Ausgangsparameter

Parameter	Datentyp	Beschreibung
ENO	BOOL	Dieser Parameter ist optional. Wenn Sie diesen Ausgang auswählen, erhalten Sie auch den EN-Eingang. Der ENO-Ausgang wird bei erfolgreicher Ausführung des Funktionsbausteins aktiviert.
RECP_DDT	Alle	Empfangspuffer. Es kann eine Variable vom Typ DDT verwendet werden. In der Beschreibung des T_BMENUA0100-DDT, Seite 149 finden Sie den Inhalt dieses DDT. Die Länge der empfangenen Daten (in Byte) wird automatisch vom System in das vierte Wort der Verwaltungstabelle geschrieben.

Asynchroner Kommunikationsfunktionsbaustein

In einer Hot Standby-Anwendung nimmt der asynchrone Kommunikationsfunktionsbaustein READ_DDT während eines Umschaltereignisses den Betrieb in der neuen primären Steuerung nicht automatisch wieder auf, es sei denn, er wurde speziell konfiguriert, wie nachfolgend beschrieben.

Anhand des nachstehenden Verfahrens können Sie festlegen, dass die asynchronen Kommunikations-EFBs den Betrieb im Anschluss an eine Umschaltung automatisch wieder aufnehmen:

- Programmieren Sie Ihre Anwendung so, dass nicht alle EFB-Instanzen mit der Standby-Steuerung ausgetauscht werden. Heben Sie dazu die Auswahl des Attributs **Austausch auf STBY** für die EFB-Instanz auf.

Überlegungen bei der Konfiguration der Funktion

Beachten Sie Folgendes bei Verwendung der EF READ_DDT:

- Wenn in Ihrer Anwendung mehr als ein BMENUA0100-Modul in einem Rack vorhanden ist, verwenden Sie separate Instanzen eines WORD-Arrays für jeden GEST-Pin. Jeder Baustein verwaltet ein eigenes WORD-Verwaltungsarray.
- Sie müssen in GEST[3] keinen Wert für den Längenparameter angeben, da keine Daten zu senden sind. Am Ende des Vorgangs (wenn das Aktivitätsbit in GEST[0] auf 0 gesetzt ist) wird die Länge mit der Länge der in den Ausgangsparameter RECP_DDT kopierten Daten festgelegt, wenn in GEST[1] oder mit einem zusätzlichen Statuscode kein Fehler gemeldet wird. Siehe das Hilfethema in Control Expert *Fehlercodes der EFBs mit STATUS-Parameter* (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*) für eine Beschreibung dieser zusätzlichen Statuscodewerte.
- Der Timeout-Wert 0 gibt an, dass kein Timeout vorliegt. In diesem Fall wird eine während des Austauschvorgangs auftretende Kommunikationsverzögerung oder ein Kommunikationsverlust nicht erkannt. Der Parameter RECP_DDT behält seinen vorherigen Wert bei. Um dieses Szenario zu vermeiden, setzen Sie den Timeout auf einen Wert ungleich Null.
- Im Falle der Betriebsrückmeldung 16#01 (Request nicht verarbeitet) oder 16#02 (Falsche Antwort) im Wort GEST[1] der Verwaltungstabelle kann ein zusätzlicher Statuscode im Längenparameter (GEST[3]) gemeldet werden. Die in diesem Feld zurückgegebenen Statuscodes entsprechen einem Teilbereich der möglichen STATUS-Parametercodes der Kommunikations-EFBs. Mögliche Werte für READ_DDT sind 30ss hex und 4001 hex. Siehe das Hilfethema in Control Expert *Fehlercodes der EFBs mit STATUS-Parameter* (siehe *EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek*) für eine Beschreibung dieser zusätzlichen Statuscodewerte.
- Je nach dem im Parameter DDT_NAME angegebenen DDT werden einige Konsistenzprüfungen für die empfangenen Daten durchgeführt. Wird eine Abweichung festgestellt, dann wird im Betriebsrückmeldungsbyte (dem höherwertigen Byte von GEST[1]) der Code 16#02 (Falsche Antwort) gesetzt. Beachten Sie, dass der Baustein die Gültigkeit des Datentyps der als Empfangspuffer konfigurierten Variablen (RECP_DDT) nicht überprüft. Stellen Sie sicher, dass der Datentyp der mit dem Parameter RECP_DDT verknüpften Variablen mit dem Typ der empfangenen Daten übereinstimmt.

⚠WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Vergewissern Sie sich, dass die dem Ausgangsparameter RECP_DDT zugeordnete Variable vom Typ DDT dem Typ der in den Empfangspuffer geschriebenen Daten entspricht.
- Überprüfen Sie, ob die im ADR-Parameter festgelegte Adresse dem richtigen Modul entspricht, insbesondere, wenn mehrere identische Module im gleichen Netzwerk konfiguriert sind.

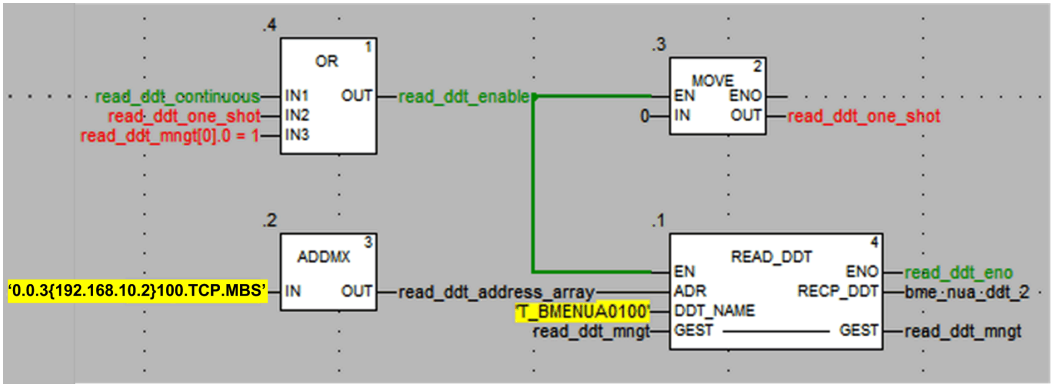
Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Konfiguration der Elementarfunktion READ_DDT

Um die Elementarfunktion READ_DDT zu konfigurieren, führen Sie die folgenden Schritte aus:

Schritt	Aktion
1	Legen Sie die Adresse des Zielgeräts in ADR fest (verwenden Sie einen ADDM-Funktionsbaustein, um diese Adresse in einem expliziten Zeichenfolgenformat anzugeben).
2	Legen Sie den Parameter DDT_NAME mit dem Namen des zu lesenden DDT fest.
3	Rufen Sie die Funktion READ_DDT zum Starten der Kommunikation auf (wobei der EN-Eingangspin auf 1 gesetzt sein muss, sofern konfiguriert).
4	Überwachen Sie das Aktivitätsbit (im niederwertigen Byte des Parameters GEST[0]), bis die Kommunikation abgeschlossen ist (das Aktivitätsbit wird vom System nach Beendigung der Kommunikation auf 0 gesetzt). Führen Sie diese Funktion nur einmal aus, um zu verhindern, dass die Statuswerte gelöscht werden. Beispielsweise führt das Setzen des EN-Pins auf 0 während des Betriebs dazu, dass die Funktion erneut aufgerufen wird.
5	Prüfen Sie die Rückmeldungsparameter in GEST[1]. Wenn die Rückmeldung 16#0000 ist, wurde der RECP_DDT-Puffer mit empfangenen Daten gefüllt. Die Größe der empfangenen Daten (in Byte) wird in das vierte Wort (GEST[3]) der Verwaltungstabelle geschrieben.

READ_DDT-EF - Beispiel



In diesem Beispiel wird die READ_DDT-EF ggf. gestartet:

- Kontinuierlich durch Setzen der Variablen read_ddt_continuous.

  HINWEIS: Bei einem erkannten Fehler können Rückmeldungscodes im zweiten Wort der Variablen read_ddt_mngt nicht gelesen werden.

- Nur einmal, durch Setzen der Variablen read_ddt_one_shot.

Konfiguration der elementaren Funktion READ_NUA_DDT

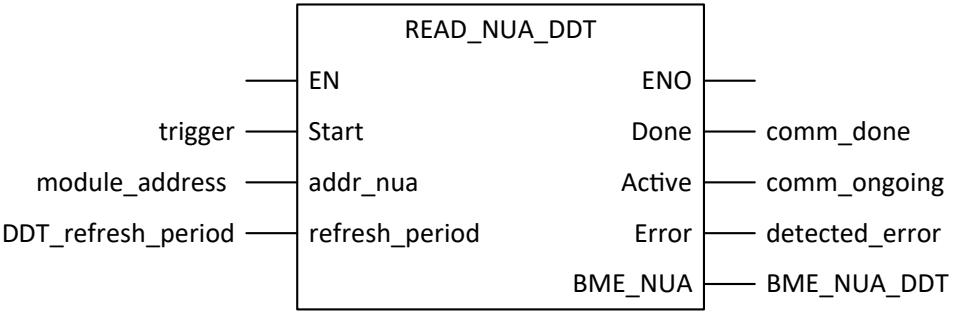
Verwenden Sie den Funktionsbaustein `READ_NUA_DDT` für den Zugriff auf die Diagnoseinformationen des BMENUA0100-Moduls.

Die `Start`-, `addr_nua`- und `refresh_period`-Eingangsparameter definieren den Vorgang.

Als zusätzliche Parameter können EN und ENO konfiguriert werden.

HINWEIS: Informationen zur Verwendung dieses Funktionsbausteins in einem Hot Standby-System finden Sie im Abschnitt Asynchrone Kommunikationsfunktionsbausteine (siehe *Modicon M580 Hot Standby - Häufig verwendete Architekturen - Systemhandbuch*).

Darstellung in FBD



Eingangsparameter

Parameter	Datentyp	Beschreibung
EN	BOOL	Dieser Parameter ist optional. Wenn dieser Eingang auf 1 gesetzt wird, ist der Funktionsbaustein aktiviert und kann den Algorithmus des Funktionsbausteins auflösen. Wenn dieser Eingang auf Null gesetzt wird, wird der Baustein deaktiviert und löst den Funktionsbausteinalgorithmus nicht auf.
Start	BOOL	Das Lesen des BMENUA0100-DDT erfolgt kontinuierlich.
addr_nua	string[32]	Adresse des BMENUA0100-Moduls, das ADDMX() zum Lesen übergeben wird. Zeichenfolge fester Länge, die die Adresse des Ziel-BMENUA0100 enthält. Die Adresse ist das Ergebnis der ADDMX-Funktion. (Beispiel: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) zeigt das Modul an der IP-Adresse 192.168.10.2 mit UnitId 100 (lokaler Server des Moduls), verbunden mit dem integrierten Ethernet-Port.
refresh_period	TIME	Aktualisierungszeitraum des DDT.

Ausgangsparameter

Parameter	Datentyp	Beschreibung
ENO	BOOL	Dieser Parameter ist optional. Wenn Sie diesen Ausgang wählen, erhalten Sie auch den EN-Eingang. Der ENO-Ausgang ist nach der erfolgreichen Ausführung des Funktionsbausteins aktiviert.
Fertig	BOOL	Die Kommunikation ist abgeschlossen.

Parameter	Datentyp	Beschreibung
Aktiv	BOOL	Die Kommunikation läuft.
Fehler	BOOL	Fehler am Kommunikationsfunktionsbaustein erkannt.
BME_NUA	T_BMENUA0100	Der BMENUA0100-DDT, Seite 149, der unverändert verwendet werden kann.

OPC UA-Diagnose

Einführung

Das BMENUA0100-Modul weist sowohl OPC UA-Server-Variablen als auch spezifische Datenelemente (DataItems) auf, die zur Identifizierung der im Modul ausgeführten Anwendung und zur Diagnostizierung von Modulvorgängen verwendet werden können.

OPC UA - Variable SERVICE_LEVEL

Die Variable SERVICE_LEVEL stellt einem Client Informationen zum Status der Steuerung und zur Funktionsfähigkeit des OPC UA-Servers zur Verfügung. Der Zugriff auf die Variable SERVICE_LEVEL erfolgt direkt unter der OPC UA-Server-Knotenstruktur. Die Variable SERVICE_LEVEL ist ebenfalls im Element OPCUA_STATUS.SERVICE_LEVEL des BMENUA0100-Modul-DDT, Seite 149 dupliziert und kann programmgesteuert durch Ausführen der Elementarfunktion READ_DDT, Seite 154 aufgerufen werden, wenn sich die Anwendung im Zustand RUN befindet.

HINWEIS:

- In redundanten Architekturen muss der OPC UA-Client die SERVICE_LEVEL-Variable sowohl im primären als auch im Standby-BMENUA0100-Modul überwachen, um den Redundanzmechanismus zu verwalten. Wenn der Client erkennt, dass der SERVICE_LEVEL-Wert des Standby-Moduls größer ist als der SERVICE_LEVEL-Wert des primären Moduls, muss der Client eine Umschaltung vom primären zum Standby-Modul auslösen.
- Der SERVICE_LEVEL muss während des Betriebs stets vom SCADA-System überwacht werden, um die ordnungsgemäße Funktionsfähigkeit des OPC UA-Servers sicherzustellen.

Die folgenden Variablen auf Dienstebene (Service Level) gelten für alle Firmwareversionen des BMENUA0100-Moduls, ausgenommen wie angegeben:

SERVICE_LEVEL-Wert	Status Steuerung / OPC UA-Server	
	Firmware = V1.0	**Firmware ≥ V1.1**
0	BMENUA0100 ist in der Bootphase. Die Steuerung befindet sich im Zustand NOCONF (Keine Konfiguration) oder ERROR (Fehler). Beispiel für den Zustand ERROR: Die MAST-Task befindet sich im HALT-Zustand.	
1	Der OPC UA-Server wurde gestartet. Das Durchsuchen der Datenwörterbuch-Liste wird ausgeführt.	
5	Das Durchsuchen des Datenwörterbuchs wurde gestartet.	
10	Überlauf der Datenwörterbuch-Größe.	
20	Das Durchsuchen des Datenwörterbuch-Typs wird ausgeführt.	
50	Das Durchsuchen der Datenwörterbuch-Variable wird ausgeführt.	
100	Das Durchsuchen des Datenwörterbuchs ist abgeschlossen. Das Auslesen des Steuerungsstatus läuft. Der Adressraum wird mit dem neuen Inhalt des Datenwörterbuchs aktualisiert.	
120[1]	Steuerung im STOP-Zustand.	Steuerung im Zustand STOP STANDBY oder HALT STANDBY (nur Hot Standby-Steuerung)
150[1]	Steuerung im Zustand WAIT STANDBY (nur Hot Standby-Steuerung)	
199[1]	Steuerung im Zustand RUN STANDBY (nur Hot Standby-Steuerung)	
202[2]	<Nicht zutreffend>	Nur Standalone-Steuerung: Steuerung befindet sich im Zustand STOP STANDALONE. Nur Hot Standby-Steuerung: Wenn sich beide Steuerungen im STOP- oder HALT-Zustand befinden, wird ein BMENUA0100 als Master mit Dienstebene = 202 deklariert. Der Adressraum ist OK und nutzbar.
255	Steuerung im RUN-Modus (oder RUN PRIMARY für Hot Standby-Steuerung). OPC UA-Server ist voll funktionsfähig.	

1. Dieser Wert muss nicht festgelegt werden, bevor der Server betriebsbereit wird.

2. Diese Dienstebene gilt nur für BMENUA0100 mit einer Firmware ab V1.10.

HINWEIS: Je größer das Datenwörterbuch, umso länger ist die Erfassungszeit des Datenwörterbuchs (d. h. die Zeit, die das Modul benötigt, um das Datenwörterbuch zu durchsuchen und zu laden). Während der Erfassung des Datenwörterbuchs behält SERVICE_LEVEL den Wert 100 bei, bis die Erfassung abgeschlossen ist. Wenn eine Generierungsänderung in Control Expert durchgeführt wird, bei der ein neues Datenwörterbuch generiert wird, startet der OPC UA-Server den Prozess des Durchsuchens des Datenwörterbuchs neu. Während dieses Prozesses können Aktualisierungen der überwachten Elemente angehalten werden, wobei die Werte der überwachten Elemente auf ihrem zuletzt aktualisierten Wert eingefroren werden.

Variablen des OPC UA-Servers

Sie können diese Variablen online mit einem OPC UA-Clientgerät wie dem Tool UaExpert von Unified Automation anzeigen. Navigieren Sie in der OPC UA-Server-Knotenstruktur zu **Serverstatus > Generierungsinfos**, um die folgenden OPC UA-Server-Variablen anzuzeigen:

Variable	Beschreibung
BuildDate	Das Datum, an dem die Anwendung in der Steuerung generiert wurde.
BuildNumber	Die Nummer des aktuellen Builds der Steuerungsanwendung.
ManufacturerName	„Schneider Electric“.
ProductName	“BMENUA0100”.
ProductUri	Dieerem Modul zugewiesene eindeutige Uniform Resource Identifier.
SoftwareVersion	Die Version der Modul-Firmware.

OPC UA-spezifische DataItems

Das BMENUA0100-Modul unterstützt die folgenden spezifischen DataItems. Der Zugriff auf diese DataItems erfolgt über den OPC UA-Server-Stack. Diese DataItems gleichen zwar den Steuerungsdatenelementen, die über die Control Expert-Software erreicht werden können, sind jedoch nicht mit Steuerungssymbolen verknüpft und nicht über die Control Expert-Software erreichbar:

DataItem	Datentyp	Standardwert	Beschreibung
#AddressSpaceState	INT16	0	Der Status des Adressraums mit seiner Auflistung von Objekten und Knoten. Mögliche Werte: **0.** Leer **1.** Generiert **2.** Wird aktualisiert **3.** Teilweise generiert (in der Anwendung ist kein Datenwörterbuch vorhanden oder Datenwörterbuch-Überlauf)
#ApplicationName	STRING	0	Der Name der Steuerungsanwendung.
#ApplicationVersion	STRING	0	Die Version der Steuerungsanwendung.
#CurrentDataDictionaryItemsCount	INT32	0	Die Anzahl der Elemente im Datenwörterbuch, die in den Server geladen wurden.
#CurrentMonitoredItemsCount	INT32	0	Die Anzahl der vom Server überwachten Elemente.
#DeviceIdentity	STRING	0	Der Name der Steuerungsreferenz.
#PLCDatadicReady	BYTE	1	Überwacht den Ladestatus des Datenwörterbuchs der Steuerung: 1. Das Steuerungsdatenwörterbuch ist nicht verfügbar. Mögliche Erklärungen: • Die Datenwörterbuch-Funktion ist in der Control Expert-Anwendung nicht verfügbar oder aktiviert und kann nicht in die Steuerung integriert werden. • Das Laden/Durchsuchen des Datenwörterbuchs wird im OPC UA-Server ausgeführt. 2. Das Steuerungsdatenwörterbuch ist verfügbar, z. B.: • Das Laden/Durchsuchen des Datenwörterbuchs durch den OPC UA-Server wurde erfolgreich abgeschlossen. • Zurzeit wird ggf. ein Vorladevorgang (gemäß den Projekteinstellungen des Control Expert-Datenwörterbuchs) ausgeführt.
#PLCQualStatus	INT16	0	Überwacht den Kommunikationsstatus einer Steuerung. Mögliche (hex.) Werte: • 00C0 hex.: Die Kommunikation mit der Steuerung ist korrekt.

