SIEMENS

SIMATIC NET

Industrial Ethernet - CloudConnect SIMATIC CC7

Betriebsanleitung

SIMATIC CloudConnect 712 (6GK1411-1AC00)
SIMATIC CloudConnect 716 (6GK1411-5AC00)

03/2023
C79000-G8900-C503-10

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ **GEFAHR**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **WARNUNG**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **VORSICHT**
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠ **WARNUNG**
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C503-10
Ⓟ 03/2023 Änderungen vorbehalten

Vorwort

VORSICHT

Lesen Sie das Handbuch vor dem Einsatz, um Verletzungen zu vermeiden.

Produkte

In diesem Dokument finden Sie Informationen zu folgenden Produkten:

SIMATIC CC712 / SIMATIC CC716
Hardware-Erzeugnisstand 1
Firmware-Version V2.1
Gateway zum Anschluss einer SIMATIC S7-, OPC UA- oder Modbus-Station an ein Cloud-System, OPC UA-Server für SIMATIC S7-Daten

Bild 1 SIMATIC CC716

Die MAC-Adresse des Geräts finden Sie unterhalb der Buchse für die Spannungsversorgung. Die Artikelnummer finden Sie unten auf der Gehäusefrontseite.

Den Hardware-Erzeugnisstand finden Sie auf der rechten Gehäuseseite als Platzhalter "X". "X 2 3 4" beispielsweise zeigt den Hardware-Erzeugnisstand 1 an.

Gültigkeit

Das Handbuch ist gültig für folgende Produkte:

Produktname	Artikelnummer	Funktionen
SIMATIC CloudConnect 712	6GK1411-1AC00	Anschluss von 1 Prozess-Station über Ethernet
SIMATIC CloudConnect 716	6GK1411-5AC00	Anschluss von bis zu 7 Prozess-Stationen Zusätzlich: 1 Digitaleingang, 1 Digitalausgang, PROFIBUS DP-Anschluss

Einzelne Passagen oder Kapitel, die nur für das CC716 gültig sind, sind mit der Kurzform des Geräts gekennzeichnet.
Beispiel: "PROFIBUS (CC716)"

Zweck des Handbuchs

Dieses Handbuch beschreibt die Eigenschaften der Module und zeigt Anwendungsbeispiele. Es unterstützt Sie bei Montage, Anschluss und Inbetriebsetzung der Module.

Die erforderlichen Projektierungsschritte werden beschrieben. Weiterhin finden Sie Hinweise für den Betrieb und zu Diagnosemöglichkeiten.

Vorausgesetzte Kenntnisse

Für Montage, Inbetriebnahme und Betrieb des Moduls werden Kenntnisse auf folgenden Gebieten vorausgesetzt:

- Datenübertragung über Ethernet / Internet / PROFIBUS
- Cloud-Systeme, MQTT
- OPC UA
- Automatisierungstechnik

Terminologie: Bezeichnungen und Abkürzungen

In diesem Dokument finden Sie folgende Begriffe und Abkürzungen:

- **CC712**

  Kurzform für das Gateway SIMATIC CloudConnect 712

- **CC716**

  Kurzform für das Gateway SIMATIC CloudConnect 716

- **Gerät / Gateway / Modul**

  Bezeichnungen für beide Produkte "SIMATIC CC712" und "SIMATIC CC716"

  Falls Inhalte im Handbuch nur für eine der beiden Gerätevarianten gültig ist, wird dies explizit erwähnt.

- **Station**

  Prozess-Station (SIMATIC S7 / OPC UA-Station mittels OPC UA-Client / Modbus)

- **WBM**

  Web Based Management

  Webseiten des Geräts für Projektierungs- und Diagnosedaten

- **API**

  Application Programming Interface

  HTTP-basierte AP-Schnittstelle zur Konfiguration des WBM

- **DB**

  Datenbaustein einer SIMATIC-CPU

Neu in dieser Ausgabe

- Unterstützung IEC62443 SL1
- Erzeugung von Elliptic curve-Zertifikaten
- Neustart und Herunterfahren per WBM
- Eigenes Zeitstemepel-Nutzdaten-Format projektierbar
- IPv6-Präfix Länge einstellbar

Abgelöste Ausgabe

Ausgabe 12/2022

Aktuelle Handbuchausgabe und Applikationsbeispiel im Internet

Die aktuelle Ausgabe dieses Handbuchs finden Sie auf den Internet-Seiten des Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621/man)

Ein Applikationsbeispiel finden Sie hier:
Link: (https://support.industry.siemens.com/cs/ww/de/view/109766675)

Querverweise

In diesem Dokument werden Querverweise zu anderen Kapiteln verwendet.

