M580

Integriertes Modul BMENUA0100 OPC UA

Installations- und Konfigurationshandbuch

Übersetzung der Originalbetriebsanleitung

05/2022

PHA83352.02

www.se.com

Rechtliche Hinweise

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

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

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

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

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

Inhaltsverzeichnis

Sicherheitshinweise 7
Bevor Sie beginnen 8
Start und Test 9
Betrieb und Einstellungen 10
Informationen zum Dokument 11
Merkmale des Moduls BMENUA0100 14
Merkmale des Moduls 14
Modulbeschreibung 16
Modul-LEDs 21
Normen und Zertifizierungen 23
Normen und Zertifizierungen 23
BMENUA0100-Modulstandard 23
Kompatibilität der BMENUA0100-Firmware mit EcoStruxure™ Control Expert 24
Funktionsbeschreibung des Moduls BMENUA0100 25
Einstellungen der Cybersicherheit-Betriebsart 25
Betriebsmodus der Cybersicherheit 25
OPC UA-Dienste 31
Betriebskenndaten des BMENUA0100-OPC UA-Servers 32
OPC UA-Server 33
BMENUA0100 – OPC UA-Server-Stack – Dienste 35
BMENUA0100 – OPC UA-Server-Stack – Datenzugriffsdienste 36
BMENUA0100 – OPC UA Server-Stack – Erkennungs- und Sicherheitsdienste 38
BMENUA0100 – OPC UA-Server-Stack – Veröffentlichungs- und Abonnementdienste 41
BMENUA0100 – OPC UA-Server-Stack – Transportdienste 45
Erkennen von PAC-Variablen 46
Zuordnung von Control Expert-PAC-Variablen zu OPC UA-Datenlogikvariablen 46
Hot Standby und Redundanz 50
OPC UA-Server – Redundanz 50
Unterstützte Architekturen 59

Unterstützte Konfigurationen des BMENUA0100-Moduls....59
Isoliertes Steuerungsnetzwerk mit M580-Hot Standby-PACs....62
Nicht isoliertes flaches Netzwerk mit M580-Hot Standby....64
Flaches Netzwerk mit mehreren M580-Standalone-CPUs und einem einzelnen SCADA-System....67
Flaches Netzwerk mit mehreren M580-Standalone-CPUs und redundantem SCADA....69
Flaches Netzwerk mit M580-Hot Standby-CPUs und redundantem SCADA....71
Hierarchisches Netzwerk mit mehreren M580-Standalone-CPUs, die an das Steuerungsnetzwerk angeschlossen sind, und redundantem SCADA....73
Hierarchisches Netzwerk mit mehreren M580-Hot Standby-CPUs und redundanten SCADA-Verbindungen....75
Inbetriebnahme und Installation....77
Inbetriebnahme-Checkliste für das BMENUA0100-Modul....77
Inbetriebnahme des BMENUA0100-Moduls....78
Installation der Software BMENUA0100....81
Konfiguration....84
Konfiguration der Cybersicherheitseinstellungen des BMENUA0100-Moduls....84
Einführung in die Webseiten des BMENUA0100-Moduls....84
Startseite „Home“....89
Einstellungen....92
Zertifikatverwaltung....105
Zugriffssteuerung....114
Konfigurationsverwaltung....116
Konfiguration des BMENUA0100-Moduls in Control Expert....118
Konfiguration der IP-Adresseinstellungen....118
Konfiguration der Quellzeitstempelung....122
Verwaltung der quellzeitgestempelten Variablen....123
Konfiguration des Netzwerkzeitdienstes....128
SNMP-Agent-Konfiguration....131
Konfiguration der Einstellungen der M580-CPU für den OPC UA-Client - Serververbindungen....135
Konfiguration der Sicherheitseinstellungen der M580-CPU....135

Diagnose ... 136
Diagnose-LEDs ... 136
BMENUA0100 - Abgeleiteter Datentyp (DDT) ... 140
Konfiguration der Elementarfunktion READ_DDT ... 145
Konfiguration der elementaren Funktion READ_NUA_DDT ... 150
OPC UA-Diagnose ... 151
Syslog ... 156
Modbus-Diagnose ... 159
SNMP-Diagnose ... 161
OPC UA-Diagnose-Webseite ... 161
Optimieren der Leistung des BMENUA0100-Moduls ... 164
Optimierung der Leistung des BMENUA0100-Moduls ... 164
Fehlerbehebung für das BMENUA0100-Modul ... 167
Firmwareaktualisierung ... 171
Tool EcoStruxure™ Automation Device Maintenance ... 171
Anhänge ... 173
CPU-Verbindungen ... 174
Verbindungen zwischen OPC UA Server und CPU ... 174
Architekturen für die Dienstweiterleitung (IP) ... 175
Unterstützte Architekturen für die Dienstweiterleitung (IP) ... 176
Nicht unterstützte Architekturen für die Dienstweiterleitung (IP) ... 179
IP-Weiterleitung und OPC UA-Kommunikation ... 180
IP-Weiterleitung - Auswirkungen auf die Leistung ... 180
IP-Weiterleitung und OPC UA - Auswirkungen auf die Leistung ... 181
IPSEC-Windows-Skripts ... 183
Skripts zur Konfiguration der IKE/IPSEC-Windows-Firewall ... 183
Einrichtung einer Windows-Zertifizierungsstelle ... 186
Vorbereitung ... 186
Überblick über die Installation von Microsoft Windows ADCS ... 187
Installation von ADCS (Active Directory Certificate Server) ... 188
Anwendung der Vorlage der Zertifizierungsstelle ... 210
Glossar ... 215
Index ... 216

Sicherheitshinweise

Wichtige Informationen

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



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



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

⚠ GEFAHR

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

⚠ WARNUNG

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

⚠ VORSICHT

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

HINWEIS

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

Bitte beachten

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

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

Bevor Sie beginnen

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

⚠WARNUNG

UNBEAUFSICHTIGTE GERÄTE

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

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

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

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

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

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

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

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

Start und Test

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

⚠WARNUNG

GEFAHR BEIM GERÄTEBETRIEB

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

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

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

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

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

Vor dem Einschalten der Anlage:

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

Betrieb und Einstellungen

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

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

Informationen zum Dokument

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.

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

Gültigkeitsanmerkung

Diese Dokumentation ist gültig für das M580-System bei Verwendung von EcoStruxure™ Control Expert 15.0 oder höher.

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

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

Weiterführende Dokumentation

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

Titel der Dokumentation	Referenznummer
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 (Englisch), NHA89119 (Französisch), NHA89120 (Deutsch), NHA89121 (Italienisch), NHA89122 (Spanisch), NHA89123 (Chinesisch)
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(Englisch), 33002440(Französisch), 33002441(Deutsch), 33003702(Italienisch), 33002442 (Spanisch), 33003703(Chinesisch)
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)
EcoStruxure™ Control Expert, Installationshandbuch	35014792 (Englisch), 35014793 (Französisch), 35014794 (Deutsch), 35014795 (Spanisch), 35014796 (Italienisch), 35012191 (Chinesisch)

Titel der Dokumentation	Referenznummer
Web Designer für FactoryCast - Benutzerhandbuch	35016149(Englisch), 35016150(Französisch), 35016151(Deutsch), 35016152(Italienisch), 35016153 (Spanisch), 35016154(Chinesisch)
Modicon-Steuerungsplattform Cybersicherheit, Referenzhandbuch	EIO0000001999 (Englisch), EIO0000002001 (Französisch), EIO0000002000 (Deutsch), EIO0000002002 (Italienisch), EsIO0000002003 (Spanisch), EIO0000002004 (Chinesisch)

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

Merkmale des Moduls BMENUA0100

Einführung

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

Merkmale des Moduls

Einführung

Das Modicon-Servermodul BMENUA0100 OPC UA bietet leistungsstarke OPC UA-Funktionen für Modicon M580-ePAC-Systeme.

OPC UA ist eine moderne, sichere, offene und zuverlässige Kommunikationsplattform für die industrielle Kommunikation, die flexibel und skalierbar ist, von ressourcenbeschränkten IoT-Sensoren vor Ort bis hin zu Servern der Enterprise-Klasse im Rechenzentrum oder in der Cloud. Über das Verbinden und Verschieben von Daten hinaus definiert OPC UA ein umfassendes Informationsmodell zur Veröffentlichung und Verwaltung von Metainformationen und Systemkontexten, um die Automatisierungstechnik und Systemintegration zu vereinfachen.

Bei der Realisierung eines Kommunikationsstandards für moderne, vernetzte Industriebetriebe stellt OPC UA eine gemeinsame Verbindung zwischen angeschlossenen Produkten vor Ort, Automatisierungs- und Edge-Controllern sowie Unternehmensanwendungen und Analytik her. Somit ist es für Kompatibilität mit modernen IT- und Sicherheitsinfrastrukturen wie Firewalls, VPNs und Proxys ausgelegt. OPC UA wird sowohl für funktionale Anforderungen als auch für die Bandbreite skaliert.

Funktionen

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

Durch das Modul BMENUA0100 werden die folgenden Funktionen auf der Modicon M580-Plattform bereitgestellt:

Allgemein:

- Direkter und optimierter Zugriff auf das Datenwörterbuch von Control Expert für die einfache Zuordnung zwischen Control Expert und OPC UA-Variablen, Seite 46.
- Unterstützung von Hot Standby-Konfigurationen über OPC UA-Redundanz, Seite 50.
- Kompatibilität mit M580-Sicherheitssystemen als nicht störendes Modul des Typs 1 gemäß Definition des TÜV Rheinland.
- Nahtlose Ethernet-Baugruppenträger-Kommunikation.
- DHCP/FDR-Client für den Download von gespeicherten Konfigurationseinstellungen (nicht für die Cybersicherheit).
- NTP-Zeitserver, Seite 128 und Clientsynchronisation.
- Mehrere Diagnosemethoden, einschließlich LEDs, Seite 136, DDT, Seite 140, OPC_UA-Variablen und Datenelemente, Seite 151, Syslog, Seite 156, Modbus, Seite 159, SNMP, Seite 161 und sichere Webseiten, Seite 161.
- Firmware-Aktualisierung über Tool EcoStruxure™ Automation Device Maintenance, Seite 171.
- Firmware-Integritätsprüfung.
- Hardware-gesicherter Speicher.

Cybersicherheit:

- Sichere Kommunikation über HTTPS, OPC UA (optional) und IPSEC (optional).
- Über HTTPS konfigurierbare OPC UA-Sicherheit, Seite 92 auf Modulebene.
- Die Möglichkeit, den ein- und ausgehenden Kommunikationsstrom durch Aktivieren und Deaktivieren von Kommunikationsdiensten, Seite 94 zu steuern.
- IPSEC, Seite 101 basierend auf einem Pre-Shared-Key (PSK) zur Sicherung von Diensten wie SNMPv1, Modbus/TCP, Syslog und NTPv4.

  HINWEIS: Das Modul BMENUA0100 unterstützt IPSEC im Hauptmodus, nicht im aggressiven Modus. Ein IPSEC-Kanal kann entweder durch den BMENUA0100-Server oder einen dezentralen OPC UA-Client geöffnet werden. Auf einem PC-Client wird IPSEC auf Systemen mit Windows 7, 10 und Windows Server 2016 unterstützt und validiert.

Authentifizierungsmanagement:

- Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) und Benutzerauthentifizierung, Seite 114 für HTTPS- und OPC UA-Clients.
- Zertifikate, Seite 105 für OPC UA-Client-Anwendungseinheiten.

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

- DHCP/FDR-Client für den Download von anderen als für die Cybersicherheit gespeicherten Konfigurationseinstellungen.
- Direkter und optimierter Zugriff auf das Datenwörterbuch von Control Expert für die Zuordnung zwischen Control Expert-Variablen und OPC UA-Server-Variablen, Seite 46.

- 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 128 und Clientsynchronisation.
- Kompatibilität mit Hot Standby-Konfigurationen über OPC UA-Redundanz, Seite 50.
- Sicherheitskonfiguration als nicht störendes Modul des Typs 1 gemäß Definition des TÜV Rheinland.
- Mehrere Diagnosemethoden, einschließlich LEDs, Seite 136, DDT, Seite 140, OPC_UA-Variablen und Datenelemente, Seite 151, Syslog, Seite 156, Modbus, Seite 159, SNMP, Seite 131 und sichere Webseiten, Seite 159.
- Firmware-Aktualisierung über das Tool EcoStruxure™ Maintenance Expert, Seite 171.
- Hardware-gesicherter Speicher.
- Integritätsprüfung der Firmware.

Modulbeschreibung

Einführung

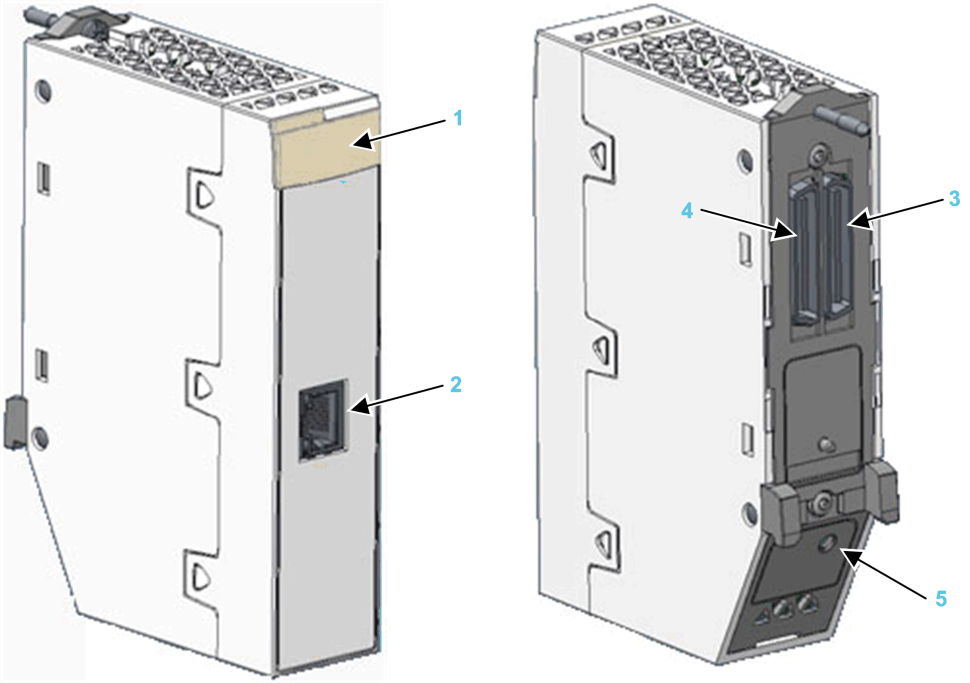
Schneider Electric bietet zwei Ethernet-Kommunikationsmodule mit einem integrierten OPC UA-Server für die Kommunikation mit OPC UA-Clients, einschließlich einem SCADA-System:

- 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 59 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 Ethernet-Verbindungs- und Aktivitäts-LEDs

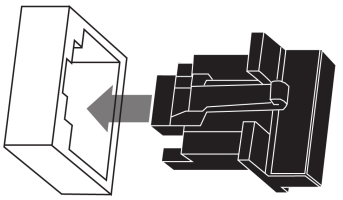
3 Ethernet-Baugruppenträger-Port

4 X Bus-Baugruppenträger-Port

5 Drehwahlschalter für die Betriebsart Cybersicherheit

Informationen zum Lesen der Modul-LEDs finden Sie im Abschnitt LED-Diagnose, Seite 136.

Wenn der Ethernet-Steuerungsanschluss nicht aktiviert ist, verwenden Sie den Stopper, der mit jedem Modul geliefert wird, um zu verhindern, dass Schmutz in den Steueranschluss 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 auch OPC UA-Clients im Baugruppenträger-Netzwerk über den BMENUA0100-Steuerungsport verbinden, sofern auf dem Computer, auf dem sich der OPC UA-Client befindet, 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-IP-Adressierung (128-Bit) 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 119 wird basierend auf der MAC-Adresse des Moduls automatisch zugewiesen, wenn eine IP-Adresse nicht konfiguriert ist. • Sicherer Zugriff auf den OPC UA-Server über IPv4- und IPv6-Protokolle. • Sicheres HTTPS-Protokoll (über IPv4) für die Firmware-Aktualisierung, Seite 171 und die Konfiguration der Cybersicherheit, Seite 84. • 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 des BMENUA0100-Moduls 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-Verbindung zur CPU: ◦ 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 höher ◦ 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 Firmware-Aktualisierung, Seite 171 und die Konfiguration der Cybersicherheit, Seite 84. ◦ NTPv4, SNMPv1 und Syslog.
X-Bus-	Das BMENUA0100-Modul verwendet die X Bus-Baugruppenträger-Kommunikation für Folgendes: • Empfang von 24-VDC-Spannung.

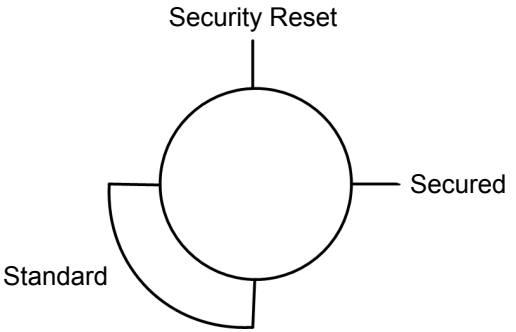
Port	Beschreibung
Baugruppenträger-Port	• Erkennung der Rack- und der Steckplatzadresse des BMENUA0100-Moduls. **HINWEIS:** Es erfolgt keine weitere Kommunikation über den X-Bus-Baugruppenträger-Port des BMENUA0100-Moduls.

Drehschalter

Auf der Rückseite des Moduls befindet sich ein Drehschalter mit drei Positionen. Verwenden Sie zum Ändern der Schalterstellung und zum Konfigurieren des Cybersicherheitmodus für das Modul nur den kleinen, mit dem Modul gelieferten Kunststoffschraubendreher.

HINWEIS
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS Verwenden Sie zum Ändern der Drehschalterposition nur den kleinen, mit dem Modul gelieferten Kunststoffschraubendreher. Die Verwendung eines Metallschraubendrehers kann den Schalter beschädigen und ihn unbrauchbar machen. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Die Positionen am Drehschalter sind:



Die Einstellungen sind:

- Secured mode (Sicherer Modus)
- Standard mode (Standardmodus)
- Security Reset (Sicherheits-Reset)

HINWEIS:

- Der Drehschalter ist nicht zugänglich, wenn das Modul im Rack platziert ist.
- Stellen Sie in einem Hot Standby-System sicher, dass die Positionen des Drehschalters des BMENUA0100-Moduls – sowohl im primären als auch im lokalen Standby-Haupttrack – identisch sind. Das System führt diese Überprüfungen nicht automatisch für Sie aus.

Informationen zu jeder Position des Drehschalters finden Sie in der Beschreibung des Betriebsmodus der Cybersicherheit, Seite 25.

Modul-LEDs

LED-Anzeige

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



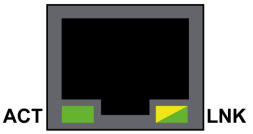
Die LEDs zeigen folgenden Informationen zum Modul an:

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 zur LED-Diagnose, Seite 136.

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 zur LED-Diagnose, Seite 139.

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 OPC UA integrierte Ethernet-Kommunikationsmodul entspricht dem folgenden behördlichen Standard:

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

1. Wenn ein BMENUA0100-Modul mit der Firmware-Version 1.01 eine mit EcoStruxure™ Control Expert V15 generierte Anwendung erhält, wobei:
   - Die **schnelle Abtastrate** ist **Aktiviert** (auf der Registerkarte „IPConfig“, Seite 120). Diese Einstellung wird nicht implementiert.
   - IPv4 für den Steuerungsport ist deaktiviert. Der Steuerungsport des Moduls wird mit der IPv4-Adresse konfiguriert, die auf der Registerkarte **IPConfig** für das Modul grau abgeblendet angezeigt wird.

     HINWEIS: Bei der grau hinterlegten 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 130 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 Firmware-Version 1.01 in einem Hot Standby-Rack mit EcoStruxure™ Control Expert V15 konfiguriert sind, gelten die in den vorhergehenden Abschnitten 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 132 angeben, damit der SNMP-Manager auf die SNMP-MIB zugreifen kann.

HINWEIS: Die BMENUA0100-Webseiten sind für alle Anwendungen gleich, unabhängig von der ausgewählten BMENUA0100-Referenz. Die für das BMENUA0100-Modul angezeigten Webseiten sind von der Firmware-Version des Moduls (z. B. 1.01, 1.10 oder 2.01) und nicht von der Modulversion (z. B. nicht BMENUA0100 oder BMENUA0100.2) abhängig.

Funktionsbeschreibung des Moduls BMENUA0100

Einführung

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

Einstellungen der Cybersicherheit-Betriebsart

Einführung

In diesem Abschnitt werden die Einstellungen der Betriebsart für das Modul BMENUA0100 beschrieben.

Betriebsmodus der Cybersicherheit

Einführung

Das BMENUA0100-Modul kann für einen Betrieb im sicheren Modus oder im Standardmodus konfiguriert werden. Der Drehwahlschalter mit 3 Positionen an der Rückseite des Moduls bestimmt den Betriebsmodus.

Die drei Drehschalterpositionen sind:

- Secured mode (Sicherer Modus)
- Standard mode (Standardmodus)
- Security Reset (Sicherheits-Reset)

HINWEIS:

- Die Standardkonfiguration des Moduls ist der sichere Modus.
- Sie können die aktuelle Position des Drehschalters auf der Startseite „Home“, Seite 89 der Modulwebseiten anzeigen.

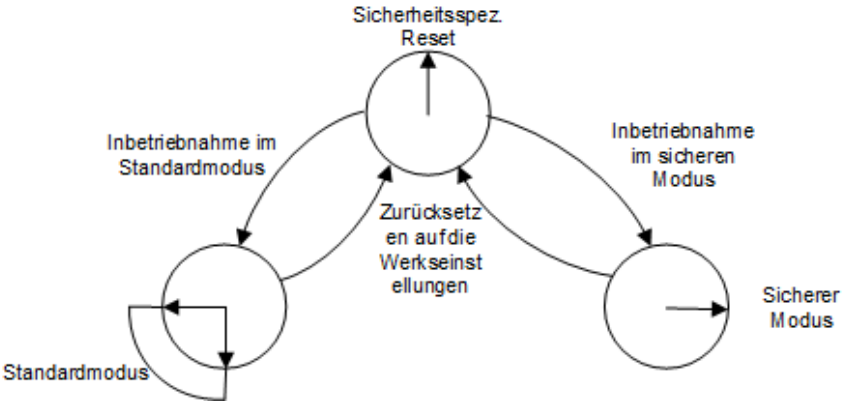
Da der Drehwahlschalter nicht zugänglich ist, während sich das Modul im Rack befindet, kann die Schalterposition nur geändert werden, wenn das Modul ausgeschaltet und aus dem Rack entfernt wird. Nach der Auswahl einer neuen Schalterposition kann das Modul wieder in das Rack eingeführt und mit Spannung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

HINWEIS: Verwenden Sie nur den kleinen Kunststoffschraubendreher, der im Lieferumfang des Moduls enthalten ist, Seite 20, um die Schalterposition zu ändern und einen Betriebsmodus für die Cybersicherheit zu konfigurieren.

Änderung des Betriebsmodus

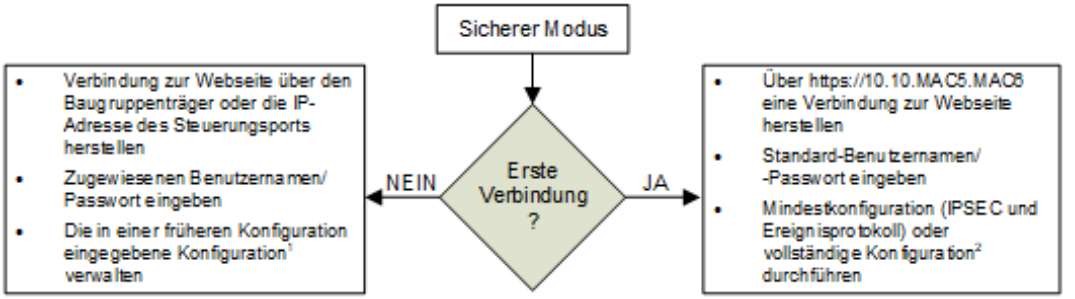
Bei jedem Wechsel des Cybersicherheitsmodus vom sicheren in den Standardmodus bzw. umgekehrt führen Sie vor der Konfiguration des neuen Modus einen Sicherheits-Reset, Seite 80 aus.

Die Position des Drehschalters bestimmt den Betriebszustand des Moduls wie folgt:



Ein neues (werkseitig vorkonfiguriertes) Modul oder ein Modul, für das ein Sicherheits-Reset durchgeführt wurde, kann für Vorgänge im Standardmodus, Seite 80 oder im sicheren Modus, Seite 78 in Betrieb genommen werden.

Das Verfahren zur Konfiguration des Moduls für Operationen im sicheren Modus variiert je nachdem, ob Sie nach dem ersten Sicherheits-Reset eine Verbindung zu den Konfigurationseinstellungen des Moduls herstellen:



1 Informationen zur Verwaltung der Konfiguration finden Sie im Kapitel zur Konfiguration, Seite 84.

2 Informationen zur Durchführung einer Konfiguration beim ersten Anschluss finden Sie unter Inbetriebnahme im sicheren Modus, Seite 78.

Sicherer Modus

Wenn das Modul im sicheren Modus betrieben wird, nimmt es keine Prozesskommunikation über den Steuerungs- oder den Baugruppenträger-Port vor, bis gültige Cybersicherheitseinstellungen konfiguriert wurden. Nach der Konfiguration des sicheren Modus können Sie die Cybersicherheitseinstellungen über die Webseiten des Moduls, Seite 84 konfigurieren, auf die über das HTTPS-Protokoll über den Baugruppenträger- oder den Steuerungsport zugegriffen werden kann. Im sicheren Modus unterstützt das Modul die Cybersicherheitsstufe, die in der Konfiguration der Cybersicherheit angegeben ist. Erst nachdem die Cybersicherheitseinstellungen konfiguriert wurden, können die Einstellungen für IP-Adresse, NTP-Client und SNMP-Agent, Seite 118 mithilfe der Konfigurationssoftware Control Expert konfiguriert werden.

Standardmodus

Im Standardmodus kann die Modulkommunikation sofort 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.

Sicherheits-Reset

Mit dem Befehl zum **Sicherheits-Reset** werden die werkseitigen Standardkonfigurationseinstellungen wiederhergestellt. Er löscht alle vorhandenen Einstellungen für Cybersicherheit, Allowlist, Zertifikate und rollenbasierte Zugriffskontrolle. Während die Wiederherstellung der Werkseinstellungen noch läuft, blinkt die LED RUN weiterhin grün. Nach Abschluss des Prozesses leuchtet die LED RUN permanent grün auf und alle Dienste werden deaktiviert. Um den Sicherheits-Reset abzuschließen, müssen Sie entweder das BMENUA0100-Modul aus- und wieder einschalten oder physisch aus dem Rack entfernen (wodurch die Spannungsersorgung abgeschaltet wird) und dann wieder in das Rack einführen (wodurch die Spannungsersorgung wieder aktiviert wird).

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

- Bei einer Einstellung über den Drehschalter: Das Modul ist nicht mehr funktionsfähig, bis das Modul aus dem Rack entfernt wird, der Drehschalter entweder auf die Position „Secured“ oder „Standard“ zurückgesetzt und das Modul erneut im Rack positioniert wird. Die erforderlichen Konfigurationen müssen angewendet werden.
- Bei einer Einstellung über die Webseiten: Nach Abschluss des Prozesses wird das Modul im Standard- oder im sicheren Modus aus- und wiedereingeschaltet (aus/ein). Sowohl die Cybersicherheit als auch die IP-Adresseinstellungen müssen konfiguriert werden.

  HINWEIS: Nach einem Sicherheits-Reset des BMENUA0100-Moduls gelten für das Modul folgende Bedingungen:

  - 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 28 für Benutzername/Passwort.
    - Standardeinstellung für die IP-Adresse: 10.10.MAC5.MAC6, Seite 118.

Standardkombination Benutzername/Passwort

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

- Sicherer Modus: admin / password
- Standardmodus: installer / Inst@ller1

Vom sicheren und Standardmodus unterstützte Funktionen

Die folgenden Funktionen werden vom BMENUA0100-Modul im sicheren Modus und im Standardmodus unterstützt:

Sicherheitsmodus	**Standardmodus**			**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 standardmäßig aktiviert)
Webbasierte CS-Konfigurationsänderung (HTTPS)	Nein	Nein	Nein	Ja	Ja	Ja
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	Alle Dienste sind konfigurierbar (standardmäßig deaktiviert)

Sicherheitsmodus	**Standardmodus**			**Sicherer Modus**		
Steuerungsport	**Deaktivieren**	**Aktivieren**		**Deaktivieren**	**Aktivieren**	
Ethernet-Port	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**
					(standardmäßig deaktiviert)	
Webdiagnose (nur Seiten „Home“ und „Diagnose“)	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
Firmware-Aktualisierung (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

Sicherheitsmodus	**Standardmodus**			**Sicherer Modus**		
Steuerungsport	**Deaktivieren**	**Aktivieren**		**Deaktivieren**	**Aktivieren**	
Ethernet-Port	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**	**Baugruppenträger**	**Baugruppenträger**	**Steuerungsport**
Filterung: Control Expert-Datenflüssean das Gerätenetzwerk (einschließlich CPU) (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:
   - Firmware-Version 2 (BMENUA0100.2) verwendet SNMP V3 mit der Sicherheitsstufe ohne Autorisierung und ohne Datenschutz.
   - Firmware vor Version 2 (BMENUA0100) verwendet SNMP V1.

   Weitere Informationen finden Sie unter SNMP-Agent-Konfiguration in Control Expert und auf den Webseiten, Seite 132.
3. NTP V4 kann so konfiguriert werden, dass ein Transport außerhalb des IPSec-Tunnels erfolgt.
4. Wenn die Sicherheitseinstellungen für Standard- und sichere Cybersicherheit auf *Keine* gesetzt sind, gibt es keine Benutzerauthentifizierung (d. h. die OPC UA-Einstellung, Seite 103 **Benutzer-ID-Tokentypen** ist auf*Anonym* festgelegt).
5. Um Control Expert einen Online-Zugriff auf die CPU oder das Gerätenetzwerk zu ermöglichen, konfigurieren Sie den PC (auf dem Control Expert installiert ist) mit einer IP-Adresse im selben Subnetz wie der BMENUA0100-Modulsteuerungsport und verwenden 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.

Betriebskenndaten des BMENUA0100-OPC UA-Servers

Einschränkungen

Maximal:

- Die Anzahl der Knoten, die im Adressraum für den Datenzugriff des BMENUA0100-OPC UA-Servers veröffentlicht werden können, beträgt 100.000 Knoten.
- Der Arbeitsspeicher, der dem OPC UA-Server des BMENUA0100-Moduls zugewiesen werden kann, beträgt 192 MB.

HINWEIS: Wenn einer der beiden Grenzwerte überschritten wird, wechselt der Server-Adressraum in den Status *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 sie auftreten, und ihre Folgen, wenn sie überschritten werden, sind nachstehend aufgeführt:

Grenzwert	Wert	OPCUA-Dienst	Dienstparameter	Ergebnis
Kumulative Sitzungsanzahl	10 s	*CreateSession*	(Nicht zutreffend)	Dienstergebniscode *Ungültig_ZuVieleSitzungen*
Minimales Sitzungs-Timeout	30 s	*CreateSession*	Angefordertes Sitzungs-Timeout	Überarbeitetes Sitzungs-Timeout
Kumulatives Sitzungs-Timeout	3600 s	*CreateSubscription*	Angefordertes SessionTimeout	Geändertes Sitzungs-Timeout
Maximale Anzahl kumulativer Abonnements	40	*CreateSubscription*	(Nicht zutreffend)	Dienstergebniscode *Ungültig_ZuVieleAbonnements*
Minimales Veröffentlichungsintervall	250 ms[1] 20 ms[2]	*CreateSubscription*	Angefordertes Veröffentlichungsintervall	Überarbeitetes Veröffentlichungsintervall
Maximales Veröffentlichungsintervall	10 s	*CreateSubscription*	Angefordertes Veröffentlichungsintervall	Geändertes Veröffentlichungsintervall
Maximale Abonnementlaufzeit	300 s	*CreateSubscription*	Min. (Angefordertes Veröffentlichungsintervall, 3.600.000) * Angeforderte Lebensdaueranzahl	Überarbeitete Lebensdaueranzahl
Maximale Anzahl von	12500	*CreateSubscription*	Max. Benachrichtigungen pro Veröffentlichung	Die maximale Kapazität der Benachrichtigungen beträgt daher (1000 / Überarbeitetes

Grenzwert	Wert	OPCUA-Dienst	Dienstparameter	Ergebnis
Benachrichtigungen pro Veröffentlichung				Veröffentlichungsintervall) * 1000 Benachrichtigungen pro Sekunde.
Minimales Abtastintervall	125 ms[1] 20 ms[2]	*CreateMonitoredtems*	Überwachung und Parameter Abtastintervall	Überarbeitetes Abtastintervall
Maximale Größe der Nachrichtenwarteschlange	100	*CreateMonitoredtems*	Überwachung und Parameter Größe der Warteschlange	Überarbeitete Warteschlangengröße
Maximale Anzahl der überwachten Elemente (kumulativ)	50.000[3] 2000[2]	*CreateMonitoredtems*	(Nicht zutreffend)	Dienstergebniscode *Ungültig_ZuVieleÜberwachteElemente*
Maximale Anzahl der Abonnements pro Sitzung	4	–	–	–
Maximale Anzahl der überwachten Elemente pro Abonnement	25.000	–	–	–

1. Wenn die globale schnelle Überwachung deaktiviert ist.

2. Wenn die globale schnelle Überwachung aktiviert ist.

3. Wenn die globale schnelle Überwachung deaktiviert und der Server wie folgt konfiguriert ist:
   - ein Abtastintervall von mindestens 1 Sekunde und
   - ein Veröffentlichungsintervall von mindestens 1 Sekunde.

OPC UA-Server

Einführung

Der Hauptzweck des Ethernet-Kommunikationsmoduls BMENUA0100 ist die Bereitstellung eines OPC UA-Kommunikationskanals über Ethernet zwischen M580-CPUs und OPC UA-Clients. Die Daten der M580-CPU werden den Variablen im Modul BMENUA0100 zugeordnet und OPC UA-Clients über einen leistungsstarken 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 des Baugruppenträger-Ports des BMENUA0100-Moduls und bauen so eine Client-Server-Verbindung auf. Das BMENUA0100-Modul kann bis zu 10 (10) gleichzeitige OPC UA-Clientverbindungen für Firmware-Version 1.1 (oder 3 (3) gleichzeitige OPC UA-Clientverbindungen für Firmware-Version 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 vollständige Definition der Funktionalität, die weitere Profile, Facets, 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, gilt für dieses Profil: *Ist ein voll ausgestattetes Profil, das für Geräte mit mehr als 50 MB Speicher und einem leistungsfähigeren Prozessor bestimmt 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 deren 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 Modul BMENUA0100 unterstützt 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)

Service Set (Dienstgruppe)	Services (Dienste)
	• CloseSecurechannel (Sicheren Kanal schließen)
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 weist der kursiv formatierte Text auf ein direktes Zitat des Quellmaterials der OPC Foundation hin. Klicken Sie auf die folgenden Links und öffnen Sie die Beschreibungen der einzelnen Facets mithilfe des *OPC Foundation Unified Architecture Profile Reporting Visualization Tool*.

Core 2017 Server Facet

Das Core 2017 Server Facet *definiert die Kernfunktionen, die für jede 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. Um eine umfassende Anwendbarkeit zu gewährleisten, 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 RegisterNodes- und UnregisterNodes-Dienste als Möglichkeit, 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 mehrere 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-Werte: 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 teilweise Aktualisierungen für dieses Array zulässig sind.

Data Access Server Facet

Das Data Access Server Facet *gibt den Support für ein Informationsmodell an, das zur Bereitstellung industrieller 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 AddressSpace-Basisverhaltens umfasst*. Eine vollständige Beschreibung dieses Facets finden Sie unter http://opcfoundation.org/UA-Profile/Server/DataAccess.

ComplexType 2017 Server Facet

Das ComplexType 2017 Server Facet *erweitert das Core Server Facet um Variablen mit strukturierten Daten, d. h. Daten, die aus mehreren Elementen bestehen, wie z. B. einer Struktur, und in denen die individuellen 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 Codierung und Decodierung dieser strukturierten Datentypen. Optional kann der Server auch alternative Codierungen unterstützen, wie z. B. eine XML-Codierung, wenn das Binärprotokoll gerade 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.

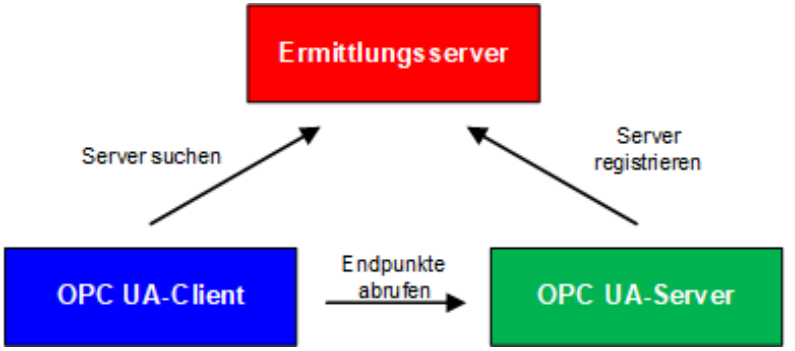
Um eine Verbindung zum OPC UA-Server im BMENUA0100-Modul herzustellen, benötigt ein OPC UA-Client Informationen, die den Server beschreiben, einschließlich seiner Netzwerkadresse, seines Protokolls und seiner Sicherheitseinstellungen. OPC UA definiert eine Reihe von Erkennungsfunktionen, die ein Client 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)
- Benutzertokentyp (vom Server unterstützte Arten der Benutzerauthentifizierung)

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



Das BMENUA0100-Modul unterstützt verschiedene Ermittlungs- 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 zur Erkennung: Discovery Service Set

Der OPC UA-Server-Stack des BMENUA0100-Moduls unterstützt das „Discovery Service Set“, das im Core 2017 Server Facet, Seite 37 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 alle Server nur auf dem lokalen OPC UA-Server.