DataItem	Datentyp	Standardwert	Beschreibung
			• 0040 hex.: Keine Kommunikation mit der Steuerung über einen Zeitraum, der kleiner ist als der Geräte-Timeout (5 s). • 0 hex.: Steuerung nicht identifiziert.
#TSEventItemsReady	BOOL	0	Ein schreibgeschütztes Element, das angibt, ob an der Quelle zeitgestempelte Variablen und an der Quelle zeitgestempelte Geräte in der M580-Steuerungsanwendung durchsucht wurden: • 0 = Nicht durchsucht • 1 = Durchsucht **HINWEIS:** Dieses Element ist nur von Bedeutung, wenn die Zeitstempelung in Control Expert und für das spezifische BMENUA0100-Modul aktiviert ist.
#TSEventSynchro	BOOL	0	Ein Element mit Lese-/Schreibzugriff, das, wenn es aktiviert ist, jedes Mal, wenn ein Schreibvorgang ausgeführt wird, einen synchronisierten Wert an alle Quellzeitstempelgeräte sendet, die mit der M580-Steuerung verbunden sind. Der Zweck besteht darin, alle überwachten Elemente mit Zeitstempel mit ihren Werten zu initialisieren. • 0 = Warten auf Aktivierung • 1 = Aktiviert **HINWEIS:** • Der Wert dieses Elements wird als 0 angezeigt. Der Wert 1 wird nicht berücksichtigt, da er nur kurzzeitig vorhanden ist und wieder auf den erwarteten Aktivierungswert 0 zurückgesetzt wird. • Dieses Element ist nur von Bedeutung, wenn die Zeitstempelung in Control Expert und für das spezifische BMENUA0100-Modul aktiviert ist.

Syslog

Einführung

Das Modul BMENUA0100 protokolliert Ereignisse in einem lokalen Diagnosepuffer und sendet dann eine Aufzeichnung dieser Ereignisse an einen dezentralen Syslog-Server, wo sie gespeichert und den Syslog-Clients zur Verfügung gestellt werden. Um vorherige Ereignisse zu diagnostizieren, können Sie die Syslog-Serverereignisdatensätze abfragen.

Für laufende Modulereignisse können Sie die Modul-Webseiten, Seite 168 verwenden, um den Status des Syslog-Dienstes zu diagnostizieren und um bestimmte Ereignisse im Diagnosepuffer anzuzeigen.

Der lokale Puffer arbeitet wie ein Ringpufferspeicher, wobei die letzten Ereignisse die ältesten Ereignisse überschreiben und ersetzen, wenn der Puffer voll ist.

Das Modul speichert Ereignisse im flüchtigen Speicher.

Die protokollierten Ereignisse beziehen sich entweder auf:

- Sicherheit/Autorisierung, Seite 167

  – ODER –

- Größere Änderungen im System (Protokoll-Audit), Seite 168

Der Syslog-Dienst ist im Rahmen der Cybersicherheitskonfiguration auf den Webseiten, Seite 102 konfigurierbar und kann daher nur aktiv sein, wenn sich das Modul im erweiterten (oder sicheren) Modus befindet. Wenn das Modul im Standardmodus ausgeführt wird, ist der Dienst deaktiviert.

Gemäß der Implementierung im BMENUA0100 -Modul, wird Syslog von IPv4 (ab Firmwareversion 1.0) und IPv6 (ab Firmwareversion 1.10) unterstützt.

HINWEIS: Syslog ist kein nativ sicheres Protokoll, muss jedoch in einem sicheren IPsec, Seite 109-Kanal über den Steuerungsport gekapselt werden.

Syslog-Nachrichtenstruktur

Das Syslog-Protokoll - RFC 5424 - definiert, wie Ereignisse zwischen dem Modul und dem dezentralen Server ausgetauscht werden. Die Struktur der Syslog-Nachrichten ist nachfolgend dargestellt:

<table>
<tr><th>Bereich</th><th>Beschreibung</th></tr>
<tr><td>PRI</td><td>Informationen zu Anlage und Schweregrad (eine Beschreibung finden Sie in den folgenden Tabellen).</td></tr>
<tr><td>VERSION</td><td>Version der syslog-Protokollspezifikation (Version = 1 für RFC 5424).</td></tr>
<tr><td>TIMESTAMP</td><td>Das Zeitstempelformat wird ausgegeben von RFC 3339 unter Verwendung des folgenden ISO8601-konformen Internet-Datums-/Uhrzeitformats: YYY-MM-DDThh:mm:ss.nnnZ
HINWEIS: -, T, :, . , 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:
<table><tr><td>YYY</td><td>Jahr</td></tr><tr><td>MM</td><td>Monat</td></tr></table></td></tr>
</table>

<table>
<tr><th>Bereich</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><td>DD</td><td>Tag</td></tr>
<tr><td>hh</td><td>Stunde</td></tr>
<tr><td>mm</td><td>Minute</td></tr>
<tr><td>ss</td><td>Sekunde</td></tr>
<tr><td>nnn</td><td>Bruchteil einer Sekunde in Millisekunden (0, wenn nicht verfügbar)</td></tr>
</table>
</td></tr>
<tr><td>HOSTNAME</td><td>Identifiziert den Computer, der die syslog-Nachricht ursprünglich gesendet hat: Voll qualifizierter Domänenname (FQDN) oder statische Quell–IPAdresse, wenn FQDN nicht unterstützt wird.</td></tr>
<tr><td>APP-NAME</td><td>Identifiziert die Anwendung, die die syslog-Nachricht initiiert hat. Das Feld enthält Informationen zur Identifikation der Einheit, die die Nachricht gesendet hat (zum Beispiel die Handelsreferenzen der Teilgeräte).</td></tr>
<tr><td>PROCID</td><td>Identifiziert den Prozess, die Einheit oder die Komponente, der/die das Ereignis sendet.</td></tr>
<tr><td>MSGID</td><td>Identifiziert den Nachrichtentyp, auf den sich das Ereignis bezieht. Beispiel: HTTP, FTP, Modbus.</td></tr>
<tr><td>MESSAGE TEXT</td><td>Dieses Feld enthält verschiedene Informationen:
• Ausstelleradresse: 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).
• Peer-Adresse: Peer-IP-Adresse, wenn ein Peer am Vorgang beteiligt ist.
• Typ: Eindeutige Nummer zur Identifizierung einer Nachricht (Beschreibung in den folgenden Tabellen).
• Bemerkung: Zeichenfolge, die die Nachricht beschreibt (Beschreibung in den folgenden Tabellen).</td></tr>
</table>

Ereignisse im Zusammenhang mit Sicherheit/ Autorisierung

- Gescheitertes Öffnen des sicheren Kanals vom OPC UA-Stack: z. B. ungültiges Zertifikat, abgelaufenes Zertifikat.
- Erfolgreiche Benutzersitzungen (Benutzername/Passwort) vom OPC UA-Stack (erfolgreiche Anmeldung)

  HINWEIS: Wenn keine Anmeldedaten eingegeben werden müssen (Standardmodus), wird das Protokoll deaktiviert, sodass keine Aufzeichnung für die erfolgreiche Verbindung erstellt wird.

- Nicht erfolgreiche Benutzersitzungen (Anmeldung/Passwort) vom OPC-UA-Stack (gescheiterte Anmeldung)

  HINWEIS: Wenn keine Anmeldung erfolgt (Standardmodus), wird das Protokoll deaktiviert, sodass keine Aufzeichnung für die gescheiterte Verbindung erstellt wird.
- Erfolgreiche HTTPS-Verbindungen zu oder von einem Tool (erfolgreiche Anmeldung): Beispielsweise eine Verbindung zum Webserver oder ein Firmware-Download über HTTPS.
- Gescheiterte HTTPS-Anmeldung bei oder von einem Tool: Beispielsweise eine gsecheiterte Verbindung zum Webserver oder ein fehlgeschlagener Firmware-Download über HTTPS.
- Erfolgreiche Trennung der Benutzersitzung (Abmeldung auf Anfrage) für HTTPS.
- Erfolgreiche Trennung der Benutzersitzung (Abmeldung auf Anfrage) für OPC UA.
- Automatische Abmeldung: Beispielsweise ein Inaktivitäts-Timeout für OPC UA oder HTTPS.
- Fehler bei der Integritätsprüfung erkannt: Beispielsweise wurde ein Fehler in einer digitalen Signatur oder ein integritätsspezifischer Fehler (Hash) erkannt.
- Erstellen eines neuen Zertifikats.
- Entfernen lokaler Zertifikate. Dies wird erreicht, indem der Drehwahlschalter verwendet wird, um den Betriebsmodus in die Stellung zum Zurücksetzen der Cybersicherheit (oder Sicherheit) zu setzen.
- Hinzufügen eines neuen Client-Zertifikats aus der Liste der zulässigen Zertifikate zum Gerät.
- Hinzufügen eines neuen Client-Zertifikats aus der Liste der zulässigen Zertifikate zum Gerät.

Ereignisse in Zusammenhang mit größeren Änderungen im System (Protokoll-Audit)

- Download der Anwendungs- oder Cybersicherheitskonfiguration in das Gerät.
- Firmware-Download in das Gerät.
- Nicht übereinstimmende Signatur für Firmware, die nicht in das Gerät heruntergeladen werden konnte.

Syslog – Webseiten-Diagnose

Verwenden Sie die Webseiten des Moduls, um den Status des auf dem Modul ausgeführten Syslog-Dienstes und bestimmte Teile des Syslog-Diagnosepuffers des Moduls zu

diagnostizieren. Sie können auch das Element SERVICES_STATUS des Modul-DDT, Seite 149 verwenden, um den Status des Syslog-Dienstes anzuzeigen.

Verwenden Sie im Menü **Diagnose > Ereignisprotokolldiagnose** die folgenden Befehle, um den Status des Syslog-Diensts des Moduls anzuzeigen:

Parameter	Beschreibung
Status	• Betriebsbereit: Das Modul wird im erweiterten (oder sicheren) Modus ausgeführt und der Syslog-Dienst ist aktiviert. • Nicht betriebsbereit: Das Modul wird im erweiterten (oder sicheren) Modus ausgeführt, aber der Syslog-Dienst ist deaktiviert.
Logserver	• Erreichbar: Es kann eine Verbindung zum dezentralen Syslog-Server eingerichtet werden. • Nicht erreichbar: Es kann keine Verbindung zum dezentralen Syslog-Server eingerichtet werden.

Geben Sie im Menü **Diagnose > Ereignisprotokolldiagnose** im Feld **Zu lesender Diagnosepuffer** den Teil des Diagnosepuffers ein, der gelesen werden soll.

Modbus-Diagnose

Einführung

Mithilfe der Modbus-Funktionscodebefehle können Sie Diagnoseaufgaben für das BMENUA0100-Modul ausführen. Modbus-Befehle können das Modul nur über seinen Baugruppenträger-Port erreichen. Da Modbus kein von Natur aus sicheres Protokoll ist, müssen Sie Modbus-Befehle in IPsec kapseln.

Nur die FC-Requests FC43/14 (Geräte-ID lesen) und FC03 (DDT-M% lesen) werden vom BMENUA0100-Modul unterstützt.

Modbus-Datenzugriff und Cybersicherheitsmodus

Das Verfahren, das Sie für den Zugriff auf Modbus-Daten verwenden können, ist vom Cybersicherheitmodus abhängig. Wenn das BMENUA0100-Modul im folgenden Modus ausgeführt wird:

- Standardmodus: Das BMENUA0100-Modul nimmt den Modbus TCP/IP-Client-Datenfluss von jedem Client an, der auf das Baugruppenträger-Ethernet-Netzwerk zugreifen kann. Verwenden Sie standardmäßige Modbus-Kommunikationsmethoden, einschließlich der Funktionsbausteine DATA_EXCH, MBP_MSTR, READ_VAR und WRITE_VAR, sowie Control Expert-Befehle.
- Erweiterter (oder sicherer) Modus Das BMENUA0100-Modul akzeptiert den Modbus TCP/IP-Client-Datenfluss nur von der M580-Steuerung. Sie können den Baustein DATA_EXCH in der Anwendung implementieren. READ_VAR und WRITE_VAR können ebenfalls verwendet werden.

  HINWEIS: Um den Modbus-Server im Modul zu adressieren, muss die Geräte-ID 100 verwendet werden. Informationen zur Einstellung dieses Werts finden Sie in der Dokumentation Ihres Modbus-Clients. Beispiel: Bei Verwendung des Bausteins DATA_EXCH kann die Geräte-ID wie folgt mit ADDMX festgelegt werden: ADDMX (0.0.3{192.168.10.2}100.TCP.MBS), wobei 192.168.168.10.2 die IP-Adresse des Baugruppenträgers des BMENUA0100-Moduls ist.

43/14: Lesen der Geräteidentifikation

Die folgenden Geräteidentifikationsdaten können mit dem Funktionscode 43 / Untercode 14 zurückgegeben werden:

Kategorie	Objekt-ID	Objektname	Typ
Basis	00 hex.	Anbietername	ASCII-Zeichenfolge
	01 hex.	Produktcode	ASCII-Zeichenfolge
	02 hex.	Haupt-/Nebenversion	ASCII-Zeichenfolge
Basis	03 hex.	Anbieter-URL	ASCII-Zeichenfolge
	04 hex.	Produktname	ASCII-Zeichenfolge
	05 hex.	Modellname	ASCII-Zeichenfolge
	06 hex.	Name der Benutzeranwendung	ASCII-Zeichenfolge
	07 bis FF hex.	Reserviert	ASCII-Zeichenfolge

SNMP-Diagnose

Einführung

Wenn der SNMP-Agent konfiguriert, Seite 139 ist, aktiviert das BMENUA0100-Modul die SNMP-Diagnose im TCP/IP-basierten Ethernet-Netzwerk durch Unterstützung der folgenden MIBs:

- MIB-II
- Link Layer Discovery Protocol (LLDP) MIB

MIB-II

MIB-II stellt einem SNMP-Manager eine Sammlung von Geräteverwaltungsvariablen zur Verfügung. Durch das Lesen dieser Variablen kann ein SNMP-Manager den Betrieb eines bestimmten Geräts diagnostizieren, zum Beispiel das Modul BMENUA0100.

LLDP MIB

Die LLDP MIB enthält Daten, die mithilfe des Link Layer Discovery Protocol in Bezug auf die Identität, die Fähigkeiten und den Standort des Ethernet-Netzwerks gesammelt wurden. Mithilfe der LLDP MIB kann ein SNMP-Manager die Topologie des Netzwerks und Fähigkeiten der Netzwerkgeräte ermitteln.

HINWEIS: Die SNMP-Kommunikation der LLDP-MIB-Daten erfolgt ausschließlich über den Baugruppenträger-Port.

OPC UA-Diagnose-Webseite

Auf der Webseite **OPC UA-Diagnose** können Sie dynamische Daten anzeigen, die den Betrieb des in das BMENUA0100-Modul integrierten OPC UA-Servers beschreiben.

HINWEIS: Die Webseite **OPC UA-Diagnose** wird alle 5 Sekunden aktualisiert.

Diagnosedaten

Die Webseite **OPC UA-Diagnose** zeigt die folgenden schreibgeschützten Daten an. Beachten Sie, dass alle numerischen Werte im Dezimalformat angegeben werden:

Bereich	Beschreibung
SPS-Diagnose	
EPAC	IP-Adresse der Steuerung.
Geräteidentität	Teilenummer der Steuerung.
Geräteversion	Firmwareversion der Steuerung.
Gerätestatus	Verbindungsstatus mit Steuerung: **Gut**, **Schlecht**, **Unsicher**, **Unbekannt**, **Fehlt**.
Frame-Timeout (in ms)	Die maximale Zeitspanne, die der OPC UA-Server nach dem Senden eines Requests auf eine Antwort von einem Gerät wartet. Beispiel: 1000.
Max. Anzahl Kanäle	Anzahl der vom OPC UA-Server in der Steuerung geöffneten Verbindungen.
Für andere Aktivitäten als die Zeitstempelung verwendete Kanäle.	Anzahl der Verbindungen, die Anwendungsdaten übertragen.
Für die Zeitstempelung verwendete Kanäle.	Anzahl der Verbindungen, die Zeitstempeldaten übertragen, Seite 133.
Request-Länge	Länge der Requests für die Kommunikation mit der Steuerung.
Anwendungsname (Gerät)	Der Control Expert-Projektname.
Anwendungsversion (Gerät)	Prüfsumme und Signaturen der Anwendung.
Datenwörterbuch vorladen	Verfügbar oder Nicht verfügbar für die Anwendung in der Steuerung.
Zeitstempelstatus	Der Zeitstempelstatus wird angezeigt: • Die Zeitstempelung wird mit Zugriff auf zeitgestempelte Variablen in der Anwendung aktiviert. • Zeitstempelung ist nicht aktiviert, kein Zugriff auf zeitgestempelte Variablen.
Liste der Geräte mit konfigurierter Quellzeitstempelung	Wenn die Zeitstempelung aktiviert ist, wird eine Liste der Geräte angezeigt, die für jedes Gerät Folgendes angibt: • Anzahl dedizierter Kanäle, die für die Abfrage der Zeitstempelereignisquelle reserviert sind. • Gerätetyp (BMECRA31310, Steuerung usw.) • IPv4-Adresse. • Reservierung des Geräte-Zeitstempelpuffers durch den in BMENUA0100 integrierten OPC UA-Server: TRUE / FALSE.
OPC-UA-Diagnose	

Bereich	Beschreibung
Endpunkt-URL (IPV4)	IPv4-Adresse des OPC UA-Servers in folgendem Format: „opc.tcp://<IPv4 address>:<port number>“. Beispiel: opc.tcp://192.168.2.142:4840
Schnelle Abtastrate	Gibt an, ob die Einstellung Schnelle Abtastrate, Seite 128 ausgewählt ist: • TRUE = Ausgewählt • FALSE = Nicht ausgewählt
Anzahl der verbundenen Sitzungen	Gesamtanzahl der vom in BMENUA0100 integrierten OPC UA-Server unterstützten Clientsitzungen.
Abonnementinformationen:	Informationen zu den Variablen, die vom OPC UA-Server überwacht werden und in einem oder mehreren Abonnements enthalten sind.
Anzahl der überwachten Elemente vom internen Serverknoten:	
Anzahl der überwachten Elemente:	
Anzahl der nicht spezifischen überwachten Elemente:	
Anzahl der überwachten Elemente mit Zeitstempel und nicht deaktiviertem Überwachungsmodus:	
Gesamtanzahl der überwachten Elemente:	
Aktuelle Anzahl der Timer	Die Anzahl der konfigurierten Abtastintervalle für den in BMENUA0100 integrierten OPC UA-Server.
Timer-Liste	Eine Liste, die jedes Abtastintervall (d. h. Timer) beschreibt, das vom in BMENUA0100 integrierten OPC UA-Server überwacht wird. Jedes Element zeigt Folgendes an: • Das Abtastintervall in ms. • Die Anzahl der überwachten Elemente. • Die Anzahl der während der letzten Ausführung generierten Requests.