Um nach dem Sprung eines Querverweises wieder zurück zur Ausgangsseite zu gelangen, unterstützen einige PDF-Reader den Befehl <Alt>+<Links-Pfeil>.

Lizenzbedingungen

Hinweis

Open Source Software

Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

Die Lizenzbedingungen finden Sie als ladbare Datei auf den WBM-Seiten des Geräts. Die Beschreibung zum Öffnen und Laden der Lizenzbedingungen finden Sie im Kapitel Benutzerdaten für das erste Anmelden am WBM (Seite 69).

Die Datei mit den Lizenzbedingungen zur Open Source Software finden Sie unter dem folgenden Namen:

- OSS_CloudConnect_99.html

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter:
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter:
https://www.siemens.com/cert (https://www.siemens.com/cert)

Gerät defekt

Bitte senden Sie das Gerät im Fehlerfall an Ihre Siemens-Vertretung zur Reparatur ein. Eine Reparatur vor Ort ist nicht möglich.

Recycling und Entsorgung

Das Produkt ist schadstoffarm, recyclingfähig und erfüllt die Anforderungen der WEEE-Richtlinie 2012/19/EU "Elektro- und Elektronik-Altgeräte".

Entsorgen Sie das Produkt nicht bei öffentlichen Entsorgungsstellen. Für ein umweltverträgliches Recycling und die Entsorgung Ihres Altgeräts wenden Sie sich an einen zertifizierten Entsorgungsbetrieb für Elektronikschrott oder an Ihren Siemens-Ansprechpartner.

Beachten Sie die örtlichen Bestimmungen.

Informationen zur Produktrückgabe finden Sie auf den Internetseiten des Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/de/view/109479891)

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar im Internet unter folgender Adresse:

Link: (https://support.industry.siemens.com/cs/ww/de/view/50305045)

Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC_support_99.pdf" auf den Internet-Seiten des Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/de/view/38652101)

Inhaltsverzeichnis

Security-Empfehlungen

1

1.1 Security-Empfehlungen

ACHTUNG
Informationssicherheit Verbinden Sie sich mit dem Gerät und ändern Sie das Standard-Passwort für den werksseitig voreingestellten Benutzer "admin", bevor Sie das Gerät betreiben.

Um das Gerät gegen Security-Bedrohungen zu härten und unbefugten Zugriff auf Gerät und/oder Netzwerk zu verhindern, beachten Sie folgende Security-Empfehlungen.

Allgemein

- Prüfen Sie regelmäßig Konfiguration und Umgebungsbedingungen des Geräts um sicherzustellen, dass diese Empfehlungen und/oder andere interne Sicherheitsrichtlinien eingehalten werden.
- Bewerten Sie die Sicherheit Ihres Standorts und verwenden Sie ein Zellenschutzkonzept mit geeigneten Produkten.
- Informieren Sie sich regelmäßig über Sicherheits-Updates der Produkte und wenden Sie diese an.
- Informieren Sie sich regelmäßig über Neuigkeiten auf den Siemens-Internetseiten.
  - Hier finden Sie Informationen zu Industrial Security:
    Link: (http://www.siemens.com/industrialsecurity)
  - Eine Auswahl an Dokumenten zum Thema Netzwerksicherheit finden Sie hier:
    Link: (https://support.industry.siemens.com/cs/ww/de/view/92651441)
- Halten Sie die Software aktuell. Verwenden Sie die jeweils aktuelle Software-Version des Geräts.