- GetEndpoints: Gibt die Endpunkte zurück, die von einem Server unterstützt werden, sowie alle Konfigurationsinformationen, die zum Einrichten eines sicheren Kanals und einer Sitzung erforderlich sind. 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 37 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 (sessionId), anhand derer die Sitzung in den Audit-Protokollen und im AddressSpace des Servers identifiziert wird.
  - 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 zum verwendet werden, um den Benutzer der Sitzung zu ändern.
- CloseSession: Beendet eine Sitzung.

  HINWEIS: Wenn „SecurityMode = Keine“, 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 ermöglicht es dem im BMENUA0100-Modul integrierten OPC UA-Hochleistungsstapel, Veröffentlichungs-/Abonnementdienste bereitzustellen, die verwendet werden, wenn das Modul eine Verbindung zu dezentralen Geräten herstellt.

Ein OPC UA-Client kann einen oder mehrere ausgewählten Knoten abonnieren und den Server diese Elemente überwachen lassen. Beim Auftreten eines Änderungsereignisses, z. B. einer Wertänderung, benachrichtigt der Server den Client über die Änderung. Dieser Mechanismus reduziert die Menge der übertragenen Daten erheblich. Dies reduziert den Bandbreitenverbrauch und ist der empfohlene Mechanismus zum Lesen von Informationen von einem OPC UA-Server.

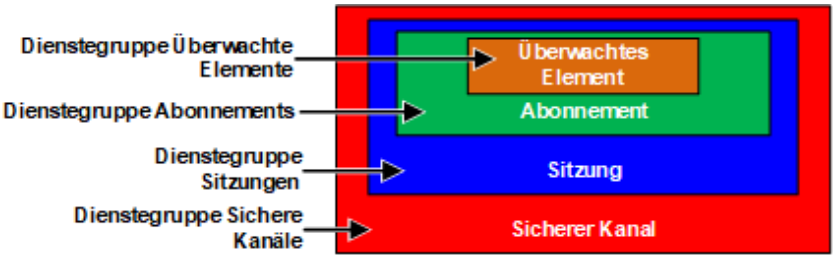
Ein OPC UA-Client kann die verschiedenen Arten von Informationen abonnieren, die ein OPC UA-Server bereitstellt. Das Abonnement fasst diese verschiedenen Arten von Daten (überwachte Elemente genannt) zu einer einzigen Datensammlung zusammen, die als Benachrichtigung bezeichnet wird.

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 CPU in einem Umfang zu erhalten, der größer ist, als die CPU 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.

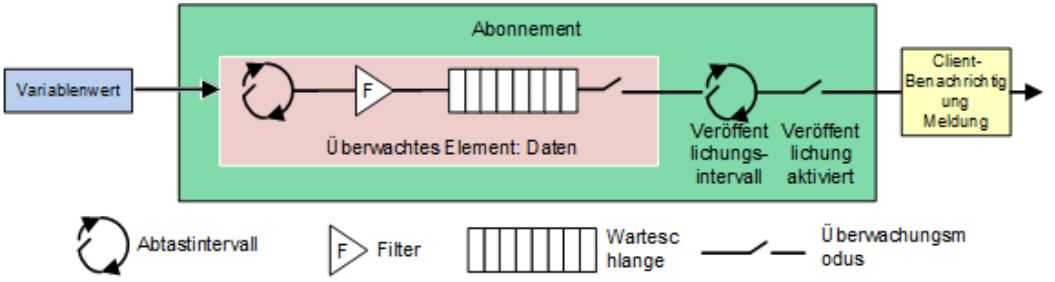
Berücksichtigen Sie bei der Einstellung eines Veröffentlichungsintervalls die Anzahl der Client- und Client-Requests, die der Server verarbeiten muss. Wenn Sie die Anzahl der Client-Requests ermitteln, müssen Sie sicherstellen, dass alle Clients online arbeiten. Beachten Sie in diesem Zusammenhang, dass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

HINWEIS: Es wird ein Veröffentlichungsintervall empfohlen, das dem Doppelten der Abtastperiode entspricht.

Änderungsereignisse

Ein Client kann ein Datenänderungsereignis, das durch eine 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 Datenproben 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. Wenn 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 mehrerer Kriterien, die verwendet werden, um festzustellen, welche Datenänderungen oder Ereignisse gemeldet und welche blockiert werden sollen.
- Überwachungsmodus: Wird zum Aktivieren oder Deaktivieren der Datenabtastung und der Weiterleitung 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 innerhalb einer Veröffentlichungsantwort sendet. Für den Fall, dass keine Meldungen erforderlich sind (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

Das Embedded DataChange Subscription Server Facet *gibt die Mindestebene für unterstützte Benachrichtigungen über Datenänderungen innerhalb von 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 ein mindestens 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 der überwachten Elemente: Monitored Item Service Set

Das „Monitored Item Service Set“ unterstützt die folgenden Dienste:

- CreateMonitoredItems: Ein asynchroner Aufruf zum Erstellen und Hinzufügen eines oder mehrerer 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 sollten vom Server sofort übernommen werden. Sie werden so schnell wie möglich wirksam.
- 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 der Abonnements: Subscription Service Set

Das „Subscription Service Set“ unterstützt die folgenden Dienste:

- CreateSubscription: Ein asynchroner Aufruf zum Erstellen eines Abonnements.
- ModifySubscription: Ein asynchroner Aufruf zum Ändern eines Abonnements. Der Server übernimmt Änderungen am Abonnement sofort, und Änderungen werden so bald wie möglich wirksam.
- DeleteSubscription: Ein asynchroner Aufruf zum Löschen von einem oder mehreren Abonnements, die zu der Clientsitzung gehören. Bei erfolgreicher Ausführung dieses Diensts werden alle dem Abonnement zugeordneten überwachten Elemente gelöscht.

- Publish: Dieser Dienst dient zwei Zwecken: Den Empfang von NotificationMessages für ein oder mehrere Abonnements zu bestätigen und den Server zur Rückgabe einer NotificationMessage oder einer Keep-Alive-Nachricht aufzufordern.
- 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.

Erkennen von PAC-Variablen

Zuordnung von Control Expert-PAC-Variablen zu OPC UA-Datenlogikvariablen

Einführung

Der in das BMENUA0100-Modul integrierte OPC UA-Server verwendet Datenwörterbuch-Requests von Unified Messaging Application Services (UMAS), um M580-PAC-Anwendungsvariablen 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 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 168 ab.

Alle erfassten Variablen werden mithilfe der geeigneten OPC UA-Stack-Dienste aus der Ansicht des Control Expert-Datenlogikmodells in die Ansicht des OPC UA-Datenlogikmodells übersetzt. Ein mit dem BMENUA0100-Modul verbundener OPC UA-Client – über seinen Steuerungsport, oder über seinen Baugruppenträger-Port über die CPU oder ein BMENOC0301/11-Kommunikationsmodul – kann diese Sammlung von Daten über die Dienste des vom Embedded 2017 UA Server Profile, Seite 34 unterstützten Data Access Server Facet, Seite 37 abrufen.

Vorladen des Datenwörterbuchs zur Vermeidung von Kommunikationsunterbrechungen

Eine mit Control Expert online durchgeführte Anwendungsänderung unterbricht die OPC UA-Server/Client-Kommunikation vorübergehend, während der Server ein aktualisiertes Datenwörterbuch erhält. Diese Unterbrechung wird durch eine inkonsistente CPU-Datenzuordnung verursacht, während das Datenwörterbuch aktualisiert wird. Während des Zeitraums des Kommunikationsausfalls ändert sich der Status der überwachten Knoten zu BAD (schlecht). Um diese Betriebsunterbrechung zu vermeiden, kann ein Synchronisierungsmechanismus zwischen dem BMENUA0100-Modul und der Control Expert-Konfigurationssoftware basierend auf dem aktualisierten Datenwörterbuch eingerichtet werden.

Diese Funktion wird in Control Expert im Fenster **Extras > Projekteinstellungen...** im Bereich **Allgemein > In SPS eingebettete Daten** unter Verwendung der Einstellungen **Vorladen bei der Generierung von Änderungen** und **Timeout bei der Generierung von**

Änderungen (siehe ™EcoStruxure Control Expert, Betriebsarten). Informationen zum Konfigurieren dieser Funktion finden Sie in der Online-Hilfe von Control Expert.

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
BYTE	Byte
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double

Elementarer Datentyp von Control Expert	OPC UA-Datentyp
STRING	Byte-Array
* In der folgenden Tabelle ist 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	0x20170517
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	0x07440100
DT[1]	DT#2017-05-17-07:44:01	Double	4.29E-154
1. Die zurückgegebenen Daten für Datums- und Uhrzeitwerte sind UATypeUInt64, d. h. die interne Codierung des IEC 1131 DT in Control Expert - BCD-Codierung (Binary Coded Decimal).			

Erkennbare Variablen

Für alle Variablen gilt, dass der OPC UA-Client nicht direkt auf eine erkannte PAC-Datenlogikvariable zugreift. Stattdessen greift der Client auf die erkannte PAC-Variable durch eine OPC UA-Datenlogikvariable zu, die im BMENUA0100-Modul existiert und der zugrunde liegenden PAC-Variable zugeordnet ist. Aufgrund der Pass-Through-Natur des Datenvariablenzugriffs ist der Erfassungsanforderungsprozess nicht optimiert, und die Erfassungsleistung des Datenwörterbuchs ist nicht repräsentativ für die PAC-Leistung.

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

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

- Strukturierte Variablen mit Unterfeldern: DDT- und Array-Variablen.
- Die Variablen der 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 und Structure.

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

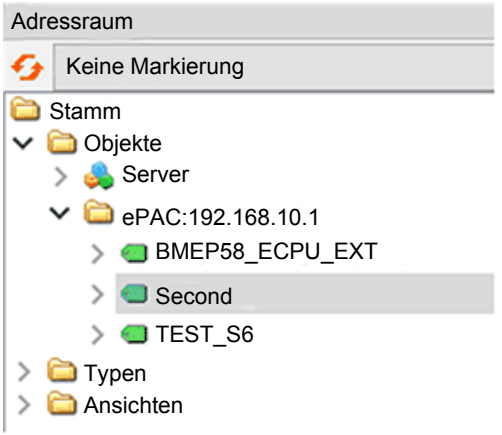
- Topologische E/A-Variablen:
  - Eingänge: %I, %IW, %ID, %IF.
  - Ausgänge: %Q, %QW, %QD, %QF.
- Lokalisierte Variablen: %M, %MW, %MD, %MF.
- Systemvariablen: %S, %SW, %SD.

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

Darstellung der erkannten Variablen im OPC UA-Client

Der OPC UA-Server im BMENUA0100-Modul kann die erkannten PAC-Variablen 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 Unified Automation UaExpert-Client-Tool), der mit dem BMENUA0100-Modul verbunden ist, PAC-Variablen in seinen Fenstern **Adressraum** anzeigen. Die IP-Adresse des M580-PAC wird durch den Knoten ePAC:192.168.10.1 angezeigt. Die untergeordneten Knoten entsprechen den Control Expert-Anwendungsvariablen:



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

Mithilfe des OPC UA-Client-Tools wurde der Knoten TEST_S6 in das Fenster **Datenzugriffsansicht** gezogen, in dem die Details der Variablen angezeigt werden:



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 ist der OPC UA-Datentyp der Variablen *Boolesch* (gibt an, dass der zugrunde liegende PAC-Datentyp BOOL ist) und ihr Wert ist *False*.

HINWEIS: Das Attribut **Serverzeitstempel** der OPC UA-Knoten wird vom OPC UA-Server des BMENUA0100-Moduls in UTC (Universal Time Coordinated) erhalten. Es wird dem Benutzer in Ortszeit angezeigt. Die Daten werden nicht an der jeweiligen Quelle, sondern vom OPC UA-Server mit einem Zeitstempel versehen. Um Kompatibilitätskonflikte mit einigen OPC UA-Clients zu vermeiden, werden sowohl Quellzeitstempel- als auch Server-Zeitstempelwerte mit dem gleichen Server-Zeitstempelwert eingerichtet.

Lesen und Schreiben erkannter Variablen im OPC UA-Client

Ein OPC UA-Tag in einem OPC UA-Client (z. B. einem SCADA), der 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 Redundanzarten

Das BMENUA0100-Modul unterstützt die folgenden Redundanztypen:

- Hot Standby-Architektur, die redundante CPUs 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.*

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

- Ein eigenständiger PAC, der zwei BMENUA0100-Module enthält.
- Zwei Hot Standby-PACs, die jeweils ein oder zwei BMENUA0100-Module enthalten.

OPC UA-Redundanz

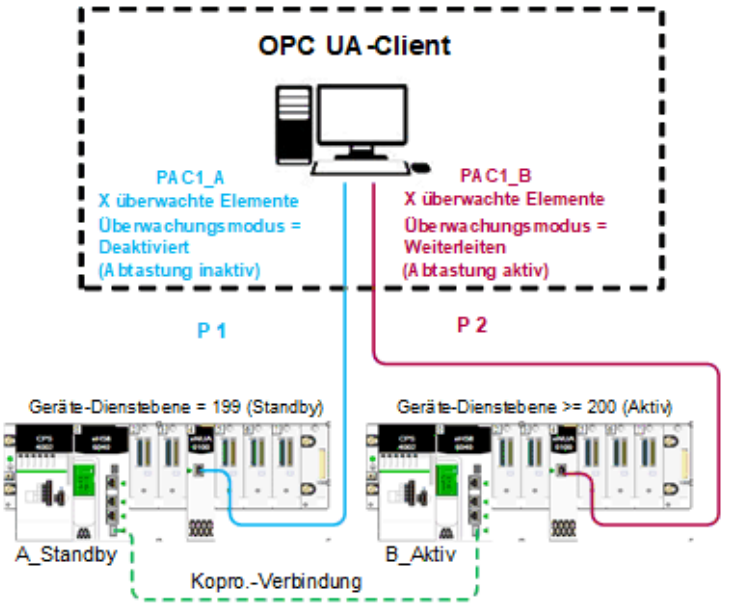
In einer nicht-transparenten, serverredundanten OPC UA-Architektur im Warm-Failover-Modus ist der OPC UA-Client für die Einrichtung von Sitzungen und die Verwaltung der Kommunikation mit redundanten Servern verantwortlich. Zu den einzurichtenden Sitzungen gehören: eine aktive Sitzung mit dem Primärserver und eine inaktive Sitzung mit dem sekundären (oder Standby-) Server. Der Client muss diese beiden Sitzungen so konfigurieren, dass sie dieselben überwachten Elemente enthalten.

Darüber hinaus ist der OPC UAC-Client dafür verantwortlich, den Serverstatus über die Variable SERVICE_LEVEL zu prüfen und abhängig vom Variablenwert die Kommunikation mit dem funktionsfähigeren Server umzuschalten.

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. Weitere Informationen zum Einstellen des *Überwachungsmodus* finden Sie in der Client-Dokumentation.

Dieses Prinzip gilt als Grundprinzip 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 aktiver Server denjenigen mit dem höheren SERVICE_LEVEL-Wert angegeben:



Hot Standby

In einer Hot Standby-Konfiguration können in jedem lokalen Hot Standby-Hauptrack bis zu zwei (2) BMENUA0100-Module installiert werden. Jedes BMENUA0100-Modul ist mit einer eindeutigen, statischen IP-Adresse konfiguriert. Die BMENUA0100-Module behalten ihre jeweiligen IP-Adressen bei und tauschen keine IP-Adressen bei einer Hot Standby-Umschaltung oder einem -Wechsel aus.

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

- Sie sind mit identischen Cybersicherheitseinstellungen, Seite 84 konfiguriert.
- Ihr Drehschalter, Seite 20 (an der Rückseite des Moduls) ist auf dieselbe Position eingestellt.
- Sie sind in der gleichen Steckplatznummer, Seite 60 in ihren entsprechenden lokalen Hauptracks installiert.

Das System führt diese Überprüfungen nicht automatisch für Sie aus.

Der BMENUA0100-Modul-DDT umfasst die Variable SERVICE_LEVEL, Seite 151, die der CPU 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 immer die Elementarfunktion READ_DDT hinzu, um den DDT jedes BMENUA0100-Moduls zu aktualisieren. Fügen Sie in einer Hot Standby-Konfiguration den READ_DDT in einem Codeabschnitt hinzu, der ausgeführt wird, wenn sich die CPU im Standby-Modus befindet. Dieser Entwurf gibt Diagnoseinformationen zum BMENUA0100-Modul zurück, die zwischen der primären und der Standby-CPU ausgetauscht werden können. Die Anwendung kann diese Informationen nutzen, um eine Konsistenzprüfung der unterstützten Dienste und der Cybersicherheitskonfigurationen für die BMENUA0100-Module in der primären und der Standby-CPU durchzuführen.

Wenn der DDT T_M_ECPU_HSBY (siehe Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen) der Hot Standy-CPU und das CMD_SWAP-Element als HMI-Variablen in einem SCADA-System verfügbar gemacht werden, kann die SCADA-Anwendung eine Umschaltung auslösen, indem in die entsprechende zugeordnete OPC UA-Variable im BMENUA0100-Modul geschrieben wird.

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 Konsistenz der Variablenwerte zwischen dem primären und dem Standby-PAC zu gewährleisten.

Darüber hinaus müssen aus Konsistenzgründen die Anwendungen in den beiden Hot Standby-PACs synchronisiert werden.

In seltenen Fällen (vor allem, wenn das Bit ECPU_HSBY_1.PLCX_ONLINE manuell oder programmgesteuert auf „False“ gesetzt wird) kann sich einer der PACs in einem Hot Standby-System im Wartemodus befinden. In diesem Modus wird dieser PAC (der Standby-PAC) nicht mit dem primären PAC synchronisiert, und die aus diesem PAC ausgelesenen Variablen sind ungenau. Der Status eines antwortenden PAC 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 PACs bei der Ausführung verschiedener Anwendungen. Um die Konsistenz der Variablen zwischen dem primären und dem Standby-PAC zu gewährleisten, muss das Datenlayout der beiden PACs konsistent sein, wie das T_M_ECPU_HSBY-DDT-Feld zeigt:

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = false

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

HINWEIS: Für die folgenden Teilen dieses Abschnitts wurden Inhalte aus folgendem Dokument entnommen:

OPC Unified Architecture Specification Part 4: Services, Version 1.04, nachfolgend abgekürzt als *OPC UA Part 4*, gefolgt von der entsprechenden Abschnittsreferenz. Die übernommenen Inhalte sind *kursiv* formatiert.

OPC UA-Unterstützung für redundante Server, Clients und Netzwerke

OPC UA ermöglicht die Redundanz von Servern, Clients und Netzwerken. OPC UA stellt die Datenstrukturen und Dienste bereit, mit denen Redundanz auf standardisierte Weise erzielt 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 es identisch konfigurierten Clients, sich so zu verhalten, als wären sie einzelne Clients, aber nicht alle Clients erhalten zu einem bestimmten Zeitpunkt Daten. 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, Section 6.6.1.

Serverredundanz

Es gibt zwei allgemeine Modi für die Serverredundanz: transparent und nicht transparent.

Bei der transparenten Redundanz ist das Failover von Serververantwortlichkeiten 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 Maßnahmen durchführen, um weiterhin Daten zu senden oder zu empfangen.

Bei einer nicht transparenten Redundanz wird das Failover von einem Server zum anderen und Maßnahmen zum weiteren Senden oder Empfangen von Daten vom Client ausgeführt.

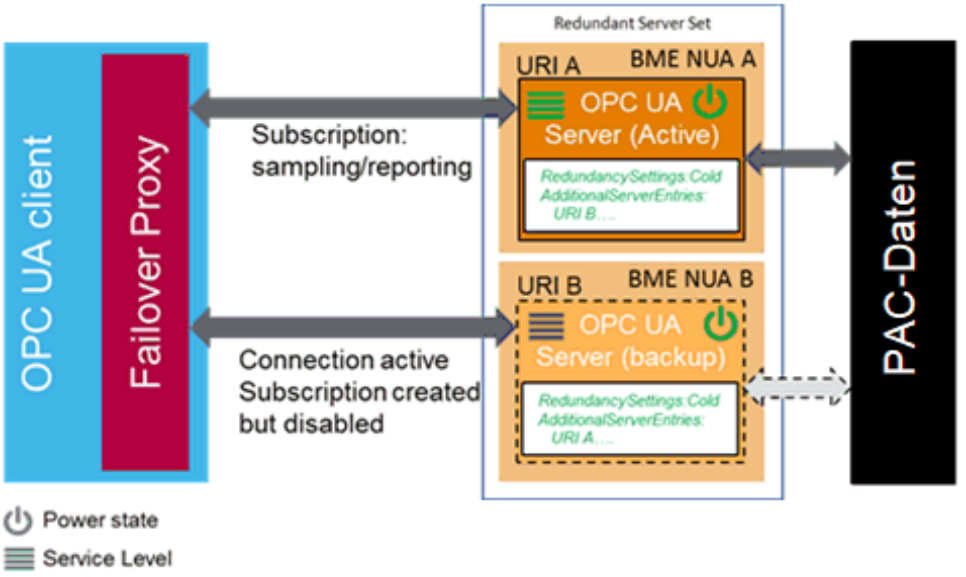
Der Client muss den redundanten Serversatz kennen und die erforderlichen Maßnahmen durchführen, um von der Serverredundanz zu profitieren.

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, Section 6.6.2

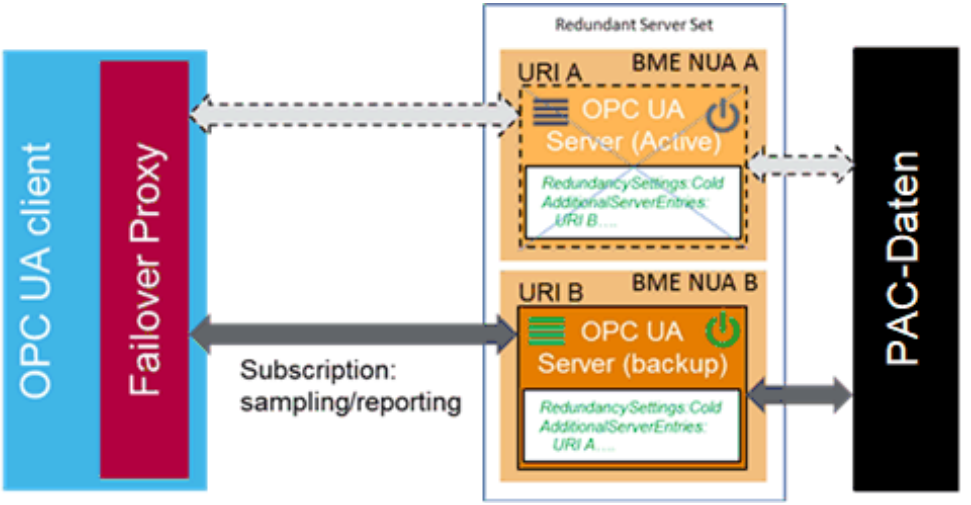
Der OPC UA-Server im BMENUA0100-Modul unterstützt die nicht transparente Serverredundanz im Warm-Failover-Modus.

OPC UA-Server – Warm-Failover-Modus

Im Warm-Failover-Modus *können die Backup-Server aktiv sein, aber keine Verbindung zu tatsächlichen Datenpunkten herstellen*. Daher kann nur ein einzelner Server Daten der Control Expert-Anwendung verbrauchen. *Die ServiceLevel-Variable ... gibt die Möglichkeit des Servers an, dem Client seine Daten zur Verfügung zu stellen. OPC UA Part 4, Section 6.6.2.4.4*



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



Failover-Verhalten des Clients

Jeder Server verwaltet eine Liste der 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.

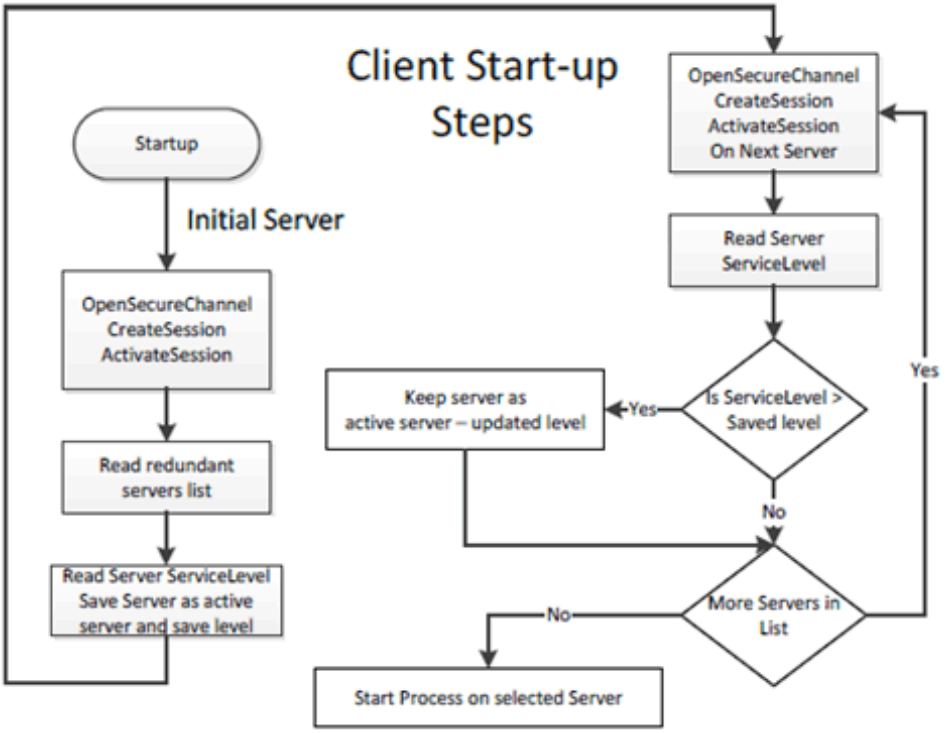
Die Liste wird gemeinsam mit dem Failover-Modus im ServerRedundancy-Objekt bereitgestellt. Damit Clients eine Verbindung zu allen Servern in der Liste herstellen können, muss jeder Server in der Liste die ApplicationDescription für alle Server im redundanten Serversatz über den FindServers-Dienst bereitstellen. 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, Section 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 zu bewältigen und ein Failover zu einem anderen Server im redundanten Serversatz durchzuführen. Die folgende Abbildung *bietet einen Überblick über die Schritte, die ein Client normalerweise durchführt, wenn er zum ersten Mal eine Verbindung zu einem redundanten Serversatz herstellt.*



Der Erstserver kann über die Standarderkennung oder aus einer persistenten Serverliste im redundanten Serversatz bezogen werden. Der Client muss jedoch immer überprüfen, mit welchem Server im Serversatz er eine Verbindung herstellen soll. Einzelne Maßnahmen hängen vom Server-Failover-Modus ab, den der Server bereitstellt, sowie vom Failover-Modus, den der Client verwendet.

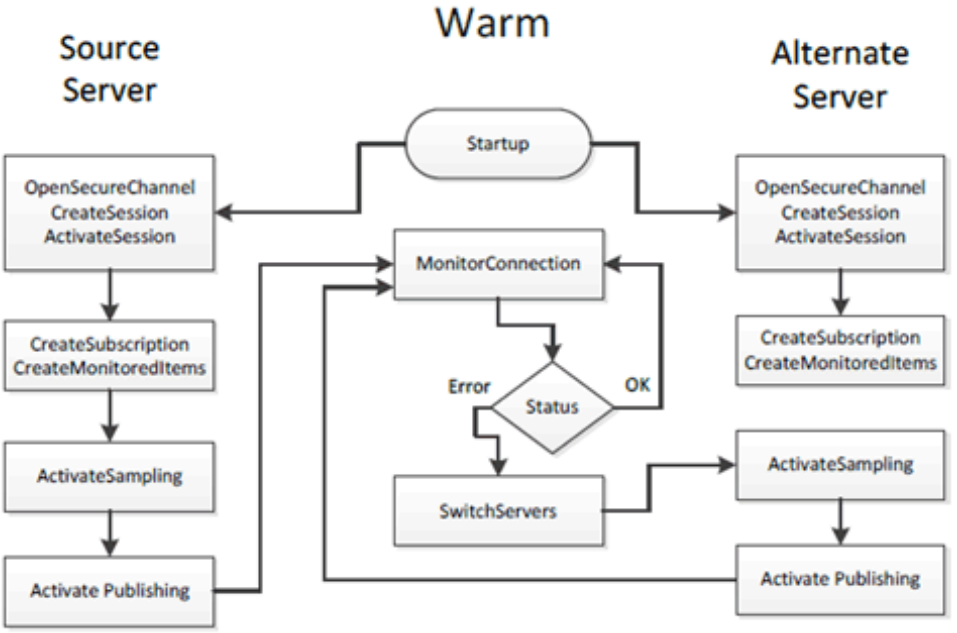
Clients, die einmal mit einem redundanten Server verbunden sind, müssen die von einem Server unterstützten Failover-Modi kennen, da sich diese Unterstützung auf die verfügbaren Optionen in Bezug auf das Clientverhalten auswirkt. Ein Client kann einen Server immer mit einem geringeren Failover-Modus handhaben, 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, Section 6.6.2.4.5.1

OPC UA-Client – Warm-Failover-Modus

Im Warm-Failover-Modus sollte *der Client zunächst eine Verbindung zu einem oder mehreren Servern im redundanten Serversatz herstellen, um den ServiceLevel zu überwachen. 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. Ungültig_KeineKommunikation. Der aktive Server wird durch Lesen der ServiceLevel-Variable von allen Servern ermittelt.*

Der Server mit dem 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 veranschaulicht die Schritte, die ein Client bei der Kommunikation mit einem Server im Warm-Failover-Modus ausführen würde.



OPC UA Part 4, Section 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 CPU) in den folgenden Konfigurationen platziert werden:

- M580-Standalone-Konfiguration
- M580-Standalone-Sicherheits-PAC-Konfiguration
- M580-Hot Standby-Konfiguration
- M580-Hot Standby-Sicherheits-PAC-Konfiguration

HINWEIS:

- Das BMENUA0100-Modul kann mit allen M580-CPUs verwendet werden.
- Falls eine Netzwerkschleife erstellt wird, wechselt das BMENUA0100-Modul in den Status NOCONF (Nicht konfiguriert). Um Schleifen und damit zusammenhängende Ereignisse zu vermeiden, teilen Sie bei Verwendung des BMENUA0100-Steuerungsports das Steuerungsnetzwerk und das CPU-Baugruppenträger-Netzwerk physisch (über die Trennung der Verdrahtung) und nicht nur logisch (über die Einstellungen für Subnetz und Subnetzmaske).

Verbindung über das HTTPS-Protokoll

Wenn in Ihrer Anwendung Verbindungsprobleme auftreten, wenden Sie sich an den lokalen IT-Support, um sicherzustellen, 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) v1.2 oder höher. Beispiel: Windows 7 benötigt 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 wird dringend empfohlen, einen Router zu verwenden, um die Racks zu isolieren und so mögliche Adresskonflikte zwischen 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-CPUs, die im selben Subnetz konfiguriert sind, wird empfohlen, Präfixe für den Gerätenamen (oder Rollennamen) aller Geräte, einschließlich M580-CPUs, zu verwenden. Diese Benennungskonvention ermöglicht es den BMENUA0100-Modulen, zwischen den M580-CPUs zu unterscheiden und festzustellen, welche CPU in welchem Rack untergebracht ist. Diese Benennungskonvention hilft, Unsicherheiten in Bezug auf ein flaches Netzwerkdesign zu beseitigen. Beispielsweise kann ein BMENUA0100-Modul ohne eindeutige Präfixe nicht bestimmen, mit welcher M580-CPU 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** eingestellt werden.

Zugriff auf den in das BMENUA0100-Modul integrierten OPC UA-Server

In den in diesem Kapitel beschriebenen topologischen Architekturen können der Ethernet-Baugruppenträger-Port des BMENUA0100-Kommunikationsmoduls und sein Steuerport verwendet werden, um den Zugriff auf den im Modul integrierten OPCUA- 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 Thema Externe Ports, Seite 18.

Maximale Anzahl der BMENUA0100-Module pro Konfiguration

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

M580-Konfigurationstyp	Maximale Anzahl der BMENUA0100-Module
Standalone	Zwei (2) im lokalen Hauptrack für Standalone[1]- und Hot Standby[1,2]-Standard- und -Sicherheitskonfigurationen
Sicherheits-PAC	
Hot Standby	
Hot Standby-Sicherheits-PAC	

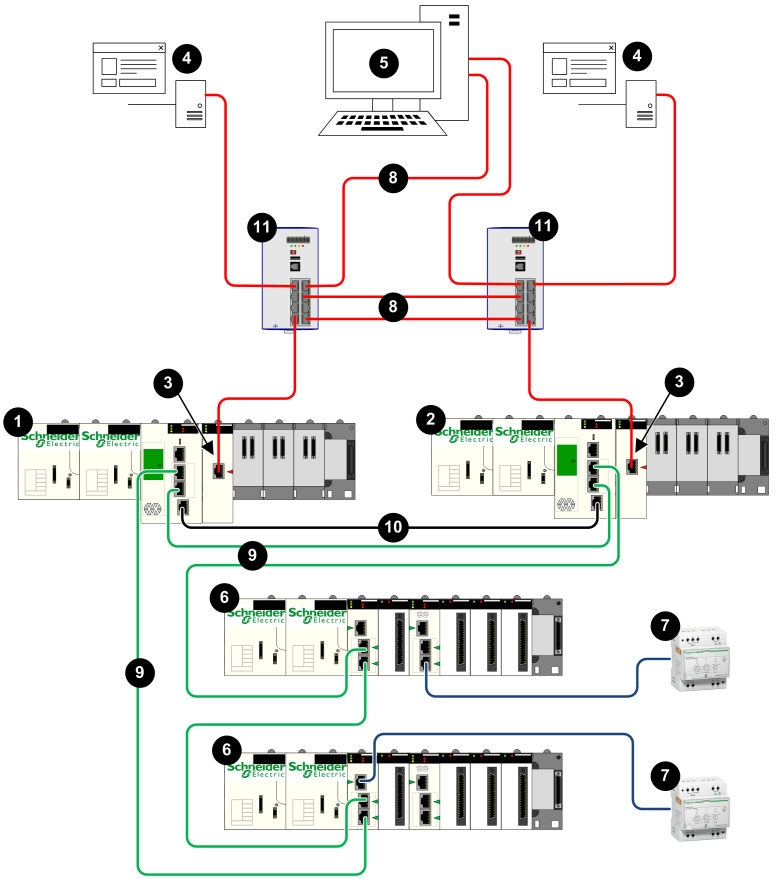
1. Wenn zwei (2) BMENUA0100-Module in einem Hauptrack verwendet werden:
   - Die Leistung jedes Moduls ist geringer als bei Verwendung eines einzelnen Moduls.
   - Aktivieren Sie den Steuerungsport in der Konfiguration für beide Module.
2. Platzieren Sie die BMENUA0100-Module in Hot Standby-Konfigurationen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

CCOTF (Change Configuration on the Fly)

Das BMENUA0100-Modul unterstützt CCOTF nicht.

Isoliertes Steuerungsnetzwerk mit M580-Hot Standby-PACs

Architektur



1 Primärer Hot Standby-PAC

2 Standby-Hot-Standby-PAC

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 CPU, als auch von den verteilten Ethernet-Geräten (7) logisch getrennt. 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.

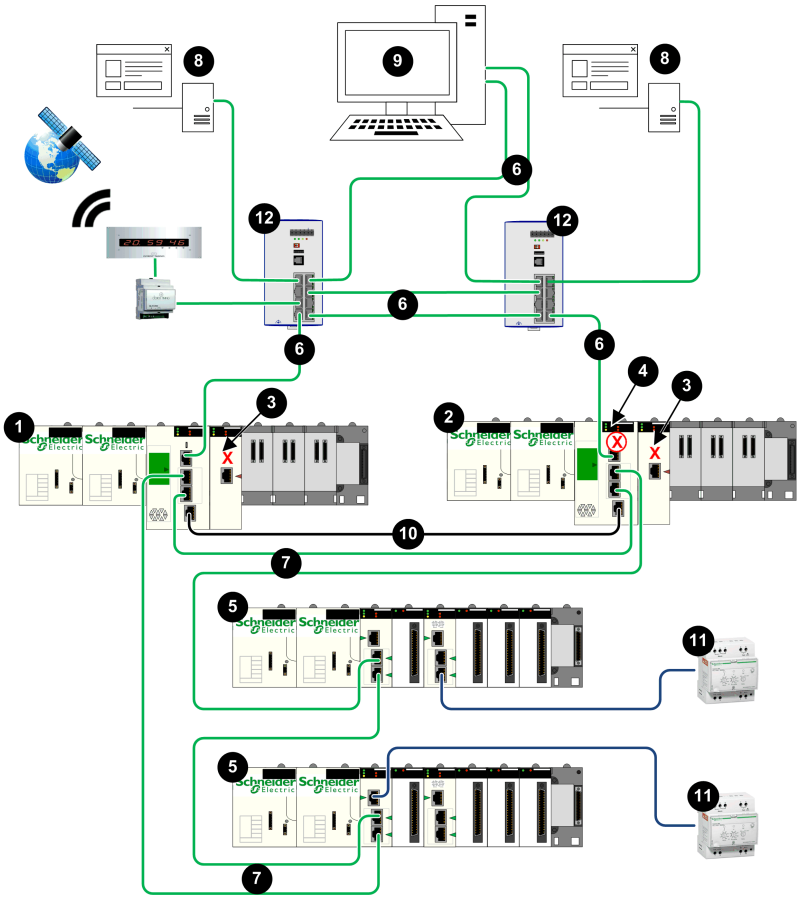
Das Modul BMENUA0100 bietet Modbus-Peer-to-Peer-Kommunikation zwischen den beiden Hot Standby-CPUs. Die CPU-Geräteports bieten Downstream-Konnektivität zu den Ethernet-Geräten im Ethernet-RIO-Hauptring.

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 CPU-Zeit 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 im PAC ausgeführten Anwendung verbraucht, die die Rohdaten konvertiert und in einem nutzbaren 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 Primärer Hot Standby-PAC

2 Standby-Hot-Standby-PAC

3 BMENUA0100 mit deaktiviertem Steuerungsport

4 Standby-CPU mit automatischer Sperrung 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-CPUs zu dualen OPC UA-Clients (SCADA-Systemen). Ihr Hauptzweck ist die Bereitstellung hoher Verfügbarkeit für die Hot Standby-PACs. Aus diesem Grund stellt diese Architektur ein nicht isoliertes flaches Netzwerk dar, 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-PACs zu den SCADA-Servern erfolgt über den primären CPU-Service-Port. Die CPU-Geräteports bieten Downstream-Konnektivität zu den Ethernet-Geräten im Ethernet-RIO-Hauptring.