Optimieren der Leistung des BMENUA0100-Moduls

Optimierung der Leistung des BMENUA0100-Moduls

Einführung

Berücksichtigen Sie bei der Optimierung der Leistung des BMENUA0100-Moduls das gesamte System. Achten Sie insbesondere auf eine effektive Gesamtkommunikation und die Arbeitsbelastung innerhalb der Netzwerkarchitektur, die die BMENUA0100-Module beinhaltet. In diesem Zusammenhang wirken sich Optimierungen der Leistung des OPC UA-Clients auch auf die Effektivität der OPC UA-Kommunikation aus.

Mehrere Einstellungen auf verschiedenen Ebenen der Architektur können die Systemleistung verbessern oder Ihr System in jeder Betriebsmodusphase (Verbindungen, Durchsuchen, Abonnement, Überwachung usw.) stabiler und robuster machen.

HINWEIS:

- Fügen Sie Elemente in Paketen mit einer maximalen Größe von 2000 Elementen hinzu. Das konfigurierte Abtastintervall ist nur relevant, wenn es größer oder gleich der Zykluszeit der MAST-Steuerung ist.
- Setzen Sie CallTimeout auf einen Wert größer oder gleich 10 Sekunden im OPC UA-Client.
- Die Einstellung General.SecureChannelLifetime für die Kommunikation mit einem OPC UA-Client wird standardmäßig auf 3.600.000 ms (1 Stunde) gesetzt. Verwenden Sie diese Standardeinstellung, um Leistungseinbußen zu vermeiden.
- Die Leistung des Systems hängt stark von der Konfiguration ab (z. B. die Anzahl der verbundenen Clients, die Anzahl der verwalteten Variablen usw.).
- Bei 2.000 überwachten Elementen kann die Aktualisierungsrate beispielsweise nur innerhalb von 20 ms erreicht werden, wenn sich die Werte von maximal 500 Elementen zwischen zwei aufeinander folgenden Veröffentlichungswiederholungen ändern.

Leistung - Beispiel

Ein OPC UA-Client kann bis zu 20.000 Elemente im Standard-Cybersicherheitsmodus überwachen.

Beispiel basierend auf:

- BMEP584040 mit einer MAST-Task-Zykluszeit von 20 ms (CPU-Last weniger als 80 %).
- BMENUA0100 in der Drehwahlschalterstellung Standard (d. h. keine sichere Kommunikation, kein IPsec-Kanal).
- Der OPC UA-Client (UAExpert) initiiert die Kommunikation mit dem auf **Keine** eingestellten Nachrichtensicherheitsmodus und überwacht 20.000 Elemente anhand von Variablen, die auf einem Array des Typs „INT“ basieren, von einem BMENUA0100 OPC UA-Server Dieser Server ist mit einem Veröffentlichungsintervall von 1 Sekunde, einem Abtastintervall von 1 Sekunde und einem Sitzungs-Timeout von 30 Sekunden konfiguriert.
- Keine andere Kommunikation als OPC UA.

Anpassung der Leistung

Datenstruktur austauschen

Der Datenanwendungsspeicher der Steuerung ist in Abhängigkeit von der Datenanwendungsdefinition in Control Expert organisiert. Je strukturierter die Variablendeklaration ist, umso mehr generiert der BMENUA0100-Server optimierte Requests für den Zugriff auf die Variablen und das Datenwörterbuch zur Laufzeit.

Für die Variablen, auf die der OPC UA-Client zugreift, gilt daher Folgendes:

- Verwenden Sie nach Möglichkeit Arrays oder Datenstrukturen.
- Aktivieren Sie die Option **Nur HMI-Variable** in **In SPS eingebettete Daten** der **Projekteinstellungen** und stellen Sie nur diese Variablen mit dem Attribut **HMI** ein, um die Größe des Datenwörterbuchs zu reduzieren.
- Heben Sie in der Sicherheitssteuerungsanwendung die Auswahl der Option **Verwendung des Prozess-Namespace** (in **Projekteinstellungen > Allgemein > In SPS eingebettete Daten > Datenwörterbuch**) auf, um die Größe des Datenwörterbuchs zu reduzieren.

Kommunikationsfähigkeiten der Steuerung

Die Kapazität des Kommunikationssystems ist von der Referenz der M580-Steuerung und einigen Konfigurationseinstellungen abhängig. Die Steuerungsreferenz bestimmt:

- Die systemweiten Verarbeitungsleistungsfunktionen der Steuerung.
- Die Anzahl der Requests pro Zyklus, die verarbeitet werden können, auch wenn dies über das Systemwort %SW90 konfigurierbar ist.
- Die maximale Anzahl der für jedes BMENUA0100-Modul verfügbaren Kanäle für den Aufbau von Verbindungen zur M580-Steuerung, Seite 184.

Darüber hinaus ist die Anzahl der zu verarbeitenden Kommunikations-Requests um so größer, je geringer die MAST-Zykluszeit ist. Insofern ist das Leistungsniveau direkt abhängig von der MAST-Zykluszeit.

OPC UA-Client, Konfiguration und Nutzung

Die Anzahl der überwachten Variablen wirkt sich auf die Leistung aus. Die für jeden OPC UA-Client konfigurierten Abtastraten und Veröffentlichungsintervalle bestimmen die Anzahl der Requests, die zur Animation der Variablen erforderlich sind. Beachten Sie, dass, wenn mehrere OPC UA-Clients mit demselben BMENUA0100-OPC UA-Server verbunden sind, diese Konfiguration mehr Requests generiert, wenn die Abtastraten und Veröffentlichungsintervalle unterschiedlich sind.

Alle über den OPC UA-Client konfigurierbaren Timeout-Werte (Durchsuchen, Verbinden, Veröffentlichen, Sitzung, Watchdog…) müssen angepasst werden, um Ihr Gesamtsystem weitmöglichst zu optimieren und zu stabilisieren. Als Nebenwirkung können diese Timeouts die Systemleistung beeinträchtigen.

Je nach Nachrichtensicherheitsmodus (Keine, Signieren, Signieren und Verschlüsseln) benötigt der Algorithmus zur Berechnung der Signatur und der Verschlüsselung zusätzliche Zeit.

Kommunikation zwischen Steuerung und Steuerung sowie zwischen Control Expert und Steuerung

Jeder IPsec-Tunnel, der zur Sicherung der Kommunikation mit Ausnahme von OPC UA oder HTTPS verwendet wird, verlangsamt den Datenverkehr, insbesondere wenn die Einstellung **Vertraulichkeit** aktiviert ist, wodurch eine Ver- und Entschlüsselung erzeugt wird.

Überwachung der Leistung

Es gibt verschiedene Möglichkeiten, die Leistung zu überwachen.

Verwendung von Control Expert

Bei Verwendung von Control Expert im verbundenen Modus können Sie auf die effektive MAST-Zykluszeit und die Last der M580-Steuerung für das System, für jede Task und für die Gesamtheit aller Tasks zugreifen, indem Sie die Systemwörter %SW110 bis %SW116 lesen. Darüber hinaus können der DDDT der M580-Steuerung und der BMENUA0100-DDT verschiedene Diagnoseinformationen in Verbindung mit der Systemleistung der Steuerung bereitstellen, z. B.:

- Dienstebene des OPC UA-Servers
- Anzahl der verbundenen OPC UA-Clients
- Status des Datenwörterbuchs, Erfassungszeit, Vorladedauer
- Ethernet-Dienststatus

- Funktionsfähigkeit des Netzwerks
- Status des Steuerungsports und des Baugruppenträger-Ports
- Anzahl der Ethernet-Pakete pro Sekunde
- Anzahl der Ethernet-Pakete mit Fehlern
- Prozentsatz der BMENUA0100-CPU-Last und des verwendeten Speichers
- Anzahl der geöffneten IPsec-Kanäle.

Verwendung der BMENUA0100-Website

Die Startseite und die Diagnoseseite der BMENUA0100-Website bieten interessante Informationen zur Leistung der OPC UA-Server. Einige Informationen kommen vom BMENUA0100-DDT, während andere vom OPC UA-Server selbst zur Verfügung gestellt werden:

- Anzahl der überwachten Elemente
- Anzahl der überwachten spezifischen Elemente
- Die verschiedenen, zurzeit ausgeführten Abtastintervalle
- Anzahl der generierten Requests für die Animationen
- Erkannte Überläufe
- Anzahl der verbundenen Clients

Verwendung des OPC UA-Clients

Der OPC UA-Client kann einige spezifische Elemente direkt unter dem OPC UA-Server überwachen, aber auch bei Bedarf die ServiceLevel-Variable oder einige BMENUA0100-DDT-Unterfelder über Anwendungsvariablen.

Andere Dienste für die Diagnose

In einem mehr technischen Ansatz können der SNMP-Agent und der Syslog-Server des BMENUA0100-Moduls dazu beitragen, weitere Diagnoseinformationen im Zusammenhang mit der Leistung der OPC UA-Server zu sammeln.

Fehlerbehebung für das BMENUA0100-Modul

Einführung

Dieser Abschnitt enthält Tipps, die Sie für einen besseren Betrieb des BMENUA0100-Moduls verwenden können.

Auswirkungen der Verwendung von UaExpert als OPC UA-Client

Wenn Sie UaExpert als OPC UA-Client zum Lesen von Datenwerten verwenden, beachten Sie, dass UaExpert die *Aktuelle Abonnementanzahl* für jede Instanz von UAExpert um den Wert 1 erhöht.

HINWEIS: Das Element *Aktuelle Abonnementanzahl* ist mit dem Server selbst vevrknüpft und darf nicht mit dem sitzungsbezogenen Element *Aktuelle Abonnementanzahl* verwechselt werden.

Erfassungszeit des Datenwörterbuchs und MAST-Periode

Die für das Laden der Variablensammlung im Datenwörterbuch erforderliche Zeit hängt von der Anzahl der Datenwörterbuch-Elemente und der konfigurierten MAST-Periode ab. Für eine Anwendung, die den OPC UA-Server im BMENUA0100-Modul zur Überwachung von Elementen benötigt, deren Anzahl sich dem Maximum von 100.000 nähert, wurden die folgenden Ergebnisse beobachtet und können aufschlussreich sein.

Für eine nicht sicherheitsbezogene Anwendung mit 99.000 Elementen:

MAST-Periode	Beobachtete Erfassungszeit des Datenwörterbuchs
20 ms	23 s
100 ms	46 s
200 ms	74 s

Für eine sicherheitsbezogene Anwendung mit 99.000 Elementen:

MAST-Periode	Beobachtete Erfassungszeit des Datenwörterbuchs
25 ms	15 s
200 ms	72 s

Konfigurieren von Abonnements mit mehr als 30.000 überwachten Elementen

Wenn Sie ein oder mehrere Abonnements erstellen möchten, die zusammen mehr als 30.000 überwachte Elemente umfassen, konfigurieren Sie jedes Abonnement im jeweiligen

OPC UA-Client mit einem Wert **Anzahl „Life Time“** von 300 Sekunden, der der Max. Abonnement-Lebensdauer, Seite 37 entspricht, den der OPC UA-Server im BMENUA0100-Modul unterstützen kann.

Verwenden von GPOs / LGPOs

Verwalten Sie Zertifikate auf einem Host-PC mithilfe eines der folgenden Tools, die über das Windows ™-Betriebssystem verfügbar sind:

- Gruppenrichtlinienobjekte (GPOs: Group Policy Objects) zur zentralen Verwaltung von Benutzereinstellungen in einer zentralisierten Active Directory-Umgebung oder
- Lokale Gruppenrichtlinienobjekte (LGPOs: Local Group Policy Objects) zur dezentralen Verwaltung von Benutzereinstellungen für einzelne PCs.

In beiden Fällen kann die Verwendung von Gruppenrichtlinienobjekten (GPOs) oder lokalen Gruppenrichtlinienobjekten (LGPOs) dazu beitragen, unbefugten Zugriff auf Ihren PC und dessen Anwendungen zu verhindern. Die Verwendung von GPOs und LGPOs deaktiviert den Zugriff auf die Windows Microsoft Management Console (MMC) und unterstützt nur die Implementierung der von der Software konfigurierten Genehmigungsliste.

Übernehmen der MMC-Gruppenrichtlinienverwaltung

Verwalten Sie Zertifikate mithilfe der von Microsoft Windows bereitgestellten Tools,™ um das Hinzufügen nicht autorisierter Zertifikate zum PC oder das Ändern selbstsignierter Zertifikate eines OPC UA-Clients zu verhindern. Ohne Verwaltung kann ein Benutzer nicht autorisierte Zertifikate in die vom Sicherheitsadministrator verwaltete BMENUA0100-Genehmigungsliste einfügen.

Die Tools umfassen Richtlinien zur Verwaltung von Gruppenrichtlinien, die vom GPO (Group Policy Object), einem Plug-In der Microsoft Management Console (MMC), angewendet werden. Entwerfen Sie Ihre Richtlinien so, dass sie den Zugriff auf die Windows MMC deaktivieren und nur Zugriff auf Einträge in der Konfiguration der Genehmigungsliste gewähren, die ordnungsgemäß von der Software hinzugefügt wurden.

OPC UA-Client-Sperre

Wenn Sie einen OPC UA-Client, dem ein Benutzername zugewiesen wurde, mit dem OPC UA-Server verbinden, der in das BMENUA0100-Modul integriert ist, werden die Einstellungen für die Benutzerkonto-Richtlinien, Seite 101 des BMENUA0100-Moduls angewendet. Beispiel: Wenn die Anzahl der **Max. Anmeldeversuche** erreicht oder überschritten wurde, kann sich der OPC UA-Client (**BadInternalError**) für die Zeit, die als **Dauer der Kontosperrung** festgelegt wurde, nicht anmelden.

Aktivieren von Netzwerkdiensten nur über eine IPv6-Verbindung

Das BMENUA0100-Modul unterstützt nur die Verwendung von IPv6 für IP-Adressierung und -Kommunikation. Wenn nur IPv6 aktiviert, Seite 126 ist, sind die Netzwerkdienste für **CPU-zu-CPU-Datenfluss** und **Control Expert-Datenflüsse zum Gerätenetzwerk** nicht verfügbar. Diese Dienste werden nur von IPv4 unterstützt.

Diese Funktionen können jedoch weiterhin auf der Webseite **Einstellungen > Netzwerkdienste** aktiviert werden. Wenn diese Dienste aktiviert werden, wenn nur IPv6 aktiviert ist, werden die Dienste (**CPU zu CPU** und **CE zu Gerätenetzwerk**) als EIN auf der **Startseite** angezeigt, sind tatsächlich aber nicht aktiviert.

Nur die Datenflussfilterfunktion für **Datenflüsse von Control Expert ausschließlich zur CPU** wird von der IPv6-Kommunikation unterstützt. In diesem Fall wird auf der **Startseite**, wenn nur die IPv6-Kommunikation aktiviert ist, für **Nur CE zu CPU** ordnungsgemäß EIN angegeben.

BOOLs als BYTE in Steuerungsdatenstrukturen

Im OPC UA-Server des BMENUA0100-Moduls wird jedes Element des Steuerungs-DDT einem Byte in der Steuerung zugewiesen, selbst wenn es im BMENUA0100 als BOOL oder EBOOL definiert ist. Mithilfe des OPC UA-Protokolls kann ein Client ein BOOL- oder EBOOL-Element einer BMENUA0100-Instanz im DDT der Steuerung global lesen oder schreiben, mit einem gültigen Bytewert ungleich 0 oder 1 (z. B. 255). Entwerfen Sie Ihre Anwendung für das Schreiben oder Lesen von BOOL- oder EBOOL-Werten von nur 0 oder 1, da nur diese Werte im BMENUA0100-Modul gültig sind.

Firmwareaktualisierung

Tool EcoStruxure™ Automation Device Maintenance

Einführung in das Tool EcoStruxure™ Automation Device Maintenance

Verwenden Sie das Tool EcoStruxure™ Automation Device Maintenance, um die Firmware des BMENUA0100-Moduls zu aktualisieren. EcoStruxure™ Automation Device Maintenance ist ein webbasiertes Tool, mit dem Sie folgende Aufgaben durchführen können:

- Manuelle Erkennung von einem oder mehreren BMENUA0100-Modulen in Ihrem Projekt basierend auf den IP-Adressen.
- Aktualisierung der BMENUA0100-Module auf die neueste Firmwareversion über das Web.

Vor der Aktualisierung der Firmware müssen Sie Folgendes durchführen:

- Stellen Sie eine Verbindung zum BMENUA0100 mit der Installer-Rolle (Monteur) her.
- Trennen Sie die mit dem Modul verbundenen Clients (Web, OPC UA, andere Steuerungen).