  Hinweise auf Produktneuigkeiten und neue Software-Versionen finden Sie unter folgender Adresse:
  Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621/pm)
- Wenn Siemens Sicherheitslücken (Security Incidents) in den Produkten feststellt und behebt, wird dies in Security Advisories veröffentlicht. Sie finden die Dokumente für CC7 auf der folgenden Internseite der Siemens AG:

  Link:
  (https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications)

- Das Gateway verfügt über zwei Schnittstellen zur Netztrennung und Durchsetzung des Zellschutzkonzepts:
  - Prozess-Schnittstelle (P2)
    Die Schnittstelle (P2) dient dem Anschluss an das Subnetz der Prozess-Stationen und dem Zugriff auf das WBM der Baugruppe zur Projektierung. Dieses Netzwerk wird als internes, geschütztes Netzwerk betrachtet.
  - Cloud-Schnittstelle (P1)
    Die Schnittstelle (P1) dient dem Anschluss an das Internet oder an einen Router, über den der Broker oder das Netz mit externen OPC UA-Clients erreichbar ist. Dieses Netzwerk wird als externes Netzwerk betrachtet. Der Übergang in ungeschützte Netze wie z. B. dem Internet muss durch eine separate Firewall geschützt werden.

  Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Von der Cloud-Schnittstelle (P1) kann nicht mittels IP-Routing auf Geräte am internen Netzwerk an der Prozess-Schnittstelle (P2) zugegriffen werden. Ein IP-Routing wird nicht unterstützt.

- Es besteht auch die Möglichkeit, die Prozess-Stationen und den Cloud-Broker im selben Subnetz zu betreiben. In diesem Fall liegt der Cloud-Broker dann ebenso wie die Prozess-Stationen im internen, geschützten Netzwerk. Dieser Anwendungsfall ist für selbst administrierte Broker vorgesehen und sollte nicht für externe Cloud-Systeme im Internet wie z. B. MindSphere, AWS, Azure usw. genutzt werden.
  Hierzu wird in Kapitel Schnittstellen-Konfiguration (Seite 76) die Option "Cloud-Schnittstelle im selben Subnetz" angeboten. Wenn die Option aktiviert ist, wird die ungenutzte Schnittstelle P1 abgeschaltet und ein Zugriff auf das Gateway über diese ungenutzte Schnittstelle verhindert.
- Setzen Sie zur Anbindung des internen geschützten Netzwerks an externe Netzwerke eine Firewall ein. Konfigurieren Sie diese mit restriktiven Regeln.
- Für den Betrieb von unsicherer Infrastruktur wird keine Produkthaftung übernommen.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk zusätzliche Security-Komponenten die einen verschlüsselten VPN-Tunnel (IPsec, OpenVPN) bereitstellen.
- Trennen Sie Verbindungen ordnungsgemäß (z. B. Abmeldung im WBM).
- Prüfen Sie die Benutzerdokumentation anderer Siemens-Produkte, die zusammen mit dem Gerät verwendet werden, auf weitere Sicherheitsempfehlungen.

Physischer Zugang

Beschränken Sie den physischen Zugang zu Geräten auf qualifiziertes Personal, da das steckbare Speichermedium sensible Daten enthalten kann.

Security-Funktionen des Produkts

- Bedenken Sie, mit welchen Diensten Sie über öffentliche Netze einen Zugriff auf Prozess-Stationen ermöglichen möchten.
- Dieses Produkt darf nicht ohne zusätzlich vorgeschaltete Schutzeinrichtungen am ungeschützten/vertrauenswürdigen Netzwerken (z. B. am Internet) betrieben werden.

- Nutzen Sie die Möglichkeiten der Security-Einstellungen in der Projektierung des Produkts:
  - Aktivieren Sie die Security-Funktionen des Produkts und der beteiligten Geräte.
  - Verwenden Sie sichere Protokollvarianten (siehe unten).
- Die Konfigurationsdateien können mit und ohne Benutzerdaten, Passwörter, Zertifikaten und privaten Schlüssel gespeichert werden. Die Ablage von Konfigurationsdateien die sensible Benutzerdaten enthalten, erfolgt dabei immer verschlüsselt. Optional kann zusätzlich auch ein Passwort gegen unbefugte Benutzung vergeben werden.
  Achten Sie darauf, dass die Konfigurationsdateien außerhalb des Geräts ordnungsgemäß geschützt sind. Sie können die Dateien an einem sicheren Ort speichern und sie über sichere Kommunikationskanäle übertragen.
- Nutzen Sie einen zentralen Logging-Server, um Änderungen und Zugriffe zu protokollieren. Betreiben Sie Ihren Logging-Server innerhalb des geschützten Netzwerkbereichs und prüfen Sie regelmäßig die Logging-Informationen.
- Wenn Sie Kommunikation mit Geräten benötigen, die Verfahren für die verschlüsselte Kommunikation verwenden, die aufgrund bekannter Schwachstellen nicht mehr empfohlen werden, können Sie die Legacy-Cipher-Unterstützung je nach Bedarf aktivieren oder deaktivieren, siehe Kapitel MQTT-Konfiguration (Seite 111) bzw. HTTP-Profile (Seite 115).