Der Standby-CPU-Service-Port (4) wird automatisch deaktiviert. Hierfür wird in der Control Expert-Konfigurationssoftware auf der Konfigurationsregisterkarte **Service-Port** der primären und der Standby-CPU die Option **Automatisches Sperren des Service-Ports auf der Standby-CPU** ausgewählt.

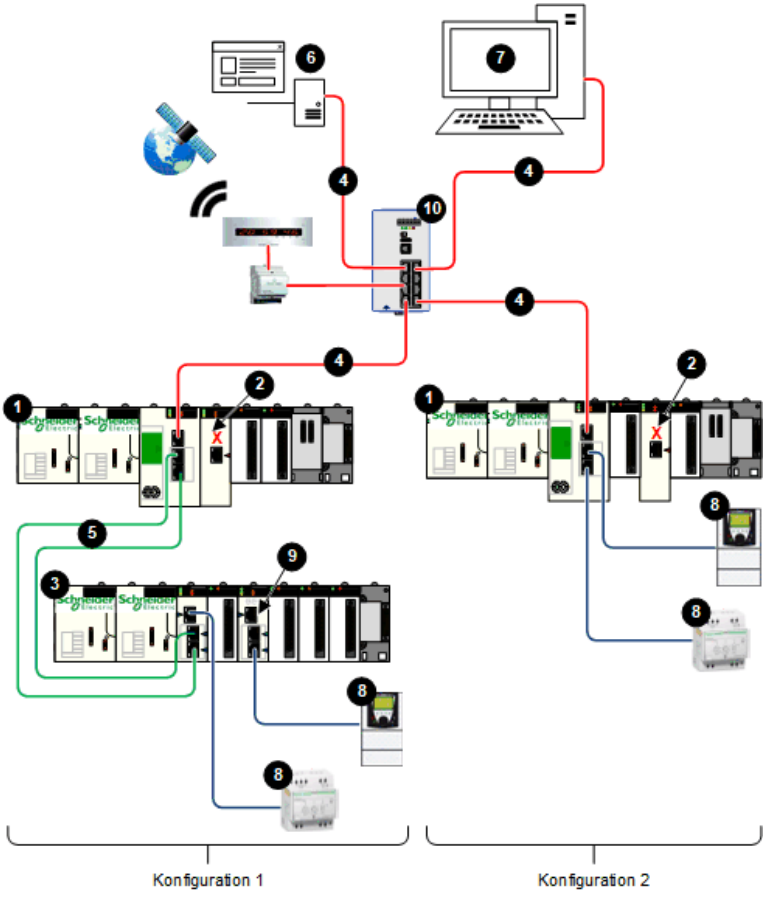
> **HINWEIS:** Der Service-Port der Standby-CPU wird deaktiviert, um die unbeabsichtigte Einrichtung einer Ethernet-Kommunikationsschleife zu verhindern, bei der sowohl das Steuerungsnetzwerk als auch der Ethernet-RIO-Hauptring Teil des gleichen Subnetzes sind. Siehe *M580 Hot Standby Systemplanungshandbuch*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

In dieser flachen Netzwerkstruktur können alle Geräte, einschließlich CPU, CRAs und BMENUA0100-Modul, Clients desselben NTP-Servers sein, der sich im Steuerungsnetzwerk befindet. Somit wird die CPU-Zeit mit dem Modul BMENUA0100 synchronisiert.

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

Flaches Netzwerk mit mehreren M580-Standalone-CPUs und einem einzelnen SCADA-System

Architektur



1 Standalone-PAC

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 ermöglicht eine Verbindung zu einem einzelnen OPC UA-Client (einem SCADA-System) von mehreren M580-Standalone-CPUs. 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 wird für jeden Standalone-PAC deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt. Die Upstream-Kommunikation von jedem PAC zu dem einzelnen SCADA-Server erfolgt über den CPU-Service-Port.

In Konfiguration 1 wird die Downstream-Konnektivität vom PAC zur X80-Ethernet-RIO-Station (4) über die dualen Gerätenetzwerk-Ports der CPU bereitgestellt. Weitere Downstream-Konnektivität wird vom CRA-Service-Port und einem BMENOS0300-Switch (9) an die verteilten Ethernet-Geräte geliefert.

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

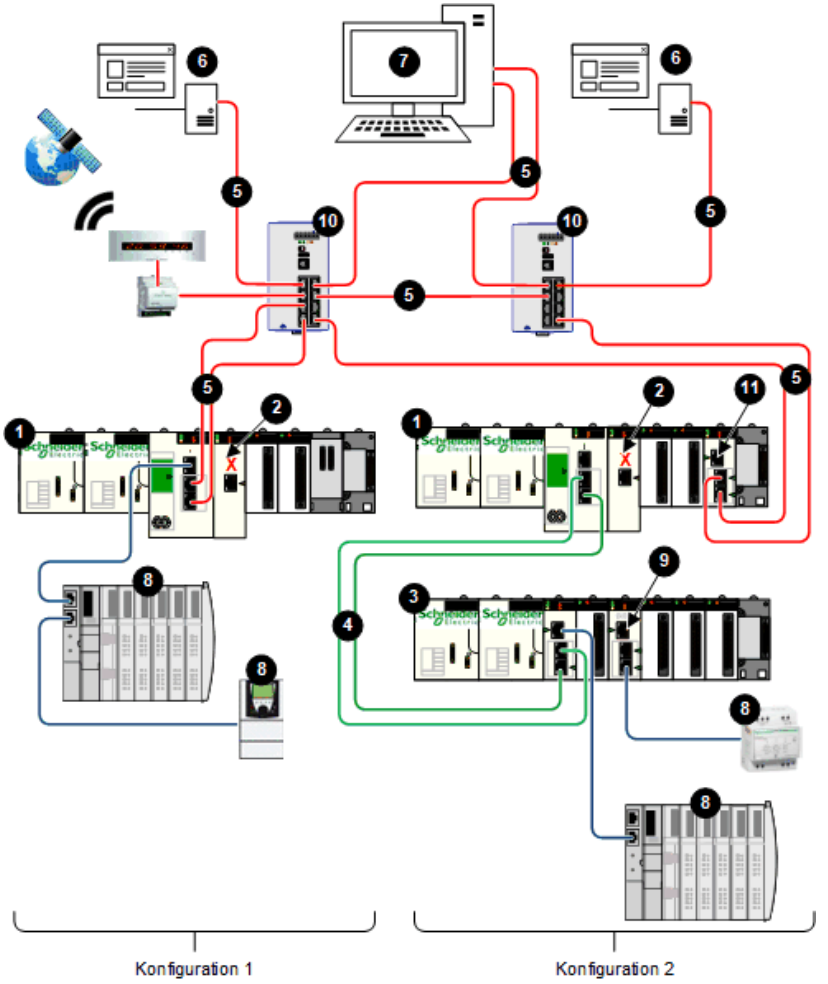
In dieser flachen Netzwerkstruktur sind alle Netzwerkgeräte – einschließlich CPU, CRAs und BMENUA0100-Modul – NTP-Clients eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Dadurch werden die CPU-Zeit und die BMENUA0100-Modulzeit synchronisiert.

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

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

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

Architektur



1 Standalone-PAC

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- oder ein BMENOC0301/11-Modul

Beschreibung

Diese Architektur ermöglicht eine hohe Verfügbarkeit des Steuerungsnetzwerks über redundante Verbindungen zwischen OPC UA-Clients (SCADA-Systemen) und mehreren M580-Standalone-CPUs. 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 wird für jeden Standalone-PAC deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

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

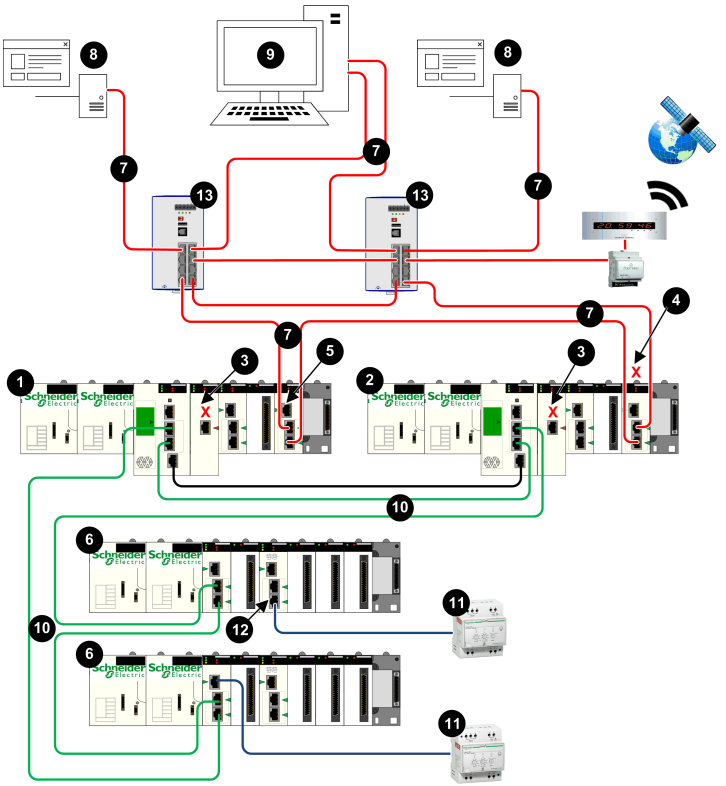
In Konfiguration 2 wird die Upstream-Konnektivität zu den SCADA-Servern über die Gerätenetzwerk-Ports eines BMENOS0300- oder eines BMENOC0301/11-Moduls bereitgestellt. Das RSTP-Redundanzprotokoll wird verwendet, um zur Vermeidung von logischen Ethernet-Schleifen jedem Port Rollen zuzuweisen. Die Downstream-Konnektivität vom PAC wird über die CPU-Gerätenetzwerk-Ports zur dezentralen X80-Ethernet-E/A-Station bereitgestellt. Weitere Downstream-Konnektivität wird sowohl vom CRA-Service-Port als auch von einem BMENOS0300-Switch (9) an die verteilten Ethernet-Geräte geliefert.

In dieser flachen Netzwerkstruktur sind alle Netzwerkgeräte – einschließlich CPU, CRAs und BMENUA0100-Modul – NTP-Clients eines NTP-Servers, der sich im Steuerungsnetzwerk befindet. Dadurch werden die CPU-Zeit 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 im PAC ausgeführten Anwendung verbraucht, die die Rohdaten konvertiert und in einem nutzbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

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

Architektur



1 Primärer Hot Standby-PAC

2 Standby-Hot-Standby-PAC

3 BMENUA0100 mit deaktiviertem Steuerungsport

4 BMENOS0300 oder BMENOC0301/11 mit deaktiviertem Baugruppenträger-Port

5 BMENOS0300 oder BMENOC0301/11 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 Hochverfügbarkeit mit redundanten Verbindungen, die redundante OPC UA-Clients (SCADA-Systeme) mit redundanten Hot Standby-PACs in einen einzelnen Subnetz verbinden.

Jeder PAC ist über ein BMENOS0300- oder BMENOC0301/11-Modul mit SCADA verbunden. Um die unbeabsichtigte Bildung von Ethernet-Schleifen zu verhindern, ist der Baugruppenträger-Port des BMENOS0300- oder des BMENOC0301/11-Moduls deaktiviert. In diesem Beispiel ist dies das Modul im Standby-PAC (4) mit einem deaktivierten Baugruppenträger-Port. Außerdem wird das RSTP-Redundanzprotokoll verwendet, um zur Vermeidung von logischen Ethernet-Schleifen jedem Port Rollen zuzuweisen.

Der BMENUA0100-Steuerungsport wird für jeden Standalone-PAC deaktiviert (3). 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 CPU-Gerätenetzwerk-Ports bereitgestellt. Weitere Downstream-Konnektivität von den X80-Ethernet-RIO-Stationen wird sowohl vom CRA-Service-Port als auch von einem BMENOS0300-Switch (12) an die verteilten Ethernet-Geräte geliefert.

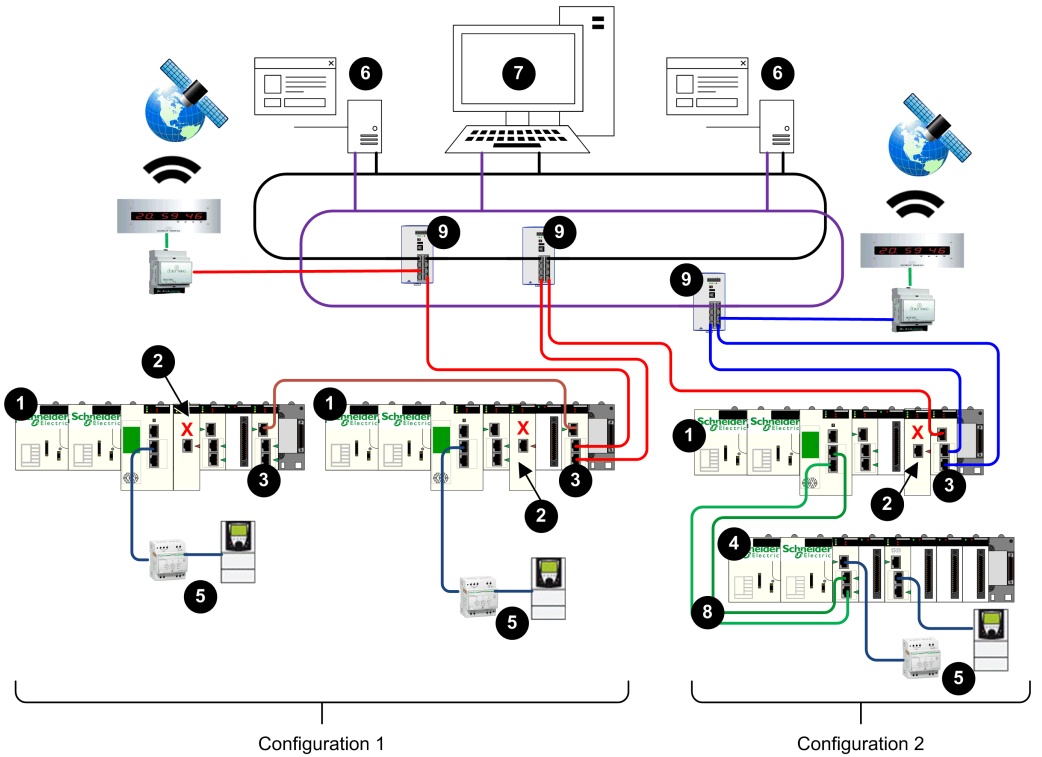
In dieser flachen Netzwerkstruktur sind alle Netzwerkgeräte – einschließlich Hot Standby-CPUs und BMENUA0100-Modul – NTP-Clients eines NTP-Severs, der sich im

Steuerungsnetzwerk befindet. Dadurch werden die CPU-Zeit 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 im PAC ausgeführten Anwendung verbraucht, die die Rohdaten konvertiert und in einem nutzbaren Format speichert. Die formatierten Datensätze können dann von einer übergeordneten Anwendung, wie beispielsweise einem SCADA-System, verwendet werden.

Hierarchisches Netzwerk mit mehreren M580-Standalone-CPUs, die an das Steuerungsnetzwerk angeschlossen sind, und redundantem SCADA

Architektur



1 Standalone-PAC

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 PACs zu den OPC UA-Clients (SCADA-Systemen) erfolgt über die dualen Gerätenetzwerk-Ports des BMENOC0321-Moduls, wobei das RSTP-Redundanzprotokoll zur Vermeidung logischer Ethernet-Schleifen verwendet wird.

HINWEIS: Diese Architektur erfordert die Konfiguration von statischen Routen in den Geräten des Steuerungsnetzwerks, um die verschiedenen Subnetze der einzelnen CPU-PACs umzuleiten.

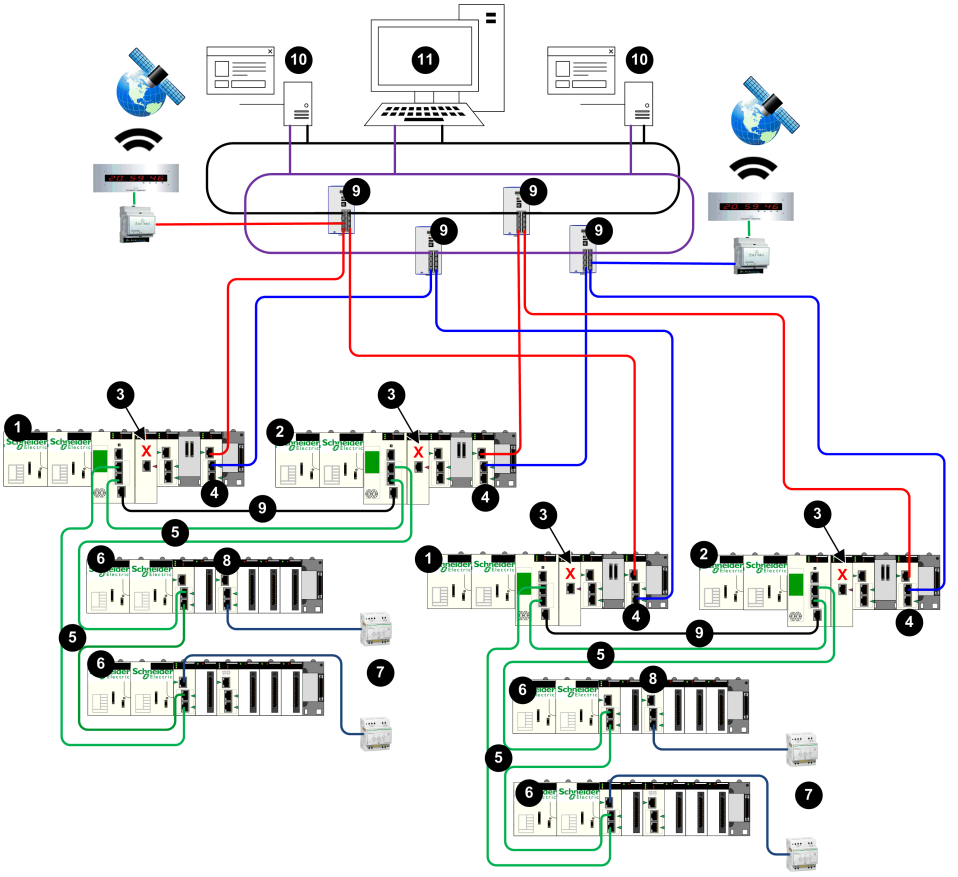
Der BMENUA0100-Steuerungsport (2) wird für jeden Standalone-PAC deaktiviert. Die IPv4-Ethernet-Kommunikation mit dem BMENUA0100-Modul wird über den Baugruppenträger-Port bereitgestellt.

Konfiguration 1 umfasst zwei PACs, 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 CPUs ermöglichen eine Downstream-Kommunikation mit den verteilten Ethernet-Geräten.

Konfiguration 2 umfasst einen einzelnen PAC mit X80-Ethernet-RIO-Station. Dieser PAC nutzt das Modul BMENOC0321 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 CRA-Service-Port und einen BMENOS0300-Switch zu den verteilten Ethernet-Geräten.

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

Architektur



1 Primärer Hot Standby-PAC

2 Standby-Hot-Standby-PAC

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-PACs zu den OPC UA-Clients (SCADA-Systemen) erfolgt über die dualen Gerätenetzwerk-Ports der BMENOC0321-Module, wobei das RSTP-Redundanzprotokoll zur Vermeidung logischer Ethernet-Schleifen verwendet wird.

HINWEIS: Diese Architektur erfordert die Konfiguration von statischen Routen in den Geräten des Steuerungsnetzwerks, um die verschiedenen Subnetze der einzelnen CPU-PACs umzuleiten.

Der BMENUA0100-Steuerungsport (3) ist für jeden PAC 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 CPUs ermöglichen eine Downstream-Kommunikation mit den X80-Ethernet-RIO-Stationen. Eine weiterführende Downstream-Kommunikation von der X80-Ethernet-RIO-Station zu den verteilten Ethernet-Geräten erfolgt sowohl über den CRA-Service-Port als auch über 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 118.
2. Konfigurieren Sie den Router/SLAAC-Server (für IPV6 im SLAAC-Modus).
3. Wählen Sie die Operationen im gesicherten Modus für das Modul aus:

a. Stellen Sie den Drehschalter, Seite 20 an der Rückseite des Moduls auf die Position Gesicherter Betriebsmodus, Seite 27.

b. Installieren Sie das Modul, Seite 82 in einem Ethernet-Steckplatz im Rack.

4. Konfigurieren Sie die Cybersicherheitseinstellungen über die Webseiten, Seite 84 des Moduls:

a. Erstellen Sie die Konfiguration der Cybersicherheit über die Webseite Einstellungen, Seite 92.

b. Stellen Sie den **PKI-Modus** auf „Selbstsigniert und CA“ ein.

c. Erstellen Sie für Clientgeräte, die PKI nicht unterstützen, eine Allowlist, Seite 112 mit **vertrauenswürdigen Clientzertifikaten**.

d. **Übernehmen** Sie die Konfigurationsdatei.

5. Führen Sie eine manuelle Zertifikatregistrierung, Seite 111:

a. Generieren Sie eine Zertifikatsignierungsanforderung (CSR).

b. Schieben Sie das Zertifizierungsstellenzertifikat.

c. Übertragen Sie das Gerätezertifikat.

6. Fügen Sie das Zertifizierungsstellenzertifikat den OPC UA-Clientgeräten hinzu.
7. Testen Sie die Kommunikation zwischen dem OPC UA-Client und dem -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 neues BMENUA0100-Modul werkseitig ausgeliefert wird, ist der Betriebsmodus der Cybersicherheit standardmäßig auf den sicheren Modus eingestellt. Um das neue Modul für einen Betrieb im sicheren Modus zu konfigurieren, befolgen Sie die Schritte im unten beschriebenen Szenario für die Inbetriebnahme im sicheren Modus, Seite 27.

Um den Cybersicherheitsmodus für ein zuvor konfiguriertes Modul zu ändern, einschließlich eines neuen Moduls, das Sie für einen Betrieb im Standardmodus konfigurieren möchten, führen Sie einen Sicherheits-Reset, Seite 80 für das Modul aus. Nach dem Sicherheits-Reset können Sie das Szenario für die Inbetriebnahme im sicheren Modus, Seite 27 oder die Inbetriebnahme im Standardmodus, Seite 27 durchführen.

Inbetriebnahme im sicheren Modus

Die Inbetriebnahme eines BMENUA0100-Moduls für den Betrieb im sicheren Modus erfordert den Abschluss 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, der die Standardkombination aus Benutzername und Passwort, Seite 28 im sicheren Modus verwendet, kann das Modul im sicheren Modus in Betrieb nehmen.

HINWEIS: Führen Sie diese Konfigurationsschritte in der folgenden 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 sicheren Modus mit manueller Registrierung finden Sie unter Manuelle Registrierung, Seite 111.

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 Sicherheits-Reset, Seite 80 durch, bevor Sie mit den folgenden Schritten fortfahren.

So nehmen Sie das Modul im 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 118.

2. Konfigurieren der Einstellungen für die Cybersicherheit:

a. Während das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 20, um den Drehschalter auf die Position **Secured** einzustellen.

b. Installieren, Seite 81 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 unter der konfigurierten IP-Adresse.

d. Wenn Ihr Internetbrowser eine Meldung anzeigt, Seite 86, die auf ein mögliches Sicherheitsrisiko hinweist, stellen Sie die Verbindung her, indem Sie auf **Risiko akzeptieren und fortfahren** (oder eine ähnliche Option, je nach Browser) klicken.

e. Geben Sie auf der Anmeldeseite des Benutzers die Standardkombination aus Benutzername/Passwort, Seite 28 ein.

f. Ändern und bestätigen Sie das Passwort. Informationen zu den Passwortanforderungen finden Sie im Abschnitt zur Benutzerverwaltung, Seite 114. Die Modulseite, Seite 89 **Home** wird angezeigt.

g. Navigieren Sie von der Startseite **Home** zu den Webseiten des Moduls und konfigurieren Sie die Cybersicherheitseinstellungen.

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 118.

c. Wenn die Control Expert-Projektkonfiguration abgeschlossen ist, stellen Sie eine Verbindung zum PAC her und übertragen Sie das Projekt in den PAC.

HINWEIS: Wenn die Konfiguration in das BMENUA0100-Modul geladen wird, ändert sich der Modulstatus von NICHT KONFIGURIERT in KONFIGURIERT. Die SECURE-LED, Seite 139 gibt an, ob das Modul konfiguriert oder nicht konfiguriert ist und ob der OPC UA-Server mit einem OPC UA-Client verbunden ist.

Inbetriebnahme im Standardmodus

Im Standardmodus ist keine Cybersicherheitskonfiguration erforderlich. Nur die IP-Adress-, NTP-Client- und SNMP-Agent-Einstellungen werden mit dem Control Expert-Konfigurationstool 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/Passwort, Seite 28 des Installationsprogramms, um das Modul im Standardmodus in Betrieb zu nehmen.

So nehmen Sie das Modul im Standardmodus in Betrieb.

1. Während das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 20, um den Drehschalter auf die Position **Standard** einzustellen.
2. Platzieren Sie das Modul in einem Ethernet-Steckplatz im lokalen Ethernet-Hauptrack und schalten Sie das Modul aus und wieder ein.
3. Öffnen Sie das Konfigurationstool von Control Expert.
4. Erstellen Sie in Control Expert ein **Neues Projekt**, fügen Sie dem Projekt ein BMENUA0100-Modul aus dem **Hardwarekatalog** hinzu und konfigurieren Sie dann die Einstellungen für die IP-Adresse, Seite 118, den NTP-Client, Seite 128 und den SNMP-Agent, Seite 131.
5. Wenn die Control Expert-Projektkonfiguration abgeschlossen ist, stellen Sie eine Verbindung zum PAC her und übertragen Sie das Projekt in den PAC.

   HINWEIS: Beim Betrieb im Standardmodus ist die SECURE-LED aus.

Sicherheits-Reset

Führen Sie für ein zuvor konfiguriertes Modul oder für ein neues Modul, das Sie für einen Cybersicherheitbetrieb im Standardmodus konfigurieren möchten, einen Sicherheits-Reset durch, bevor Sie mit der Cybersicherheitskonfiguration 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 Drehschalters an der Rückseite des Moduls vornehmen.

Webseiten: Für ein BMENUA0100-Modul, das derzeit für den Betrieb im sicheren Modus konfiguriert ist:

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

   HINWEIS: Der Sicherheits-Reset ist abgeschlossen, wenn die RUN-LED dauerhaft grün leuchtet und sowohl die NS-Steuerungsport-LED als auch die BS-Baugruppenträger-Port-LED dauerhaft 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 sicheren Modus fortfahren.

Drehschalter: Für jedes BMENUA0100-Modul:

1. Während das Modul vom Rack getrennt ist, verwenden Sie den mit dem Modul gelieferten Kunststoffschraubendreher, Seite 20, um den Drehschalter auf die Position **Security Reset** einzustellen.
2. Installieren, Seite 81 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 119: 10.10.MAC5.MAC6.

   Nach Abschluss des Vorgangs leuchtet die RUN-LED dauerhaft grün, und sowohl die NS-Steuerungsport-LED als auch die BS-Baugruppenträger-Port-LED leuchten dauerhaft rot. Sie können den Strom abschalten, das Modul aus dem Rack entfernen und dann entweder mit der Inbetriebnahme im sicheren Modus, Seite 27 oder der Inbetriebnahme im Standardmodus, Seite 27 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 Sicherheitsspannungsversorgung oder der CPU vorbehalten ist.

HINWEIS: Wenn Ihre Anwendung mehrere PACs (die nicht gepaart mit Hot Standby-PACs sind) mit einem BMENUA0100-Modul umfasst, installieren Sie die Module so, dass die Steckplatznummer jedes BMENUA0100-Moduls eindeutig ist. Wenn beispielsweise bei einer Anwendung mit zwei PACs ein BMENUA0100-Modul im PAC1-Rack in Steckplatz 4 eingesetzt wird, setzen Sie ein BMENUA0100-Modul im PAC2-Rack in einen anderen Steckplatz als Steckplatz 4.

Sicherheitshinweise zur Erdung

Jedes BMENUA0100-Modul ist mit Erdungskontakten ausgestattet.

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

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

⚠⚠ GEFAHR

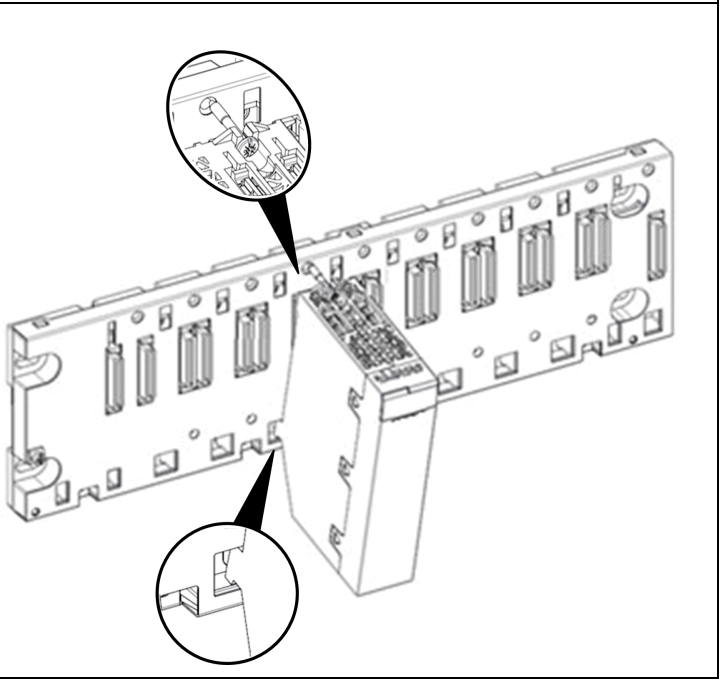
GEFAHR EINES ELEKTRISCHEN SCHLAGS

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

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

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 weder für die Spannungsversorgung noch für die CPU vorgesehen 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 unter 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 IPv6-Protokoll, Seite 120.

Um das BMENUA0100-Modul im sicheren Modus zu betreiben, ist eine Cybersicherheitskonfiguration erforderlich. Sie muss vorgenommen werden, bevor die IP-Adresse, der NTP-Client und die SNMP-Einstellungen mithilfe von Control Expert konfiguriert werden können, Seite 118. Eine Cybersicherheitskonfiguration kann nur lokal für jedes BMENUA0100-Modul erfolgen, indem ein Konfigurations-PC mit einem HTTPS-Browser mit dem BMENUA0100-Modul verbunden wird:

- Steuerungsport, wenn der Steuerungsport aktiviert ist.
- Baugruppenträger-Port (über ein BMENOC0301/11-Modul oder die CPU), wenn der Steuerungsport deaktiviert ist.

HINWEIS: Bevor das BMENUA0100-Modul die Gültigkeit der auf den Webseiten angegebenen Cybersicherheitseinstellungen überprüft, stellt es zunächst die IP-Adresseinstellungen für den Steuerungsport und den Baugruppenträger-Port ein, die in Control Expert konfiguriert, Seite 118 sind.

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

HINWEIS:

- Wenn Sie ein selbstsigniertes Zertifikat verwenden, melden einige Browser die Verbindung zwischen dem PC und dem Modul möglicherweise als „Ungesichert“.
- Um BMENUA0100-Module in einem Hot Standby-System im sicheren Modus zu betreiben, überprüfen Sie, ob die Cybersicherheitseinstellungen für das BMENUA0100-Modul im primären PAC die gleichen sind wie die Cybersicherheitseinstellungen für das BMENUA0100-Modul im Standby-PAC. Das System führt diese Überprüfung nicht automatisch für Sie aus.

Die Zugänglichkeit der Webseiten richtet sich nach dem Cybersicherheitsmodus:

Webseite oder Gruppe	Sicherer Modus	Standardmodus
Home, Seite 89	✓	✓
Einstellungen (Gerätesicherheit), Seite 92	✓	–
Zertifikatverwaltung, Seite 105	✓	–
Zugriffssteuerung, Seite 114	✓	–
Konfigurationsverwaltung, Seite 116	✓	–
Diagnose, Seite 161	✓	✓
✓: Zugriff auf Webseiten ist möglich. –: Zugriff auf Webseiten ist nicht möglich.		

Anfängliche Konfiguration der Cybersicherheitseinstellungen

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

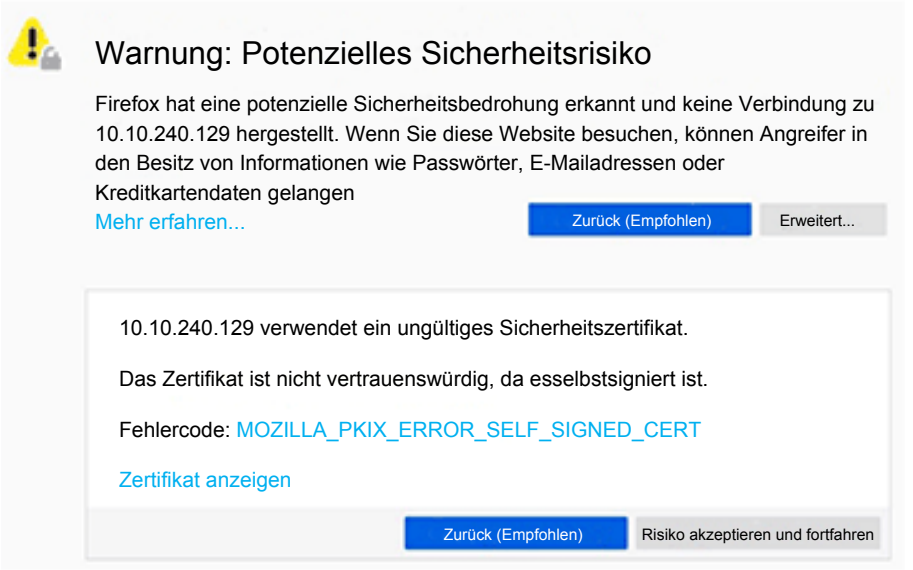
- Es wurde nie konfiguriert und behält seine ursprüngliche werkseitige Standardkonfiguration bei.
- Es wurde zuvor konfiguriert, aber die werkseitige Standardkonfiguration wurde durch Ausführung des Befehl zum Sicherheits-Reset, Seite 28 beibehalten.

Nachdem ein Modul mit Cybersicherheitseinstellungen konfiguriert wurde und wenn es im sicheren Modus ausgeführt wird, können Sie die Cybersicherheitseinstellungen ebenfalls über die Webseiten ändern.

Anweisungen zur Anwendung einer Anfangskonfiguration auf das Modul finden Sie im Abschnitt zur Inbetriebnahme, Seite 78.

Erste Anmeldung bei den Webseiten

Wenn Sie sich bei einem nicht konfigurierten BMENUA0100-Modul anmelden, wird der folgende Bildschirm angezeigt:



Trotz der Warnmeldung ist die Verbindung über HTTPS gesichert. Fahren Sie mit der ersten Anmeldung fort, indem Sie auf **[Risiko akzeptieren und fortfahren]** (oder eine ähnliche Option, je nach Browser) klicken.

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

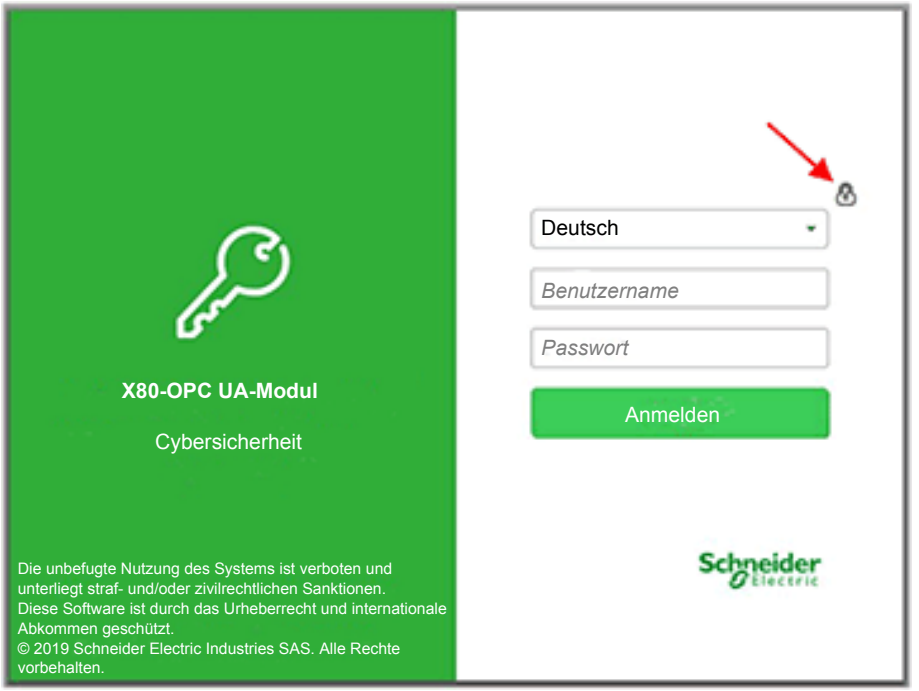
Anmeldung bei den Webseiten

Bei der ersten Anmeldung gibt der Sicherheitsadministrator die Standardkombination aus Benutzername und Passwort, Seite 28 ein. Unmittelbar danach muss der Administrator das Standardpasswort des Administrators 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 114 **Zugriffssteuerung > 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 Ihren **Benutzernamen** und das **Passwort** ein.

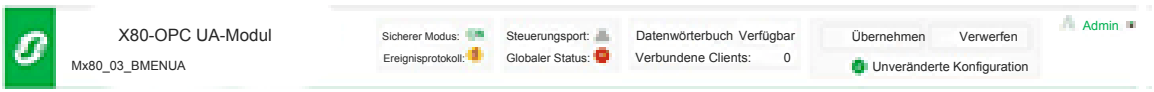


HINWEIS: Der Cybersicherheitsmodus des Moduls wird durch das Schloss-Symbol oben rechts im Dialogfeld angezeigt (siehe der rote Pfeil in der Abbildung). Schloss befindet sich in folgendem Zustand:

- Geschlossen (wie oben dargestellt): Das Modul wird im sicheren Modus, Seite 27 ausgeführt.
- Offen: Das Modul wird im Standardmodus, Seite 27 ausgeführt.