Detaillierte Informationen zur Installation und Verwendung des Tools EcoStruxure™ Automation Device Maintenance finden Sie in der Online-Hilfe (siehe EcoStruxure Automation Device Maintenance, Firmware-Upgrade-Tool, Online-*Hilfe*).

HINWEIS: Das Softwaretool Unity Loader™ von Schneider Electric kann nicht zur Aktualisierung der Firmware für das BMENUA0100-Modul verwendet werden.

HINWEIS: Nach der Aktualisierung der Firmware des BMENUA0100-Moduls von Version 1.xx auf Version 2.xx, wenn sich das BMENUA0100-Modul im Standardmodus befindet, müssen Sie einen Vorgang Zurücksetzen der Sicherheit, Seite 33 durchführen, um die werkseitigen Standardeinstellungen des Moduls wiederherzustellen. Wählen Sie dann einen Cybersicherheits-Betriebsmodus - Erweiterter (oder sicherer) Modus oder Standardmodus - für das Modul aus.

Downgrade der Firmware

Es ist möglich, ein Downgrade der Firmwareversion des BMENUA0100-Moduls durchzuführen, z. B. von Version 1.1 auf Version 1.0. Führen Sie nach dem Downgrade der Softwareversion über das EcoStruxure™ Automation Device Maintenance-Tool den Vorgang Zurücksetzen der Cybersicherheit (oder Sicherheit), Seite 33 durch, um die werkseitigen

Standardeinstellungen des Moduls wiederherzustellen. Wählen Sie dann einen Cybersicherheits-Betriebsmodus - Erweiterter (oder sicherer) Modus oder Standardmodus - für das Modul aus.

Anhänge

Inhalt dieses Abschnitts

Steuerungsverbindungen

Inhalt dieses Kapitels

Verbindungen des OPC UA-Servers zur Steuerung

Geöffnete Verbindungen

Die Anzahl der Verbindungen, die vom BMENUA0100-Modul zur M580-Steuerung geöffnet werden können, ist von der Kapazität der Steuerung abhängig. Somit ist die Leistung des BMENUA0100-Moduls von der Zeit abhängig, die für die Ausführung der MAST-Task erforderlich ist, sowie von der jeweils ausgewählten Steuerung. Die maximale Anzahl der Verbindungen, die jedes BMENUA0100-Modul zur M580-Steuerung öffnen kann:

Steuerungsmodell	Maximale Anzahl der von jedem BMENUA0100-Modul geöffneten Verbindungen
BMEP581020(H)	9
BMEP5820•0	9
BMEP5830•0	12
BMEP5840•0	15
BMEP585040	15
BMEP586040(C)	18
BMEH582040	9
BMEH584040(C)	15
BMEH586040	18

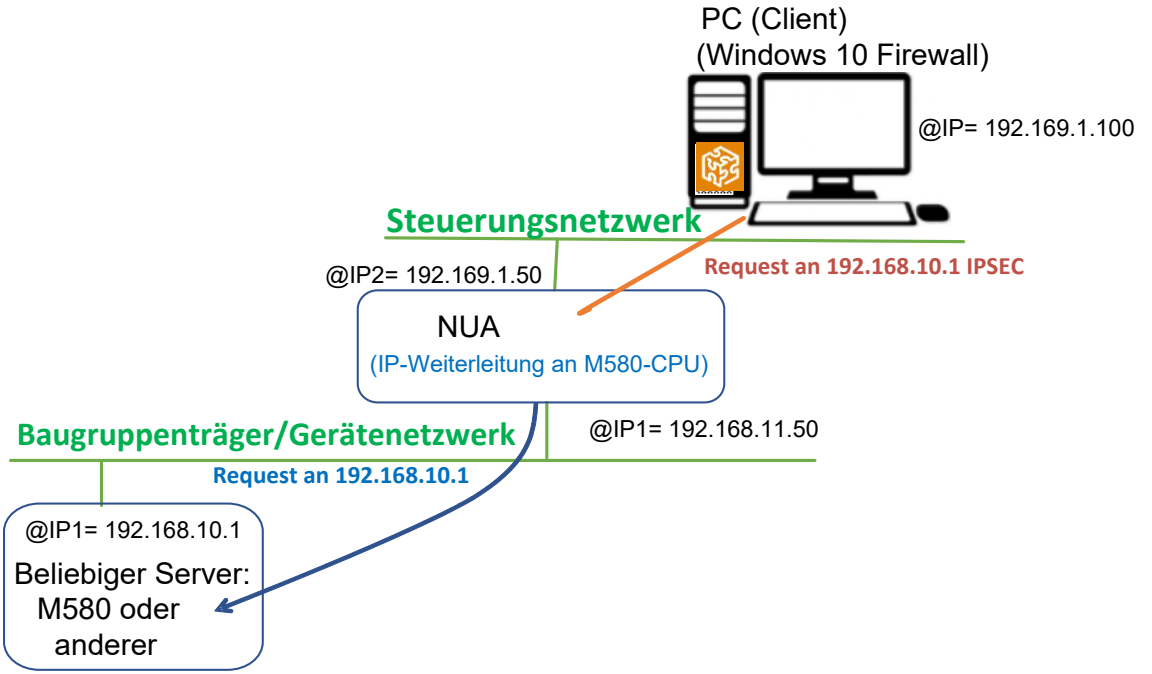
Architekturen für die Dienstweiterleitung (IP)

Inhalt dieses Kapitels

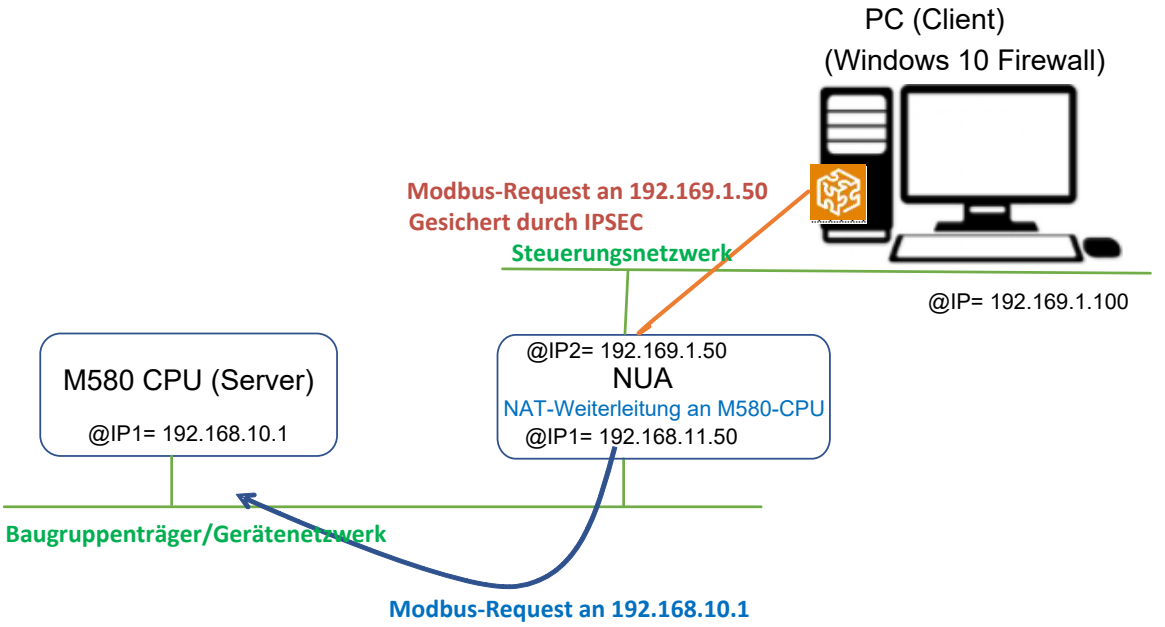
In diesem Kapitel werden die Architekturen vorgestellt, die von der Dienstweiterleitungsfunktion (IP) des BMENUA0100-Moduls unterstützt bzw. nicht unterstützt werden.

Unterstützte Architekturen für die Dienstweiterleitung (IP)

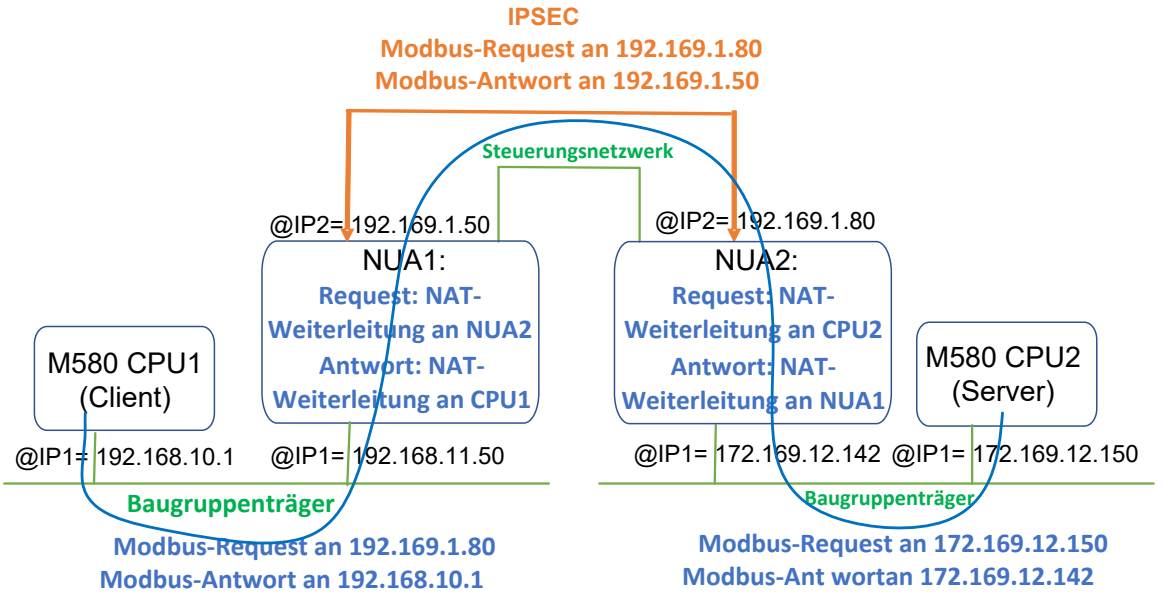
IP-Weiterleitung vom Windows-Client (Steuerungsnetzwerk) an einen beliebigen Client (Baugruppenträger/Gerätenetzwerk)



NAT-Weiterleitung vom Windows-Client (Steuerungsnetzwerk) zur M580-Steuerung (Baugruppenträger/Gerätenetzwerk)

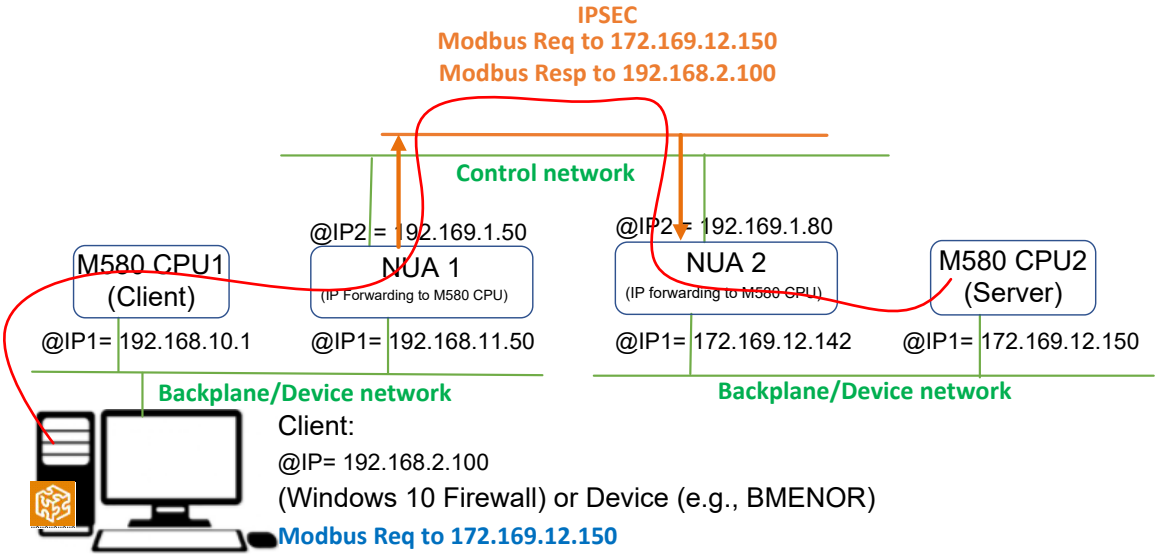


NAT-Weiterleitung zwischen Baugruppenträgern für die Kommunikation zwischen M580-Steuerungen



Nicht unterstützte Architekturen für die Dienstweiterleitung (IP)

IP-Weiterleitung zwischen Baugruppenträgern/ Gerätenetzwerken



IP-Weiterleitung und OPC UA-Kommunikation

Inhalt dieses Kapitels

Sowohl die IP-Weiterleitung als auch OPC UA beanspruchen die verfügbare Kommunikationsbandbreite des BMENUA0100-Moduls. In diesem Abschnitt finden Sie Testergebnisse hinsichtlich der Modulleistung, wenn nur die IP-Weiterleitung bzw. wenn sowohl die IP-Weiterleitung als auch die OPC UA-Kommunikation verwendet wird.

IP-Weiterleitung - Auswirkungen auf die Leistung

Wenn nur die IP-Weiterleitung - und nicht die OPC UA-Kommunikation - aktiviert ist, wirkt sich dies wie folgt auf die BMENUA0100-Modulbandbreite aus:

IPsec	Vertraulichkeit	Weiterleitung	Framelänge (Byte)	Bandbreite (KByte/Sek.)
Nein	N/A	Alle weiterleiten	1000	8800
Nein	N/A	Benutzerdefinierte Regel	1000	10600
Ja	Nein	Alle weiterleiten	1000	3400
Ja	Nein	Benutzerdefinierte Regel	1000	4000
Ja	Ja	Alle weiterleiten	1000	2600
Ja	Ja	Benutzerdefinierte Regel	1000	2500

HINWEIS: Diese Werte dienen lediglich als Beispiel. Verwenden Sie sie zur Einschätzung der Auswirkungen verschiedener Parameter (IPsec, Vertraulichkeit usw.) auf die Leistung. Die tatsächliche Leistung hängt von der jeweiligen Infrastruktur ab.

Die Auswirkungen auf die Bandbreite werden in folgenden Fällen angezeigt:

- Nur der Kommunikationsfluss der IP-Weiterleitung wird unterstützt und es ist kein OPC UA-Kommunikationsfluss enthalten.
- IPsec wird verwendet (IPsec = Ja) und nicht verwendet (IPsec = Nein).

- Frames sind mit Vorzeichen versehen (Vertraulichkeit = Nein), im Gegensatz zu Frames, die beide mit Vorzeichen versehen und verschlüsselt sind (Vertraulichkeit = Ja), und IPsec wird verwendet (in beiden Fällen).
- Es werden benutzerdefinierte Regeln für die IP-Weiterleitung im Vergleich zu „Alle weiterleiten“ angewendet.

  HINWEIS: Die Framelänge hat nur einen geringen Einfluss auf die Gesamtleistung.

IP-Weiterleitung und OPC UA - Auswirkungen auf die Leistung

Wenn sowohl die IP-Weiterleitung als auch die OPC UA-Kommunikation aktiviert sind, wirkt sich dies wie folgt auf die BMENUA0100-Modulbandbreite aus:

Anzahl der überwachten OPC UA-Elemente pro Abonnement	IPsec	Vertraulichkeit	Weiterleitung	Bandbreite (KByte/Sek.)
0	Nein	N/A	Benutzerdefinierte Regel	10600
0	Ja	Nein	Benutzerdefinierte Regel	4000
0	Ja	Ja	Benutzerdefinierte Regel	2500
20000	Nein	N/A	Benutzerdefinierte Regel	8800
20000	Ja	Nein	Benutzerdefinierte Regel	2900
20000	Ja	Ja	Benutzerdefinierte Regel	2000

HINWEIS: Diese Werte dienen lediglich als Beispiel. Verwenden Sie sie zur Einschätzung der Auswirkungen verschiedener Parameter (IPsec, Vertraulichkeit usw.) auf die Leistung. Die tatsächliche Leistung hängt von der jeweiligen Infrastruktur ab.

Die Auswirkungen auf die Bandbreite werden in folgenden Fällen angezeigt:

- Die gesamte Paketweiterleitung erfolgt über eine benutzerdefinierte Regel (keine Weiterleitung an alle).
- OPC UA-Kommunikationsflüsse sind nicht enthalten (Anzahl der überwachten OPC UA-Elemente = 0) und enthalten (= 2000).

HINWEIS: Die Anzahl der überwachten OPC UA-Elemente hat nur geringe Auswirkungen.

IPsec-Windows-Skripte

Inhalt dieses Kapitels

Skripts zur Konfiguration der IKE/IPsec-Windows-Firewall

Um IPsec auf einem PC auszuführen, auf dem sich entweder die Control Expert-Konfigurationssoftware oder ein OPC UA-Client (z. B. SCADA) befindet, müssen Sie der Host-Firewall eine Netzwerkkonfiguration hinzufügen. Für jede auf den Webseiten konfigurierte IPsec-Regel kann ein zugehöriges Skript (mit der Bezeichnung IPSecWindowsConf.bat) über das Zahnradsymbol heruntergeladen werden. Führen Sie dieses Skript aus, um die Host-Firewall in die Konfiguration einzufügen.

- IKE/IPsec im **Transport**-Modus für die Datenflüsse lokal im BMENUA0100.
- IKE/IPsec im **Tunnel**-Modus für die an den Ethernet-Baugruppenträger weitergeleiteten Datenflüsse
- Passthrough-Regeln für HTTPS, sicheres OPC UA und einige andere Protokolle, für die **IPSEC-Verwendung** = FALSE gilt.

Die folgenden Beispiele zeigen Konfigurationsskripts für die Windows-Firewall mit und ohne IPsec-Vertraulichkeit.

In jedem Skriptbeispiel müssen Sie Werte für die folgenden Variablen angeben:

- **`endpoint1`**: Der Wert der dezentralen IP-Adresse in der IPsec-Konfiguration.
- **`endpoint2`**: Die IP-Adresse des BMENUA0100-Steuerungsports.
- **`Auth1psk`**: Die PSK-Einstellung in der IPsec-Konfiguration.