Authentifizierung und Benutzer

Hinweis

Zugänglichkeitsrisiko - Gefahr des Datenverlusts

Verlieren Sie die Passwörter für das Gerät nicht. Der Zugriff auf das Gerät kann nur durch Zurücksetzen des Geräts auf die Werkseinstellungen wiederhergestellt werden, wodurch sämtliche Konfigurationsdaten entfernt werden.

- Ersetzen Sie die Standardpasswörter für alle Benutzerkonten bevor Sie das Gerät einsetzen.
- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern. Nutzen Sie aktuelle Empfehlungen zur Definition starker Passwörter, z. B. vom Bundesamt für Sicherheit in der Informationstechnik (Link: (https://www.bsi.bund.de)).
- Verwenden Sie Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter (wie Passwort1, 123456789, abcdefgh) oder sich wiederholende Zeichen (wie abcabc). Diese Empfehlung gilt auch für auf dem Gerät konfigurierte symmetrische Passwörter/Schlüssel.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.
- Verwenden Sie ein Passwort nicht für verschiedene Benutzer und Systeme.
- Bewahren Sie Passwörter an einem sicheren Ort (nicht online) auf, damit Sie sie bei Verlust zur Hand haben.
- Ein Passwort muss geändert werden, wenn es unbefugten Personen bekannt geworden ist oder der Verdacht dazu besteht.

Zertifikate und Schlüssel

- Im Gerät ist ein voreingestelltes SSL/TLS-Zertifikat für den Zugriff auf das WBM vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes höherwertiges Zertifikat mit Schlüssel.
  Verwenden Sie ein Zertifikat, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Ändern Sie bei Verdacht auf eine Sicherheitsverletzung sofort alle Zertifikate und Schlüssel.
- Verifizieren Sie Zertifikate anhand des Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern. Verwenden Sie hierzu einen zweiten, sicheren Übertragungsweg.
- Bevor Sie das Gerät zur Reparatur an Siemens zurückschicken, ersetzen Sie die aktuellen Zertifikate und Schlüssel durch temporäre Wegwerfzertifikate und -schlüssel, die bei der Rückkehr des Geräts zerstört werden können.

Protokolle

Sichere und unsichere Protokolle

- Vermeiden oder deaktivieren Sie unsichere Protokolle und Dienste, wie z. B. HTTP oder NTP.

  Diese Protokolle sind aus historischen Gründen verfügbar, jedoch nicht für einen sicheren Einsatz gedacht. Setzen Sie unsichere Protokolle auf dem Gerät mit Bedacht ein.
- Aktivieren Sie nur Protokolle, die Sie für den Einsatz des Systems benötigen.
- Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle und Dienste:
  - Syslog
  - DHCP-Optionen 66/67
  - S7
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzvorkehrungen gesichert ist.
  - Das Protokoll NTP bietet mit NTP (secure) eine sichere Alternative.
  - Das Protokoll HTTP bietet mit HTTPS eine sichere Alternative.
  - Eine OPC UA-Station mit aktiver Verschlüsselung bietet eine sichere Alternative zur unverschlüsselten S7-Station.
- Beschränken Sie die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- Wenn Sie unsichere Protokolle und Dienste benötigen, betreiben Sie diese nur innerhalb eines geschützten Netzwerkbereichs.