Webseiten-Banner

Jede Webseite verfügt über ein Banner oben auf der Seite:



Das Banner enthält die folgenden Informationen zum BMENUA0100-Modul:

- Sicherer Modus:
  - EIN: Das Modul wird im sicheren Modus, Seite 27 ausgeführt.
  - AUS: Das Modul wird im Standardmodus, Seite 27 ausgeführt.
- Ereignisprotokoll:
  -  Der Ereignisprotokollierungsdienst ist deaktiviert.
  -  Der Ereignisprotokollierungsdienst ist aktiviert, der Protokollserver ist erreichbar.
  -  Der Ereignisprotokollierungsdienst ist aktiviert, der Protokollserver ist nicht erreichbar.
  -  Der Ereignisprotokollierungsdienst ist aktiviert, aber es wurde ein Fehler festgestellt.
- 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 zurzeit angeschlossenen OPC UA-Clients.

- Konfiguration übernehmen/verwerfen: Gibt den Status der aktuellen Cybersicherheit-Webseitenkonfiguration des Moduls an:
  - Unveränderte Konfiguration: Die Cybersicherheitskonfiguration enthält keine ausstehenden oder ungültigen Änderungen. Die Befehle **Übernehmen** und **Verwerfen** sind deaktiviert.
  - Ausstehende Konfiguration: Eine oder mehrere Änderungen an der Cybersicherheitskonfiguration wurden noch nicht angewendet. Die Befehle **Übernehmen** und **Verwerfen** sind bei aktiviert.
  - Unzulässige Konfiguration: Die Cybersicherheitskonfiguration ist unvollständig oder nicht korrekt. Der Befehl **Übernehmen** ist deaktiviert, der Befehl **Verwerfen** ist aktiviert. In diesem Zustand wird auf der grafischen Benutzeroberfläche der Webseite neben jedem betroffenen Menüpunkt ein roter Kreis angezeigt, der die Anzahl der ungültigen Konfigurationseinstellungen enthält, die über diesen Menüpfad erreichbar sind. Wenn Sie zu einer Seite mit einer ungültigen Konfigurationseinstellung navigieren, identifiziert die GUI die ungültige Konfigurationseinstellung.

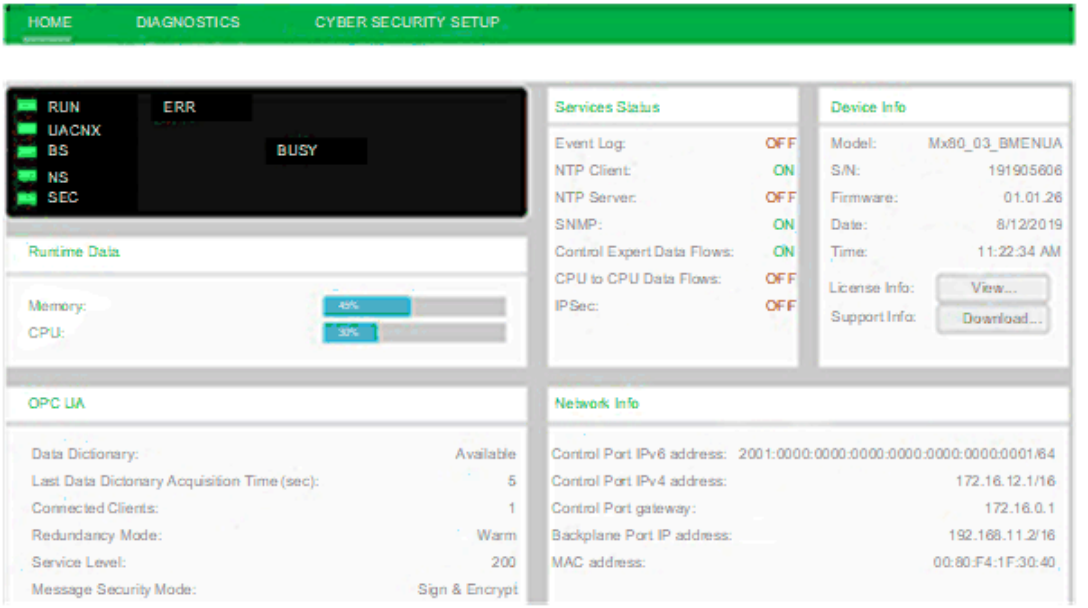
Webseiten-Hilfe

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

Startseite „Home“

Einführung in die Startseite

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



Verwenden Sie die Seite **Home**, um folgende Vorgänge durchzuführen:

- Öffnen Sie die Navigationsstruktur, die Links zu den Webseiten des BMENUA0100-Moduls enthält. Wenn das Modul im folgenden Modus ausgeführt wird:
  - Sicherer Modus, Seite 27 – Die Menüs DIAGNOSE und KONFIGURIEREN DER CYBERSICHERHEIT-EINSTELLUNGEN werden angezeigt und sind für den Sicherheitsadministrator zugänglich.
  - Standardmodus, Seite 27 – Nur das Menü DIAGNOSE ist zugänglich.
- Anzeigen des Status, Seite 136 der Modul-LEDs, Seite 21.
- Anzeigen von Datensammlungen für das Modul, einschließlich:
  - Laufzeitdaten, Seite 91
  - OPC UA, Seite 91
  - Dienststatus, Seite 91
  - Netzwerkinfo, Seite 92
  - Geräteinfo, Seite 92

  HINWEIS: Wenn der Drehschalter auf der Rückseite des Moduls auf die Position Security Reset, Seite 28 eingestellt ist, kann keine Kommunikation mit dem Modul erfolgen. Somit ist kein Zugriff auf die Webseiten – einschließlich der Seite **Home** – möglich.

Laufzeitdaten

Im Bereich **OPC UA** wird Folgendes angezeigt:

- **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 140.

OPC UA

Im Bereich **Laufzeitdaten** wird Folgendes angezeigt:

- **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 (REDUNDANCY_MODE).

  HINWEIS: Die oben beschriebenen fünf Elemente basieren auf Elementen im T_BMENUA0100-DDT, Seite 140.
- **Nachrichtensicherheitsmodus**: Die auf der OPCUA-Webseite, Seite 103 konfigurierte Einstellung: Keine, Signieren oder Signieren und Verschlüsseln.

Dienststatus

Im Bereich **Dienststatus** wird der Status – aktiviert (EIN) oder deaktiviert (AUS) – der folgenden Dienste, wie im T_BMENUA0100-DDT, Seite 140 ausgewiesen, angezeigt:

- **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-Datenfluss** (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, das in Control Expert, Seite 118 eingegeben und im T_BMENUA0100-DDT, Seite 140 ausgewiesen wurde. 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 Modell, Seriennummer und Firmware-Version (FW_VERSION im T_BMENUA0100-DDT, Seite 140), Datum und Uhrzeit für das BMENUA0100-Modul angezeigt.

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

Klicken Sie auf **Herunterladen...**, um Kontaktinformationen für den technischen Support anzuzeigen.

HINWEIS: Nachdem Sie auf **Herunterladen...** geklickt haben, werden Sie aufgefordert, Ihr Benutzerpasswort, Seite 114 einzugeben, um fortzufahren.

Einstellungen

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

- Benutzerkontorichtlinien, Seite 93
- Ereignisprotokolle, Seite 94
- Netzwerkdienste, Seite 94
- Dienstweiterleitung, Seite 96
- IPSEC, Seite 101
- SNMP, Seite 102

- OPC UA, Seite 103
- Sicherheitsbanner, Seite 105

Nachfolgend sind die konfigurierbaren Parameter für jeden Netzknoten beschrieben.

Verwenden Sie diese Einstellungen, um die Gerätesicherheit für das BMENUA0100-Modul zu konfigurieren. Wählen Sie nach der Änderung der Einstellungen **Übergeben** oder **Abbrechen** aus.

Benutzerkontorichtlinien

Verwenden Sie diese Einstellungen, um die Benutzerkontorichtlinien zu konfigurieren:

Parameter	Beschreibung
Maximale Inaktivität der Sitzung (Minuten)	Die Timeout-Dauer der Leerlaufsitzung für HTTPS-Verbindungen. Wenn während dieser Zeit keine Verbindung aufgebaut wird, wird die Benutzersitzung automatisch beendet. Standard = 15 Min. **HINWEIS:** Für OPC UA-Verbindungen besteht kein Inaktivitätsperiode-Timeout.
Maximale Anzahl an Anmeldeversuchen:	Die Anzahl der Anmeldeversuche, die ein Benutzer unternimmt und scheitert. Standard = 5 Versuche. Wenn der konfigurierte Höchstwert erreicht ist, wird das Benutzerkonto gesperrt.
Anmeldeversuch-Timer (Minuten)	Die maximale Dauer der Anmeldung. Standard = 3 Min.
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 gesperrten Benutzerkontos automatisch aufgehoben. Standard = 4 Min.

HINWEIS: Diese Benutzerkonto-Richtlinieneinstellungen gelten für OPC UA-Clients, Seite 170, 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 156 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 nur ab Firmware-Version 1.10 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 alle Netzwerkdienste mit Ausnahme von IPSec, das aktiviert ist.
Sicherheit freigeben	Aktiviert alle Netzwerkdienste, mit Ausnahme von IPSec, das deaktiviert ist.

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

Dienst	Beschreibung	CS Op Mode - Standard	
		Standard	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]
Datenfluss zwischen CPU und CPU[2, 3] Siehe *Konfiguration des Kommunikationsflusses*	Ermöglicht die Aktivierung und Deaktivierung der Modbus-Kommunikation zwischen M580-CPUs über das BMENUA0100-Modul.	Aktiviert	Deaktiviert

Dienst	Beschreibung	CS Op Mode - Standard	
		Standard	Sicher
zwischen CPU und CPU, Seite 96.)			
Control Expert-Datenfluss zur CPU nur [2, 3] (Siehe *Konfiguration der Kommunikation für den Control Expert-Datenfluss*, Seite 96.)	Ermöglicht die Aktivierung bzw. Deaktivierung der Modbus-, EtherNet/IP-, Ping-, expliziten Nachrichtenaustausch- und FTP-Kommunikationsschnittstellen zwischen der Control Expert-Konfigurationssoftware und der CPU. BMENUA0100	Aktiviert	Deaktiviert
Control Expert-Datenfluss zum Gerätenetzwerk[2, 3] (Siehe *Konfiguration der Kommunikation für den Control Expert-Datenfluss*, Seite 96.)	Ermöglicht die Aktivierung und Deaktivierung der Modbus-, EtherNet/IP-, Ping-, expliziten Nachrichtenaustausch- und FTP-Kommunikation über das BMENUA0100-Modul zwischen der Control Expert-Konfigurationssoftware und Netzwerkgeräten, einschließlich der CPU.	Aktiviert	Deaktiviert
HTTPS am Steuerungsport	Ermöglicht die Aktivierung und Deaktivierung der HTTPS-Kommunikation über den Steuerungsport. **HINWEIS:** Wenn HTTPS deaktiviert ist und die Änderung übernommen wurde, kann nicht über den Steuerungsport 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 ohne definierte Regeln aktiviert. Der Dienst muss konfiguriert werden.

2. Informationen zu diesem Konfigurationsentwurf finden Sie im Abschnitt zur Fehlerbehebung Aktivierung von Netzwerkdiensten mit einer IPv6-Verbindung, Seite 170.

3. Wird nur von Modulen vor der Version BMENUA0100.2 unterstützt.

HINWEIS: SNMP-, NTP-, Syslog- und Modbus-Dienste sind nicht von Natur aus sichere Protokolle. Sie werden sicher gemacht, wenn sie in IPSEC eingebettet werden. Es wird empfohlen, IPSEC nicht zu deaktivieren, wenn einer der SNMP-, NTP-, Modbus- oder Syslog-Dienste aktiviert ist.

Konfiguration der Kommunikation für eine auf PCs ausgeführte dezentrale Software (nicht die NAT-Weiterleitung)

Die Software adressiert das Zielgerät (z. B. die M580-CPU) unter Verwendung der 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 für die IP-Adresse des Steuerungsports des BMENUA0100-Moduls ein.
- Richten Sie auf dem Zielgerät (z. B. der M580-CPU) unter Verwendung von IPv4 ein Standard-Gateway für die IP-Adresse des BMENUA0100-Modulsteuerungsports ein.
- Fügen Sie auf dem Host-PC einen Pfad mit folgendem Befehl hinzu:

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

Für IPv4 in allen Firmware-Versionen und für IPv6 in den Firmware-Versionen 1.10 und höher adressiert die Modbus-Kommunikationsschnittstelle im Control Expert-Verbindungsfenster die IP-Adresse des BMENUA0100-Steuerungsports. Gateways sind für diese Kommunikation nicht erforderlich.

Konfiguration des Kommunikationsflusses zwischen CPU und CPU

Die Modbus-TCP/IP-Kommunikation von CPU zu CPU über das BMENUA0100-Modul verwendet die IPv4-Steuerungsportadresse des BMENUA0100-Moduls und nicht die Adresse der Ziel-CPU.

HINWEIS:

- Bei BMENUA0100 V1.x ist die CPU-zu-CPU-Weiterleitung auf das Modbus TCP/IP-Protokoll beschränkt.
- Nur die IPv4-Adressierung (und nicht Ipv6) unterstützt Datenflüsse von Modbus TCP/IP-CPU zu CPU.

Dienstweiterleitung (IP-Weiterleitung)

Ein BMENUA0100-Modul mit einer Firmware-Version ab 2.01 umfasst 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 Tasks von diesem Dienst nicht unterstützt:

- Geräteerkennung durch das Tool EcoStruxure Automation Device Maintenance (EADM), das im automatischen Erkennungsmodus arbeitet. Die EADM-Geräteerkennung über den manuellen Erkennungsmodus wird unterstützt. (Multicast).
- Nachrichtenübertragung an die lokalen Slaves des PAC (impliziter EtherNet/IP-Nachrichtenaustausch).

Merkmale:

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

- Möglichkeit, alle Datenflüsse weiterzuleiten („Alle weiterleiten“).
- IP-Weiterleitung der in der Architektur am häufigsten verwendeten Protokolle über vordefinierte Vorlagen (z. B.: Modbus, HTTPS, SNMP usw.)
- Erstellung und Anwendung von benutzerdefinierten Vorlagen für die IP-Weiterleitung
- NAT-Weiterleitung einiger Protokolle an die lokale CPU, wenn die @remote-IP-Adresse der IP V4-Steuerungsport des BMENUA0100 ist

  HINWEIS: Die NAT-Weiterleitung gilt für die folgenden Protokolle: Modbus, Modbus über TLS, EIP Explizit, EIP Explizit über TLS, EIP Implizit, OPC UA-Client.
- Die Option zur Verwendung oder Nicht-Verwendung von IPSEC für Protokolle, die von NAT weitergeleitet werden. Siehe die Empfehlungen in den Hinweisen unten im Abschnitt IPSEC, Seite 101.

HINWEIS:

- Wenn sich mehrere BMENUA0100-Module im gleichen Rack befinden, müssen Sie nur ein BMENUA0100-Modul mit der Weiterleitungsfunktion konfigurieren.
- Multicast-Datenflüsse werden nicht weitergeleitet.
- Eine Online-Aktualisierung der IP-Weiterleitungsregeln kann dazu führen, dass einige laufende Kommunikationsvorgänge angehalten werden, wodurch Nachrichten verloren gehen.
- Damit die Dienstweiterleitung (IP-Weiterleitung) erfolgreich ist, muss sich das Ziel-IP-Netzwerk vom Quell-IP-Netzwerk unterscheiden. So ist es beispielsweise nicht möglich, die 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. Es wird empfohlen, die Weiterleitung des FTP-Protokolls nur vorübergehend zu aktivieren, wenn dies erforderlich ist.
  - Die Aktivierung des TFTP-Protokolls als benutzerdefinierte Regel führt zu demselben Ergebnis wie die Aktivierung des FTP-Protokolls. Es wird empfohlen, die Weiterleitung des TFTP-Protokolls nur vorübergehend zu aktivieren, wenn dies erforderlich ist.

Weitere Informationen über die Architektur der Dienstweiterleitung (IP) finden Sie in den folgenden Rubriken:

- Unterstützte Architekturen für die Dienstweiterleitung (IP), Seite 176
- Nicht unterstützte Architekturen für die Dienstweiterleitung (IP), Seite 179

IP-Weiterleitung und OPC-UA-Kommunikation

Sowohl die IP-Weiterleitung als auch OPC UA beanspruchen die verfügbaren 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 180.

Erstellen von Regeln:

- Um sowohl vordefinierte als auch benutzerdefinierte Regeln zu dokumentieren, klicken Sie auf **Neue Weiterleitung** und vervollständigen Sie die Einstellungen, mit denen die Regel definiert wird.

  HINWEIS: Wenn Sie einen Dienstnamen auswählen, werden die Port-Nummer und das Protokoll automatisch mit den Standardeinstellungen verknüpft. 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 aufgelisteten Regeln zu übernehmen. 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.
Protocol[1]	Das Protokoll, das dem Dienst zugeordnet ist.
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:** Es wird Folgendes empfohlen: • **Verwenden Sie nicht** IPSec für nativ gesicherte Protokolle (z. B. Modbus über TLS, EIP Explizit über TLS, DNP3 über TLS, EIP 60870 über TLS). • **Verwenden Sie** IPSEC für nicht nativ sichere Protokolle (z. B. Modbus , EIP Explizit, OPC UA-Client, EIP IO).

Einstellung	Beschreibung
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 SPS-Funktionsbaustein). • **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 + Modbus TCP-Request von einem SPS-Funktionsbaustein).
1. Automatisch ausgefüllt, aber editierbar für vordefinierte Dienstnamen.	

IPSEC

Verwenden Sie IPSEC, um die sichere IPv4-Ethernet-Kommunikation zu unterstützen.

HINWEIS: IPSEC unterstützt die IPv6-Adressierung nicht.

Verwenden Sie diese Einstellungen, um bis zu 8 IKE/IPSEC-Kanäle über IPv4 für das Modul BMENUA0100 zu konfigurieren. Wenn mehr als 4 IPSec-Verbindungen konfiguriert sind, kann es sein, dass die automatische Verbindung mit dem PAC nach der Übertragung über das BMENUA0100-Modul nicht erfolgreich ist. In diesem Fall müssen Sie manuell eine Verbindung zum PAC herstellen.

Parameter	Beschreibung
IPSEC-DIENST	• EIN: Aktiviert den IPSec-Dienst. • AUS: Deaktiviert den IPSec-Dienst.
NTP außerhalb des IPSEC autorisiert.	• Deaktiviert (deaktiviert): NTP wird nur über IPSEC ausgetauscht. • Aktiviert: NTP wird beim Öffnen des IPSEC-Kanals über IPSEC und außerhalb von IPSEC ausgetauscht, wenn der IPSEC-Kanal nicht geöffnet ist.
Neuer Link	Erstellt einen neuen IKE-/IPSEC-Kanal und fügt ihn zur Bearbeitung in die Liste ein. **HINWEIS:** Es werden bis zu 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:** Die Vertraulichkeit ist deaktiviert, wenn *NTP ohne IPSEC* aktiviert ist.

Parameter	Beschreibung
Clienttyp	Typ des dezentralen IPSEC-Endpunkts: Windows oder Gerät. **HINWEIS:** Die Standardeinstellung ist Windows. Vergewissern Sie sich, dass der konfigurierte Endpunkttyp mit dem aktuellen Client übereinstimmt.
PSK	Vorinstallierter Schlüssel mit einer Länge von 32 Hexadezimalzeichen - das Ergebnis einer vom BMENUA0100-Modul generierten Zufallszahl. Sie 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 183, indem Sie das „Windows-Skript“ von BMENUA0100 herunterladen. Verwenden Sie dazu den Befehl **Skript herunterladen** für jede dezentrale IP-Adresse. Wenn die Einstellung **IPSEC-Verwendung** für einige Protokolle geändert wurde, muss das Windows-Skript erneut aus dem BMENUA0100-Modul geladen und unter Windows ausgeführt werden. Ein Windows-Skriptbeispiel finden Sie im Thema IPSEC-Windows-Skripts, Seite 183.

HINWEIS: Wenn 8 IPSEC-Tunnels konfiguriert sind, kann die Verbindung zum PAC nach dem Herunterladen einer Anwendung ggf. nicht automatisch wiederhergestellt werden. In diesem Fall müssen Sie die Verbindung nach dem Herunterladen manuell zum PAC wiederherstellen.

HINWEIS: Wenn IPSEC aktiviert ist, läuft der Datenfluss des lokalen HTTPS-Servers über IPSEC.

SNMP

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

HINWEIS: Im sicheren Modus muss die SNMP-Version sowohl in Control Expert, Seite 133 als auch 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:

Parameter	Beschreibung
	• 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 kann 8 bis 12 Zeichen umfassen und 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 enthalten und 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 & 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 den Benutzer-ID-Tokentyp im OPC UA-Client mit **Anonym** konfigurieren.
Sicherheitsrichtlinien	• Basic256Sha256 (Standard): Sie definiert eine Sicherheitsrichtlinie für Konfigurationen mit gültiger Verschlüsselungssuite. • Basic256: Sie 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: Sie 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 ist durch den Benutzernamen und das Passwort gekennzeichnet.

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. Wenn die *SessionTimeout*-Periode abgelaufen ist, werden die Sitzungen schließlich geschlossen. Das *SessionTimeout* ist Bestandteil der OPC UA-SCADA-Clientkonfiguration.

HINWEIS: Wenn die Einstellung **Nachrichtensicherheitsmodus** des OPC UA-Servers zunächst für **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** einstellen) nicht. Stellen Sie eine Verbindung zum Server her.

So stellen Sie eine Verbindung wieder her:

1. Trennen Sie die aktuellen OPC UA-Clients.
2. Ändern Sie die OPC-UA Konfiguration auf der BMENUA0100-Webseite.
3. Warten Sie, während die LED BUSY EIN (gelb) ist, bis sie erlischt (leuchtet nicht).
4. Ändern Sie für die OPC UA-Clients deren Konfiguration (**Nachrichtensicherheitsmodus**) in die 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 eine Public-Key-Infrastruktur (PKI) mit einer Zertifizierungsstelle (Certification Authority, CA) anwenden kann (oder nicht).

Zertifikatverwaltung ohne PKI:

Verwenden Sie diese Zertifikatverwaltungsmethode, wenn Ihr System keine Zertifizierungsstelle enthält. Diese Verwaltungsmethode wird von BMENUA0100-Modulen mit einer Firmware ab Version 1.0 unterstützt. Verwalten Sie Zertifikate auf den Webseiten der **Zertifikatverwaltung** wie folgt:

- Setzen Sie **PKI-Modus** auf **Nur Selbstsignatur**.
- Verwalten Sie die **Zertifikatsvertrauensliste** mithilfe der Funktionen **Hinzufügen** und **Löschen**, um eine Allowlist für OPC UA-Clients zu erstellen, die zur Kommunikation mit dem BMENUA0100-Modul berechtigt sind.
- Exportieren Sie das BMENUA0100-Modulzertifikat in OPC UA-Clientgeräte, indem Sie den Befehl **Herunterladen** auf der Seite **PKI-Konfiguration > Gerätezertifikat** verwenden.

Zertifikatverwaltung mit PKI:

Verwenden Sie diese Zertifikatverwaltungsmethode, wenn Ihr System eine Zertifizierungsstelle enthält. Diese Verwaltungsmethode wird von BMENUA0100-Modulen mit einer Firmware ab Version 1.1 unterstützt. Verwalten Sie Zertifikate auf den Webseiten der **Zertifikatverwaltung** wie folgt:

- Stellen Sie den **PKI-Modus** auf einen der folgenden Werte ein:
  - **Nur CA**: Wenn alle installierten OPC UA-Clientgeräte PKI unterstützen.
  - **Selbstsigniert und CA**: Wenn einige der installierten OPC UA-Clientgeräte PKI nicht unterstützen.
- Wenn der **PKI-Modus** auf **Nur CA** eingestellt ist:
  - Registrieren, Seite 111 Sie jedes BMENUA0100-Modul manuell bei der Zertifizierungsstelle.
- Wenn der **PKI-Modus** auf **Selbstsigniert und CA** gesetzt ist:
  - Registrieren, Seite 111 Sie jedes BMENUA0100-Modul manuell bei der Zertifizierungsstelle.
  - Verwalten Sie die **Zertifikatsvertrauensliste** mithilfe der Funktionen **Hinzufügen** und **Löschen**, um eine Allowlist für OPC UA-Clients zu erstellen, die zur Kommunikation mit dem BMENUA0100-Modul berechtigt sind.

Aktualisieren der Zertifikatsvertrauensliste

Nach der ersten Installation der BMENUA0100-Firmware-Version 2.0 (BMENUA0100.2) oder höher müssen Sie alle vom Benutzer hinzugefügten Zertifikate aus der **Zertifikatsvertrauensliste** auf der Webseite **Zertifikatsverwaltung** entfernen. Dies können Sie folgendermaßen tun:

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

- Einstellen des Drehschalters für die Cybersicherheit auf die Position **Security Reset**

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

Diese Aufgabe muss nur bei der ersten Installation der Firmware-Version 2.0 oder höher ausgeführt werden. Sie müssen das Verfahren bei nachfolgenden Installationen höherer Firmware-Versionen nicht wiederholen.

HINWEIS: Wenn Sie die **Zertifikatsvertrauensliste** nicht löschen, wie oben beschrieben, können keine Verbindungen zu OPC UA-Clients hergestellt werden oder gehen, falls diese eingerichtet sind, verloren.

Authentifizierungsübersicht

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

- Für Firmware ab Version 1.0:
  - Selbstsigniertes Zertifikat (nur)
- Für Firmware ab Version 1.10:
  - PKI-Zertifikat, nur von einer Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters ausgestellt
  - PKI-Zertifikat, ausgestellt von einer Zertifizierungsstelle, und ein 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 Firmware ab Version 1.10 erstellt das BMENUA0100-Modul ein selbstsigniertes Zertifikat für:

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

Für die Firmware-Version 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, müssen Sie den NTP-Dienst verwenden, um die Datums- und Uhrzeiteinstellungen des BMENUA0100-Moduls zu aktualisieren und zu überprüfen, ob auf den NTP-Server zugegriffen werden kann und ob er über aktualisierte Einstellungen für Uhrzeit und Datum verfügt.
- Wenn Sie beim Versuch, Ihren OPC UA-Client mit dem BMENUA0100-Server in Ipv6 zu verbinden, einen Fehler zu einem ungültigen Zertifikat aufgrund eines ungültigen Hostnamens erhalten, kann dies durch eine komprimierte IPv6-Adresse (d. h. eine verkürzte IPv6-Adresse) verursacht werden. In diesem Fall prüfen Sie die verwendete IPv6-Adresse und ersetzen Sie sie ggf. durch ein unkomprimiertes Format.
- Das BMENUA0100-Modul verwaltet nicht automatisch das Ablaufdatum von Zertifikaten. Stattdessen müssen Sie das Ablaufdatum des Zertifikats manuell verwalten.

Verwaltung der Zertifikate

Wählen Sie auf den BMENUA0100-Modulwebseiten auf der Seite **Home** die Option **Zertifikatsverwaltung** aus, um Links zu den folgenden Seiten zur Zertifikatsverwaltung für die Anwendungsinstanz anzuzeigen:

- PKI-Konfiguration, Seite 110
- Verwaltung der Clientvertrauensliste, Seite 112
- Export von Gerätezertifikaten, Seite 113
- Manuelle Registrierung, Seite 111
- Zertifizierungsstellenzertifikate, Seite 113

Unter den Themen *Verwenden von GPOs/LGPOs*, Seite 169 und *Anwenden der MMC-Gruppenrichtlinienverwaltung*, Seite 169 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 und Zertifizierungsstellenzertifikate spezifische Erweiterungen umfassen:

Selbstsignierte Zertifikate:

- KeyUsage (als kritisch markiert):
  - DigitalSignature
  - KeyEncipherment (Keine Verwendung für TLS-Suite basierend auf kurzlebigen Schlüsseln (ephemeral) wie TLS_ECDHE_xxxx; Verwendung für TLS_RSA_xxxx)
  - KeyCertSign: Wenn der Subject-Public-Key zum Überprüfen von Signaturen auf öffentlichen Schlüsselzertifikaten verwendet wird (Wert TRUE)
  - nonRepudiation (nach OPC UA-Norm erforderlich)
  - dataEncipherment (erforderlich nach OPC UA-Standard)
- Subject Alt Name: Im Feld SAN 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

Zertifizierungsstellenzertifikate:

- KeyUsage (als kritisch markiert):
  - DigitalSignature
  - KeyEncipherment (Keine Verwendung für TLS-Suite basierend auf kurzlebigen Schlüsseln (ephemeral) wie TLS_ECDHE_xxxx; Verwendung für TLS_RSA_xxxx)
  - KeyCertSign: wenn der Betreff-Public-Key zum Überprüfen von Signaturen auf öffentlichen Schlüsselzertifikaten verwendet wird (Wert FALSE)
  - nonRepudiation (nach OPC UA-Norm erforderlich)
  - dataEncipherment (erforderlich nach OPC UA-Standard)
- Subject Alt Name: Im Feld SAN 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

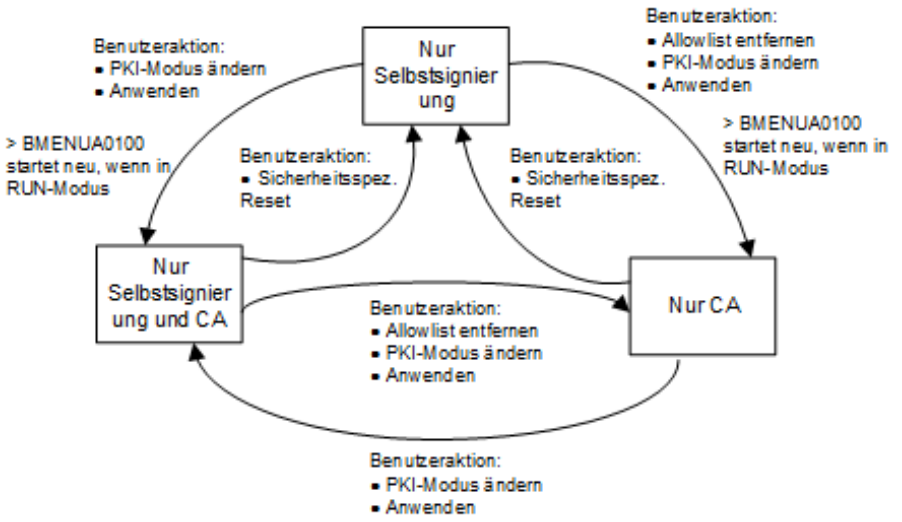
- Extended Key Usage extension:
  - id-kp-serverAuth, wenn TLS-Webserver-Authentifizierung
  - id-kp-clientAuth, wenn TLS-Webclient-Authentifizierung
- CRL Distribution points
- Authority Key Identifier
  - Kennung des öffentlichen Schlüssels, der dem privaten Schlüssel entspricht, der zum Signieren 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	Es müssen nur Zertifikate in der **Liste der vertrauenswürdigen Clientzertifikate** („Allowlist“) 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 der Firmware-Version 1.10 und höher 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:



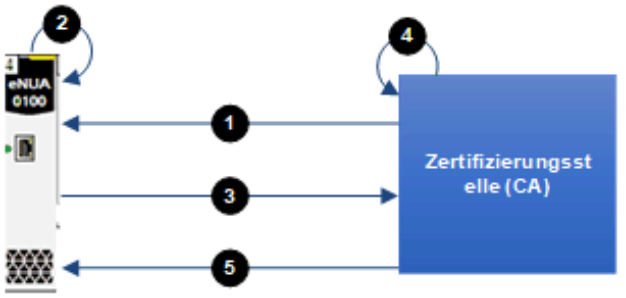
Manuelle Registrierung

Nach der Konfiguration des BMENUA0100-Moduls in Control Expert können Sie die Seite **Manuelle Anmeldung** verwenden, um eine CSR-Datei abzurufen, die an eine Zertifizierungsstelle übermittelt werden soll. Nachdem Sie die CSR-Datei übermittelt haben, können Sie das entsprechende Zertifizierungsstellenzertifikat extrahieren. Anschließend können Sie dieses Zertifizierungsstellenzertifikat in das BMENUA0100-Modul per Push übertragen. Bei den kombinierten Get- und Push-Vorgängen wird manuell ein von einer Zertifizierungsstelle eines Drittanbieters ausgestelltes Zertifikat registriert. Nach dem „Push“ des Zertifikats wendet der OPC UA-Server dieses Zertifikat zum Signieren und Verschlüsseln der Kommunikation mit dem OPC UA-Client an.

HINWEIS: Voraussetzung für die manuelle Anmeldung:

- Vergewissern Sie sich, dass der NTP-Client aktiviert, Seite 129 ist.
- Vergewissern Sie sich, dass die Zeiteinstellung für das BMENUA0100-Modul die tatsächliche Zeit ist.

Im Folgenden finden Sie eine Übersicht über den Prozess der manuellen Zertifikatregistrierung:



1 Das BMENUA0100-Modul importiert ein Zertifizierungsstellenzertifikat 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.

Weitere Informationen finden Sie im Schneider Electric-Video „How to work with PKI mode „Self-Signed & CA“ on BMENUA0100 module?“ („Arbeiten mit dem PKI-Modus „Selbstsigniert und CA“ für das Modul BMENUA0100“) 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 **Zertifikatsverwaltung**, um für ein Zertifikat Folgendes durchzuführen: **Hinzufügen**, **Herunterladen**, **Löschen**.

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 zu dem Zertifikat, das Sie der Liste hinzufügen möchten, und wählen Sie es aus.

Schritt	Aktion
3	Klicken Sie auf **Übermitteln**, 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 **ZERTIFIKATSVERWALTUNG > PKI-KONFIGURATION** exportieren, indem Sie auf die Schaltfläche **Herunterladen** klicken.

Zertifizierungsstellenzertifikate

Das Zertifizierungsstellenzertifikat ist ein öffentliches Schlüsselzertifikat, das die Zertifizierungsstelle in einer Public-Key-Infrastruktur (PKI) identifiziert. Verwenden Sie die Seite **Zertifizierungsstellenzertifikate**, um die Zertifizierungsstellenzertifikate im Gerät zu pushen.

So fügen Sie der Zertifizierungsstellenzertifikatliste ein Zertifikat aus der Zertifizierungsstelle hinzu:

Schritt	Aktion
1	Öffnen Sie die Webseiten für das Modul und geben Sie im Dialogfeld **Anmeldung** Folgendes ein: • Benutzername • Passwort Klicken Sie auf **Anmelden**.
2	Navigieren Sie zu **KONFIGURIEREN DER CYBERSICHERHEIT-EINSTELLUNGEN > ZERTIFIKATSVERWALTUNG**, um auf die Registerkarte der Zertifikatsverwaltung zuzugreifen, und wählen Sie dann die Option **Zertifizierungsstellenzertifikate** aus.

Schritt	Aktion
3	Klicken Sie in der Liste **VERTRAUENSWÜRDIGE ZERTIFIKATE** auf **HINZUFÜGEN**, um das Zertifizierungsstellenzertifikat in der Liste hinzuzufügen.
4	Wenden Sie die Änderungen auf die Konfiguration der Cybersicherheit an.

HINWEIS: Es können maximal zehn (10) Zertifizierungsstellenzertifikate hinzugefügt werden.

Zugriffssteuerung

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 der Modulwebseite über HTTPS

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

Die BMENUA0100-Webseiten bieten Tools für die Verwaltung von Benutzern. Klicken Sie auf der Seite **Home** auf die Option **Zugriffssteuerung**, um eine Liste der vorhandenen OPC UA-Benutzer, einschließlich ihrer Rollen und Berechtigungen, anzuzeigen. Auf dieser Seite können Sie Folgendes durchführen:

- Benutzer hinzufügen, Seite 115
- Profil vorhandener Benutzer aktualisieren, Seite 116
- Benutzer löschen, Seite 116

Benutzerverwaltung

Das BMENUA0100-Modul ermöglicht die rollenbasierte Zugriffssteuerung (RBAC: Role-Based Access Control). Allen Benutzern wird eine Rolle zugewiesen und sie können nur diejenigen Aufgaben durchführen, die dieser Rolle zugeordnet sind.

Die folgenden Rollen und Berechtigungen werden unterstützt:

Aufgabe	Berechtigungen			
	Cybersicherheitskonfiguration	**Firmwareaktualisierung**	**Zugriff auf Diagnose-Webseiten**	**OPC UA-Protokollzugriff**
SECADM	Aktualisieren, Lesen, Löschen	–	Lesen	–
OPERATOR	–	–	Lesen	Verbinden
ENGINEER	–	–	Lesen	Verbinden
INSTALLER	–	Aktualisieren	Lesen	–

Jedes BMENUA0100-Modul unterstützt maximal 15 gleichzeitige Benutzer.

Es können keine benutzerdefinierten Rollen oder Berechtigungsgruppen konfiguriert werden. Es kann keine auf IP-Adressen basierende Allowlist für die Zugriffssteuerung konfiguriert werden.

Hinzufügen von Benutzern

Ein Sicherheitsadministrator kann auf **Neuer Benutzer** klicken und dann die folgenden Parameter angeben, um einen neuen Benutzer hinzuzufügen:

Parameter	Beschreibung
Benutzername	Benutzer-ID. Der Benutzer gibt diese ID zusammen mit dem Passwort ein, um Zugang zu den zulässigen Funktionen zu erhalten.
Passwort Passwort bestätigen	Benutzerpasswort. Da das Passwort nicht als Klartext angezeigt wird, geben Sie diesen Wert zur Bestätigung der Richtigkeit zweimal ein. **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 Ziffer (0 bis 9) • ein Sonderzeichen ~ ! @ $ % ^ & * _ + - = `| \ ( ) [ ] : " ' < >
Rollen	Wählen Sie die Benutzerrolle aus, die die Berechtigungen definiert, die dem Benutzer gewährt werden: • SEDADM (Sicherheitsadministrator) • Operator (Bediener) • Engineer (Techniker) • Installer (Monteur)

Klicken Sie auf **Änderungen übernehmen**, nachdem diese Parameter konfiguriert wurden, um den neuen Benutzer zu erstellen.

Aktualisieren von Benutzern

Um die Einstellungen eines vorhandenen Benutzers zu bearbeiten, kann ein Sicherheitsadministrator für das Profil, das bearbeitet werden soll, auf das Bearbeitungssymbol (Stift) klicken. Klicken Sie auf **Änderungen übernehmen**, um Ihre Änderungen zu speichern. Das gleiche Dialogfeld, in dem ein neuer Benutzer hinzugefügt wird, wird geöffnet. Hier können Sie die Konfiguration des ausgewählten Benutzers ganz oder teilweise aktualisieren.