Windows-Firewall-Skript mit Vertraulichkeit

HINWEIS: Wenn Vertraulichkeit in der IPsec-Konfiguration aktiviert ist, verwenden Sie `qmsecmethods=esp:sha256-aes128`.

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess
```

```
netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-
sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Windows-Firewall-Skript ohne Vertraulichkeit

HINWEIS: Wenn Vertraulichkeit in der IPsec-Konfiguration nicht aktiviert ist, verwenden Sie `qmsecmethods=esp:sha256-None`.

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess
```

```
netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-
sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Einrichtung einer Windows-Zertifizierungsstelle

Inhalt dieses Kapitels

In diesem Kapitel wird beschrieben, wie Sie eine Microsoft Windows™-Zertifizierungsstelle einrichten, die in einem unternehmensweiten Benutzerauthentifizierungs- und -autorisierungssystem verwendet werden kann.

Vorab durchzuführende Aufgaben

Im Folgenden werden die erforderlichen Elemente sowie die vorbereitenden Schritte beschrieben, die Sie vor der Installation des Zertifikatservers durchführen müssen.

Erforderliche Elemente

Sie benötigen folgende Elemente:

- Microsoft Windows™ Server Manager: Dieses Tool kann von der Microsoft-Website heruntergeladen werden.
- Microsoft Windows Active Directory Certificate Server (ADCS): Diese kommerzielle Software ist Bestandteil von Windows Server. Das BMENUA0100-Modul unterstützt die Serverversionen 2016 und 2019.
- Die Datei TemplatePackage.zip, die von Schneider Electric heruntergeladen werden kann.

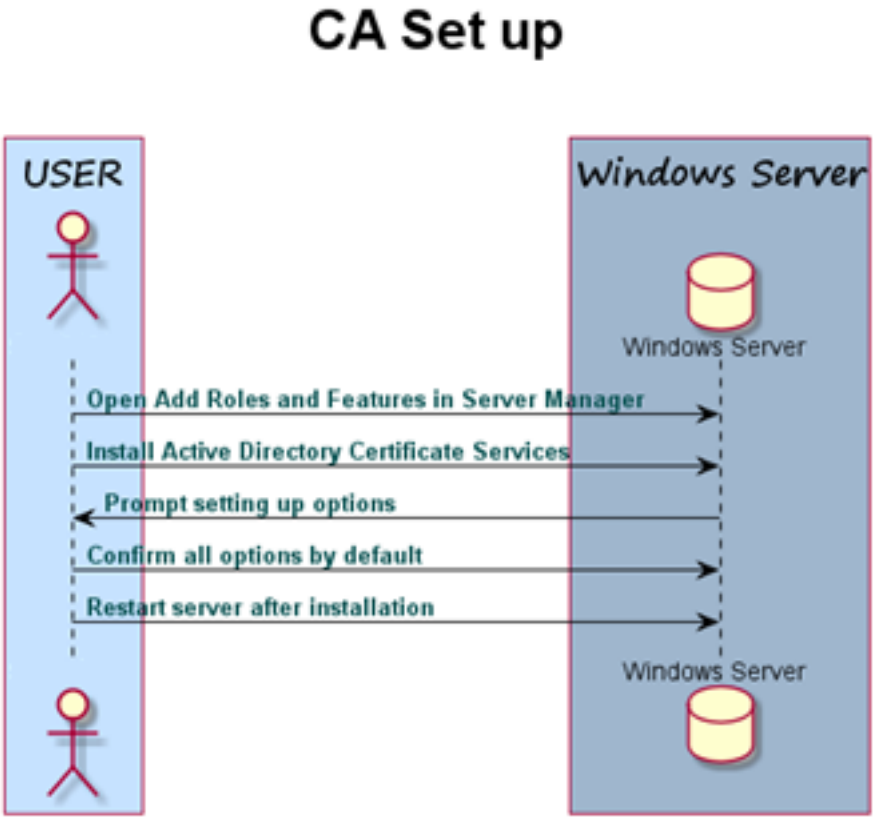
Vorausgehende Softwareinstallationen

Führen Sie die Installationsdatei von Active Directory Certificate Server aus und folgen Sie dann den angegebenen Schritten, um einen Benutzer und ein Passwort zu erstellen.

Server Manager sollte auf dem Host-PC vorinstalliert sein. Wenn nicht, kann die Software von der Microsoft-Website heruntergeladen werden.

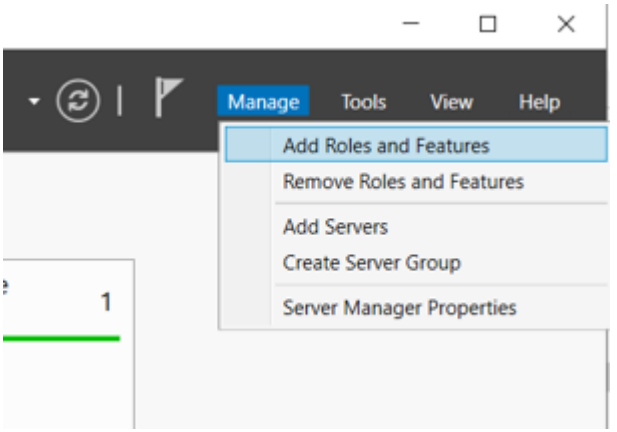
Übersicht über die Installation von Microsoft Windows Active Directory Certificate Server

Die folgende Abbildung bietet eine Übersicht über den Einrichtungsprozess der Zertifizierungsstelle (CA: Certificate Authority):

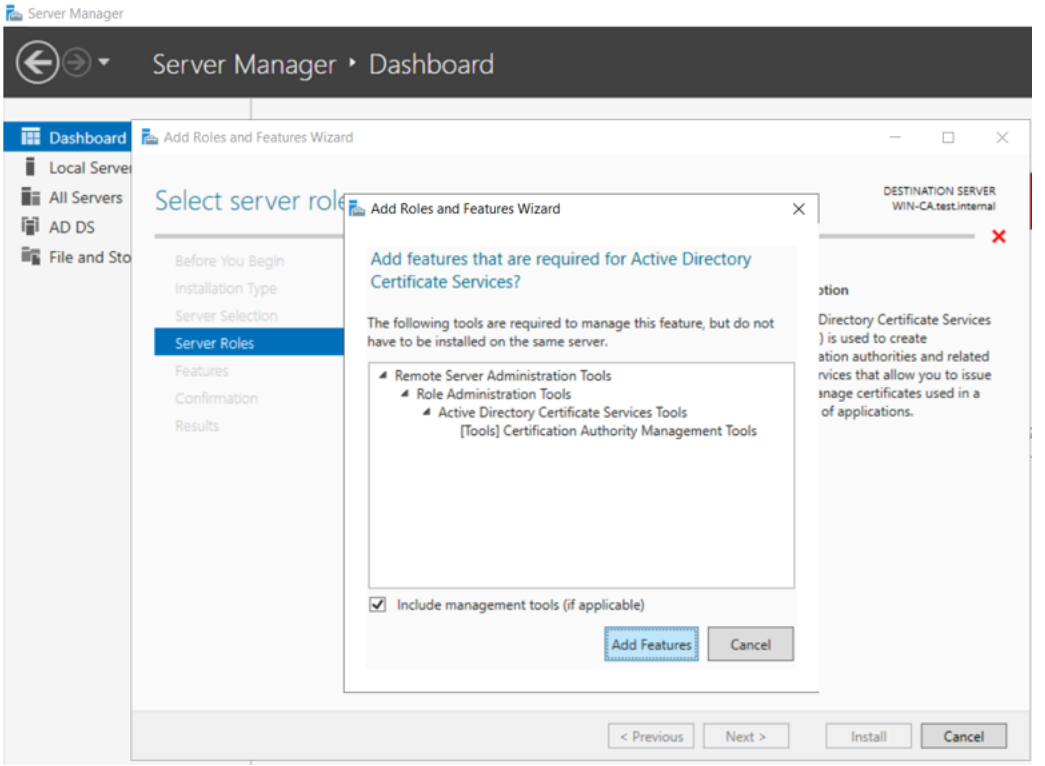


Installation von ADCS (Active Directory Certificate Server)

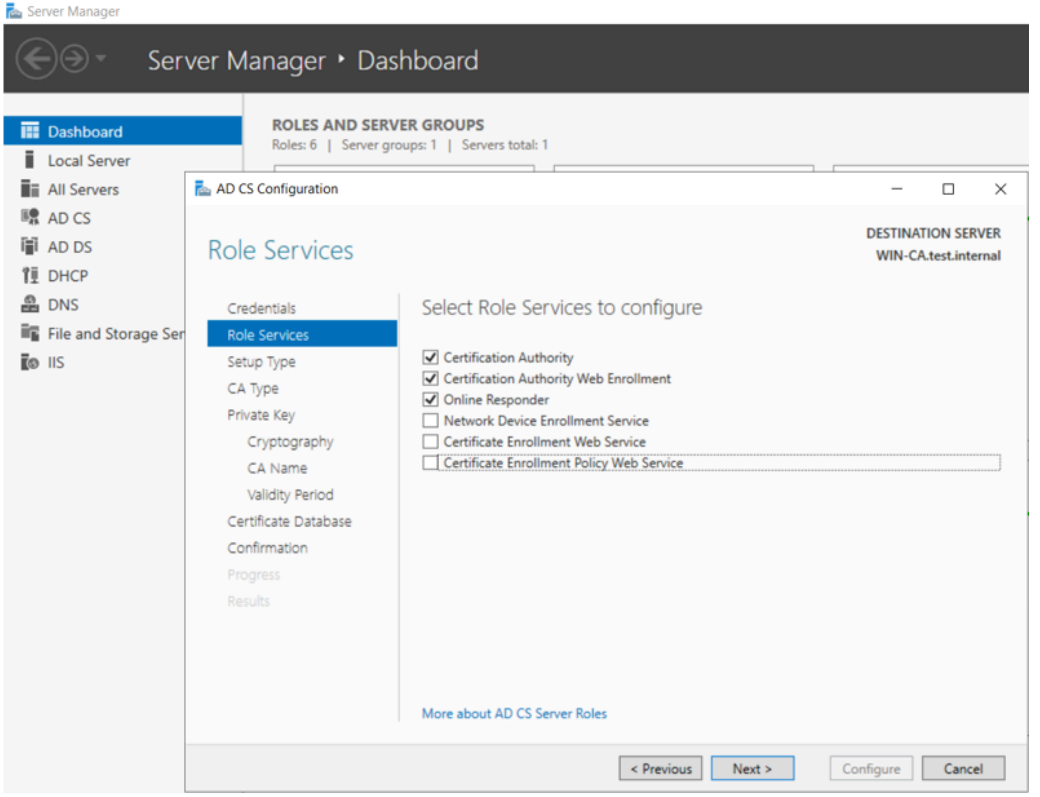
1. Starten Sie Microsoft Windows™ Server Manager und öffnen Sie das Dashboard.
2. Wählen Sie **Verwalten > Rollen und Funktionen hinzufügen** aus.



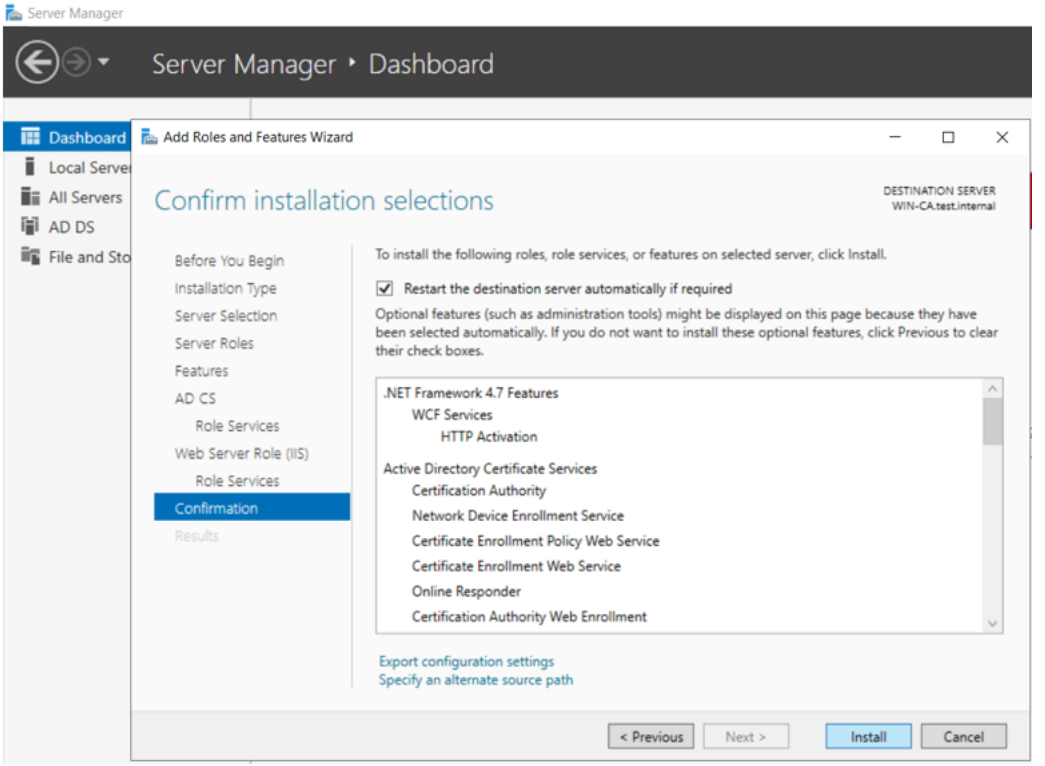
3. Fügen Sie die erforderlichen Rollen und Funktionen hinzu und integrieren Sie die Managementtools:



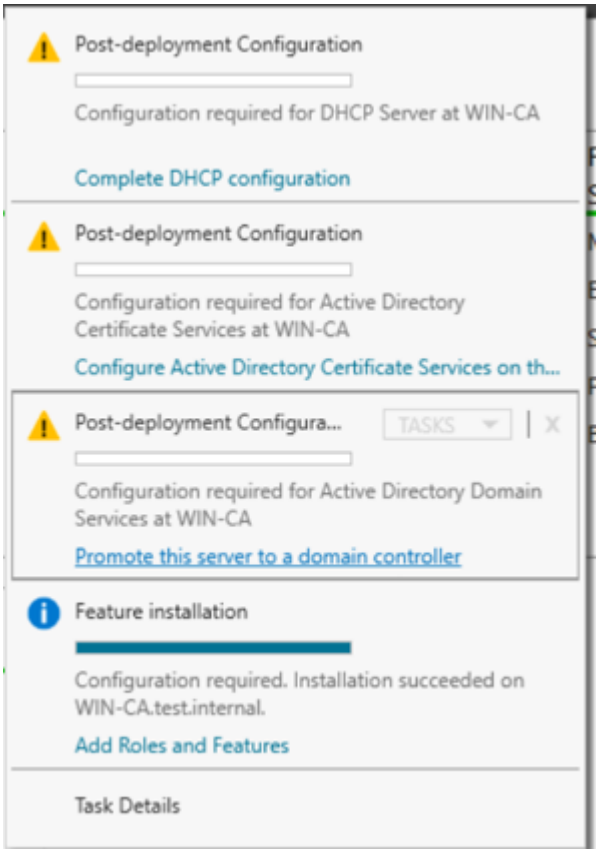
4. Wählen Sie die zu konfigurierenden Rollendienste aus:



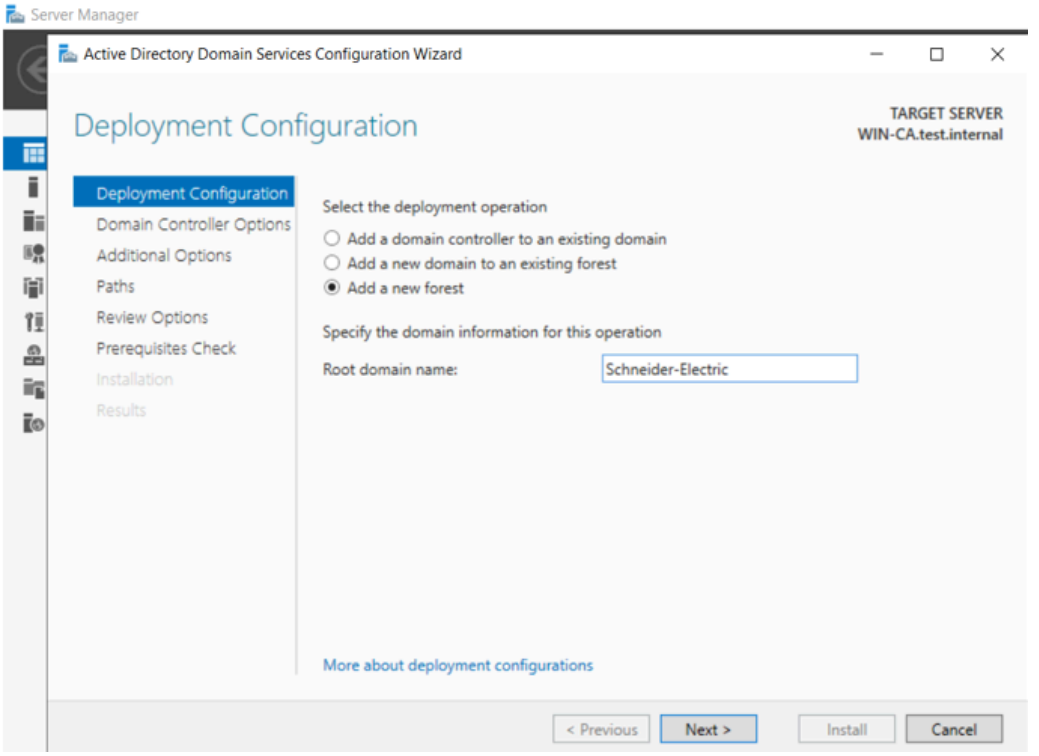
5. Bestätigen Sie die Installationsauswahl:



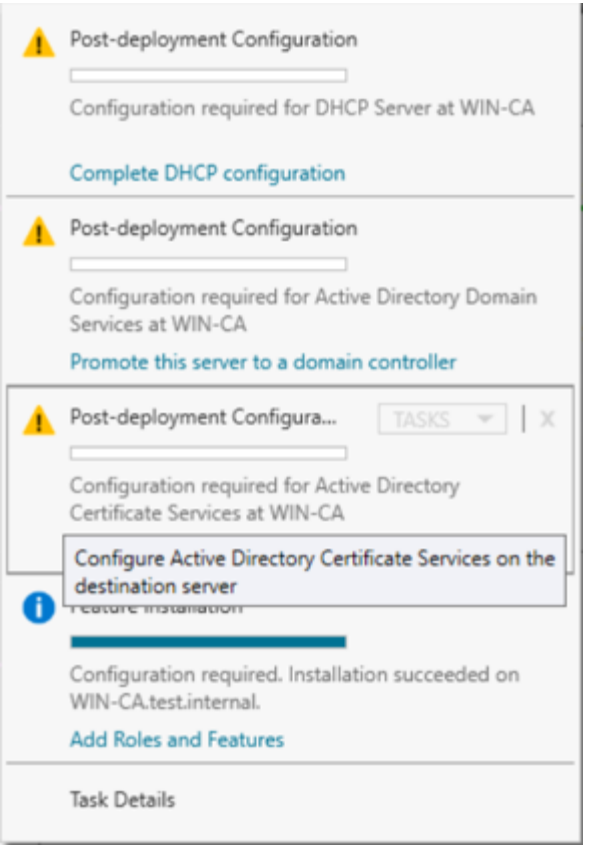
6. Klicken Sie auf **Installieren**. Server Manager zeigt den Installationsstatus an:



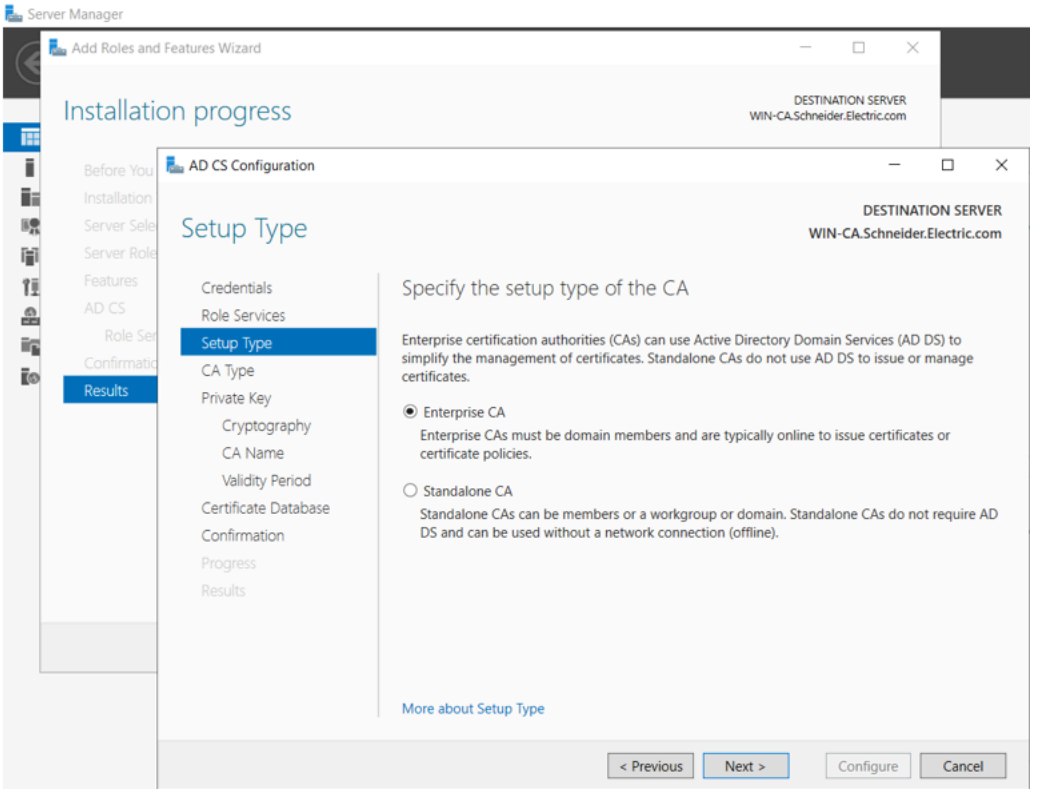
7. Wählen Sie den Implementierungsvorgang aus, indem Sie eine neue Gesamtstruktur erstellen oder zu einer bestehenden Gesamtstruktur hinzufügen, und geben Sie die Domäne an:



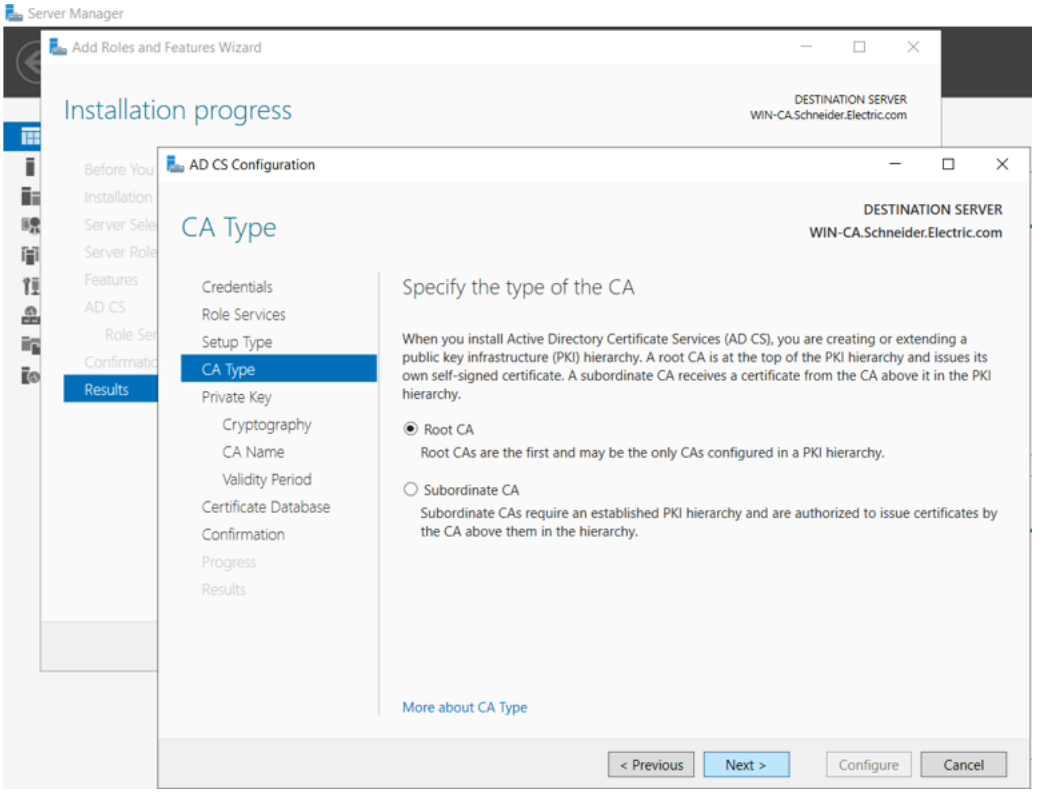
8. Server Manager zeigt die Auswahlmöglichkeiten an:



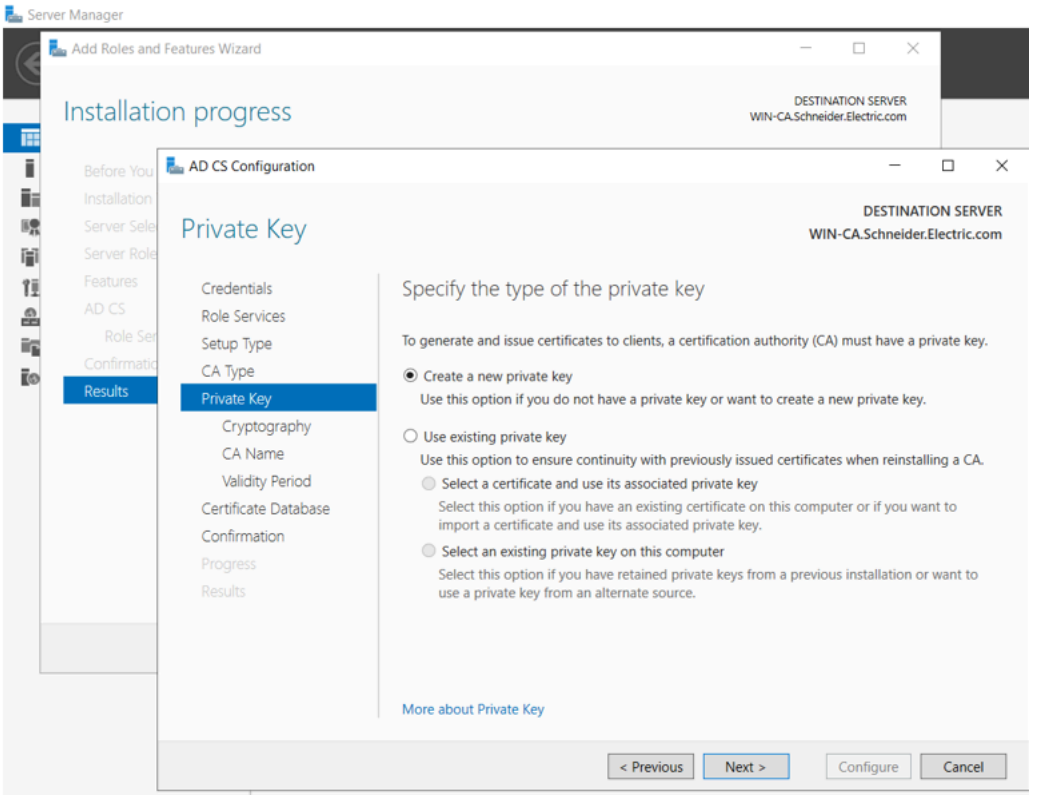
9. Geben Sie den Typ der einzurichtenden Zertifizierungsstelle an:



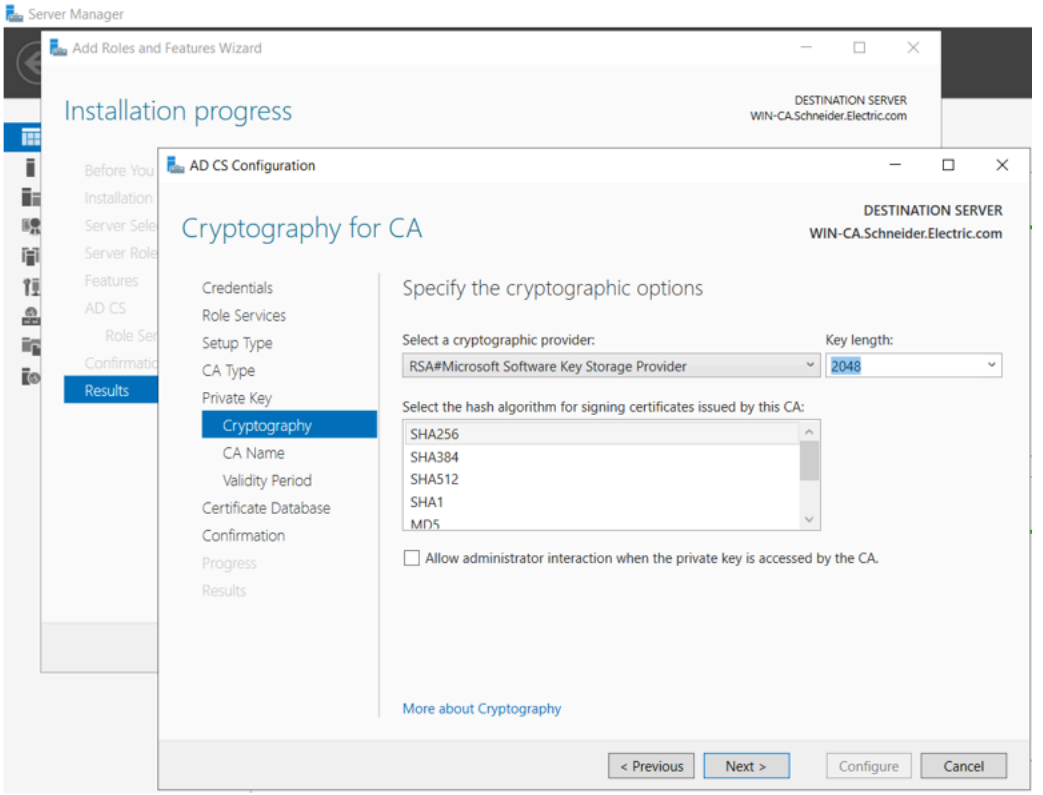
10. Geben Sie den Typ der Zertifizierungsstelle an:



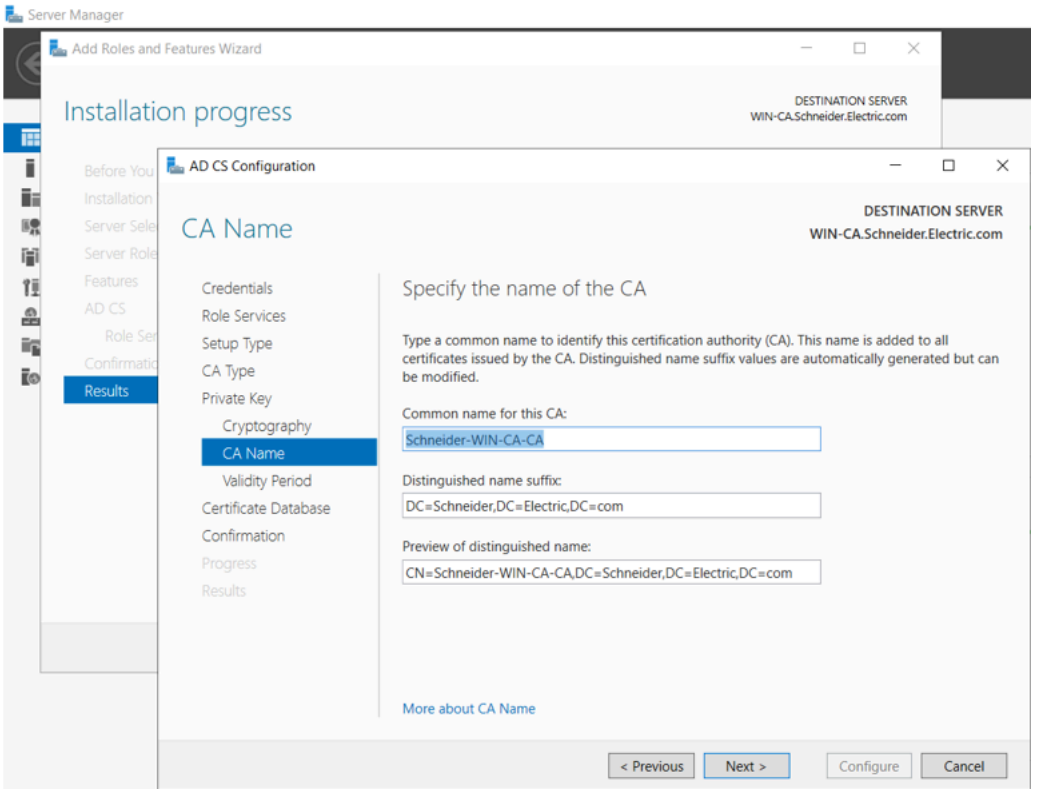
11. Geben Sie den Typ des privaten Schlüssels an:



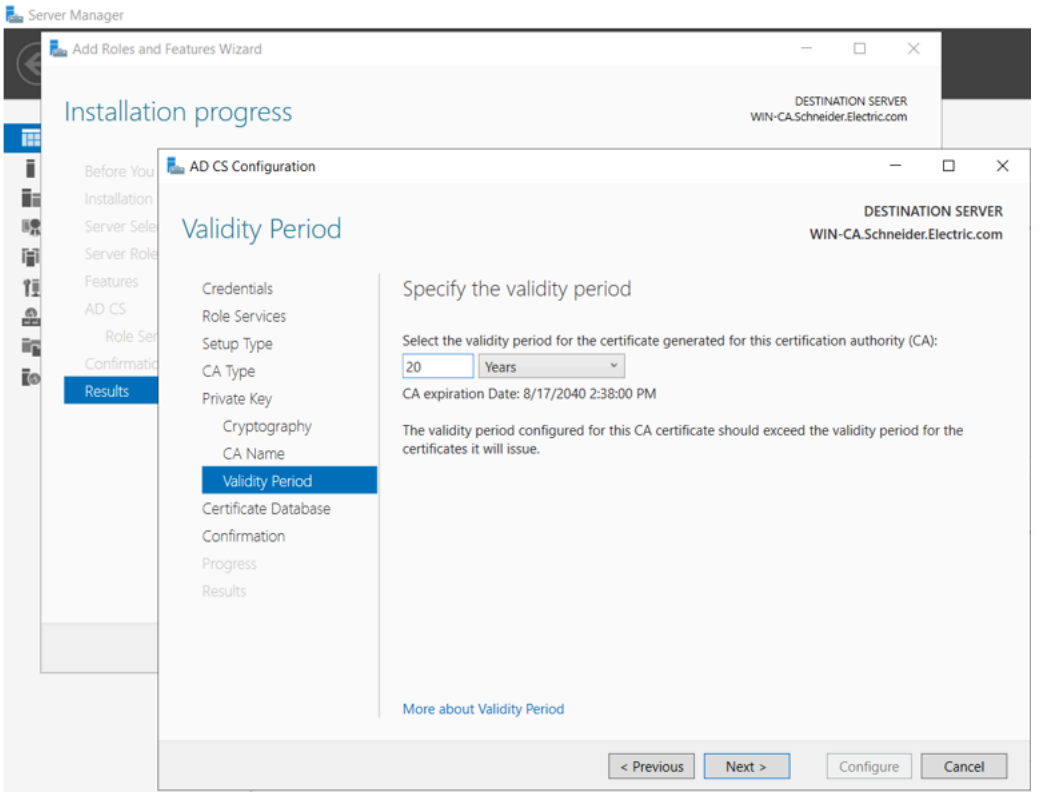
12. Nehmen Sie die kryptografische Auswahl vor:



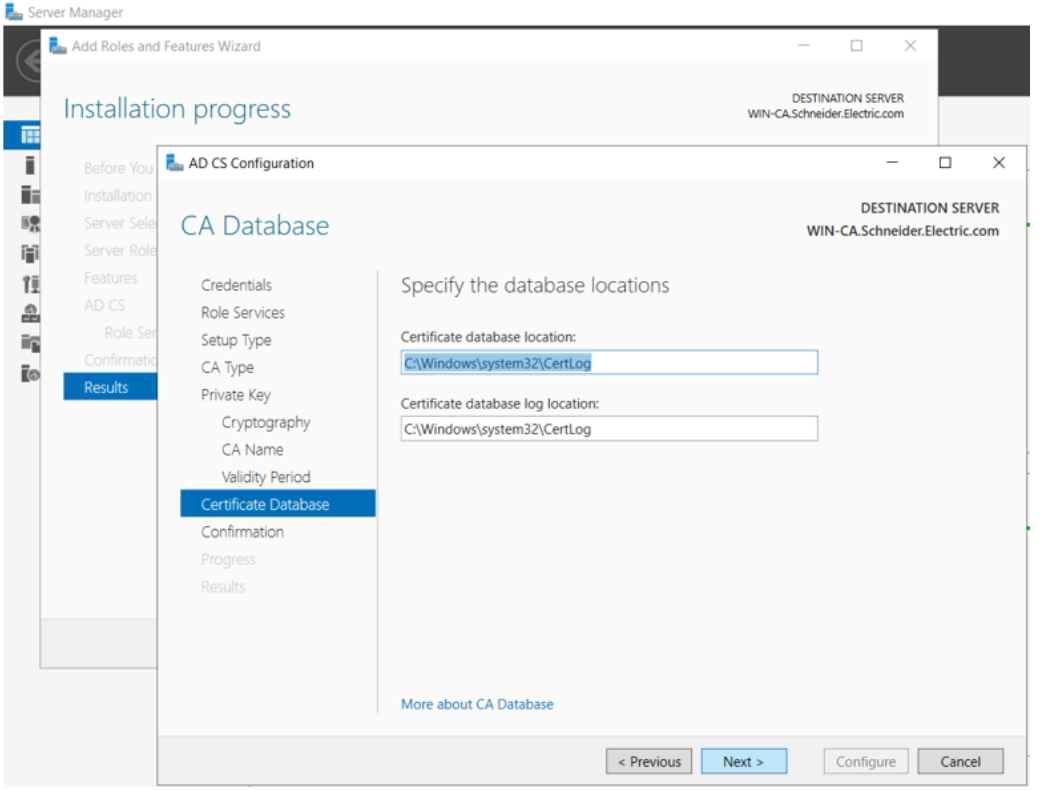
13. Nehmen Sie die Namensauswahl für die Zertifizierungsstelle vor:



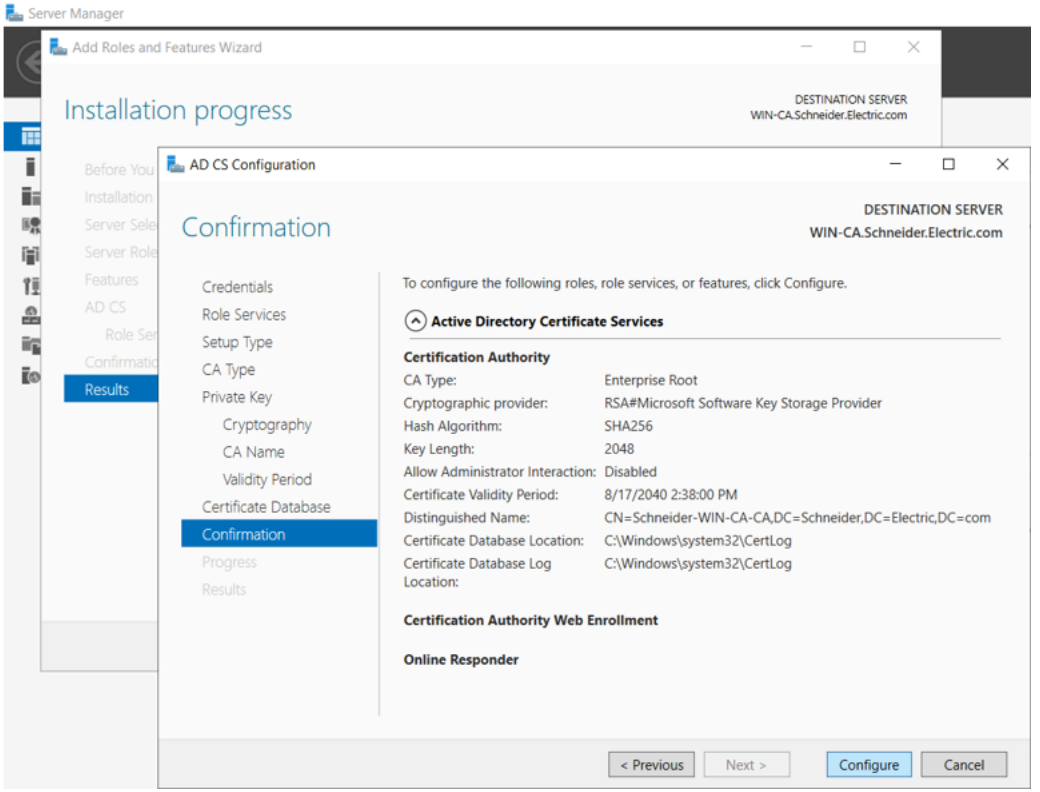
14. Geben Sie die Gültigkeitsdauer an. Die typische Gültigkeitsdauer eines CA-Zertifikats beträgt 5 Jahre:



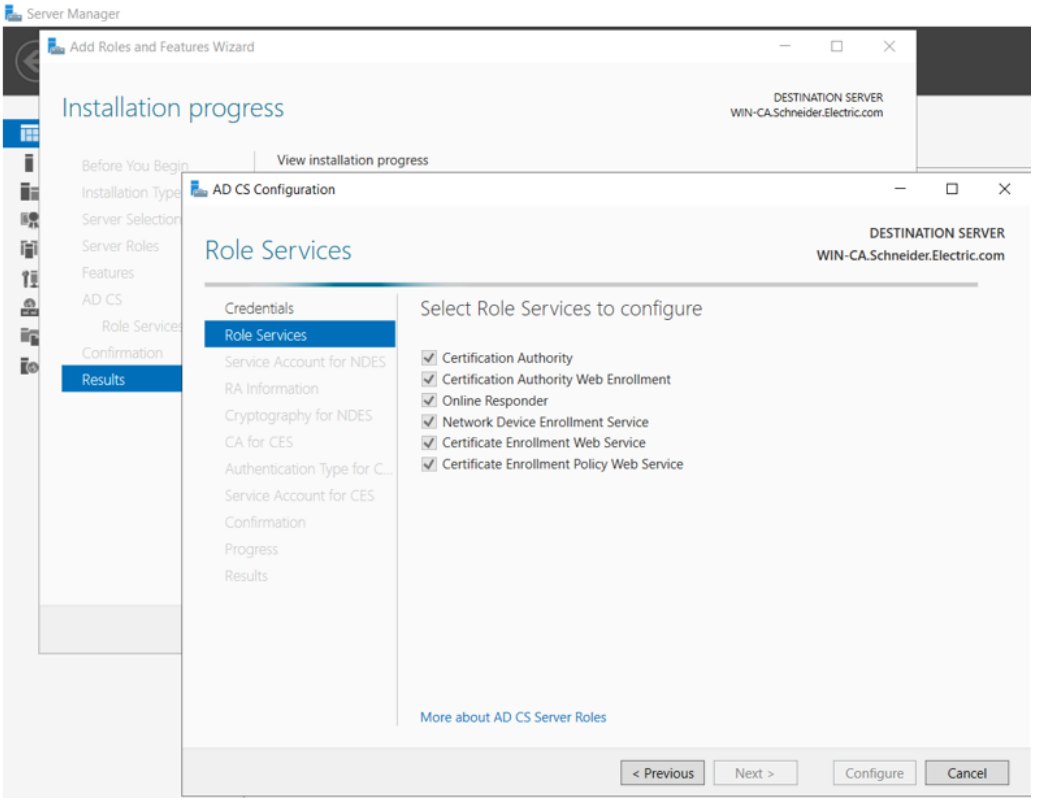
15. Geben Sie die Speicherorte der Zertifikatdatenbank und des Protokolls an:



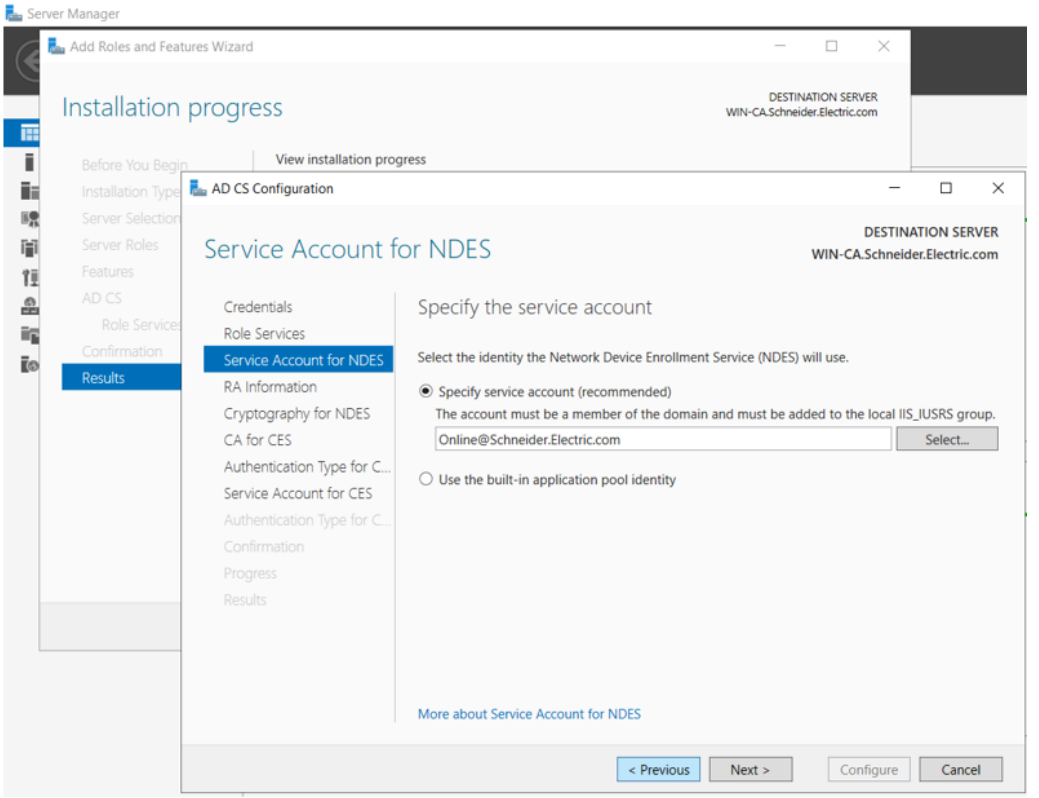
16. Bestätigen Sie die ausgewählten Active Directory-Zertifikatdienste und klicken Sie, wenn zutreffend, auf **Konfigurieren**:



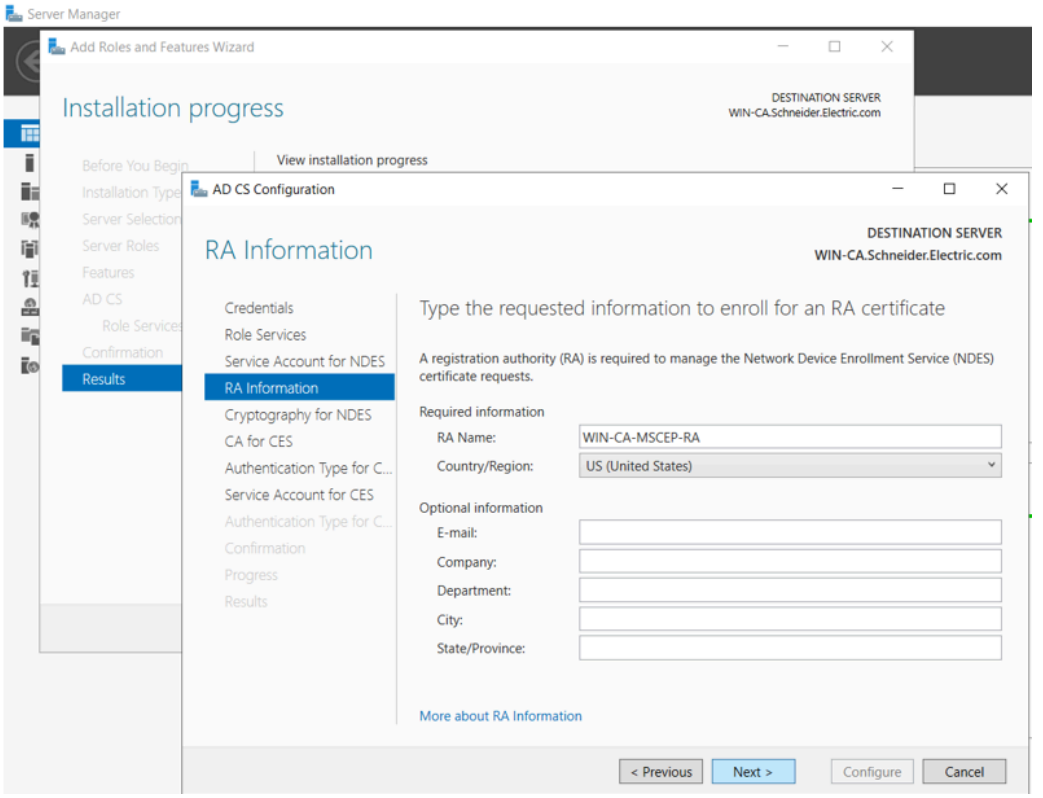
17. Wählen Sie die Rollendienste aus, die konfiguriert werden sollen:



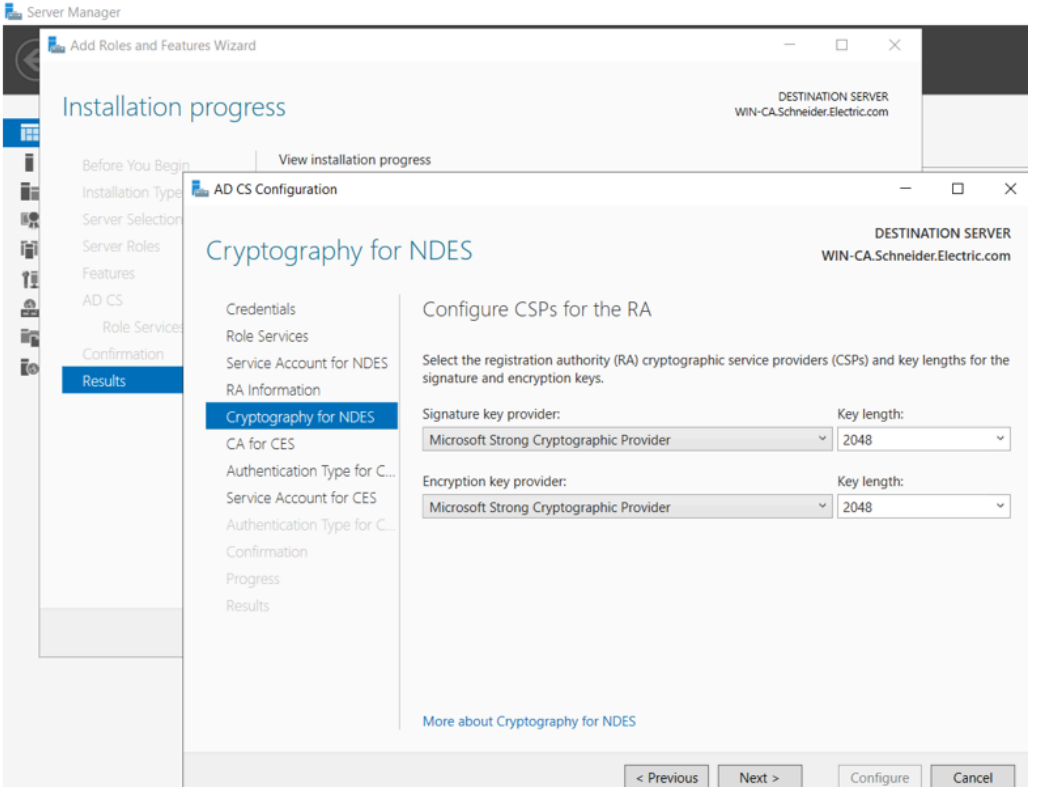
18. Geben Sie das Dienstkonto an:



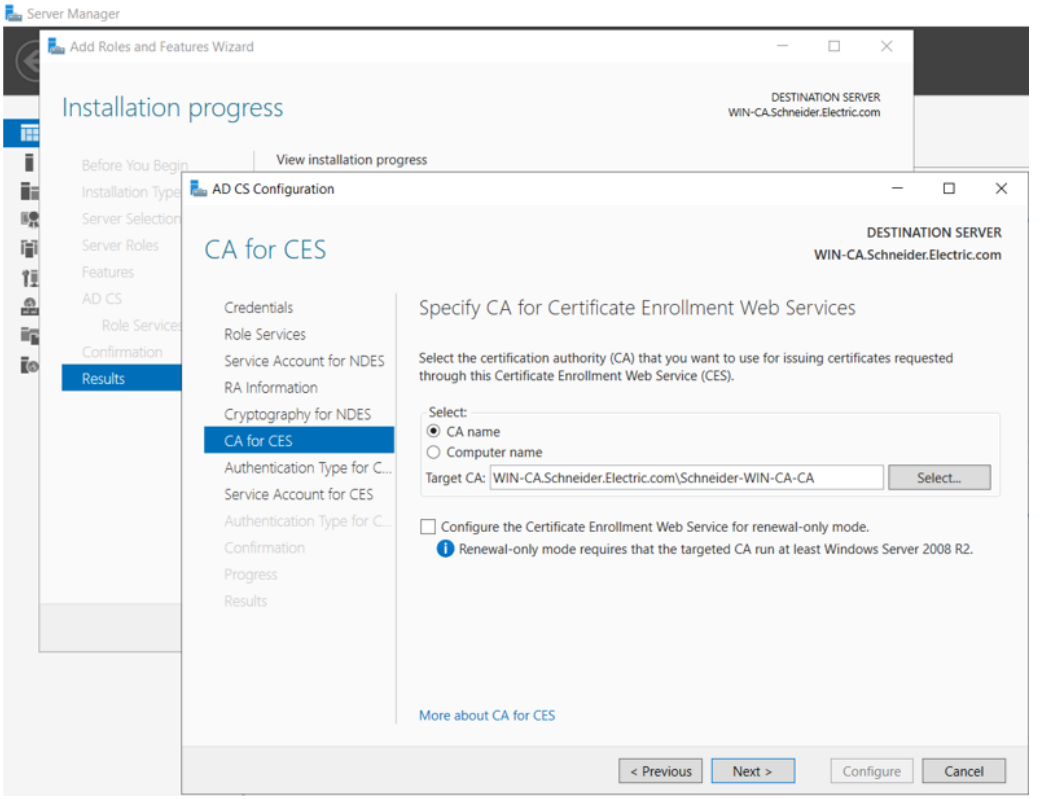
19. Geben Sie die Informationen ein, die zur Registrierung für ein Zertifikat der Registrierungsbehörde (RA: Registration Authority) erforderlich sind:



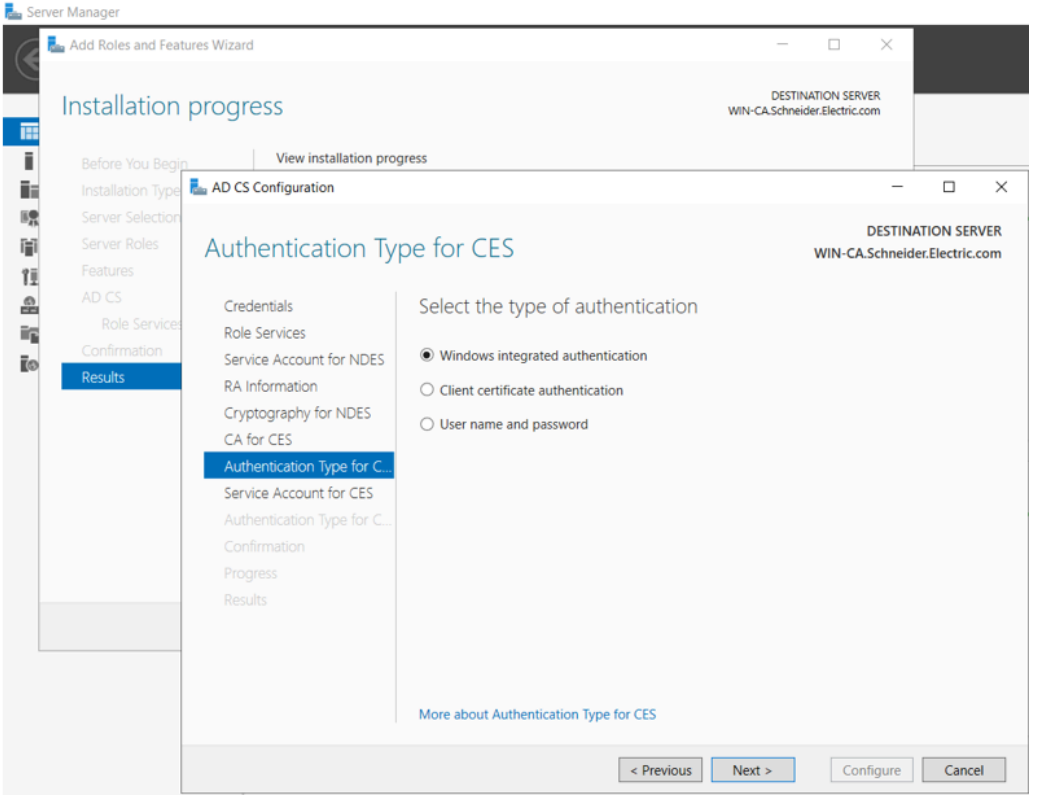
20. Wählen Sie die Verschlüsselungseinstellungen für die RA aus:



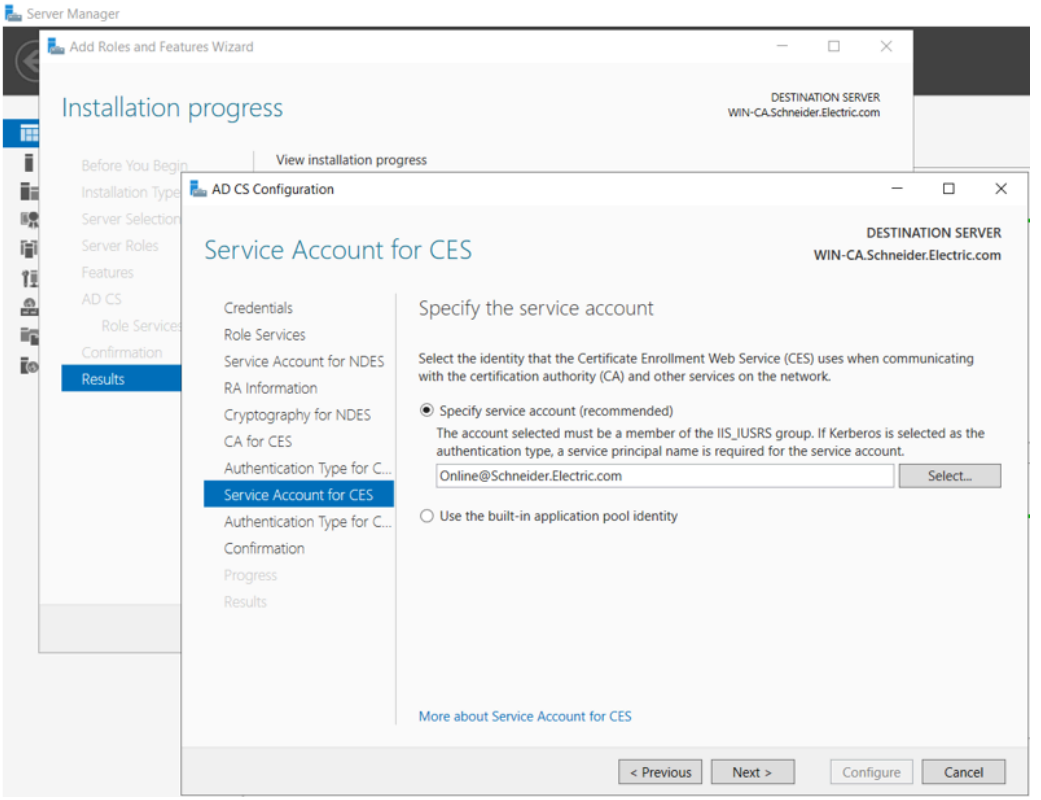
21. Geben Sie die Zertifizierungsstelle für Webdienste zur Zertifikatregistrierung an:



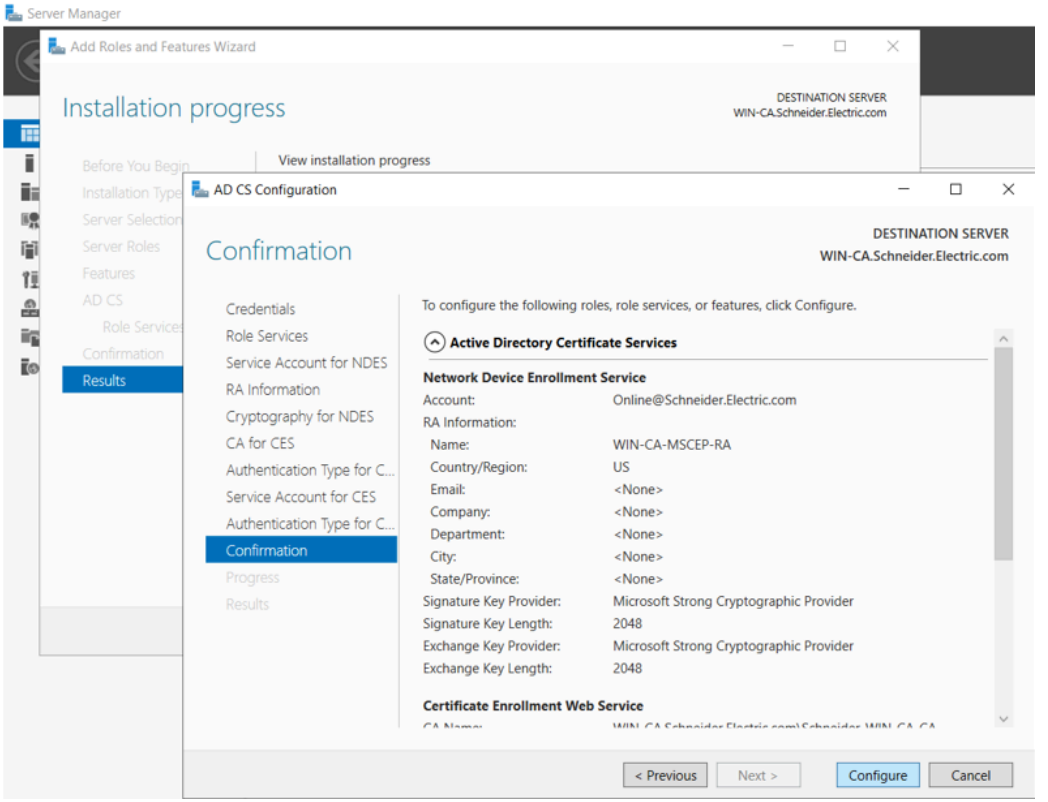
22. Wählen Sie einen Authentifizierungstyp aus:



23. Geben Sie das Dienstkonto an:



24. Bestätigen Sie die Rollen, Dienste und Funktionen und klicken Sie auf **Konfigurieren**:



Damit ist die Einrichtung von Active Directory Certificate Server abgeschlossen.

Anwendung der Vorlage der Zertifizierungsstelle

Der letzte Schritt bei der Einrichtung einer Microsoft Windows-Zertifizierungsstelle (CA: Certificate Authority) ist die Anwendung der von Schneider Electric bereitgestellten CA-Vorlage.

Die Vorlage und die zugehörigen Elemente sind in der von Schneider Electric bereitgestellten Datei „TemplatePackage.zip“ enthalten.

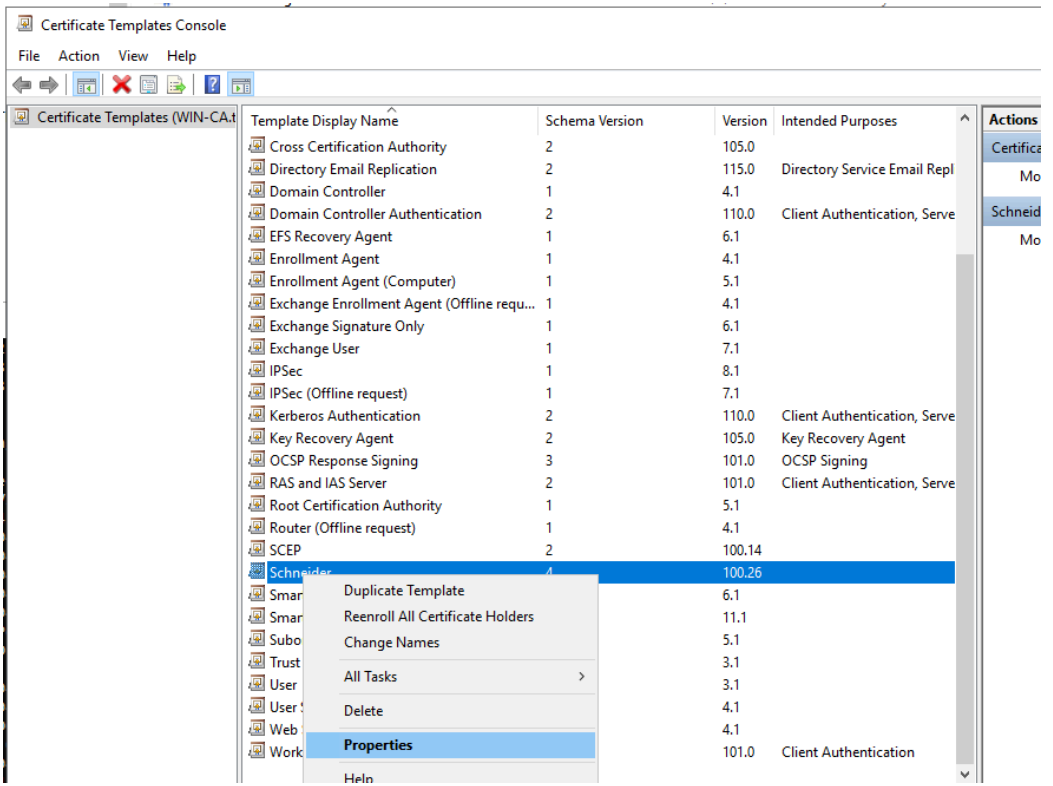
Gehen Sie vor wie folgt, um das Zertifikat zu übernehmen:

1. Dekomprimieren Sie die Datei „TemplatePackage.zip“ und kopieren Sie deren Inhalt (einen Ordner mit der Bezeichnung „TemplatePackage“) in einen anderen Speicherort als C:\Windows\System32...

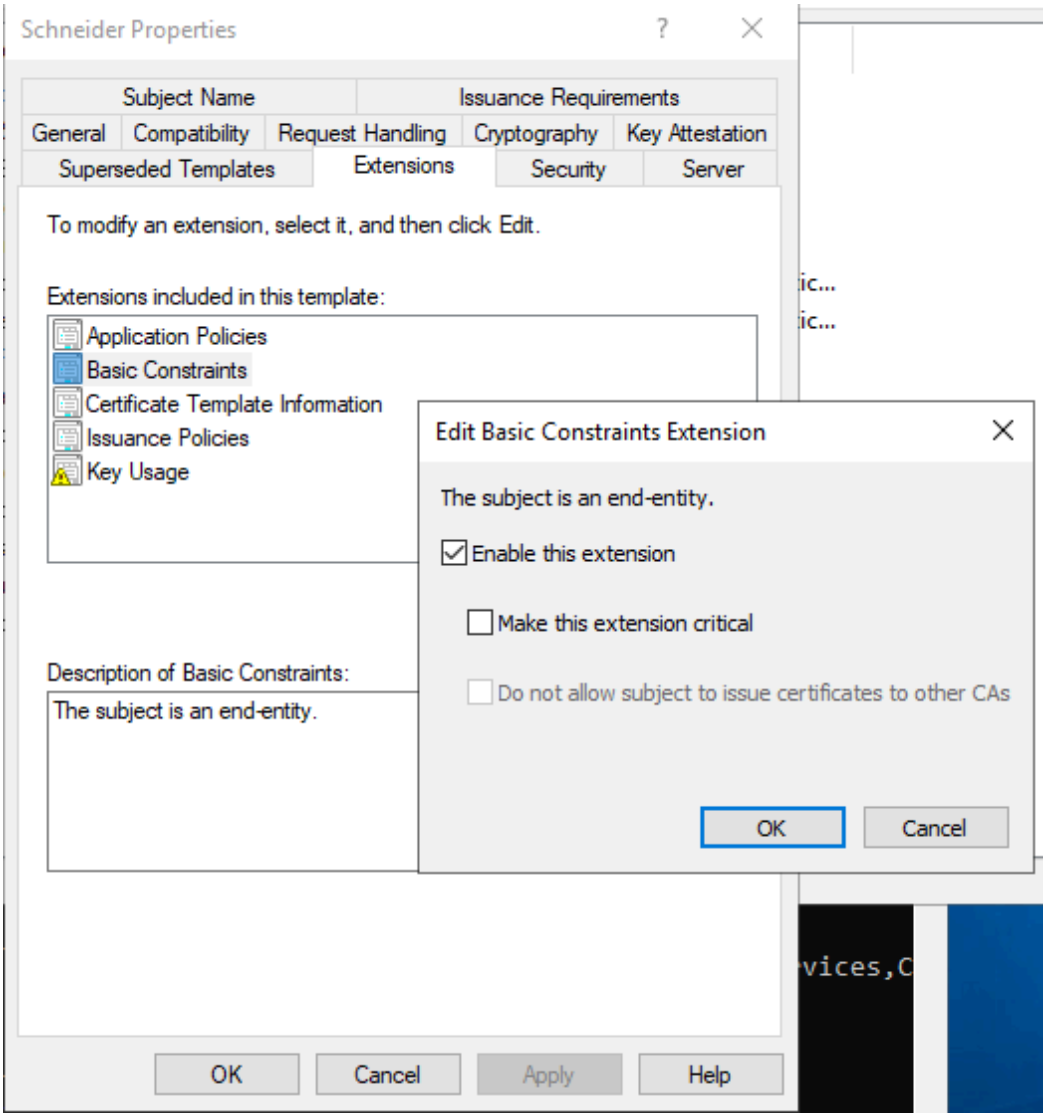
   Sie können diesen Ordner beispielsweise in das Verzeichnis „C:\Users\Administrator\Desktop\“ kopieren.
2. Starten Sie Microsoft Windows PowerShell (oder ein anderes Befehlstool) als Administrator.
3. Navigieren Sie zu dem Ordner, in dem Sie TemplatePackage abgelegt haben. Beispiel:

   ```
   > cd C:\Users\Administrator\Desktop\TemplatePackage
   ```
4. Führen Sie die Vorlage im Ordner TemplatePackage wie folgt aus:

   ```
   > .\ImportCertificateTemplate.ps1
   ```
5. Öffnen Sie auf dem Host-PC die Zertifikatvorlagenkonsole, klicken Sie mit der rechten Maustaste auf das Schneider-Zertifikat und wählen Sie **Eigenschaften** aus:



6. Öffnen Sie im Fenster **Schneider-Eigenschaften** die Registerkarte **Erweiterungen**, doppelklicken Sie auf **Grundlegende Einschränkungen**, wählen Sie im Dialogfeld **Grundlegende Einschränkungen bearbeiten** die Option **Diese Erweiterung aktivieren** aus und klicken Sie auf **OK**:



Durchführen einer manuellen Registrierung

Informationen zur Durchführung dieser Aufgabe finden Sie im Abschnitt Manuelle Zertifikatregistrierung, Seite 119.

Klicken Sie auf den in dieses Hilfethema eingebetteten Link, um eine „How To“-Videopräsentation aufzurufen.

Glossar

I

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.

R

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.

S

SNTP:

(*Simple Network Time Protocol*) Siehe NTP.

T

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.

Index

W

Z

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, sollten Sie um Bestätigung der in dieser Veröffentlichung gegebenen Informationen nachsuchen.

PHA83352.04