Außerbetriebnahme

- Um zu verhindern, dass unbefugte Personen an vertrauliche Daten im Gerätespeicher gelangen, nehmen Sie das Gerät ordnungsgemäß außer Betrieb.
- Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück. Setzen Sie auch das Speichermedium auf Werkseinstellungen zurück.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Hinweis zum Firmware-/Software-Support

Informieren Sie sich regelmäßig über neue Firmware-/Software-Versionen oder Sicherheits-Updates und wenden Sie diese an. Ab der Veröffentlichung einer neuen Version werden Vorgängerversionen nicht mehr unterstützt und nicht gewartet.

1.2 Ports

Server-Ports

Die folgende Tabelle gibt Ihnen einen Überblick über die offenen Ports in diesem Gerät.

- **Protokoll / Funktion**

  Protokolle, die das Gerät unterstützt.
- **Portnummer (Protokoll)**

  Portnummer, die dem Protokoll zugeordnet ist.
- **Voreinstellung des Ports**
  - Offen

    Der Port ist zu Beginn der Projektierung offen.
  - Geschlossen

    Der Port ist zu Beginn der Projektierung geschlossen.
- **Port konfigurierbar**

  Gibt an, ob die Portnummer im WBM einstellbar ist.
- **Authentifizierung**

  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet oder ob eine Authentifizierung konfiguriert werden kann.
- **Verschlüsselung**

  Gibt an, ob die Übertragung verschlüsselt ist oder ob die Verschlüsselung konfiguriert werden kann.

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Port konfigurierbar	Authentifizierung	Verschlüsselung
HTTP [1) 2)]	80 (TCP)	Offen	Ja	Nein	Nein
HTTPS [2)]	443 (TCP)	Offen	Ja	Ja	Ja
OPC UA-Server-Port	4840 (TCP)	Geschlossen	Ja	Ja, wenn Security aktiviert ist.	Ja, konfigurierbar

1) Wird in Werkseinstellungen auf HTTPS umgeleitet.

2) Protokoll kann in Werkseinstellungen nur an der Prozess-Schnittstelle (P2) genutzt werden.

Client-Ports

Achten Sie darauf, in Ihrem Projektierungs-PC den Port 443 (HTTPS) sowie im Subnetz zur Cloud in zwischengeschalteten Routern/Gateways die benötigten Client-Ports der verwendeten Dienste in der jeweiligen Firewall freizuschalten.

Dies können sein:

- Broker-Port
  - MQTT ungesichert: 1883 (TCP)
  - MQTT über TLS: 8883 (TCP)
  - HTTP: 80 (TCP)
  - HTTPS: 443 (TCP)

  Die Portnummern sind im WBM einstellbar.
- OPC UA-Client / 4840 (TCP)

  Die Portnummer ist im WBM einstellbar.
- NTP / 123 (UDP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- Syslog / 514 (UDP)

  Die Portnummer ist im WBM einstellbar.
- Modbus/TCP / 502 (TCP)

  Die Portnummer ist im WBM einstellbar.
- S7 /102 (TCP)

Vorgesehene Betriebsumgebung 2

2.1 Anwendung

Anwendungen des Gateways

Die Gateways CC712 und CC716 sind für die Anbindung von Prozess-Stationen in geschützten Automatisierungszellen an interne oder externe Cloud-Systeme über MQTT bzw. HTTP und/oder den Anschluss von externen OPC UA-Clients konzipiert.
Unterstütze Prozess-Stationen, Cloud-Systeme und OPC UA-Funktionen finden Sie im folgenden Unterkapitel.
Eine Absicherung der Automatisierungszellen nach außen stellen Sie z. B. durch die Firewall-Funktionalität eines SCALANCE S sicher.
Konkrete Konfigurationsbeispiele der anzubindenden Automatisierungszellen inklusive Anlagenskizzen finden Sie im Kapitel Konfigurationsbeispiele (Seite 21).

2.2 Funktionen und Kommunikationsdienste

Prozess-Stationen

Das Gateway kann mit folgenden Prozess-Stationen und deren unterstützten Produkten kommunizieren:

- SIMATIC S7-300/400/1200/1500/LOGO!

  S7-Kommunikation über:

  - Ethernet
  - PROFIBUS/MPI (CC716)

  Beispiele von unterstützten Produkten sind z. B. die SINUMERIK-Produkte für SIMATIC S7-300.