Löschen von Benutzern

Um einen vorhandenen Benutzer zu löschen, kann ein Sicherheitsadministrator in der Liste mit der rechten Maustaste auf diesen Benutzer klicken 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 **Home** die Option **Konfigurationsverwaltung** aus, um Links zu den folgenden Verwaltungsseiten für die Konfiguration der Cybersicherheit anzuzeigen:

- EXPORTIEREN, Seite 116
- IMPORTIEREN, Seite 117
- RESET, Seite 118

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 115.
2	Geben Sie das zugewiesene Passwort im Feld **Passwort bestätigen** erneut 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 bestehenden 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	Wählen Sie die zu importierende Konfigurationsdatei aus und klicken Sie auf **OK**.
3	Geben Sie auf der Seite **IMPORTIEREN** 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**. Ein Dialogfeld wird geöffnet, in dem Sie darüber informiert werden, 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 86 zu öffnen.

Schritt	Beschreibung
6	Geben Sie Ihren Benutzernamen und Ihr Passwort für den Sicherheitsadministrator ein und klicken Sie auf **Anmeldung**. 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 (siehe Schritt 3 oben), wird die Konfiguration automatisch angewendet, und dieser Schritt (7) wird automatisch durchgeführt.

Zurücksetzen einer Konfiguration

Klicken Sie auf der Seite **RESET** auf **Zurücksetzen**, um die bei Auslieferung eingestellten werkseitigen Standardeinstellungen für die Cybersicherheit im lokalen BMENUA0100-Modul wiederherzustellen. Diese Aktion hat dieselbe Auswirkungen wie das Einstellen des Drehschalters auf die Position Security Reset, Seite 28 (Sicherheits-Reset).

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 BMENUA0100-Konfigurationsfensters konfiguriert werden. Darüber hinaus können die IP-Adresseinstellungen dem Steuerungsport dynamisch über die SLAAC-Methode (Stateless Address Auto-configuration, Autokonfiguration von zustandslosen Adressen) zugewiesen werden.

Wenn das BMENUA0100-Modul in einem Standalone-PAC verwendet wird, werden die IP-Adresseinstellungen nur für ein einzelnes Modul konfiguriert. Wenn zwei Instanzen des BMENUA0100-Moduls in einer Hot Standby-PAC-Architektur (ein BMENUA0100-Modul in jedem PAC) verwendet werden, enthält die Control Expert-Konfigurationsregisterkarte **IP-Konfig.** Einstellungen für zwei Module (A und B). In einer Hot Standby-PAC-Architektur 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 Sammlung von internetfähigen Protokollen besteht) konfiguriert werden:

- IPv4-Stack: Unterstützt nur die 32-Bit-Adressierung. Eine IPv4-IP-Adresse beispielsweise ist: 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 ist ein Beispiel für eine IPv6-128-Bit-IP-Adresse aufgeführt: 2001:0578:0123:4567:89AB:CDEF:0123:4567.

  HINWEIS: Beim ersten Einschalten (oder nachdem der Drehschalter des Moduls auf **Security Reset** eingestellt, das Modul eingeschaltet, der Drehschalter auf die Einstellung **Secured** zurückgesetzt und das Modul dann erneut eingeschaltet wurde) wird dem Steuerungsport die IPv4-Standardadresse 10.10.MAC5.MAC6 zugewiesen. Dabei ist MAC5 der Dezimalwert des 5. Oktetts der MAC-Adresse des Moduls, und MAC6 ist der Dezimalwert des 6. Oktetts. 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 einen M580-PAC weitergeleitet wird. Control Expert V15 kann über die IPv6-Adresse des BMENUA0100 mit einem M580-PAC 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 für die Konfiguration des BMENUA0100-Moduls.
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 diese IP-Parameter für jedes BMENUA0100-Kommunikationsmodul in Ihrem Projekt:

Parameter		Beschreibung
Steuerungsport		Aktiviert/deaktiviert den Steuerungsport des BMENUA0100-Moduls. Bei Einstellung: • 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		
	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: Zeigt 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 ist (siehe oben), geben Sie eine gültige IPv6-Adresse für den Steuerungsport ein. **HINWEIS:** Das BMENUA0100-Modul kann keine doppelten IPv6-Adressen erkennen. Erfragen Sie bei Ihrem Netzwerkadministrator, ob es keine doppelten IPv6-Adressen im gleichen Netzwerksegment gibt.

Parameter		Beschreibung
	Länge des Subnetz-Präfixes	Wird automatisch für eine statische IPv6-Adresse festgelegt, die der Anzahl der SLAAC-spezifischen IPv6-Adressen entspricht, die das Subnetz-Präfix 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** für die Eingabe einer statischen IPv4 IP-Adresse für den Steuerungsport.
	IPv4 @	Gewählter Modus: • **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 (s.o.), geben Sie eine gültige IPv4-Subnetzmaske für den Steuerungsport ein, die den Netzwerkanteil der IPv4-Adresse bestimmt.
	Standard-Gateway	Wenn **Statisch** als **Modus** ausgewählt ist (s.o.) geben Sie eine gültige IPv4-Adresse für das Standard-Gateway ein.
Baugruppenträger-Port		
	IPv4 @	Geben Sie eine gültige IPv4-Adresse für den Baugruppenträger-Port ein.
Zeitstempelung von Quellen		Weitere Informationen finden Sie unter Konfigurieren der Quellzeitstempelung, Seite 122.

Parameter	Beschreibung
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 Standardabtastperiode 250 ms deaktiviert, was die Überwachung von äquivalenten 20.000 Elementen des Typs INT ermöglicht. **HINWEIS:** Eine Änderung dieser Einstellung ist erst nach dem vollständigen Herunterladen der Anwendung wirksam.
OPCUA-TCP-Überwachungsport	Der TCP-Port für die OPCUA-Kommunikation: • Standardmäßig: Voreinstellung für Port 4840 • Durch anderen 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:

- Das Fenster **Ethernet-Netzwerk** (das über **Extras > Ethernet-Netzwerkmanager...** geöffnet wird) zeigt Einstellungen für den Baugruppenträger-Port und den Control-Port für das BMENUA0100-Modul an, einschließlich Informationen für den NTP-Server, den SNMP-Manager und - für ein Hot Standby-System - für das Standby-Modul BMENUA0100 (B).
- Auf der Seite **Adressserver** der CPU (das im **DTM-Browser** durch Doppelklicken auf die CPU und anschließende Auswahl von **Dienste > Adressserver** geöffnet wird) wird die IP-Adresse des Baugruppenträger-Ports des BMENUA0100-Moduls angezeigt. In einer Hot Standby-Konfiguration zeigt die Seite **Adressserver** der CPU die IP-Adresse des Baugruppenträger-Ports für beide BMENUA0100-Module an.

Konfiguration der Quellzeitstempelung

Die Quellzeitstempelung wird von der Firmware-Version 2.01 (und 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.

Aktivieren der Quellzeitstempelung

Die Quellzeitstempelung wird im Fenster der Projekteinstellungen aktiviert. Navigieren Sie zu **Allgemein > > Zeitstempelmodus** und wählen Sie dann die Option **System** aus.

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

Auslösen der Quellzeitstempelung

Verwenden Sie die Registerkarte **IPConfig** des Konfigurationsfensters des BMENUA0100, um die Zeitstempelung zu aktivieren und zu konfigurieren.

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

Einstellung	Beschreibung
Aktiviert	Aktiviert die Quellzeitstempelung für die Anwendung.
Abfrage des Puffers (ms)	Die Abfragerate für vom BME NUA 0100 verarbeitete Ereignis-Leseanforderungen. Gültige Einstellungen reichen von: • mindestens 250 ms, bis • max. 5000 ms in Schritten zu je 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 126.

Verwaltung der quellzeitgestempelten Variablen

Verwenden der OPC UA-Datenelemente `#TSEventItemsReady` und `#TSEventSynchro`

Sie können dieOPC UA-spezifischen Datenelemente `#TSEventItemsReady` und `#TSEventSynchro` verwenden, um den Status der quellzeitgestempelten Variablen abzurufen und festzulegen.

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 booleschen OPC UA-Knoten.

Durch das Einstellen des `#TSEventSynchro`-Elements wird ein Synchronisierungsbefehl an alle zeitgestempelten Geräte des M580-ePAC gesendet. Die Werte, die von den Geräten an den OPC UA-Client zurückgegeben werden, initialisieren die zeitgestempelten Variablen mit ihren aktuellen Werten.

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

- `UA_EGOOD`: Die Synchronisierungsanforderung wurde ordnungsgemäß an alle Zeitstempelgeräte gesendet.
- `UA_EBAD`: Die Synchronisierungsanforderung war nicht erfolgreich, da die Zeitstempelung im Control Expert-Projekt deaktiviert ist.
- `UA_EBADINVALIDSTATE`: Die Synchronisierungsanforderung war nicht erfolgreich, da die Zeitstempelung für das BMENUA0100-Modul durch die Funktion %MW400 , Seite 126 ausgeschaltet wurde.
- `UA_EBADINUSE`: Die Synchronisierungsanforderung war nicht erfolgreich, da das BMENUA0100-Modul den Zeitstempelpuffer nicht reservieren konnte.
- `UA_EBADDISCONNECT`: Zeitüberschreitung bei der Synchronisierungsanforderung. Die Werte konnten nicht im angegebenen Zeitrahmen geschrieben werden.

Um diese Initialisierung durchzuführen, verwenden Sie einen OPC UA-Client - z. B. UaExpert -, um die folgende Reihenfolge von Tasks auszuführen:

1. Überwachen des Elements `#TSEventItemsReady`, das angibt, dass das BMENUA0100-Modul bereit ist, die zeitgestempelten Variablen des ePAC-Puffers (einschließlich von M580-CPU, BMECRA, BMEERT) zu verwalten, und dann warten, bis der Wert auf 1 (true) geändert wird.
2. Hinzufügen von überwachten Datenelementen, die als quellzeitgestempelte Variablen konfiguriert sind, zu einem oder mehreren Abonnements.
3. Festlegen des `#TSEventSynchro`-Schreibbefehl, um den Wert und den Quellzeitstempel jedes Elements zu aktualisieren.

HINWEIS:

- Das BMENUA0100-Modul liest alle konfigurierten zeitgestempelten Variablen im ePAC. 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.
- Es wird empfohlen, den Datenänderungsfilter auf **Status/Wert/Zeitstempel** einzustellen. Andernfalls ist es möglich, dass verschiedene OPC UA-Clients - z. B. Clients, die Werte nur bei Status-/Wertänderungen aktualisieren - einen anderen 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.
- Da `#TSEventSynchro` an mehrere Zeitstempelgeräte gesendet wird, gibt die Einstellung `#TSEventSynchro` die Antwort `UA_EBADDISCONNECT` zurück, die angibt, dass der Befehl abgelaufen ist und nicht erfolgreich war. Dies gilt auch dann, wenn viele Geräte erfolgreich reagieren.
- Wenn das Abonnement so bearbeitet wird, dass es beispielsweise nur eine Variable für ein Gerät enthält, führt die Ausführung von `#TSEventSynchro` zum Verlust zuvor zurückgegebener Werte für zuvor abonnierte Geräte und Variablen.

Ermitteln der für die Zeitstempelung reservierten M580-CPU-Kanäle

Für die Kommunikation zwischen dem BMENUA0100-Modul und einer M580-CPU, bei der die Zeitstempelung in Control Expert aktiviert ist, sind 25 % der CPU-Kanäle für die Unterstützung der Zeitstempelfunktion reserviert. Maximal 75 % der CPU-Kanäle bleiben für die Übertragung anderer Kommunikationsrequests verfügbar.

Für die BMEP584040-CPU beispielsweise:

- 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 an unterstützten quellzeitgestempelten Variablen.

Die Formel zur Ermittlung der maximalen Anzahl an quellzeitgestempelten Variablen für ein Gerät lautet wie folgt:

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

Beispiel:

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

  ((16 / 4) x 82 = 328 Gesamtvariablen

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

  1 x 82 = 82 Gesamtvariablen

  Wenn **Abfrage des Puffers** = 500 ms: 164 Variablen pro Sekunde.
- BMEERT: 1 Verbindung, 1 Kanal, max. 20 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. Zeitgestempelte Variablen in den M580-CPUs, BMECRA- und BMEERT-Modulen können jedoch jeweils nur von 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 **IPConfig** 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 Baustein `WRITE_VAR`, um das Wort %MW400 auf 2 zu setzen, das das Lesen und Verwalten von Variablen mit Zeitstempel für dieses Modul aktiviert.

   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. Verwenden Sie für das andere BMENUA0100-Modul, für das Sie den Zeitstempelpuffer nicht reservieren möchten, den Baustein `WRITE_VAR`, um das Wort %MW400 auf 1 zu setzen, das das Lesen und Verwalten von Variablen mit Zeitstempel für dieses Modul deaktiviert.

HINWEIS: Sie müssen diese Schritte nach jeder Änderung der Betriebsart 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.

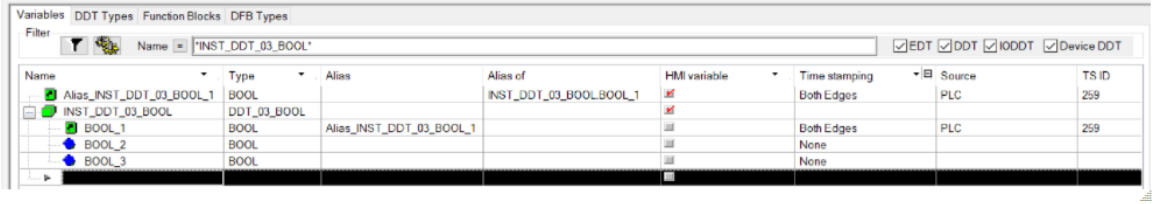
HINWEIS:

Wenn die Einstellung **Aktiviert** deaktiviert ist, sind die vom BMENUA0100-Modul gelesenen Variablenwerte die Werte im ePAC-Speicher.

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.

Überwachung zeitgestempelter Aliasvariablen

Das BME NUA 0100-Modul erkennt die in Control Expert erstellten BOOL- oder EBOOL-Aliasvariablen mit Zeitstempel, erkennt jedoch keine entsprechenden „Alias von“-Variablen. Nachstehend finden Sie ein Beispiel für Alias- und „Alias von“-Variablen:



Um vom BME NUA 0100-Modul erkannt zu werden, müssen die Aliasvariablen in das Datenwörterbuch integriert werden.

BOOL- oder EBOOL-Aliasvariablen und ihre entsprechenden „Alias von“-Variablen teilen dieselbe logische Adresse im M580-Speicher und dieselbe Ereignis-ID im M580-Zeitstempelpuffer. Die Quellzeitstempelung wird nur für die Aliasvariablen, nicht für die „Alias von“-Variablen verwaltet. Mit anderen Worten: Sie müssen die Aliasvariable (OPC UA-Knoten) im OPC UA-Client abonnieren, um die Quellzeitstempelung vom Gerät anstatt vom BME NUA 0100-Modul zu empfangen.

Da weder die BOOL- noch die EBOOL-„Alias von“-Variable von der BME NUA 0100-Firmware als quellzeitgestempelt angesehen wird, muss das Alias in das Datenwörterbuch integriert werden. In diesem Fall müssen Sie die Aliasvariable als überwachtes Element in einem OPC UA-Abonnement hinzufügen, um die vom Gerät eingestellte Quellzeitstempelung zu realisieren.

Konfiguration des Netzwerkzeitdienstes

Einführung

Das Ethernet-Kommunikationsmodul BMENUA0100 mit integriertem OPC UA-Server unterstützt die Version 4 des Netzwerkzeitprotokolls (NTP: Network Time Protocol). 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 CPU 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 136 leuchtet weiterhin, bis die Uhrzeit des BMENUA0100-Moduls 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-Adresse sowohl für den **primären NTP-Server** als auch für den **sekundären NTP-Server** auf 0.0.0.0 gesetzt ist, kann das BMENUA0100-Modul nicht als NTP-Client oder NTP-Server betrieben werden.

NTP-Server:

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

- Im sicheren Modus wird der NTP-Server aktiviert, wenn Folgendes zutrifft:
  - Die IP-Adresse des primären oder des sekundären NTP-Servers wird auf einen Wert festgelegt, der nicht null ist (d. h. auf einen anderen Wert als 0.0.0.0), und
  - der NTP-Server wird in den Konfigurationseinstellungen der Webseite, Seite 94 **Netzwerkdienste** aktiviert.
- Im Standardmodus wird der NTP-Server aktiviert, wenn die IP-Adresse des **primären NTP-Servers** oder des **sekundären NTP-Servers** auf einen Wert festgelegt wird, der nicht null ist (d. h. ein anderer Wert als 0.0.0.0).

  HINWEIS: Wenn das BMENUA0100-Modul als NTP-Client eines Servers im Baugruppenträger-Netzwerk (**Primärer NTP-Server** oder **Sekundärer NTP-Server**) konfiguriert ist, wird der NTP-Server des BMENUA0100-Moduls in keinem Fall aktiviert, auch wenn sich kein NTP-Server im Baugruppenträger-Netzwerk befindet.

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 die NTP-Abfrageperiode 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.
- Das BMENUA0100-Kommunikationsmodul ruft die Uhrzeit vom NTP-Server ab.
- 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.

Das BMENUA0100-Kommunikationsmodul führt keine Uhrzeiteinstellung durch. Beim Einschalten oder Aus- und Wiedereinschalten steht der Zeitwert des Moduls auf 0, dies entspricht dem 1. Januar 1980 00:00:00:00.

Konfigurieren des Dienstes

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

Schr-itt	Aktion
1	Erweitern Sie im **Projekt-Browser** den Knoten **SPS-Bus** und öffnen Sie das Dialogfeld für die Konfiguration des BMENUA0100-Moduls.
2	Klicken Sie auf die Registerkarte **NTP**.
3	Nehmen Sie die erforderlichen Änderungen an den verschiedenen Feldern auf der Konfigurationsseite **Netzwerkzeitdienst** vor. (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.

Parameter		Beschreibung
		HINWEIS: Verwenden Sie standardmäßig die Haupt-IP-Adresse der CPU.
	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-Dienstadressen für **NUA(A)** und **NUA(B)** im selben Netzwerk befinden, z. B. das Netzwerk, auf das über den Baugruppenträger-Port zugegriffen werden kann, oder das Netzwerk, auf das über den Steuerungsport zugegriffen werden kann.

HINWEIS: Bei einem Betrieb im sicheren Modus ist sicherzustellen, dass der NTP-Dienst im Bereich Aktivierung der Netzwerkdienste, Seite 94 auf der Webseite **Einstellungen** aktiviert ist.

SNMP-Agent-Konfiguration

Über SNMP

Alle Firmware-Versionen des BMENUA0100-Moduls unterstützen den SNMP-Agent der Version 1 (V1). Die Firmware-Version 2 (und höher) des Moduls (BMENUA0100.2) unterstützt auch Version 3 (V3) des SNMP-Agenten.

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. Derartige Benachrichtigungen informieren das Verwaltungsgerät über Ereignisse, wie z. B. Kaltstarts und die Unfähigkeit der Software, 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. Cybersicherheitsbezogene SNMP-Parameter werden auf den Webseiten des Moduls konfiguriert.

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

- Sicherer Modus: Sie können den SNMP-Agent sowohl in Control Expert als auch auf den Webseiten des BMENUA0100-Moduls konfigurieren.

  HINWEIS: Im sicheren Modus muss die SNMP-Version sowohl in Control Expert als auch auf der SNMP-Webseite, Seite 102 identisch konfiguriert werden. Wenn diese Einstellungen nicht übereinstimmen, startet der SNMP-Dienst nicht.

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

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

  - Das Modul BMENUA0100.2, das mit einer Firmware-Version 2 oder höher ausgestattet ist, betreibt SNMP V3 mit der Sicherheitsstufe ohne Authentifizierung und ohne Datenschutz.
  - Das BMENUA0100-Modul mit einer älteren Firmware als Version 2 betreibt SNMP V1.

SNMP-Parameter

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

HINWEIS: Im sicheren Modus muss die SNMP-Version sowohl in Control Expert als auch auf der SNMP-Webseite, Seite 102 identisch konfiguriert werden. Wenn diese Einstellungen nicht übereinstimmen, startet der SNMP-Dienst nicht.

Feld	Parameter	Beschreibung	Wert
SNMP-Version	SNMP V1	Wählen Sie dies aus, um SNMP V1 zu verwenden.	Aktiviert/Deaktiviert
	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 Traps-Nachrichten sendet.	
Agent	Standort (SysLocation)	Position des betroffenen Geräts	31 Zeichen (maximal)
	Kontakt (SysContact)	Informationen zur Kontaktperson für die Gerätewartung	
	SNMP-Manager aktivieren	Deaktiviert (Standard): Sie können die Parameter für den **Standort** und den **Kontakt** ändern. Aktiviert: Sie können die Parameter für den **Standort** und den **Kontakt** nicht ändern.	Aktiviert/Deaktiviert
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	15 Zeichen (maximal)
	Get		
	Trap		

Feld	Parameter	Beschreibung	Wert
		SNMP-Manager verwendet wird, geben Sie denselben Community-Namen ein, der vom SNMP-Manager verwendet wird.	
Sicherheit (nur SNMP V1)	„Authentifizierungsfehler“-Trap aktivieren	*Deaktiviert* (Standardeinstellung): Nicht aktiviert. *Aktiviert*: 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.	Aktiviert/Deaktiviert
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, sofern aktiviert.

SNMP MIB-2-Objektkennung

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

Objektname	OID	Wert
SysServices	1.3.6.1.2.1.1.7	74, stellt die Summe von (2**7-1 + 2**4-1 + 2**2-1) dar und weist auf die Unterstützung von Protokollen in den folgenden OSI-Schichten hin: • 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 Einstellungen der M580-CPU für den OPC UA-Client - Serververbindungen

Einführung

In diesem Kapitel werden Einstellungen beschrieben, die in der M580-CPU-Konfiguration vorgenommen werden, um eine Verbindung zwischen dem OPC UA-Server im BMENUA0100-Modul und einem OPC UA-Client zu unterstützen.

Konfiguration der Sicherheitseinstellungen der M580-CPU

Konfigurieren der CPU-Dienste

Um die Kommunikation zwischen dem OPC UA-Server im BMENUA0100-Modul und einem OPC UA-Client zu unterstützen, aktivieren Sie die folgenden Einstellungen auf der Registerkarte „Sicherheit“der M580-CPU:

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

Wenn beide Dienste in der CPU 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 21 des BMENUA0100-Moduls für die verschiedenen Betriebszustände des Moduls aufgeführt.

HINWEIS: Der Status der SECURE-LED für den konfigurierten und nicht konfigurierten Modulstatus wird im Anschluss an die Erstpräsentation separat beschrieben.

Betriebszustand		**LED RUN (grün)**	**LED UACNX (grün/rot)**	**LED ERR (rot)**	**LED BS-Baugrup-penträger (grün/rot)**	**LED NS-Steuerung-sport (grün/rot)**	**LED BUSY (Gelb)**	**LED SECURE (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	Blinken	Blinken	Grün Blinken Rot AUS	Grün Blinken Rot AUS	Blinken	Grün Blinken Rot AUS
Nicht konfiguriert		AUS	AUS	Blinken	Blinkt rot, wenn keine Verbindung zu einem Ethernet-Baugrup-penträger-	AUS, wenn kein Kabel angeschlos-sen und an ein anderes Gerät	AUS	Siehe LEDs für die Cybersi-cherheit unten, Seite 139.

Betriebszustand		**LED RUN (grün)**	**LED UACNX (grün/rot)**	**LED ERR (rot)**	**LED BS-Baugruppenträger (grün/rot)**	**LED NS-Steuerungsport (grün/rot)**	**LED BUSY (Gelb)**	**LED SECURE (grün/rot)**
					Port besteht. Blinkt andernfalls grün.	angeschlossen ist. Blinkt andernfalls grün.		
Konfiguriert	Nach der Erkennung einer doppelten IPv4-Adresse am Baugruppenträger-Port	Blinken	Siehe Beschreibung der UACNX-LED unten, Seite 138	/	Grün AUS Rot EIN	/	/	Siehe die Beschreibung der LED „Sicherer Kommunikationsstatus“ unten, Seite 139.
	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 angeschlossen; Aus, wenn kein Kabel angeschlossen	EIN, wenn eine Erfassung des Datenwörterbuchs läuft; Blinken bei Überlauf des Datenwörterbuchs; sonst 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		AUS	AUS	EIN	Grün AUS	Grün AUS	AUS	Grün AUS

Betriebszustand		LED RUN (grün)	LED UACNX (grün/rot)	LED ERR (rot)	LED BS-Baugruppenträger (grün/rot)	LED NS-Steuerungsport (grün/rot)	LED BUSY (Gelb)	LED SECURE (grün/rot)
(Das Modul wird neu gestartet)					Rot EIN	Rot EIN		Rot EIN
Sicherheits-Reset	Verarbeitung läuft	Blinken	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rot EIN	EIN	Grün AUS Rot AUS
	Vollständig	EIN	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Grün AUS Rot AUS
Sicherheits-Reset steht aus[3]		AUS	AUS	EIN	Grün AUS Rot EIN	Grün AUS Rot EIN	AUS	Rot Blinken
Betriebssystemaktualisierung		Blinken	AUS	AUS	Grün AUS Rot EIN	Grün AUS Rotes Leuchten	EIN	Grün AUS Rot AUS

1. Der Autotest wird schnell durchgeführt und die LED blinkt nicht visuell.

   HINWEIS: Wenn das Modul im Autotest-Status verbleibt, überprüfen Sie den Drehschalter, um sicherzustellen, dass er nicht beschädigt ist.

2. Siehe erkannte Fehlercodes von SERVICES_STATUS im T_BMENUA0100-DDT, Seite 140.

3. Dieser Status ergibt sich aus der Änderung des Drehschalters vom Standardmodus in den sicheren Modus bzw. umgekehrt, ohne dass als Zwischenschritt ein Sicherheits-Reset durchgeführt wird, Seite 26.

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

LED UACNX, wenn Modul im konfigurierten Zustand

Die Farbe (rot oder grün) und der Status (blinkend oder permanent) 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	Rot Blinken	Rot Leuchten
Datenwörterbuch verfügbar	Grün Blinken	Grün Leuchten

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 Drehschalter befindet sich nicht in der Position „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 22 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.
	Grün Blinken	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).

BMENUA0100 - Abgeleiteter Datentyp (DDT)

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 145 (EF) in der Control Expert-Software.

HINWEIS: Wenn der Modul-DDT aus einem beliebigen Grund nicht gelesen werden kann - beispielsweise wenn die IP-Adresse des Baugruppenträgers nicht ordnungsgemäß konfiguriert ist - können Sie eine Moduldiagnose über die LEDs, Seite 136 durchführen.

Struktur des T_BMENUA0100-DDT

Der BMENUA0100-DDT umfasst folgende Elemente:

Element	Typ	Nummer	Beschreibung
DEVICE_NAME	STRING [16]	MW1...8	Der 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	Länge des Baugruppenträger-Ports Ipv4 / Länge des Subnetz-Präfixes.
ETH_STATUS	WORD	MW57	–

Element	Typ	Nummer	Beschreibung
PORT_CONTROL_LINK	BOOL	MW57.0	• 0: Verbindung zum Steuerungsport nicht aktiv. • 1: Verbindung zum Steuerungsport aktiv.
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0: Verbindung zum Baugruppenträger-Port nicht aktiv. • 1: Verbindung zum Baugruppenträger-Port aktiv.
GLOBAL_STATUS	BOOL	MW57.2	• 0: Das Modul ist nicht betriebsbereit. • 1: Das Modul ist betriebsbereit.
NETWORK_HEALTH	BOOL	MW57.3	• 0: Netzwerküberlastbedingung erkannt. • 1: Das Netzwerk funktioniert normal.
Reserviert	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	–
DATA_DICT	BYTE	MW58[0]	• 1: Nicht verfügbar. Mögliche Ursachen: ◦ Die Datenwörterbuchfunktion ist nicht verfügbar oder in der Control Expert-Anwendung aktiviert und kann nicht im PAC integriert werden. ◦ Das Laden/Durchsuchen des Datenwörterbuchs wird im OPC UA-Server ausgeführt. • 2: Verfügbar, z. B.: ◦ Das Laden/Durchsuchen des Datenwörterbuchs durch den OPC UA-Server wurde erfolgreich abgeschlossen. ◦ Ein Vorladevorgang (gemäß den Projekteinstellungen des Control Expert-Datenwörterbuchs) kann ausgeführt werden. • 4: Bereits aktiv. • 8: Überlauf des Datenwörterbuchs.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Zeitraum 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.
DATA_DICT_PRELOAD_DURATION	BYTE	MW59[1]	Dauer des letzten Vorladevorgangs des Datenwörterbuchs (0 bis 255 Sekunden). **HINWEIS:** Sie können die Informationen in diesem Element verwenden, um die Einstellung **Timeout bei der Generierung von Änderungen** im Konfigurationsfenster **Tools > Projekteinstellungen > Allgemein > In SPS eingebettete Daten** anzupassen und zu optimieren. Informationen zur Konfiguration

Element	Typ	Nummer	Beschreibung
			dieser Einstellung finden Sie in der Online-Hilfe von Control Expert.
SERVICE_LEVEL	BYTE	MW60[0]	• 0: Keine (Transparent) • 2: Nicht-transparenter („Warm“-) Redundanzmodus.
SERVICE_LEVEL	BYTE	MW60[1]	OPC UA-Serverfunktionsfähigkeit, Seite 151 abhängig von der Daten- und Dienstqualität.
Reserviert	WORD	MW61	–
SERVICES_STATUS	T_SERVICES_STATUS	MW62...68	–
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 1.000 Sekunden erhöht oder verringert. Die Neusynchronisierung des BMENUA0100-Moduls kann bis zu 5 Minuten in Anspruch nehmen.) ◦ 4 = NTP-Serveruhr wurde unterbrochen, der NTP-Server ist jedoch nach wie vor erreichbar. Prüfen Sie den Status und die Parameter des NTP-Servers.
NTP_SERVER_SERVICE	BYTE	MW62[1]	NTP-Serverstatus • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur gesicherter Modus): ◦ 1 = Steuerungsport nicht konfiguriert ◦ 2 = NTP-Client des Baugruppenträgers und Servers aktiviert auf den Webseiten
SNMP_SERVICE	BYTE	MW63[0]	SNMP-Serverstatus: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode: ◦ 1 = SNMP ist im sicheren Modus aktiviert und in Control Expert ist keine SNMP-IP-Adresse definiert (0.0.0.0).
Reserviert	BYTE	MW63[1]	–
WEB_SERVER	BYTE	MW64[0]	Webserverstatus: • Bit 0: 0 = Inaktiv / 1 = Aktiv

Element	Typ	Nummer	Beschreibung
			• 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 oder Firmwarepaket in Blocklist ◦ 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 sicherer Modus): ◦ 1 = Steuerungsport nicht konfiguriert **HINWEIS:** Bei Modulen mit einer Firmware-Version ab 2.01 wird der Elementwert auf 0 forciert.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Status der Weiterleitung von CPU zu CPU: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur sicherer Modus): ◦ 1 = Steuerungsport nicht konfiguriert **HINWEIS:** Bei Modulen mit einer Firmware-Version ab 2.01 wird der Elementwert auf 0 forciert.
IPSEC	BYTE	MW67[0]	IPSEC-Status: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur sicherer Modus): ◦ 1 = Steuerungsport nicht konfiguriert
Reserviert	BYTE	MW67[1]	–
EVENT_LOG_SERVICE	BYTE	MW68[0]	Status des Ereignisprotokollierungsdiensts: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur sicherer Modus): ◦ 1 = Fehler im Dienstereignisprotokoll ◦ 2 = Fehler in der Ereignisprotokollkonfiguration
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Status des Protokollservers:

Element	Typ	Nummer	Beschreibung
			• Bit 0: 0 = Quittierung vom Syslog-Server empfangen / 1 = Keine Quittierung vom Syslog-Server empfangen
FW_VERSION	T_FW_ VERSION	MW69...72	Firmware-Version des Moduls
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]	Status des Steuerungsports IPv4: • Bit 0: 0 = Inaktiv / 1 = Aktiv • Bits 4 bis 7: Fehlercode (nur 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).
MEM_USED_PERCENT	BYTE	MW78[0]	Vom OPC UA-Server verwendeter Prozentwert des internen RAM.
CPU_USED_PERCENT	BYTE	MW78[1]	Prozentwert der verwendeten internen CPU.
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Cybersicherheitsstatus.
SECURE_MODE	BYTE	MW79[0]	• 0: Das Modul läuft im Standardmodus. • 1: Das Modul läuft im sicheren Modus.
CYBERSECURITY_STATE	BYTE	MW79[1]	Cybersicherheitsstatus: • 0: Sicherer Modus AUS. (SECURE-LED AUS) • 1: Eine sichere Kommunikation ist aktiviert und läuft fehlerfrei. (SECURE-LED GRÜN) • 2: Kommunikationsbereit. (SECURE-LED BLINKT GRÜN)

Element	Typ	Nummer	Beschreibung
			• 3: Sichere Kommunikation läuft mit geringfügigen Fehlern. (SECURE-LED BLINKT ROT) • 4: Sichere Kommunikation wurde aufgrund eines kritischen Fehlers angehalten. (SECURE-LED ROT)
IPSEC_CHANNELS	BYTE	MW80[0]	Die Anzahl der geöffneten IPSEC-Kanäle:
Reserviert	BYTE	MW80[1]	–

Konfiguration der Elementarfunktion READ_DDT

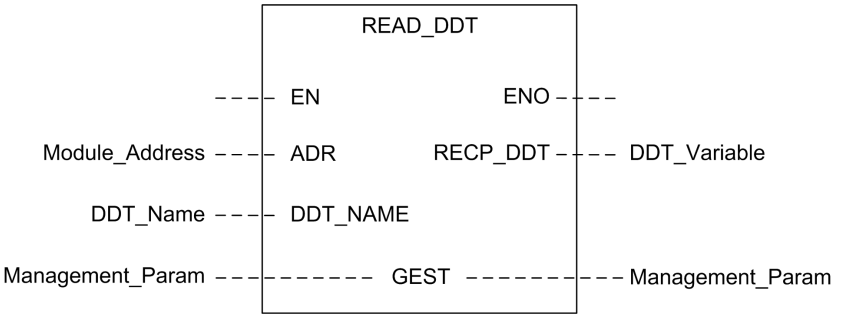
Übersicht

Verwenden Sie den Funktionsbaustein `READ_DDT`, um das Lesen von Nachrichten für das BMENUA0100-Kommunikationsmodul zu konfigurieren.

Die Definition des Vorgangs erfolgt über die Parameter `ADR`, `DDT_NAME` und `GEST`.

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

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 lösen. Wenn dieser Eingang auf Null gesetzt wird, ist der Funktionsbaustein deaktiviert und kann den Algorithmus des Funktionsbausteins nicht lösen.
ADR	Beliebiges Array of 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 der Geräte-ID 100 (Ortsserver des Moduls) an, 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>Parameter</th><th>Datentyp</th><th colspan="3">Beschreibung</th></tr>
<tr><td rowspan="5">GEST</td><td rowspan="5">Array [0...3] of INT</td><td colspan="3">Die Verwaltungsparameter bestehen aus vier Wörtern. Weitere Informationen zu diesen Parametern finden Sie im Control Expert-Hilfethema Struktur der Verwaltungsparameter (siehe ™EcoStruxure Control Expert, Kommunikationsbausteinbibliothek).</td></tr>
<tr><td>Wort-nr.</td><td>Höherwertiges BYTE</td><td>Niederwertiges BYTE</td></tr>
<tr><td>0</td><td>Austauschnummer</td><td>Aktivitätsbit: Rang 0
Abbruchbit: Rang 1
Bit für unmittelbare Kenntnis: Rang 2</td></tr>
<tr><td>1</td><td>Betriebsrückmeldung (siehe ™EcoStruxure Control Expert, Kommunikationsbausteinbibliothek)</td><td>Kommunikationsrückmeldung (siehe ™EcoStruxure Control Expert, Kommunikationsbausteinbibliothek)</td></tr>
<tr><td>2</td><td colspan="2">Timeout (siehe ™EcoStruxure Control Expert, Kommunikationsbausteinbibliothek)</td></tr>
<tr><td></td><td></td><td>3</td><td colspan="2">Länge (siehe ™EcoStruxure Control Expert, Kommunikationsbausteinbibliothek)</td></tr>
</table>

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.
RECP_DDT	Beliebig	Empfangspuffer. Es kann eine Variable vom Typ DDT verwendet werden. In der Beschreibung des T_BMENUA0100-DDT, Seite 140 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

Bei einer Umschaltung in einer Hot Standby-Anwendung nimmt der asynchrone Kommunikationsfunktionsbaustein READ_DDT nicht automatisch den Betrieb auf dem neuen primären PAC wieder auf, außer dies 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 dem Standby-PAC ausgetauscht werden. Dazu müssen Sie die Auswahl des Attributs **Austausch auf STBY** für die EFB-Instanz aufheben.

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 als Länge die Länge der in den Ausgabeparameter RECP_DDT kopierten Daten festgelegt, wenn in GEST[1] oder mit einem zusätzlichen Statuscode kein erkannter Fehler gemeldet wird. Eine Beschreibung dieser zusätzlichen Statuscodewerte finden Sie im Control Expert-Hilfethema *Fehlercodes der EFBs mit STATUS-Parameter* (siehe ™*EcoStruxure Control Expert, Kommunikationsbausteinbibliothek*).
- Ein Timeout-Wert von 0 bedeutet eine unendliche Wartezeit. In diesem Fall wird eine während des Austauschvorgangs auftretende Kommunikationsverzögerung oder ein Kommunikationsverlust nicht erkannt. Während dieser unbegrenzten Wartezeit behält der Parameter RECP_DDT 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 den READ_DDT sind 0x30ss und 0x4001. Eine Beschreibung dieser zusätzlichen Statuscodewerte finden Sie im Control Expert-Hilfethema *Fehlercodes der EFBs mit STATUS-Parameter* (siehe ™*EcoStruxure Control Expert, Kommunikationsbausteinbibliothek*).
- Abhängig von dem im Parameter DDT_NAME angegebenen DDT werden einige Konsistenzprüfungen der empfangenen Daten durchgeführt. Wird eine Abweichung festgestellt, dann wird im Betriebsrückmelungsbyte (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.

⚠VORSICHT

UNERWARTETES VERHALTEN DER ANWENDUNG

- 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.