- Modbus-Steuerungen

  Kommunikation über Ethernet (Modbus/TCP)

- OPC UA-Station

  Kommunikation über Ethernet und integriertem OPC UA-Client

Protokolle für die Cloud-Verbindung

Für die Kommunikation mit einem Cloud-Broker bzw. Cloud-Server unterstützt das Gateway folgende Protokolle:

- MQTT

  Gemäß OASIS-Standard Version 3.1 / 3.1.1 / 5.0

- HTTP

  Versionen HTTP/1.0 und HTTP/1.1, optional über TLS

Unterstützte Cloud-Systeme

Das Gateway unterstützt den Anschluss an Cloud-Systeme, die eine Broker-Funktionalität mit den oben genannten Voraussetzungen und den nachfolgend beschriebenen Funktionen unterstützen.

Der Cloud-Zugang ("Cloud-Profil") des Gateways ist auf die Kommunikation mit folgenden Cloud-Systemen abgestimmt und unterstützt die jeweils aufgeführten Dienste und Funktionen:

- MindSphere (Siemens)

  Dienst: MindConnect IoT Extension

  Funktion: Publisher

- AWS (Amazon)

  Dienst: IoT Core

  Funktion: Publisher und Subscriber

- Azure (Microsoft)

  Dienst: IoT Hub

  Funktion: Publisher und Subscriber

- IBM Cloud (IBM)

  Dienst: Watson IoT Platform

  Funktion: Publisher und Subscriber

- Andere Cloud

  Profil für ein anderes Cloud-System

  Funktion: Publisher und Subscriber

OPC UA-Server für Prozessdaten

Für die Übertragung von Prozessdaten kann das Gateway als OPC UA-Server eingesetzt werden. Das Gateway liest Prozessdaten aus einer angeschlossenen Prozess-Station aus und stellt sie als OPC UA-Server einem oder mehreren OPC UA-Clients zur Verfügung.

Die Server-Funktion ist in der Projektierung zu- bzw. abschaltbar.

Der OPC UA-Server unterstützt folgende Funktionen:

- Lesen und Schreiben von Variablen
- Beobachtung von Variablen (MonitoredItems) über Subscriptions
- Hierarchisches Address Browsing

Der OPC UA-Server ist auf Basis des "Micro Embedded Device 2017 Server Profile" der OPC Foundation implementiert. Zu Details siehe:
Link: (https://profiles.opcfoundation.org/profile/1659)

Der OPC UA-Server unterstützt die für dieses Profil relevanten Funktionen aus folgenden Spezifikationen:

- IEC/TR 62541-1 (08-2012) OPC Unified Architecture - Part 1: Overview and Concepts
- IEC/TR 62541-2 (02-2009) OPC Unified Architecture - Part 2: Security Model

  Zu den unterstützten Security-Profilen siehe Kapitel OPC UA-Security (Seite 97).
- IEC 62541-3 (08-2012) OPC Unified Architecture - Part 3: Address Space Model

  Zu den unterstützten Datentypen siehe Kapitel Datenpunkte (Seite 142).
- IEC 62541-4 (08-2012) OPC Unified Architecture - Part 4: Services
- IEC 62541-5 (08-2012) OPC Unified Architecture - Part 5: Information Model
- IEC 62541-6 (08-2012) OPC Unified Architecture - Part 6: Mappings
- IEC 62541-7 (09-2010) OPC Unified Architecture - Part 7: Profiles

Projektierung über das WBM

Die Parameter des Gateways projektieren Sie im Web Based Management (WBM). Das WBM besteht aus Webseiten, die im Gateway gespeichert sind. Von einem Projektierungs-PC aus verbinden Sie sich über HTTPS mit dem WBM des Gateways. Das WBM erreichen Sie in Werkseinstellungen nur über die Prozess-Schnittstelle (P2).

2.3 Konfigurationsbeispiele

Nachfolgend finden Sie Beispiele für mögliche Konfigurationen mit dem Gateway "CloudConnect 7".

Anschluss von Prozess-Stationen

In den abgebildeten Konfigurationen liest das Gateway Prozessdaten aus einer bzw. mehreren S7-Stationen aus und überträgt sie per MQTT an einen Cloud-Broker und/oder stellt die Daten über den OPC UA Server für OPC UA Clients bereit.