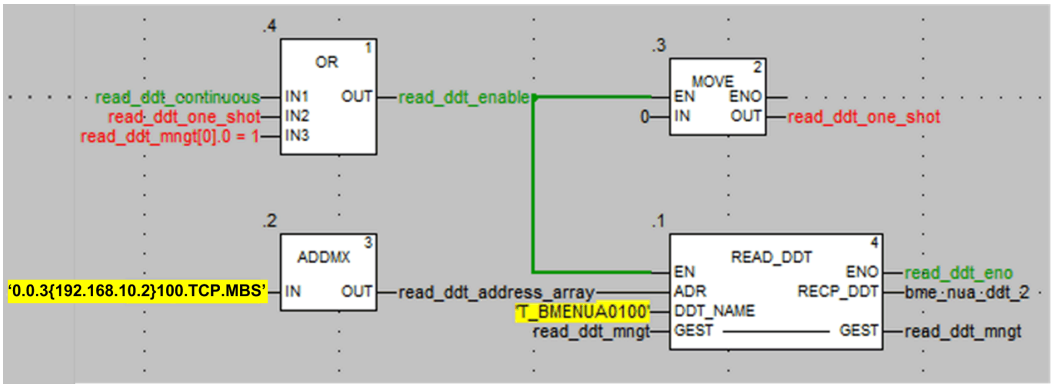
Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

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 Zeichenkettenformat 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 Berichtsparameter 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 möglicherweise 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.

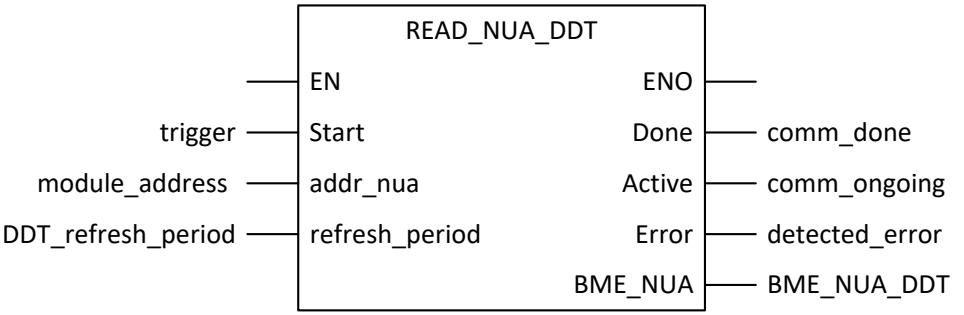
Konfiguration der elementaren Funktion READ_NUA_DDT

Verwenden Sie den Funktionsbaustein `READ_NUA_DDT`, um auf die Diagnoseinformationen des BMENUA0100-Moduls zuzugreifen.

Die Eingangsparameter `Start`, `addr_nua` und `refresh_period` definieren die Operation.

Als zusätzliche Parameter können EN und ENO konfiguriert werden.

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 Funktionsbaustein lösen. Wenn dieser Eingang auf Null gesetzt wird, ist der Funktionsbaustein deaktiviert und kann den Algorithmus des Funktionsbausteins nicht lösen.
Starten	BOOL	Das Lesen der BMENUA0100-DDT erfolgt kontinuierlich.

Parameter	Datentyp	Beschreibung
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) gibt das Modul an der IP-Adresse 192.168.10.2 mit Geräte-ID 100 (lokaler Server des Moduls) an, das mit dem integrierten Ethernet-Port verbunden ist.
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.
Done	BOOL	Die Kommunikation ist abgeschlossen.
Active	BOOL	Die Kommunikation läuft.
Fehler	BOOL	Fehler am Kommunikations-FB erkannt.
BME_NUA	T_BMENUA0100	Der BMENUA0100-DDT, Seite 140, 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 Ermittlung der im Modul ausgeführten Anwendung und zum Diagnostizieren von Modulvorgängen verwendet werden können.

OPC UA – Variable SERVICE_LEVEL

Die Variable SERVICE_LEVEL gibt einem Client Informationen zum Status der CPU und dem Zustand OPC UA-Servers. Der Zugriff auf die Variable SERVICE_LEVEL erfolgt direkt unter der OPC UA-Server-Knotenstruktur. Die Variable SERVICE_LEVEL ist auch im

Element OPCUA_STATUS.SERVICE_LEVEL des BMENUA0100-Modul-DDT, Seite 140 dupliziert und kann programmgesteuert durch Ausführen der Elementarfunktion READ_ DDT, Seite 145 aufgerufen werden, wenn sich die Anwendung im Zustand RUN befindet.

HINWEIS: In redundanten Architekturen muss der OPC UA-Client die Variable SERVICE_LEVEL sowohl im primären als auch im Standby-Modul BMENUA0100 überwachen, um den Redundanzmechanismus zu verwalten. Wenn der Client erkennt, dass der Wert SERVICE_LEVEL des Standby-Moduls größer ist als der Wert SERVICE_LEVEL des primären Moduls, muss der Client eine Umschaltung vom Primär- auf das Standby-Modul auslösen.

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

SERVICE_LEVEL-Wert	**Status der CPU / des OPC UA-Servers**	
	Firmware = V1.0	**Firmware ≥ V1.1**
0	BMENUA0100 ist in der Bootphase. CPU weist den Status NOCONF oder ERROR auf. Beispiel für den Zustand ERROR: Die MAST-Task befindet sich im HALT-Zustand.	
1	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 Lesen des CPU-Status wird ausgeführt. Der Adressraum wird mit dem neuen Inhalt des Datenwörterbuchs aktualisiert.	
120[1]	CPU im STOP-Zustand.	CPU im Zustand STOP STANDBY oder HALT STANDBY (nur Hot Standby-CPU).
150[1]	CPU im WAIT STANDBY-Zustand (nur Hot Standby-CPU).	
199[1]	CPU im RUN STANDBY-Zustand (nur Hot Standby-CPU).	
202[2]	<Nicht zutreffend>	Nur Standalone_CPU: CPU im Zustand STOP STANDALONE. Nur Hot Standby-CPU: Wenn sich beide CPUs im STOP- oder HALT-Zustand befinden, wird eine BMENUA0100-CPU als Master mit Dienstebene = 202 deklariert. Der Adressraum ist OK und nutzbar.

SERVICE_LEVEL-Wert	Status der CPU / des OPC UA-Servers	
	Firmware = V1.0	Firmware ≥ V1.1
255	CPU im RUN-Zustand (oder RUN PRIMARY für Hot Standby-CPU). OPC UA-Server ist voll funktionsfähig.	
1. Dieser Wert muss nicht festgelegt werden, bevor der Server betriebsbereit wird. 2. Diese Dienstebene gilt nur für die BMENUA0100-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, bleibt SERVICE_LEVEL beim Wert 100, 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 zurzeit überwachten Elemente gestoppt werden, wobei die Werte der überwachten Elemente auf ihren 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 im PAC erstellt wurde.
BuildNumber	Die Nummer des aktuellen PAC-Anwendungs-Builds.
ManufacturerName	Immer „Schneider Electric“.
ProductName	Immer „BMENUA0100“.
ProductUri	Der dem Modul zugewiesene eindeutige Uniform Resource Identifier.
SoftwareVersion	Die aktuelle 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. Obwohl sie ähnlich wie PAC-

Datenelemente über die Control Expert-Software erreichbar sind, sind diese speziellen DataItems nicht mit PAC-Symbolen 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.** Aktualisieren **3.** Teilweise generiert (in der Anwendung ist kein Datenwörterbuch vorhanden oder Datenwörterbuch-Überlauf)
#ApplicationName	STRING	0	Der Name der PAC-Anwendung.
#ApplicationVersion	STRING	0	Die Version der PAC-Anwendung.
#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 CPU-Referenz.
#PLCDatadicReady	BYTE	1	Überwacht den Ladestatus des PAC-Datenwörterbuchs: 1. Das PAC-Datenwörterbuch ist nicht verfügbar. Mögliche Erklärungen: • Die Datenwörterbuchfunktion ist nicht verfügbar oder in der Control Expert-Anwendung aktiviert und kann nicht in den PAC integriert werden. • Das Laden/Durchsuchen des Datenwörterbuchs wird im OPC UA-Server ausgeführt. 2. Das PAC-Datenwörterbuch ist verfügbar, z. B.: • Das Laden/Durchsuchen des Datenwörterbuchs durch den OPC UA-Server wurde erfolgreich abgeschlossen. • Ein Vorladevorgang (gemäß den Projekteinstellungen des Control Expert-Datenwörterbuchs) kann ausgeführt werden.

DataItem	Datentyp	Standardwert	Beschreibung
#PLCQualStatus	INT16	0	Überwacht den Kommunikationsstatus eines PAC. Mögliche (hex.) Werte: • 0x00C0: Die Kommunikation mit dem PAC ist korrekt. • 0x0040: Keine Kommunikation mit dem PAC über einen Zeitraum, der unter dem Geräte-Timeout (5 s) liegt. • 0x0: PAC ist nicht identifiziert.
#TSEventItemsReady	BOOL	0	Ein schreibgeschütztes Element, das angibt, ob quellzeitgestempelte Variablen und Quellzeitstempel in der M580 ePAC-Anwendung durchsucht wurden: • 0 = Nicht durchsucht • 1 = Durchsucht **HINWEIS:** Dieses Element ist nur sinnvoll, wenn die Zeitstempelung in Control Expert aktiviert und für das spezifische BMENUA0100-Modul aktiviert ist.
#TSEventSynchro	BOOL	0	Ein Lese-/Schreibelement, das, wenn es aktiviert ist, bei jeder Ausführung eines Schreibvorgangs einen synchronisierten Wert an das gesamte Quellzeitstempelgerät sendet, das mit dem M580-ePAC verbunden ist. Der Zweck besteht darin, alle überwachten Elemente mit Zeitstempel auf ihre aktuellen Werte zu initialisieren. • 0 = Warten auf Aktivierung • 1 = Aktiviert **HINWEIS:** • Der Wert dieses Elements wird immer als 0 angezeigt. Der Wert 1 wird nie angezeigt, da er nur vorübergehend vorhanden ist, und kehrt wieder zum erwarteten Aktivierungswert 0 zurück. • Dieses Element ist nur sinnvoll, wenn die Zeitstempelung in Control Expert aktiviert 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. Zum Diagnostizieren älterer Ereignisse können Sie die Syslog-Server-Ereignisaufzeichnungen abfragen. Für aktuelle Modulereignisse können Sie die Modul-Webseiten, Seite 159 verwenden, um den Zustand des Syslog-Diensts 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 158

  – ODER –

- Größere Änderungen im System (Protokoll-Audit), Seite 158

Der Syslog-Dienst ist im Rahmen der Cybersicherheitskonfiguration auf den Webseiten, Seite 94 konfigurierbar und kann daher nur dann aktiv sein, wenn das Modul im sicheren Modus ausgeführt wird. Wenn das Modul im Standardmodus ausgeführt wird, ist der Dienst deaktiviert.

Wie im BMENUA0100-Modul implementiert, wird syslog von IPv4 (Firmware-Version 1.0 und höher) und IPv6 (Firmware-Version 1.10 und höher) unterstützt.

HINWEIS: Syslog ist kein nativ sicheres Protokoll, sondern muss in einem sicheren IPSEC, Seite 101-Kanal über den Steuerungsport gekapselt werden.

Syslog-Meldungsstruktur

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

Feld	Beschreibung
PRI	Informationen zur Anlage und Schwere (eine Beschreibung finden Sie in den folgenden Tabellen).
VERSION	Version der syslog-Protokollspezifikation (Version = 1 für RFC 5424).

<table>
<tr><th>Feld</th><th>Beschreibung</th></tr>
<tr><td>TIMESTAMP</td><td>Das Zeitstempelformat wird von RFC 3339 ausgestellt, welches das folgende Internet-basierte ISO8601-Datums- und -Zeitformat empfiehlt: YYY-MM-DDThh:mm:ss.nnnZ
HINWEIS: -, T, :, ., Z sind vorgeschriebene Zeichen und Teil des Zeitstempelfelds. T und Z müssen in Großbuchstaben geschrieben werden. Z gibt die Zeit als UTC an.
Beschreibung des Inhalts des Zeitfelds:
<table><tr><td>YYY</td><td>Jahr</td></tr><tr><td>MM</td><td>Monat</td></tr><tr><td>DD</td><td>Tag</td></tr><tr><td>hh</td><td>Stunde</td></tr><tr><td>mm</td><td>Monat</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 das Gerät, das die syslog-Meldung ursprünglich gesendet hat: Voll qualifizierter Domänenname (FQDN) oder statische Quell-IP-Adresse, wenn FQDN nicht unterstützt wird.</td></tr>
<tr><td>APP-NAME</td><td>Identifiziert die Anwendung, die die syslog-Meldung initiiert hat. Das Feld enthält Informationen zur Identifikation der Einheit, die die Meldung 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.
Erhält NILVALUE, wenn nicht verwendet.</td></tr>
<tr><td>MSGID</td><td>Identifiziert den Typ der Meldung, auf die sich das Ereignis bezieht, zum Beispiel HTTP, FTP, Modbus.
Erhält NILVALUE, wenn nicht verwendet.</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). Erhält Null, wenn nicht verwendet.
Peer-Adresse: Peer-IP-Adresse, wenn ein Peer an dem Vorgang beteiligt ist. Erhält Null, wenn nicht verwendet.
Typ: Eindeutige Nummer zur Identifizierung einer Meldung (Beschreibung in den folgenden Tabellen).
Bemerkung: Zeichenfolge, die die Meldung beschreibt (Beschreibung in den folgenden Tabellen).</td></tr>
</table>

Ereignisse im Zusammenhang mit Sicherheit/ Autorisierung

- Fehlgeschlagene sichere Kanalöffnung von OPC UA-Stack: Beispielsweise ungültiges Zertifikat, abgelaufenes Zertifikat.
- Erfolgreiche Benutzersitzungen (Benutzername/Passwort) von OPC UA-Stack (erfolgreiche Anmeldung)

  HINWEIS: Wenn keine Anmeldung erfolgt (Standardmodus), wird das Protokoll deaktiviert, sodass keine Aufzeichnung der erfolgreichen Verbindung erstellt wird.
- Fehlgeschlagene Benutzersitzungen (Benutzername/Passwort) von OPC UA-Stack (fehlgeschlagene Anmeldung)

  HINWEIS: Wenn keine Anmeldung erfolgt (Standardmodus), wird das Protokoll deaktiviert, sodass keine Aufzeichnung der nicht erfolgreichen Verbindung erstellt wird.
- Erfolgreiche HTTPS-Verbindungen zu oder von einem Tool (erfolgreiche Anmeldung): Beispielsweise eine Verbindung zum Webserver oder ein Firmware-Download über HTTPS.
- Fehlgeschlagene HTTPS-Anmeldung bei oder von einem Tool: Beispielsweise eine fehlgeschlagene 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 nur ein (Hash) Fehler bei der Integrität.
- Erstellen eines neuen Zertifikats.
- Entfernen lokaler Zertifikate. Dies wird erreicht, indem die Betriebsart mit dem Drehwahlschalter auf die Position „Security Reset“ (Sicherheits-Reset) eingestellt wird.
- Hinzufügen eines neuen Clientzertifikats von der Allowlist in das Gerät.
- Entfernen eines Clientzertifikats von der Allowlist in das 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 für das Modul, um den Zustand des im Modul ausgeführten Syslog-Diensts und bestimmte Teile des Syslog-Diagnosepuffers des Moduls zu diagnostizieren. Sie können auch das Element SERVICES_STATUS des Modul-DDT, Seite 140 verwenden, um den Status des Syslog-Dienstes anzuzeigen.

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

Parameter	Beschreibung
Status	• Betriebsbereit: Das Modul wird im sicheren Modus ausgeführt und der Syslog-Dienst ist aktiviert. • Nicht betriebsbereit: Das Modul wird im sicheren Modus ausgeführt und 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 durchführen. Modbus-Befehle können das Modul nur über seinen Baugruppenträger-Port erreichen. Da Modbus kein von Natur aus sicheres Protokoll ist, müssen Sie Modbus-Befehl in IPSEC kapseln.

Nur die Requests FC43/14 (Geräte-ID lesen) und FC03 (um DDTM-W% zu 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 in Betrieb ist:

- Standardmodus: Das BMENUA0100-Modul nimmt den Datenfluss des Modbus TCP/IP-Clients von jedem Client an, der auf das Ethernet-Netzwerk des Baugruppenträgers zugreifen kann. Verwenden Sie standardmäßige Modbus-Kommunikationsmethoden, einschließlich der Funktionsbausteine DATA_EXCH, MBP_MSTR, READ_VAR und WRITE_VAR, und Control Expert-Befehle.
- Sicherer Modus: Das BMENUA0100-Modul akzeptiert den Modbus TCP/IP-Client-Datenfluss nur von der M580-CPU. 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	0x00	VendorName	ASCII-Zeichenfolge
	0x01	ProductCode	ASCII-Zeichenfolge
	0x02	MajorMinorRevision	ASCII-Zeichenfolge
Normal	0x03	VendorUrl	ASCII-Zeichenfolge
	0x04	ProductName	ASCII-Zeichenfolge
	0x05	ModelName	ASCII-Zeichenfolge
	0x06	UserApplicationName	ASCII-Zeichenfolge
	0x07...0xFF	Reserviert	ASCII-Zeichenfolge

SNMP-Diagnose

Einführung

Wenn der SNMP-Agent konfiguriert, Seite 131 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 **OPC UA-Diagnose**-Webseite wird alle 5 Sekunden aktualisiert.

Diagnosedaten

Auf der Webseite **OPC UA-Diagnose** werden die folgenden schreibgeschützten Daten angezeigt. Beachten Sie, dass alle numerischen Werte im Dezimalformat vorliegen:

Feld	Beschreibung
SPS-Diagnose	
EPAC	IP-Adresse der CPU
Geräteidentität	Teilenummer der CPU
Geräteversion	Firmeware-Version der CPU
Gerätestatus	Verbindungsstatus mit CPU: 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 CPU 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 125.
Request-Länge	Länge des Requests für die Kommunikation mit der CPU.
Anwendungsname (Gerät)	Der Control Expert-Projektname.
Anwendungsversion (Gerät)	Prüfsumme und Signaturen der Anwendung.
Datenwörterbuch vorabladen	Verfügbar oder nicht verfügbar für Anwendung in PAC.
Zeitstempelstatus	Der Zeitstempelstatus wird angezeigt: • Die Zeitstempelung wird mit Zugriff auf zeitgestempelte Variablen in der Anwendung aktiviert. • Die 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 (CRA, CPU usw.). • IPv4-Adresse. • Reservierung des Geräte-Zeitstempelpuffers durch den integrierten BMENUA0100-OPC UA-Server: true / false.
OPC UA-Diagnose	
Endpunkt-URL (IPV4)	IPv4-Adresse des OPC UA-Servers im folgenden Format: „opc.tcp://<IPv4-Adresse>:<Portnummer>“. Beispiel: opc.tcp://192.168.2.142:4840

Feld	Beschreibung
Schnelle Abtastrate	Gibt an, ob die Einstellung Schnelle Abtastrate, Seite 120 ausgewählt ist: • True = Ausgewählt • False = Nicht ausgewählt
Anzahl der verbundenen Sitzungen	Gesamtanzahl der vom BMENUA0100-Modul 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 integrierten OPC UA-Server des BMENUA0100-Moduls:
Timer-Liste	Eine Liste, die jedes Abtastintervall (d. h. Timer) beschreibt, das vom integrierten OPC UA-Server des BMENUA0100-Moduls 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 Phase der Betriebsart (Verbindungen, Durchsuchen, Abonnement, Überwachung usw.) stabiler und robuster machen.

HINWEIS:

- Schneider Electric empfiehlt, Elemente in Paketen mit einer maximalen Größe von 2.000 Elementen hinzuzufügen. Das konfigurierte Abtastintervall ist nur relevant, wenn es größer oder gleich der Zykluszeit des MAST-PAC ist.
- Schneider Electric empfiehlt, das CallTimeout im OPC UA-Client auf einen Wert größer oder gleich 10 Sekunden einzustellen.
- Die Einstellung General.SecureChannelLifetime für die Kommunikation mit einem OPC UA-Client wird standardmäßig auf 3.600.000 ms (1 Stunde) eingestellt. Schneider Electric empfiehlt die Verwendung dieser Standardeinstellung, da ein sehr niedriger Wert - z. B. 30 Sekunden - die Leistung negativ beeinflussen kann.
- 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 Standard-Drehschalterposition (d. h. keine sichere Kommunikation, kein IPSec-Kanal).
- OPC UA-Client (UAExpert) initiiert die Kommunikation mit dem auf **Keine** festgelegten Nachrichtensicherheitsmodus und überwacht 20.000 Elemente unter Bezugnahme auf Variablen, die auf einem Array vom Typ „INT“ von einem BMENUA0100-OPC UA-Server basieren. 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

Struktur für den Datenaustausch

Der Datenanwendungsspeicher der CPU ist in Abhängigkeit von der Definition der Datenanwendung 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, wird daher Folgendes empfohlen:

- Verwenden Sie nach Möglichkeit Arrays oder Datenstrukturen.
- Aktivieren Sie die Option **Nur HMI-Variable** in **In SPS eingebettete Daten** der **Projekteinstellungen** und legen Sie nur diese Variablen mit dem Attribut **HMI** fest, um die Größe des Datenwörterbuchs zu verringern.
- Deaktivieren Sie zur Reduzierung der Größe des Datenwörterbuchs im CPU-Sicherheitsprozess die Option **Nutzung des Prozess-Namespace** (in **Projekteinstellungen > Allgemein > In SPS eingebettete Daten > Datenwörterbuch**).

CPU-Kommunikationsfunktionen

Die Funktion des Kommunikationssystems richtet sich nach dem M580-CPU-Modell und einigen Konfigurationseinstellungen. Das CPU-Modell bestimmt Folgendes:

- Die systemweiten CPU-Verarbeitungsleistungsfunktionen.
- Die Anzahl der Requests pro Zyklus, die verarbeitet werden kann, auch wenn sie über das Systemwort %SW90 konfigurierbar ist.
- Die maximale Anzahl der Kanäle, die jedem BMENUA0100-Modul für die Einrichtung von Verbindungen mit der M580-CPU, Seite 174 zur Verfügung stehen.

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 Verarbeitung der Signatur und der Verschlüsselung zusätzliche Zeit.

CPU-zu-CPU- und Control Expert-zu-CPU-Kommunikation

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 Verschlüsselung und Entschlüsselung generiert wird.

Überwachung der Leistung

Es gibt verschiedene Möglichkeiten, die Leistung zu überwachen.

Verwenden von Control Expert

Mit Control Expert im verbundenen Modus können Sie auf die effektive MAST-Zykluszeit und die M580-CPU-Last für das System, für jede Task und für die Summe aller Tasks zugreifen, indem die Systemwörter %SW110 bis %SW116 gelesen werden. Darüber hinaus können der M580-CPU-DDDT und der BMENUA0100-DDT verschiedene mit der Systemleistung des PAC verbundene Diagnoseinformationen zur Verfügung stellen, z. B.:

- Dienstebene des OPC UA-Servers
- Anzahl der verbundenen OPC UA-Clients
- Status des Datenwörterbuchs, Erfassungszeit, die des Vorladens
- 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

Verwenden 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 aktuellen Animationen
- Erkannte Überläufe
- Anzahl der verbundenen Clients

Verwenden 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 durch Anwendungsvariablen.

Andere Dienste zur 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 verknüpft 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. Bei einer Anwendung, bei der der OPC UA-Server im BMENUA0100-Modul eine Zahl überwachen soll, die sich der max. Anzahl von 100.000 Elementen nähert - in diesem Fall 990.000 Elemente -, wurden die folgenden Ergebnisse beobachtet und können durchaus aufschlussreich sein.

Für eine Standardanwendung (nicht sicherheitsbezogen):

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

Für eine Sicherheitsanwendung:

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 32 entspricht, den der OPC UA-Server im BMENUA0100-Modul unterstützen kann.

Verwenden von GPOs / LGPOs

Schneider Electric empfiehlt, dass Sie Zertifikate auf einem Host-PC mithilfe eines der folgenden Tools verwalten, die unter dem Windows™-Betriebssystem verfügbar sind:

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

In beiden Fällen kann die Verwendung von GPOs oder LGPOs dazu beitragen, den unbefugten Zugriff auf Ihren PC und die darauf befindlichen Anwendungen zu verhindern, z. B. durch einen Hacker, der versucht, ein eigenes Zertifikat in Ihren PC zu schleusen, das in die autorisierte Benutzer-Allowlist im BMENUA0100-Modul aufgenommen werden soll. Die Verwendung von GPOs und LGPOs deaktiviert den Zugriff auf die Windows Management Console (MMC) und unterstützt nur die Implementierung der von der Software konfigurierten Allowlist. Auf diese Weise wird verhindert, dass ein Hacker dem OPC UA-Server ein selbstsigniertes Zertifikat von einem Hacker hinzufügen kann, der vorgibt, ein gültiger OPC UA-Client zu sein.

Übernehmen der MMC-Gruppenrichtlinienverwaltung

Schneider Electric empfiehlt, dass Sie Zertifikate mithilfe der von Microsoft Windows™ bereitgestellten Tools verwalten, um zu verhindern, dass ein Eindringling unbefugte Zertifikate zum PC hinzufügt oder selbstsignierte Zertifikate eines OPC UA-Clients ändert. Wenn dies nicht verwaltet wird, können unbefugte Zertifikate in die vom Sicherheitsadministrator verwaltete BMENUA0100-Allowlist aufgenommen werden.

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 Allowlist-Konfiguration zulassen, 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 93 des BMENUA0100-Moduls angewendet. Wenn beispielsweise die Anzahl der **maximalen Anmeldeversuche** erreicht oder überschritten wird, kann sich der OPC UA-Client (**BadInternalError**) während des als **Kontosperrdauer** festgelegten Zeitraums 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 118 ist, sind die Netzwerkdienste **CPU-zu-CPU-Datenflüsse** und die **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 sind, wenn nur IPv6 aktiviert ist, werden die Dienste (**CPU zu CPU** und **CE zu Gerätenetzwerk**) auf der Seite **Home** als EIN angezeigt. Tatsächlich werden sie jedoch nicht aktiviert.

Nur die **Control Expert-Funktion zur Datenflussfilterung (nur in die CPU)** unterstützt die IPv6-Kommunikation. Wenn nur die IPv6-Kommunikation aktiviert ist, wird auf der **Home**-Seite richtig angezeigt, dass **Nur CE zu CPU** EIN ist.

Als BYTE in CPU-Datenstrukturen angezeigte BOOLs

Im OPC-UA-Server des BMENUA0100-Moduls wird jedes Element des ePAC-DDT einem Byte in der CPU zugeordnet, selbst wenn es im BMENUA0100-Modul als BOOL oder EBOOL definiert ist. Mithilfe des OPC UA-Protokolls kann ein Client ein BOOL- oder EBOOL-Element einer BMENUA0100-Instanz im CPU-DDT global lesen oder schreiben, mit einem anderen gültigen Bytewert als 0 oder 1 (z. B. 255). Es wird empfohlen, Ihre Anwendung so zu gestalten, dass sie Werte vom Typ 0 oder 1 schreibt oder liest, 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:

- Erkennen Sie manuell ein oder mehrere BMENUA0100-Module in Ihrem Projekt basierend auf IP-Adressen.
- Aktualisierung der BMENUA0100-Module auf die neueste Firmware-Version über das Web.

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. Sie können die Unity Loader-Software nicht mit dem Steuerungsport des BMENUA0100-Moduls verbinden, um Projekte herunterzuladen oder die CPU- oder die Modul-Firmware zu aktualisieren.

Downgrade der Firmware

Es ist möglich, die Firmware-Version des BMENUA0100-Moduls herabzusetzen, z. B. von der höheren Version 1.1 auf die niedrigere Version 1.0. Führen Sie dazu nach dem Downgrade der Softwareversion mithilfe des Tools EcoStruxure™ Automation Device Maintenance einen Sicherheits-Reset, Seite 28 durch, um die werkseitigen Standardeinstellungen des Moduls wiederherzustellen. Wählen Sie dann einen Cybersicherheitsmodus - gesicherter Modus oder Standardmodus - für das Modul aus.

Anhänge

Inhalt dieses Abschnitts

CPU-Verbindungen 174
Architekturen für die Dienstweiterleitung (IP) 175
IP-Weiterleitung und OPC UA-Kommunikation 180
IPSEC-Windows-Skripts 183
Einrichtung einer Windows-Zertifizierungsstelle 186

CPU-Verbindungen

Inhalt dieses Kapitels

Verbindungen zwischen OPC UA Server und CPU 174

Verbindungen zwischen OPC UA Server und CPU

Geöffnete Verbindungen

Die Anzahl der Verbindungen, die das BMENUA0100-Modul zur M580-CPU öffnen kann, richtet sich nach der Kapazität der CPU. Somit hängt die Leistung des BMENUA0100-Moduls von der zur Ausführung der MAST-Task benötigten Zeit und der ausgewählten CPU ab. Nachfolgend ist die maximale Anzahl der von jedem BMENUA0100-Modul zur M580-CPU geöffneten Verbindungen aufgelistet:

CPU-Modell	Maximale Anzahl der von jedem BMENUA0100-Modul geöffneten Verbindungen
BMEP581020	9
BMEP5820•0	9
BMEP5830•0	12
BMEP5840•0	15
BMEP585040	15
BMEP586040	18
BMEH582040	9
BMEH584040	15
BMEH586040	18

Architekturen für die Dienstweiterleitung (IP)

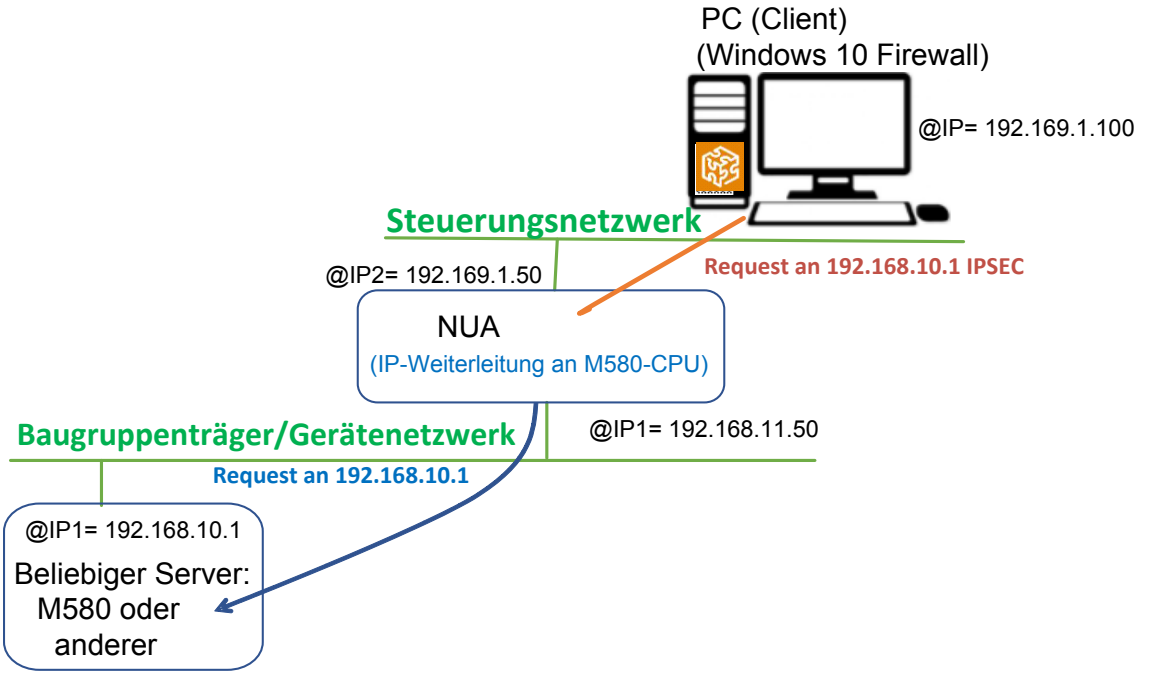
Inhalt dieses Kapitels

Unterstützte Architekturen für die Dienstweiterleitung (IP) 176
Nicht unterstützte Architekturen für die Dienstweiterleitung (IP) 179

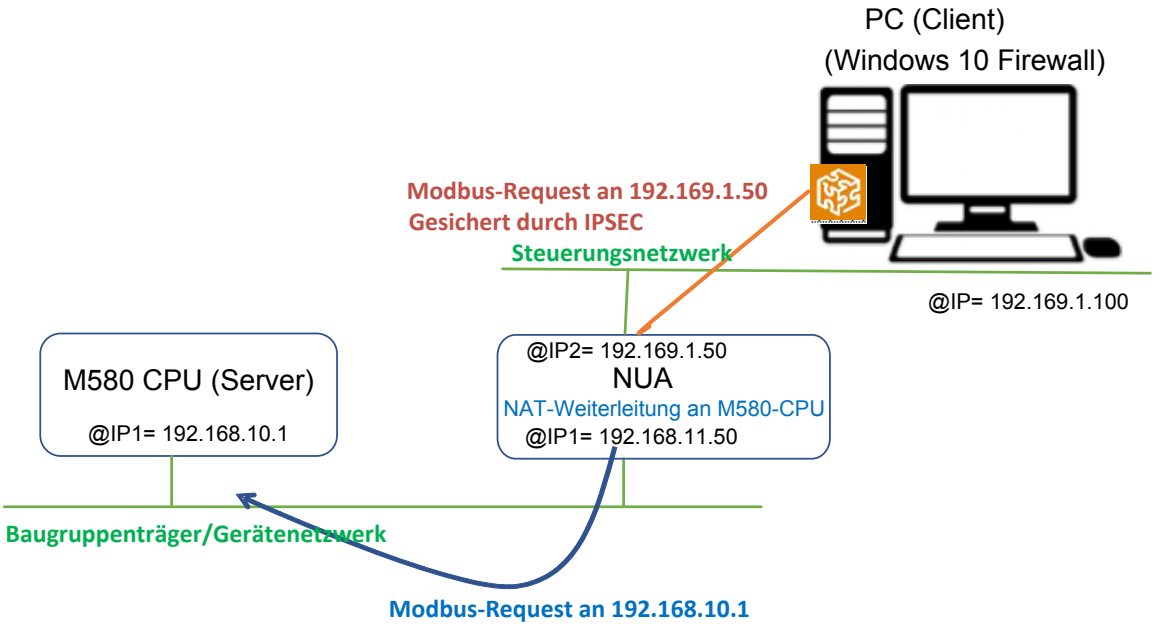
In diesem Kapitel werden die Architekturen vorgestellt, die von der Dienstweiterleitungsfunktion (IP) des BMENUA0100-Moduls unterstützt bzw. nicht unterstützt werden.

Unterstützte Architekturen für die Dienstweiterleitung (IP)

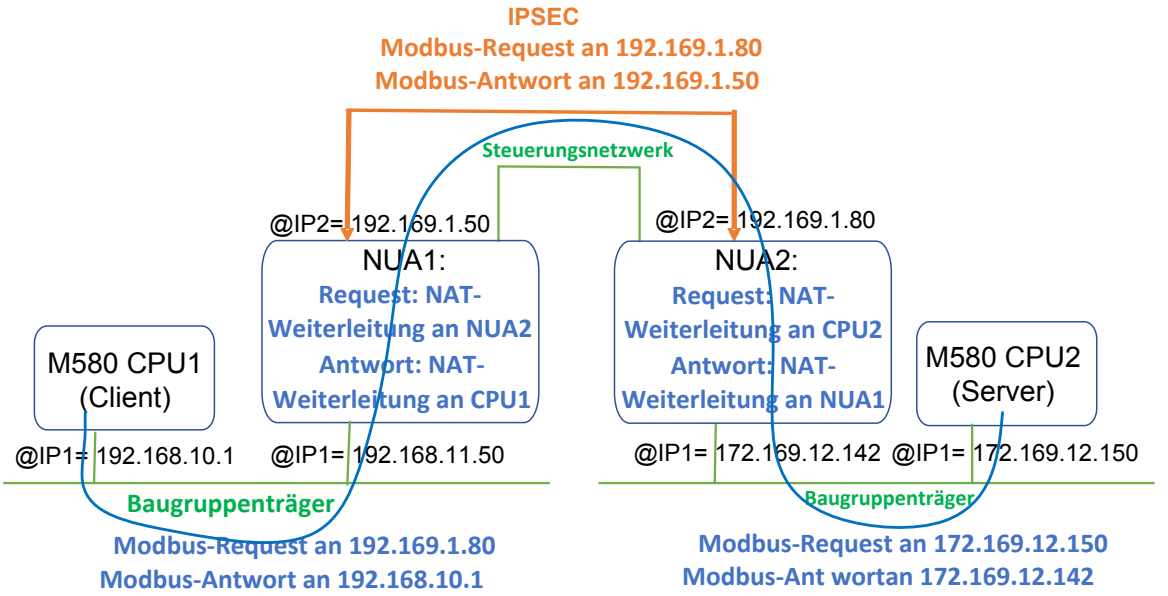
IP-Weiterleitung vom Windows-Client (Steuerungsnetzwerk) an einen beliebigen Client (Baugruppenträger/Gerätenetzwerk)



NAT-Weiterleitung vom Windows-Client (Steuerungsnetzwerk) an die M580-CPU (Baugruppenträger/Gerätenetzwerk)

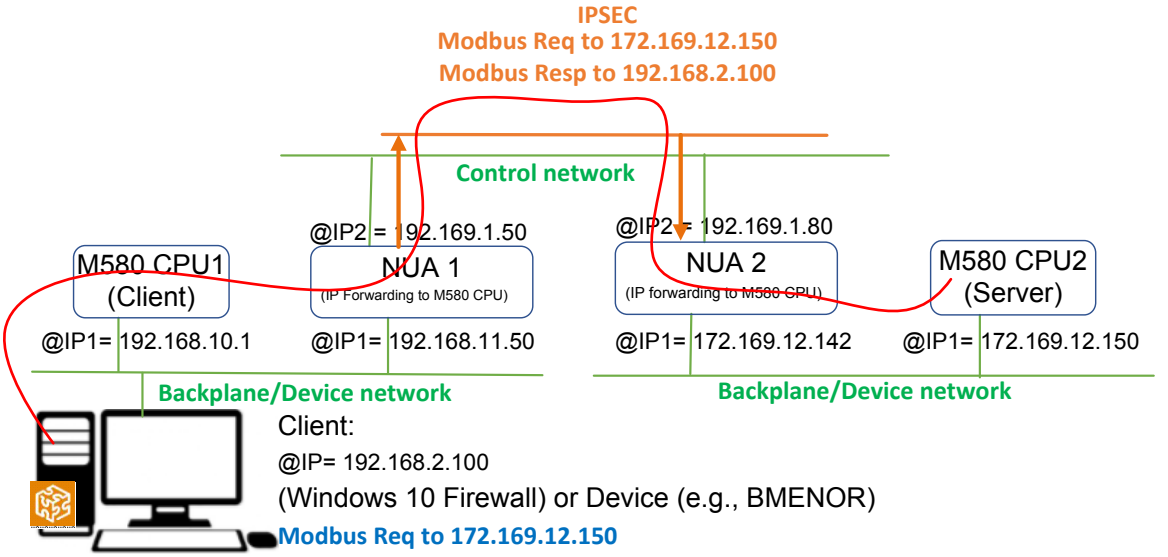


NAT-Weiterleitung zwischen Baugruppenträgern für die Kommunikation zwischen M580-CPU und M580-CPU



Nicht unterstützte Architekturen für die Dienstweiterleitung (IP)

IP-Weiterleitung zwischen Baugruppenträgern/ Gerätenetzwerken



IP-Weiterleitung und OPC UA-Kommunikation

Inhalt dieses Kapitels

IP-Weiterleitung - Auswirkungen auf die Leistung 180
IP-Weiterleitung und OPC UA - Auswirkungen auf die Leistung 181

Sowohl die IP-Weiterleitung als auch OPC UA beanspruchen die verfügbaren 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 wurde, lag der Einfluss auf die BMENUA0100-Modulbandbreite folgendermaßen:

IPSec	Vertraulichkeit	Weiterleitung	Framelänge (Byte)	Bandbreite (KByte/Sek.)
Nein	Ohne Bedeutung	Alle weiterleiten	1000	8800
Nein	N/A	Benutzerdefinier-te Regel	1000	10600
Ja	Nein	Alle weiterleiten	1000	3400
Ja	Nein	Benutzerdefinier-te Regel	1000	4000
Ja	Ja	Alle weiterleiten	1000	2600
Ja	Ja	Benutzerdefinier-te Regel	1000	2500

HINWEIS: Diese Werte dienen lediglich als Beispiel. Verwenden Sie sie zur Einschätzung der Leistungsauswirkungen unterschiedlicher Parameter (IPSEC, Vertraulichkeit usw.). 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 werden signiert (Vertraulichkeit = Nein) bzw. wenn Frames sowohl signiert als auch verschlüsselt werden (Vertraulichkeit = Ja), und IPSEC wird (in beiden Fällen) verwendet.
- Es werden benutzerdefinierte Regeln für die IP-Weiterleitung im Vergleich zu „Alle weiterleiten“ angewendet.

HINWEIS: Die Framelänge hat nur einen leichten 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 wurden, hatte dies folgende Auswirkungen auf die BMENUA0100-Modulbandbreite:

Anzahl der überwachten OPC UA-Elemente pro Abonnement	IPSec	Vertraulichkeit	Weiterleitung	Bandbreite (KByte/Sek.)
0	Nein	Ohne Bedeutung	Benutzerdefinierte Regel	10600
0	Ja	Nein	Benutzerdefinierte Regel	4000
0	Ja	Ja	Benutzerdefinierte Regel	2500
20000	Nein	Ohne Bedeutung	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 Leistungsauswirkungen unterschiedlicher Parameter (IPSEC, Vertraulichkeit usw.). 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-Skripts

Inhalt dieses Kapitels

Skripts zur Konfiguration der IKE/IPSEC-Windows-Firewall 183

Skripts zur Konfiguration der IKE/IPSEC-Windows-Firewall

Um IPSEC auf einem PC auszuführen, auf dem die Konfigurationssoftware Control Expert oder ein OPC UA-Client (z. B. SCADA) installiert ist, müssen Sie die Netzwerkkonfiguration auf der Host-Firewall hinzufügen. Für jede auf den Webseiten konfigurierte IPSEC-Regel kann ein zugewiesenes Skript (IPSecWindowsConf.bat genannt) über das Zahnradsymbol heruntergeladen werden. Führen Sie dieses Skript aus, um die Host-Firewall auf die richtige Konfiguration einzustellen.

- IKE/IPSEC im **Transportmodus** für den lokalen Datenfluss des BMENUA0100-Moduls.
- IKE/IPSEC im **Tunnelmodus** für den Datenfluss, der an den Ethernet-Baugruppenträger weitergeleitet wird.
- Pass-through-Regeln für HTTPS, gesichertes OPCUA und einige andere Protokolle, für die **IPSEC-Verwendung**=false gilt.

Bei den folgenden Beispielen handelt es sich um Konfigurationsskripts für die Windows-Firewall mit und ohne IPSEC-Vertraulichkeit.

In jedem Skriptbeispiel müssen Sie die Ist-Werte für die folgenden Variablen angeben:

- **`endpoint1`**: Wert der dezentralen IP-Adresse in der IPSEC-Konfiguration.
- **`endpoint2`**: IP-Adresse des BMENUA0100-Steuerungsports.
- **`Auth1psk`**: PSK-Einstellung in der IPSEC-Konfiguration.

Windows-Firewall-Skript mit Vertraulichkeit

HINWEIS: Wenn Vertraulichkeit in der IPSEC-Konfiguration aktiviert ist, `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 aktiviert ist, `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

Vorbereitung 186
Überblick über die Installation von Microsoft Windows ADCS 187
Installation von ADCS (Active Directory Certificate Server) 188
Anwendung der Vorlage der Zertifizierungsstelle 210

In diesem Kapitel wird beschrieben, wie Sie eine Microsoft Windows™-Zertifizierungsstelle einrichten, die in einem unternehmensweiten Benutzerauthentifizierungs- und -autorisierungssystem verwendet werden kann.

Vorbereitung

Im Folgenden werden die erforderlichen Tools und die vorbereitenden Schritte beschrieben, die Sie vor der Installation des Zertifikatservers ausführen müssen.

Tools, die Sie benötigen

Sie benötigen folgende Elemente:

- Microsoft Windows™ Server Manager: Dieses Tool kann kostenlos von der Microsoft-Website heruntergeladen werden.
- Microsoft Windows Active Directory Certificate Server (ADCS): Diese Software ist Bestandteil von Windows Server. Sie müssen dafür eine Lizenz erwerben. Das BMENUA0100-Modul unterstützt die Serverversionen 2016 und 2019.
- Die Datei TemplatePackage.zip, die von Schneider Electric heruntergeladen werden kann.

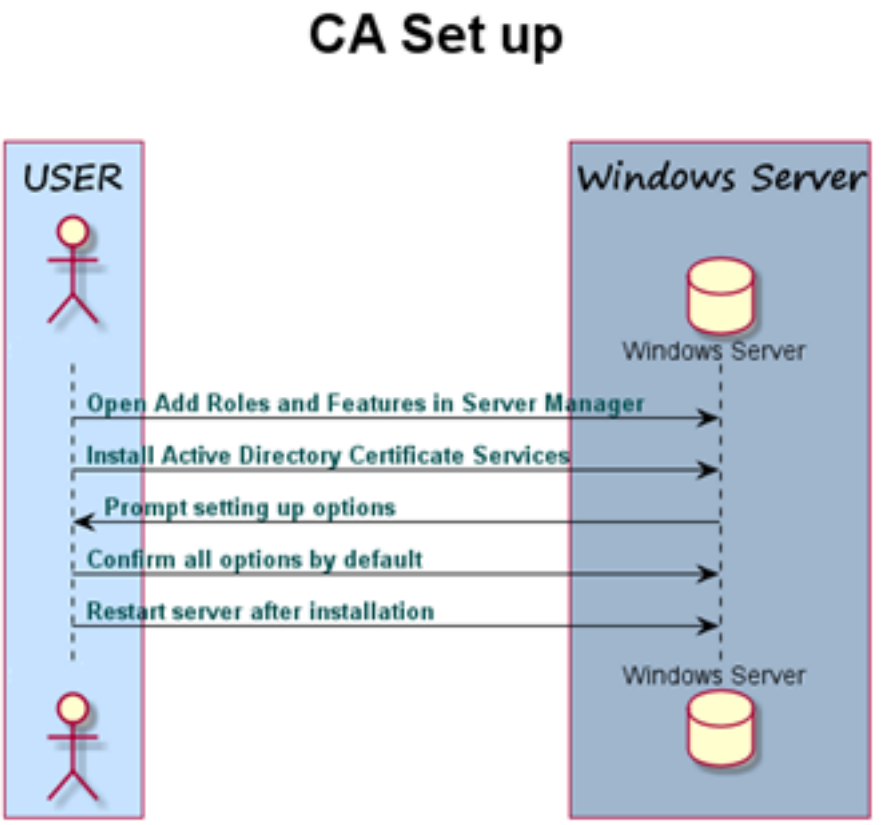
Vorläufige Softwareinstallationen

Führen Sie die ADCS-Installationsdatei aus und dann die folgenden Schritte aus, um einen Benutzer und ein Passwort zu erstellen.

Server Manager sollte auf dem Host-PC vorinstalliert sein. Wenn nicht, kann er kostenlos von der Microsoft-Website heruntergeladen werden.

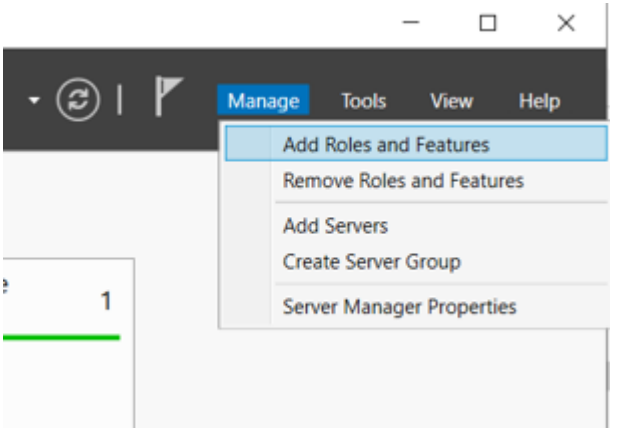
Überblick über die Installation von Microsoft Windows ADCS

Die folgende Abbildung bietet einen Überblick über den Einrichtungsprozess der Zertifizierungsstelle (CA: Certificate Authority):

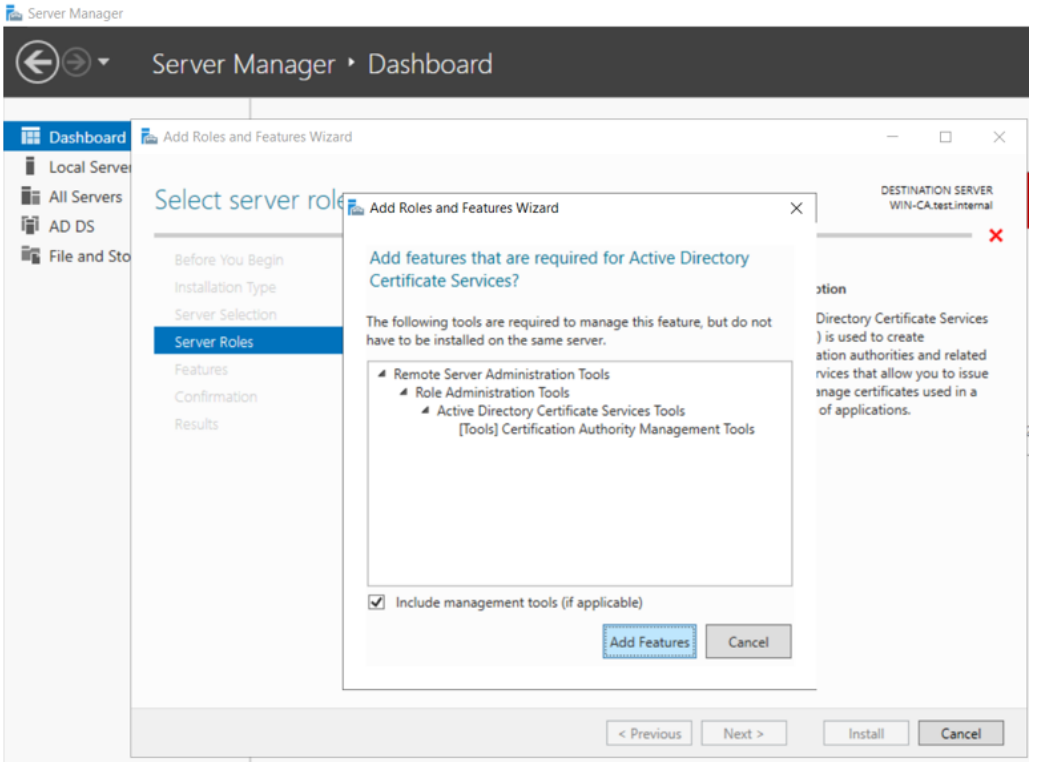


Installation von ADCS (Active Directory Certificate Server)

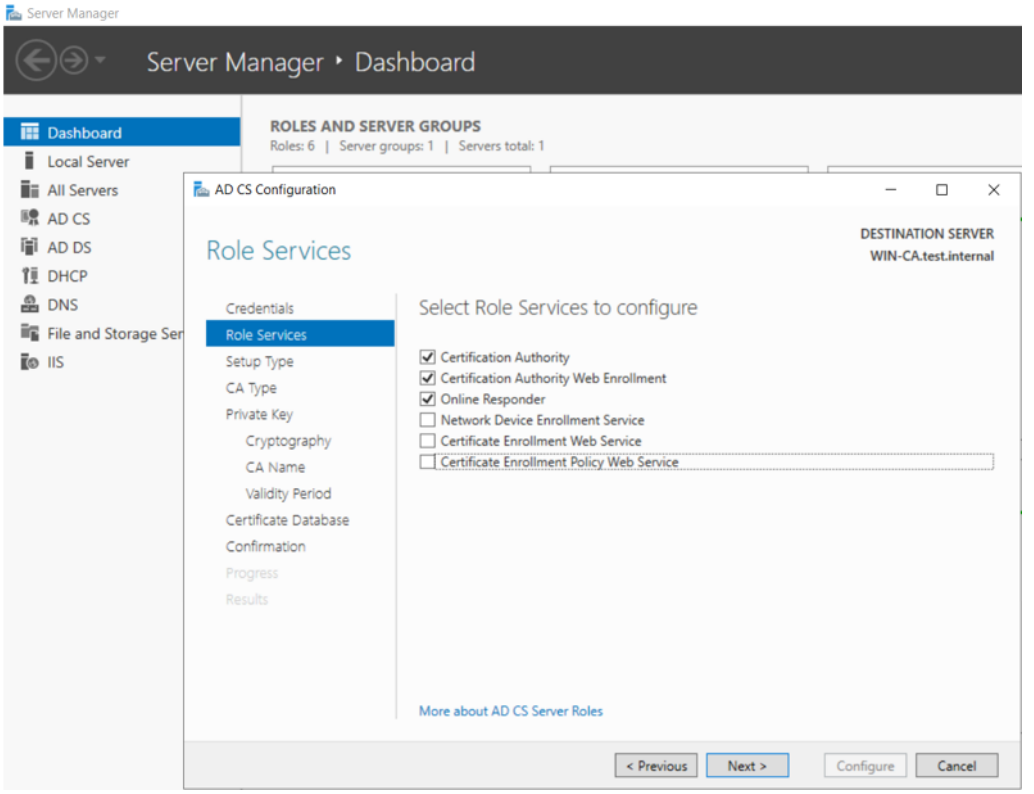
1. Starten Sie Microsoft Windows™ Server Manager und öffnen Sie das Dashboard.
2. Wählen Sie **Verwalten > Rollen und Funktionen hinzufügen** aus.



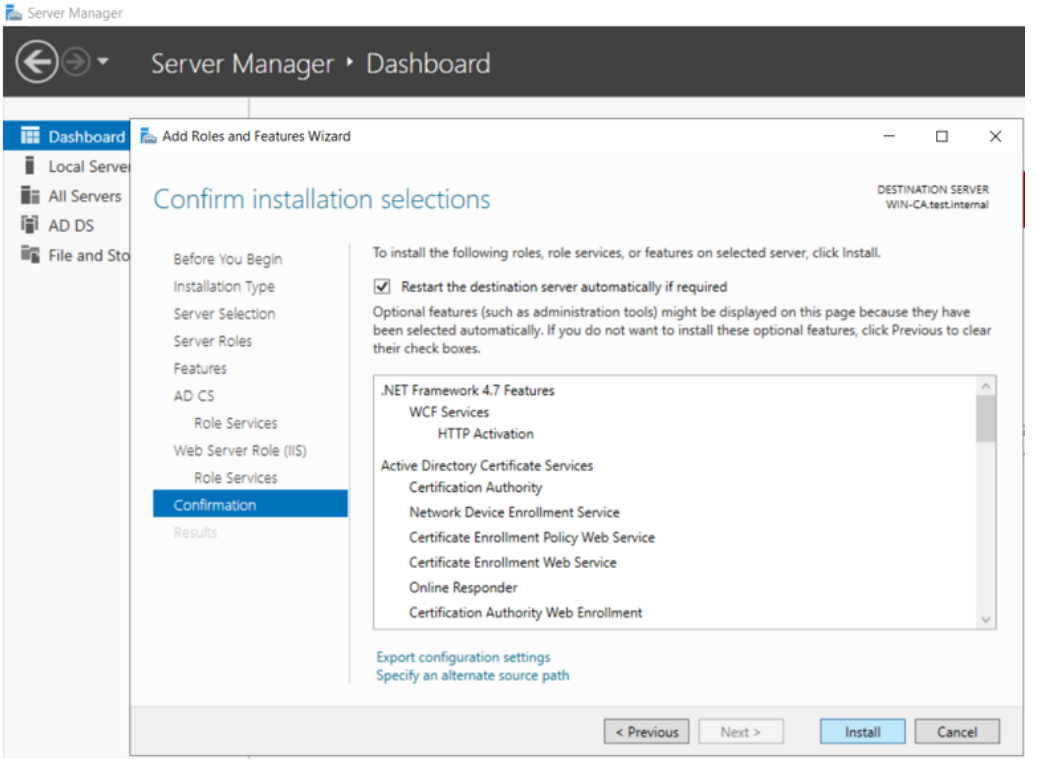
3. Fügen Sie die erforderlichen Rollen und Funktionen hinzu und integrieren Sie die Managementtools:



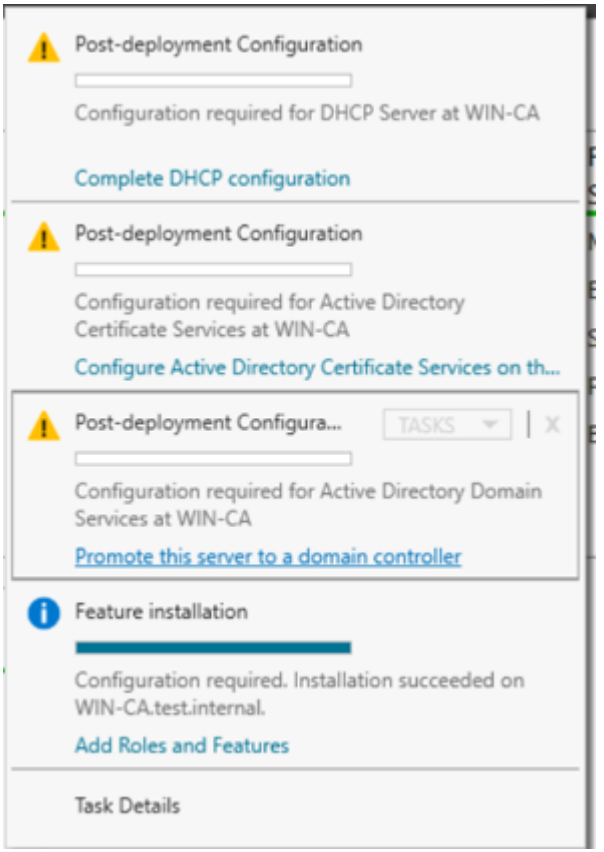
4. Wählen Sie die zu konfigurierenden Gerätedienste aus:



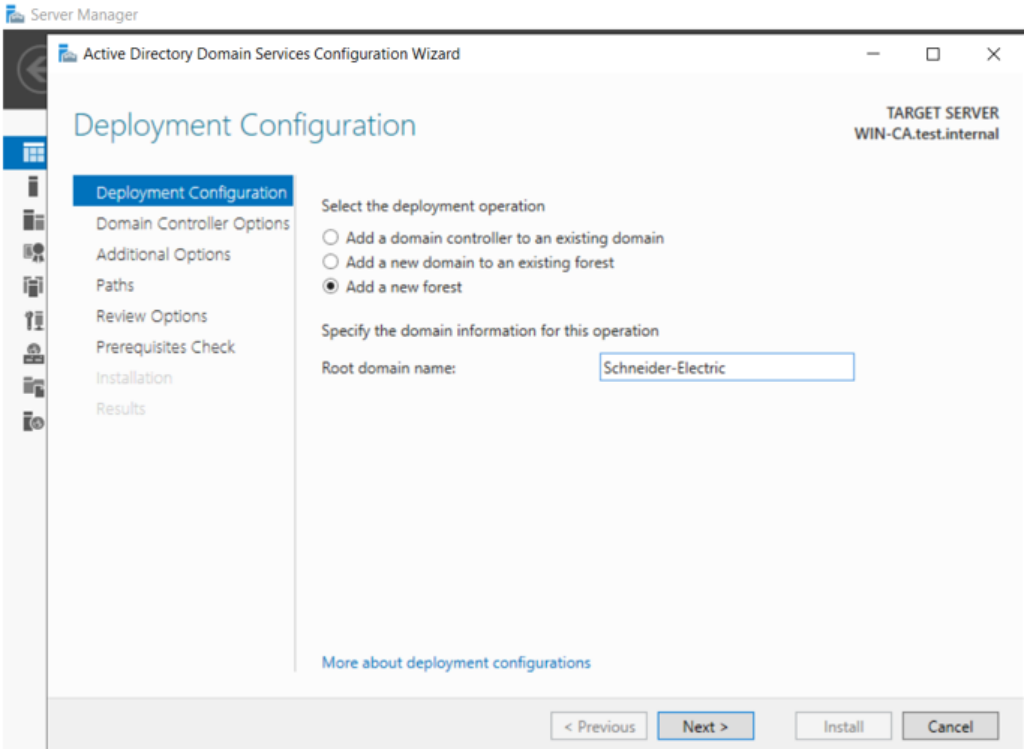
5. Bestätigen Sie die Installationsauswahl:



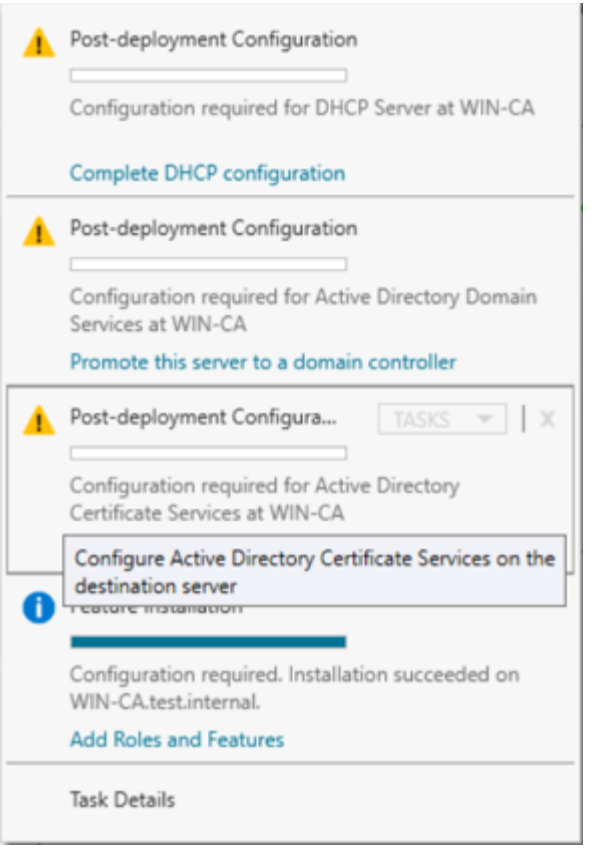
6. Klicken Sie auf **Installieren**. Server Manager zeigt den Installationsstatus an:



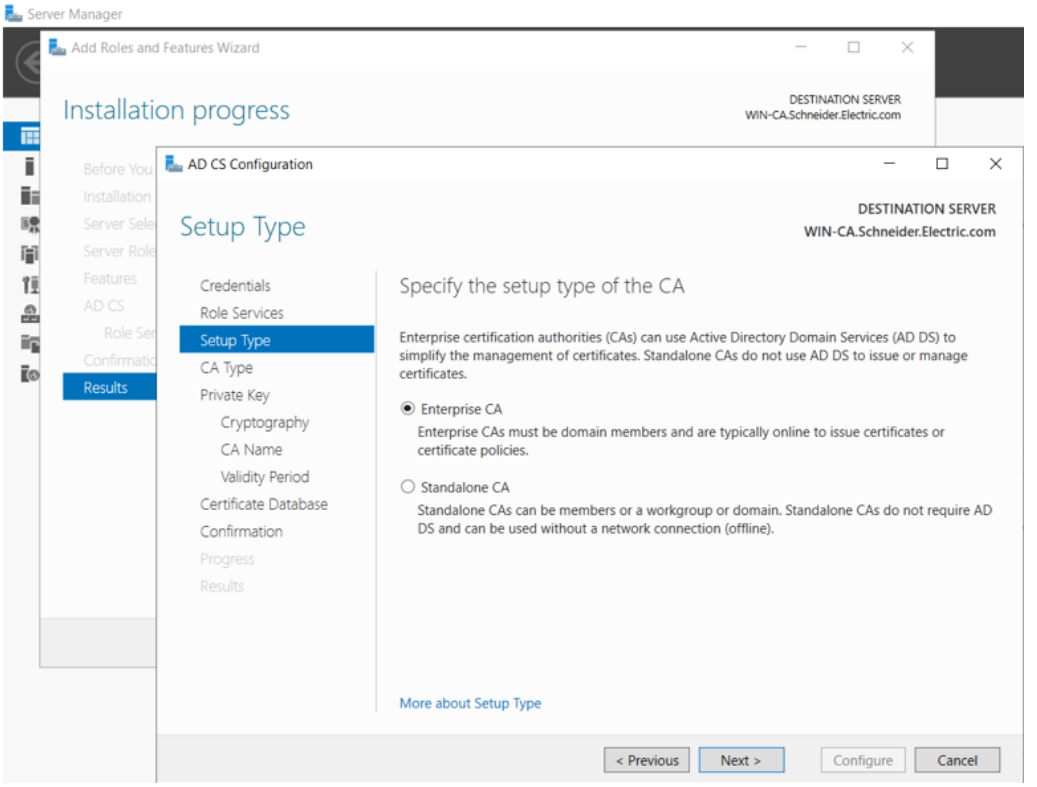
7. Wählen Sie den Implementierungsvorgang aus, indem Sie eine neue Gesamtstruktur erstellen oder zu einer bestehenden Gesamtstruktur hinzufügen und geben Sie die Domäne an:



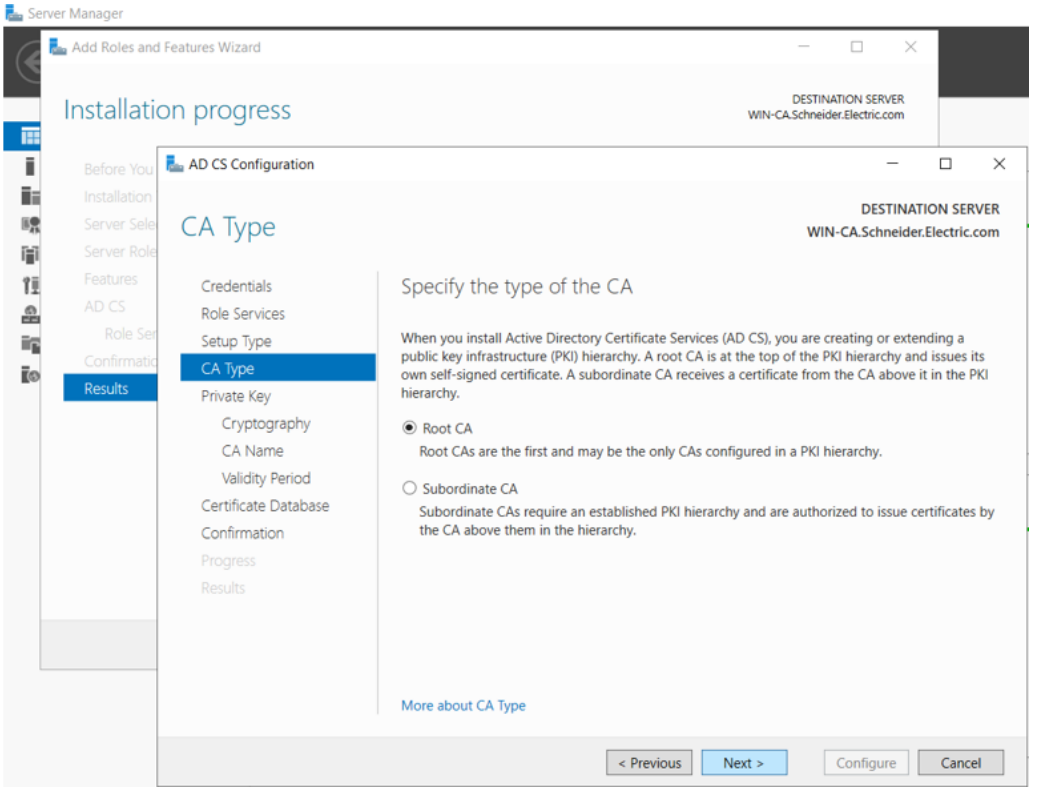
8. Server Manager zeigt die Auswahlmöglichkeiten an:



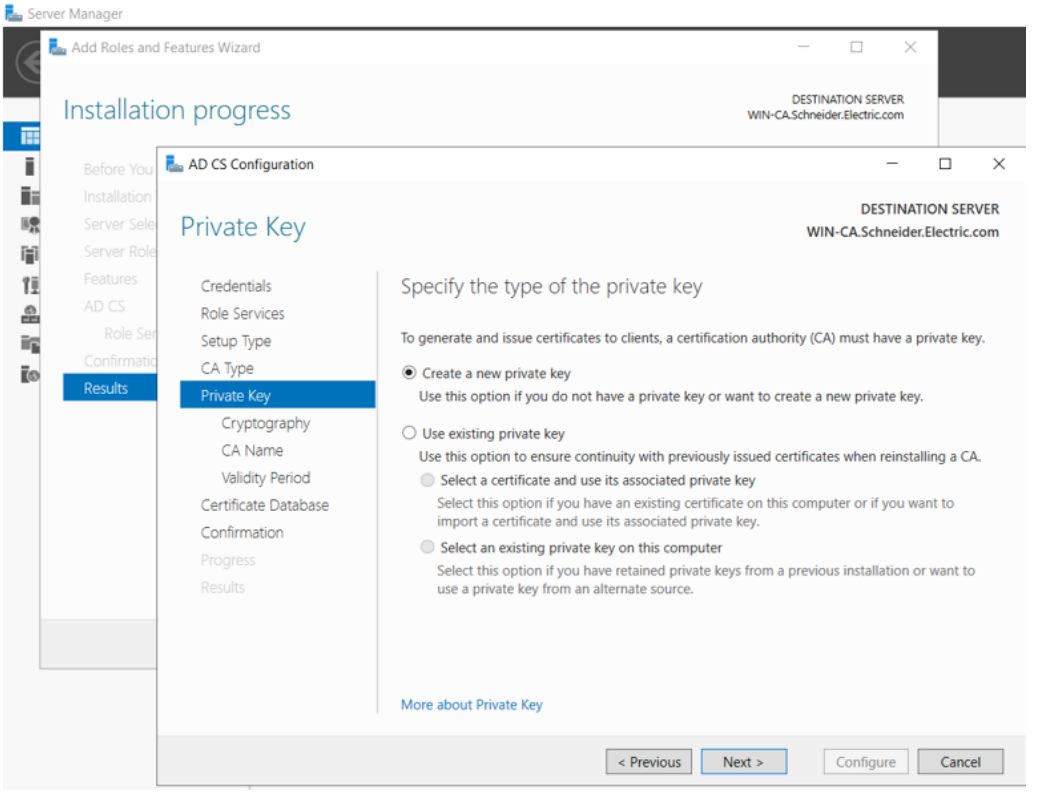
9. Geben Sie den Typ der einzurichtenden Zertifizierungsstelle an:



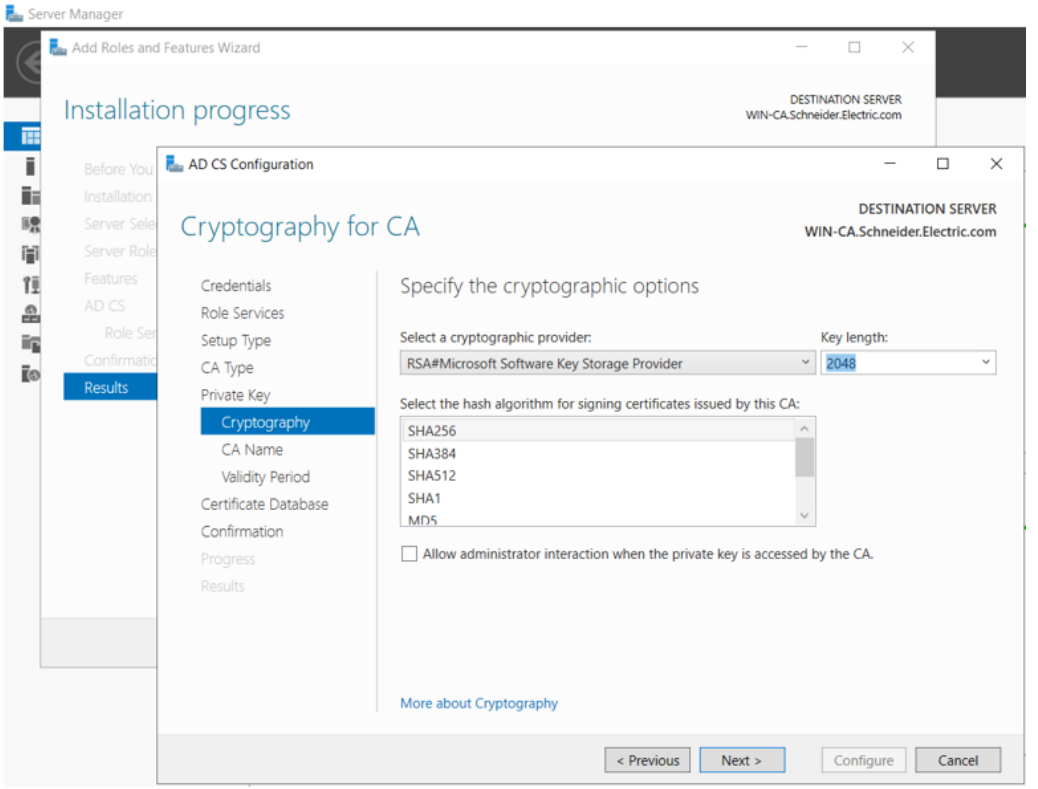
10. Geben Sie den Typ der Zertifizierungsstelle an:



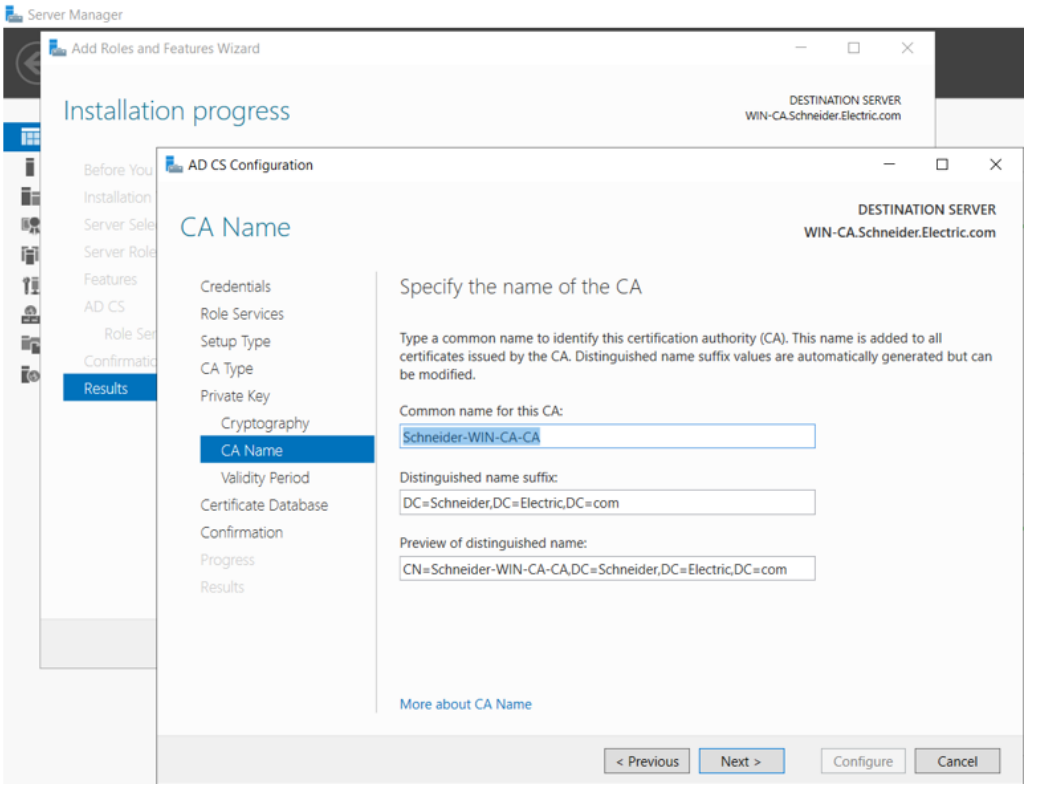
11. Geben Sie den Typ des privaten Schlüssels an:



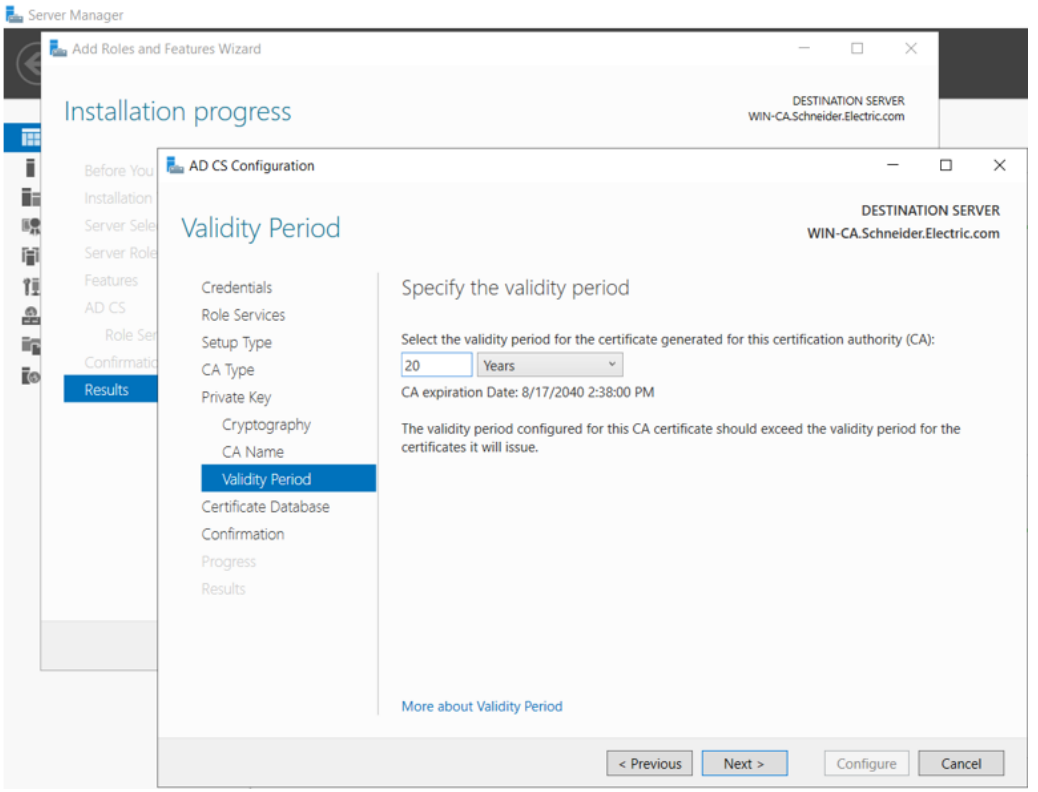
12. Nehmen Sie die kryptografische Auswahl vor:



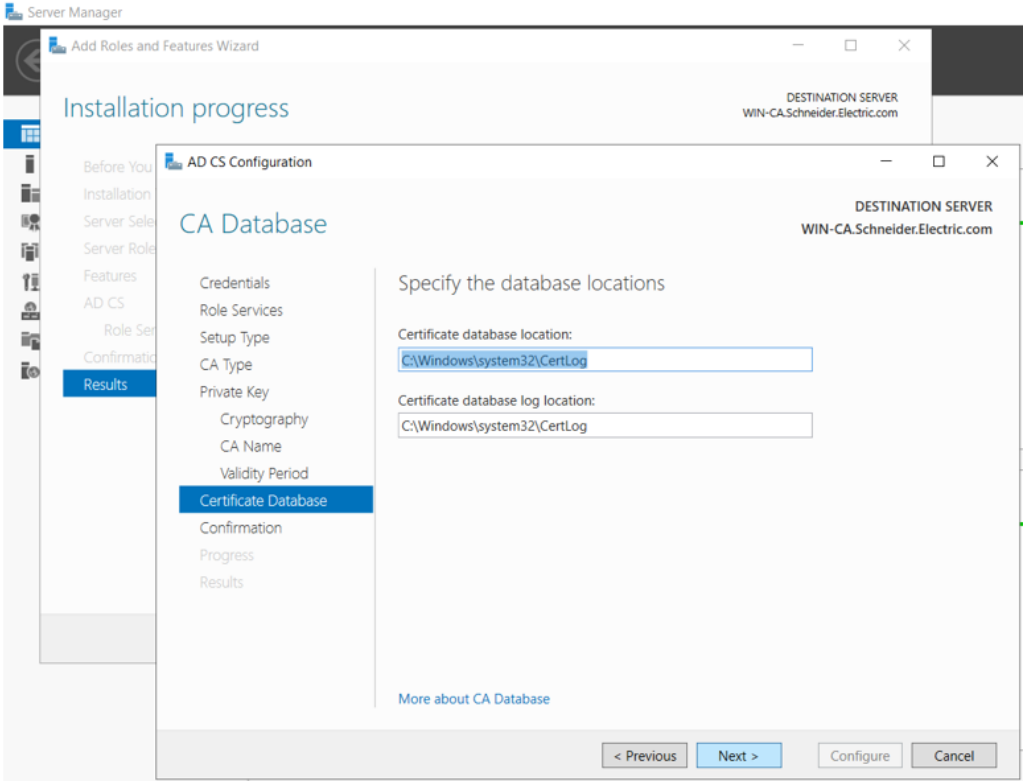
13. Nehmen Sie die Namensauswahl für die Zertifizierungsstelle vor:



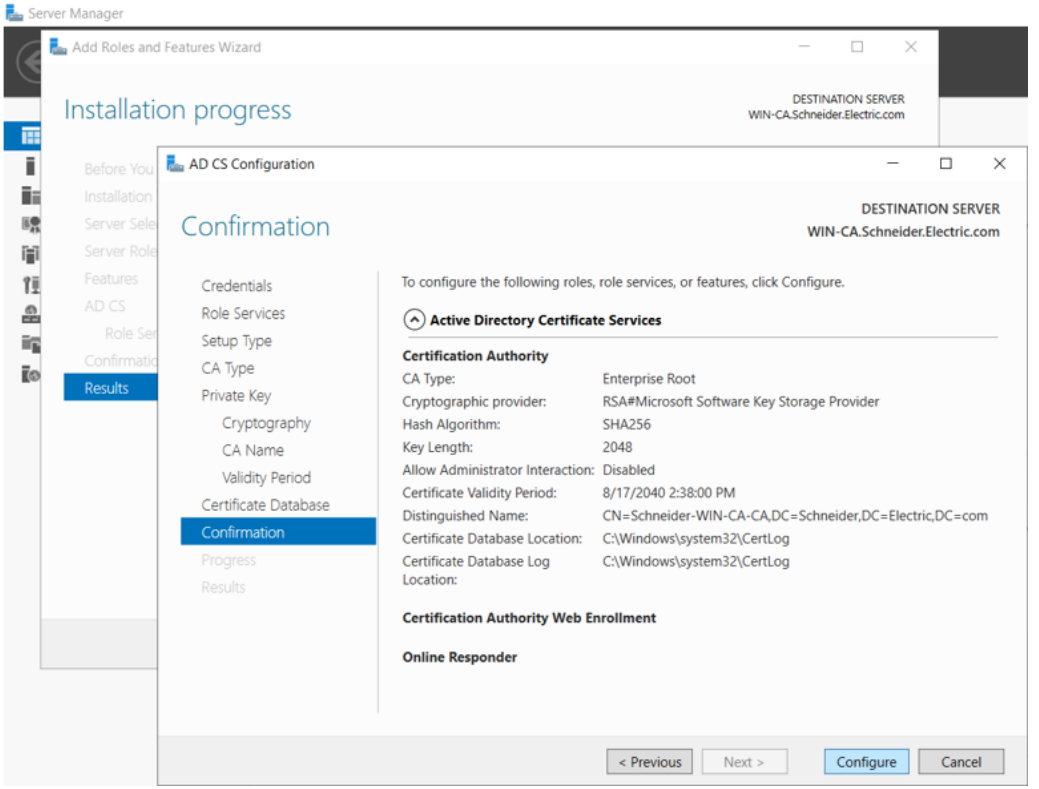
14. Geben Sie die Gültigkeitsdauer an. Der empfohlene Gültigkeitszeitraum eines CA-Zertifikats beträgt 5 Jahre:



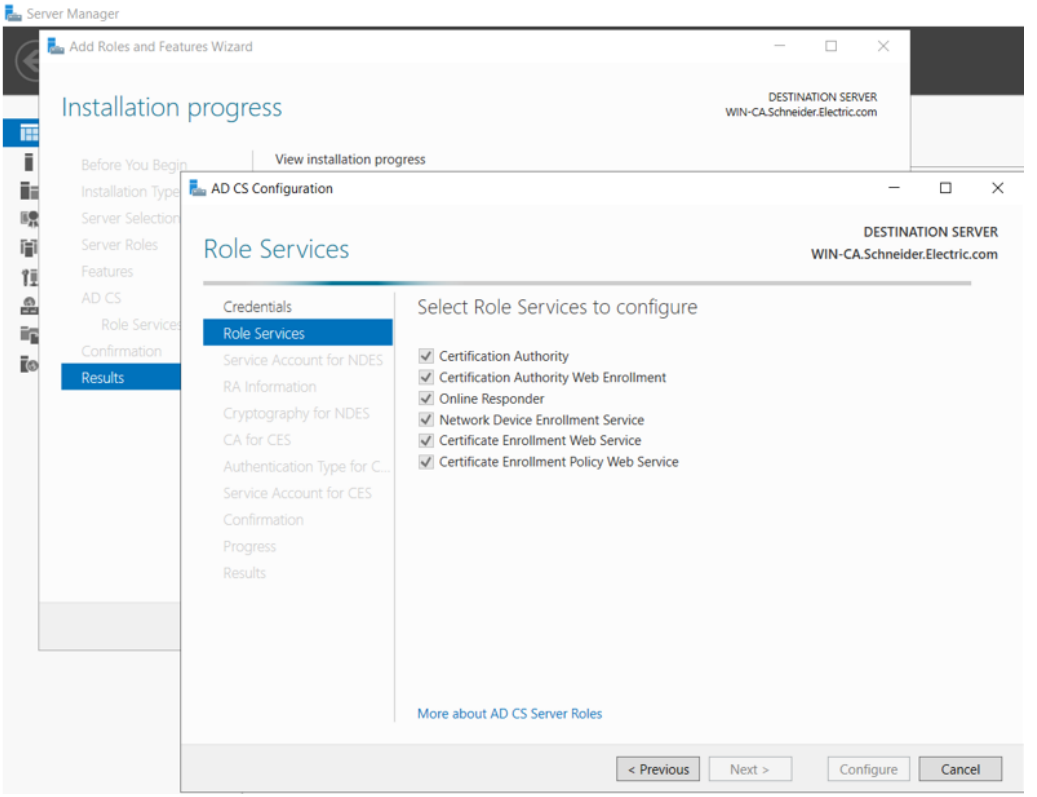
15. Geben Sie die Speicherorte der Zertifikatdatenbank und des Protokolls an:



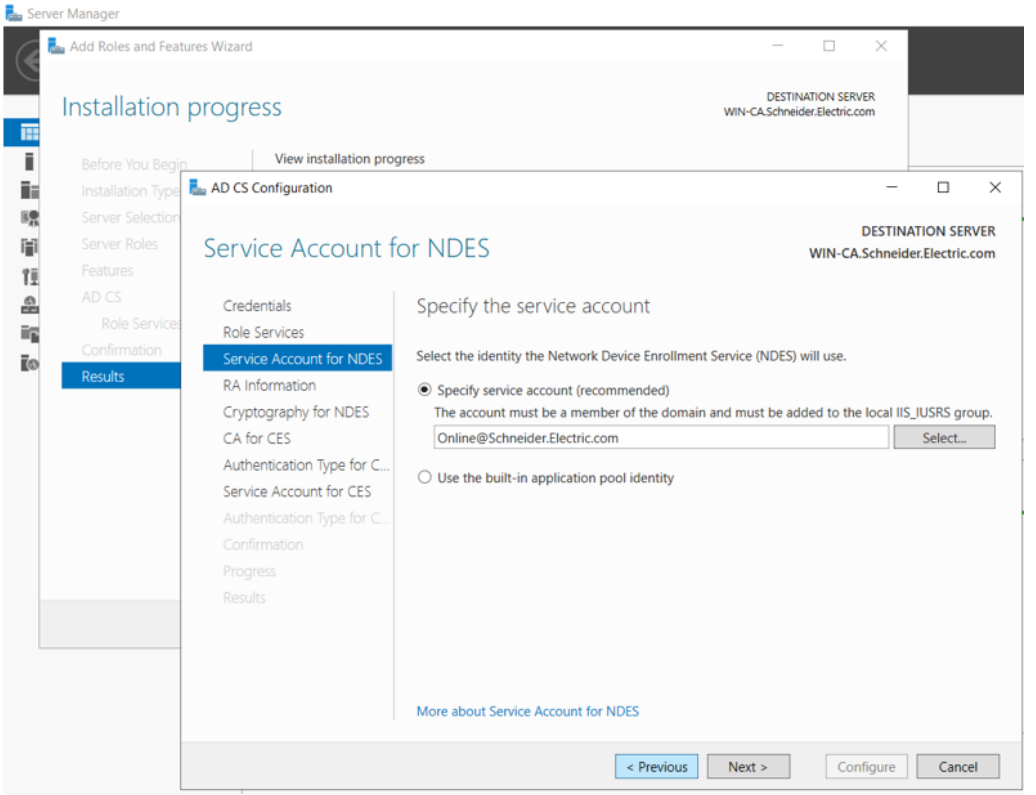
16. Bestätigen Sie die ausgewählten Active Directory-Zertifikatdienste und klicken Sie bei Bedarf auf **Konfigurieren**:



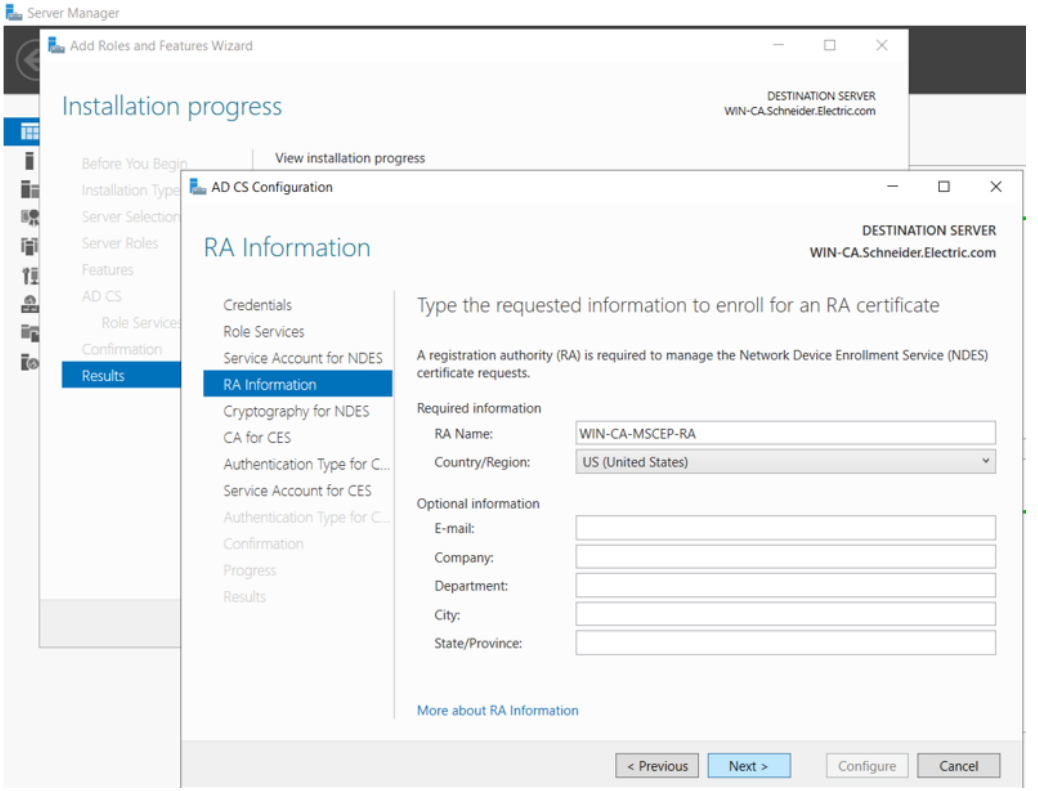
17. Wählen Sie die Rollendienste aus, die konfiguriert werden sollen:



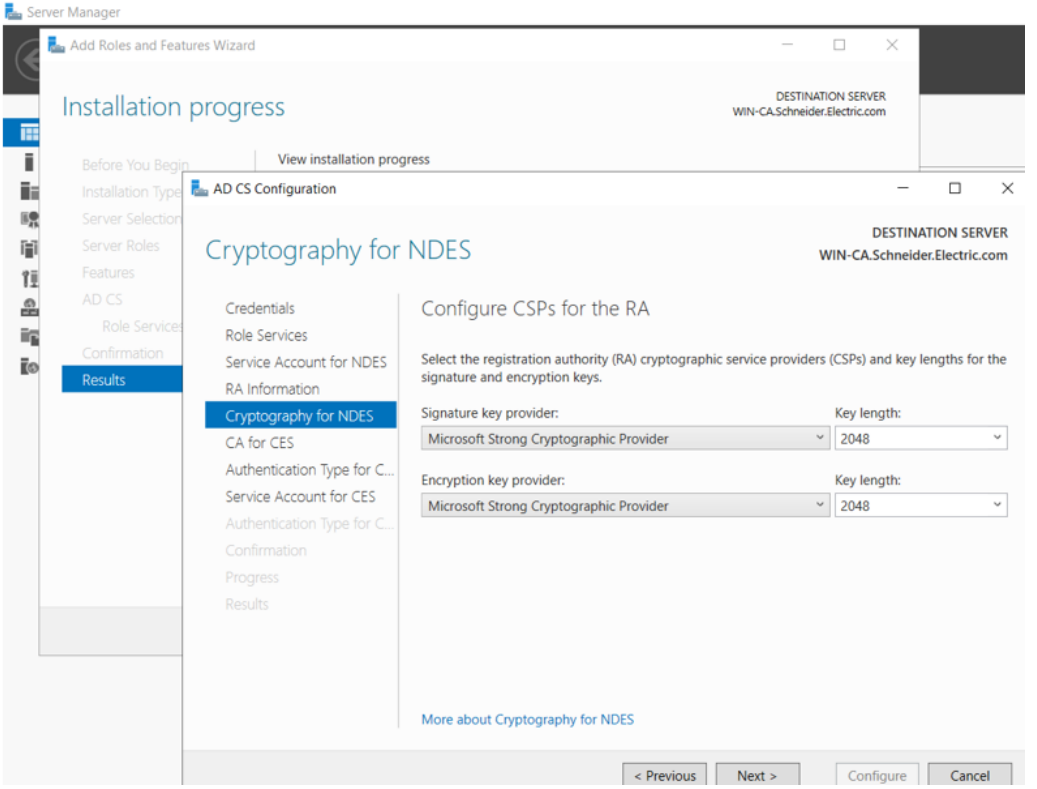
18. Geben Sie das Dienstkonto an:



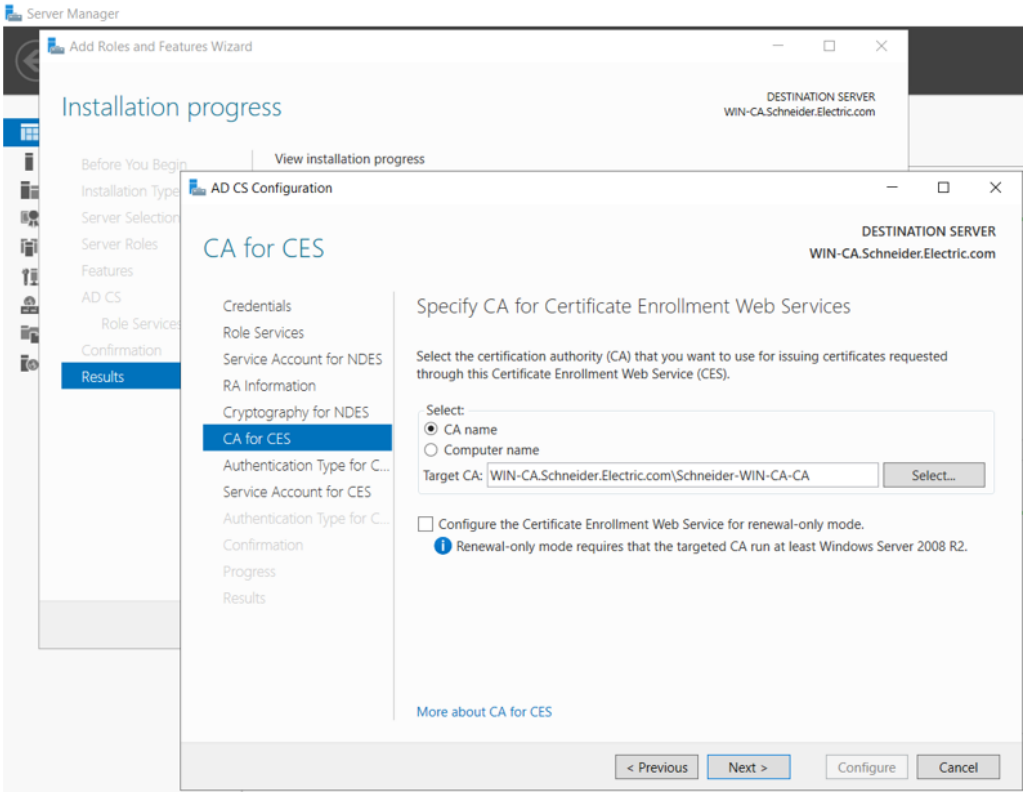
19. Geben Sie die Informationen ein, die für eine Zertifizierung durch die Registrierungsbehörde (RA) erforderlich:



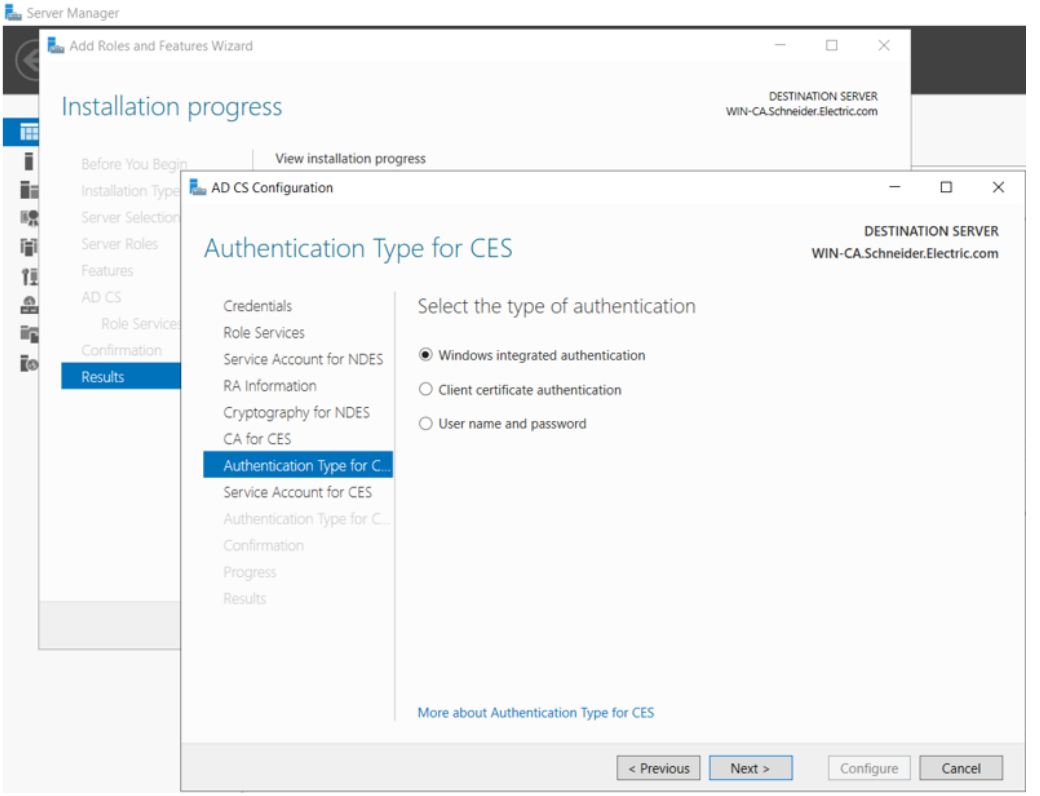
20. Wählen Sie die Verschlüsselungseinstellungen für die RA aus:



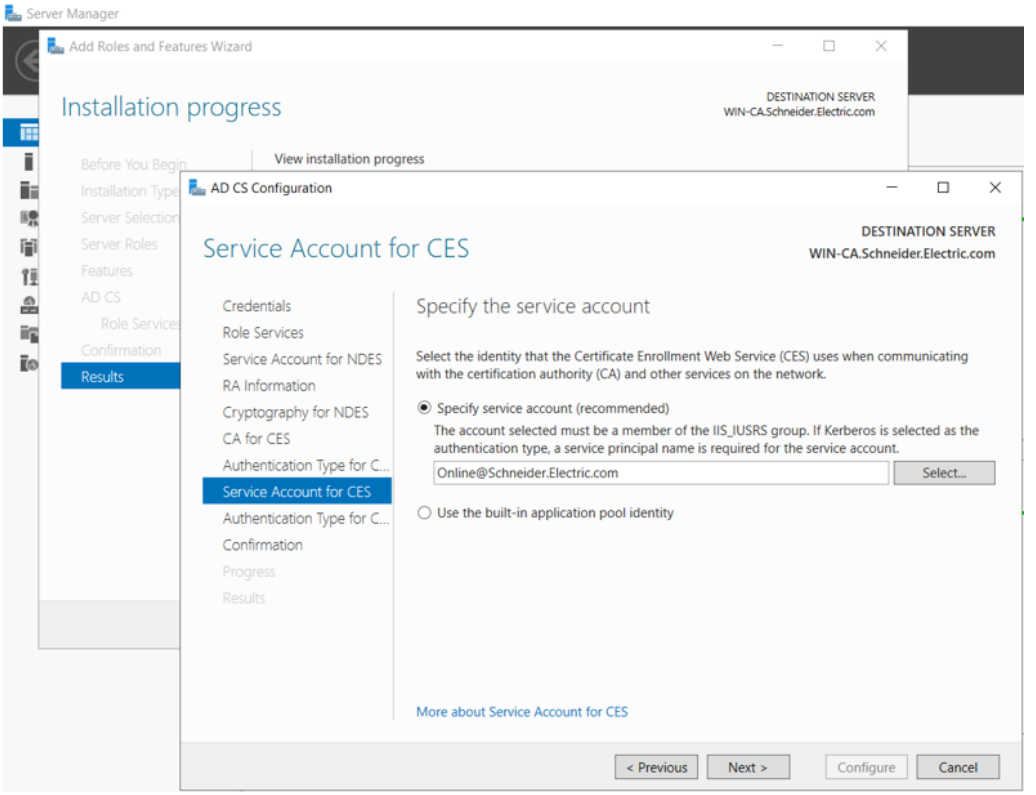
21. Geben Sie die Zertifizierungsstelle für Webdienste zur Zertifikatregistrierung an:



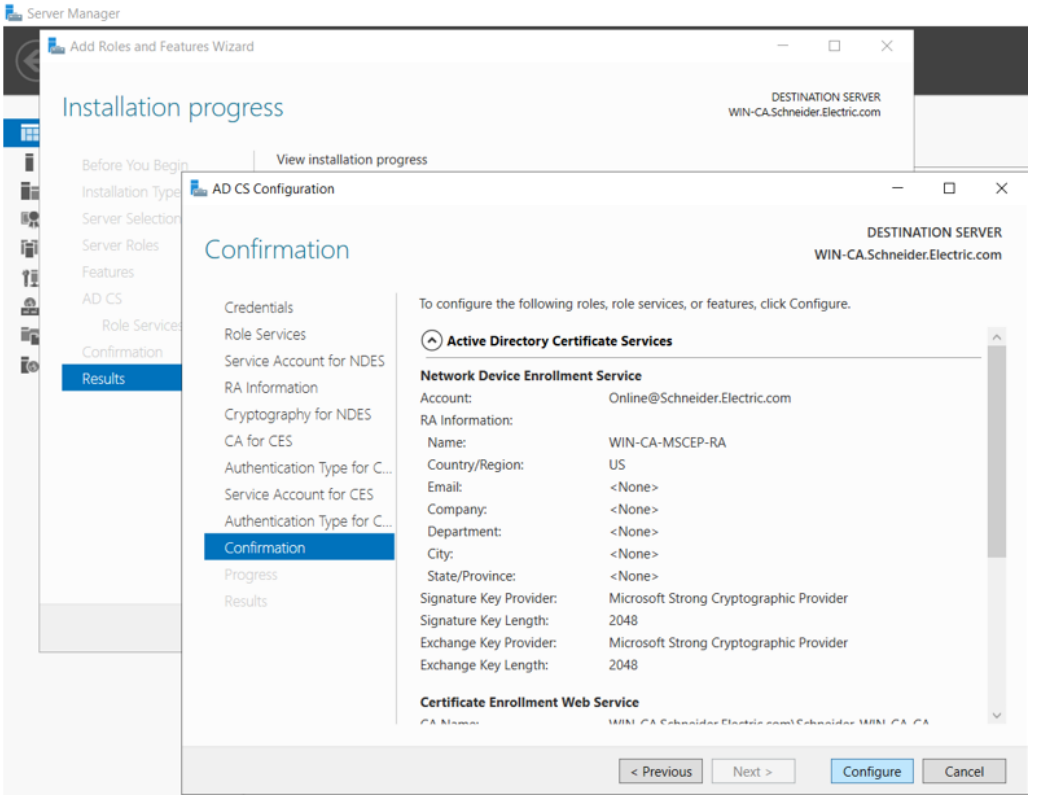
22. Wählen Sie einen Authentifizierungstyp aus:



23. Geben Sie das Dienstkonto an:



24. Bestätigen Sie die Rollen, Dienste und Funktionen und klicken Sie dann auf **Konfigurieren**:



Dadurch wird der ADCS-Setup 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.

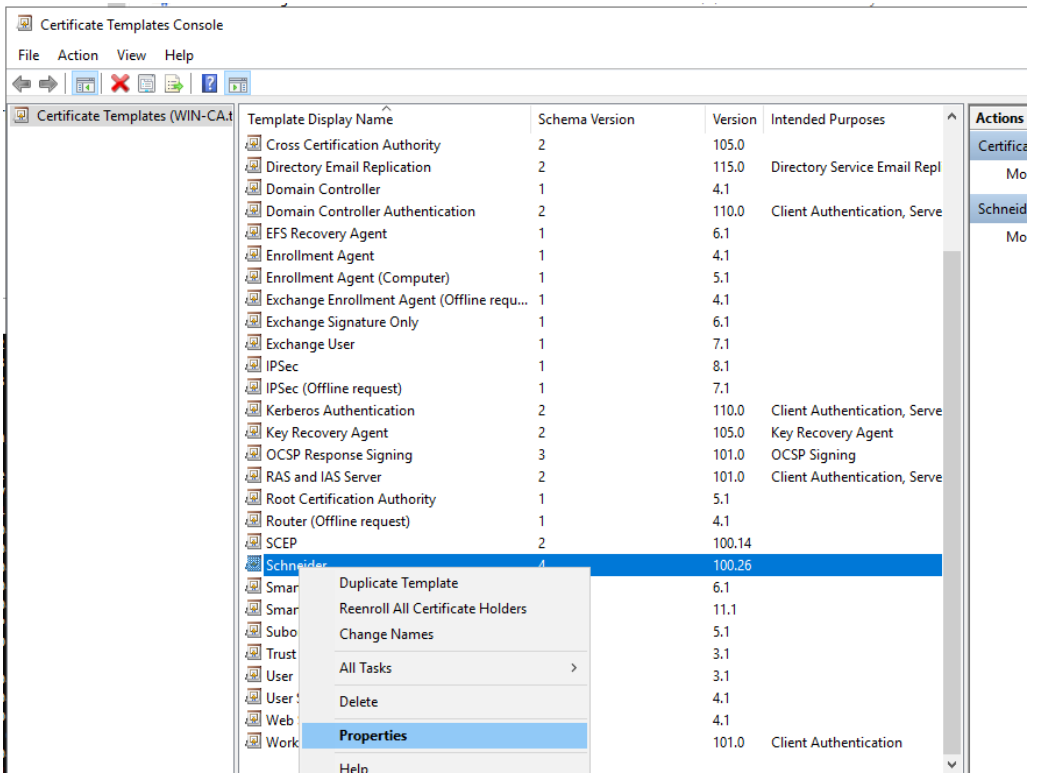
Gehen Sie vor wie folgt, um das Zertifikat zu übernehmen:

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...

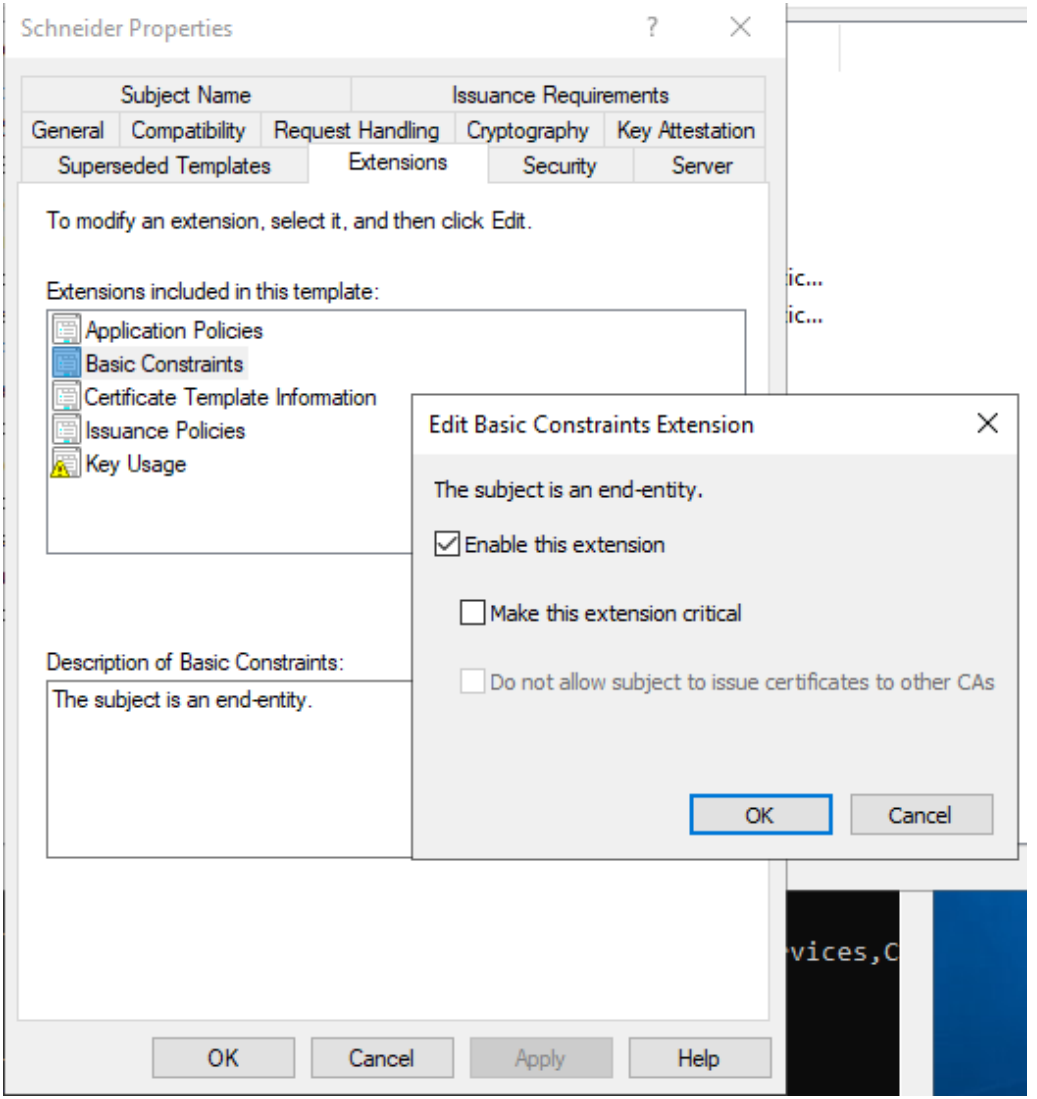
   Sie können diesen Ordner beispielsweise in das Verzeichnis „C:\Users\Administrator\Desktop\“ kopieren.
2. Starten Sie Microsoft Windows PowerShell als Administrator.
3. Navigieren Sie in PowerShell zu dem Ordner, in dem Sie das TemplatePackage platziert haben, z. B.:.

   ```
   > cd C:\Users\Administrator\Desktop\TemplatePackage
   ```
4. Führen Sie in PowerShell 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 **Properties** aus:



6. Öffnen Sie im Fenster **Schneider Properties** die Registerkarte **Extensions**, doppelklicken Sie auf **Basic Constraints**, wählen Sie im Dialogfeld **Edit Basic Constraints** die Option **Enable this extension** aus und klicken Sie auf **OK**:



Durchführen einer manuellen Registrierung

Informationen zur Durchführung dieser Aufgabe finden Sie unter Manuelle Zertifikatregistrierung, Seite 111.

Klicken Sie auf den in diesem 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

A

Architekturen 59

B

Betriebsmodus 25
BMENUA0100
  Beschreibung 16

C

CCOTF 61
Cybersicherheitsstatus-LED 139

D

DHCP-BOOTP
  M580-CPU 135
Diagnose
  Modbus 159
Diagnose^ 136
Drehschalter 20

F

Firmware
  Upgrade 171
Flaches Netzwerk
  Modulplatzierung 60

H

HTTPS
  Port 443 59

I

Inbetriebnahme 77–78
IP-Weiterleitung 96

K

Kompatibilität
  Modulfirmware im Vergleich zu den Control Expert-Softwareversionen 24
Konfiguration 84

L

LED
  Diagnose 136
LEDs
  Modul 21
  Steuerungsport-Verbindung 22

M

M580-CPU
  Sicherheitskonfiguration 135
Maximale Anzahl an Modulen pro Rack 61
Modulplatzierung
  Flaches Netzwerk 60

N

NTP
  Konfigurieren 128

P

Ports 16

R

READ_DDT 145

S

SNMP-Agent 131
Standards 23

T

T_BMENUA0100-DDT 140

T_CYBERSECIURITY_STATUS DDT 144
T_FW_VERSION DT 144
T_OPCUA_STATUS DDT 141
T_SERVICES_STATUS DDT 142
TFTP
  M580-CPU 135

W

Webseiten 84
  Startseite 89

Z

Zeitsynchronisation
  Konfigurieren 128
Zertifizierungen 23

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, ist es unerlässlich, dass Sie die in dieser Veröffentlichung gegebenen Informationen von uns bestätigen.

© 2022 Schneider Electric. Alle Rechte vorbehalten.

PHA83352.02