Die Prozess-Stationen in der Automatisierungszelle sind dabei an der Prozess-Schnittstelle (P2) des Gateways angeschlossen. Der Cloud-Broker wird über einen SCALANCE-S/M an der Cloud-Schnittstelle (P1) angebunden.

Eine Modbus-Station oder ein OPC UA-Server, beispielsweise das Automatisierungsgerät eines Fremdherstellers, kann zur Datenübertragung an einen Cloud-Broker ebenfalls angeschlossen werden.

- Bei Anschluss an eine SIMATIC S7 kommuniziert das Gateway über eine S7-Verbindung. Alternativ können S7-Stationen mit OPC UA-Server, z. B. eine CPU1500 oder eine CPU1200 ab FW 4.0, auch über eine OPC UA-Verbindung kommunizieren. Das Gateway ist dabei OPC UA-Client. Über OPC UA kann auch auf Daten der S7-Station mit aktivierter Bausteinoptimierung zugegriffen werden.
- Bei Anschluss an eine Modbus-Station kommuniziert das Gateway über Modbus/TCP.
- Bei Anschluss an einen OPC UA-Server kommuniziert das Gateway als OPC UA-Client mit der Prozess-Station.

Konfiguration eines CC712

Hier ist die Prozess-Station eine SIMATIC S7-300.

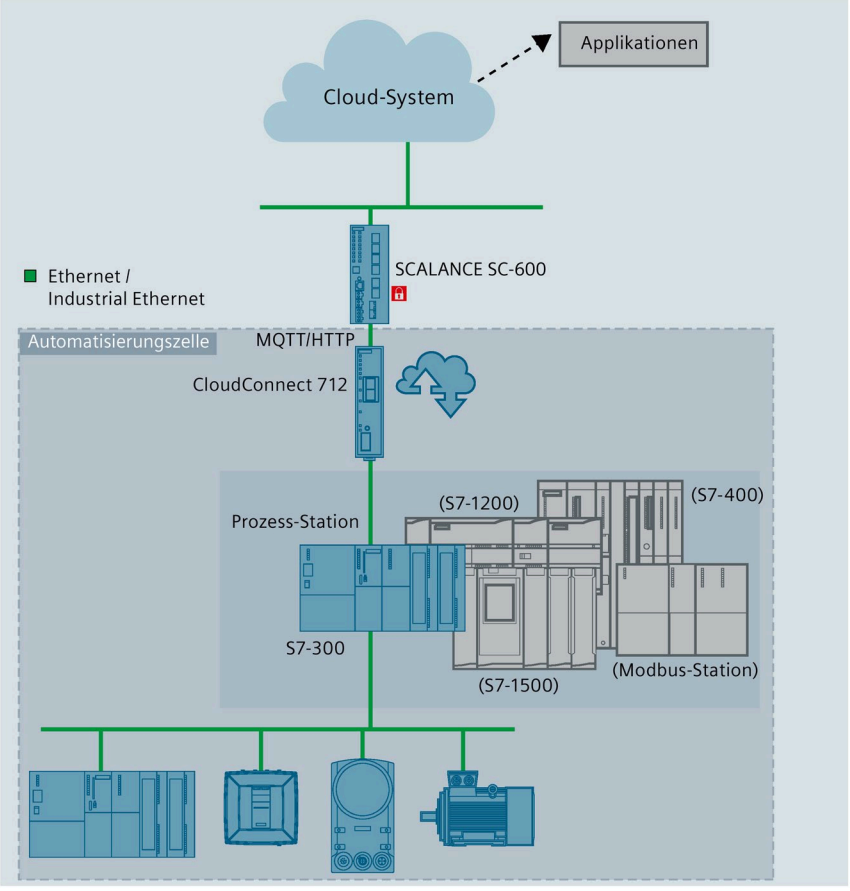


Bild 2-1 CloudConnect 712: Anbindung einer Station an die Cloud

Konfiguration eines CC716

Über das Gateway CC716 können bis zu 7 Stationen über Ethernet oder PROFIBUS angeschlossen werden. Das Gateway überträgt die Daten per MQTT an einen Cloud-Broker.

Im abgebildeten Beispiel ist eine S7-300 über Ethernet angeschlossen, eine S7-1200 und eine S7-400 über PROFIBUS und eine S7-1500 über OPC UA.

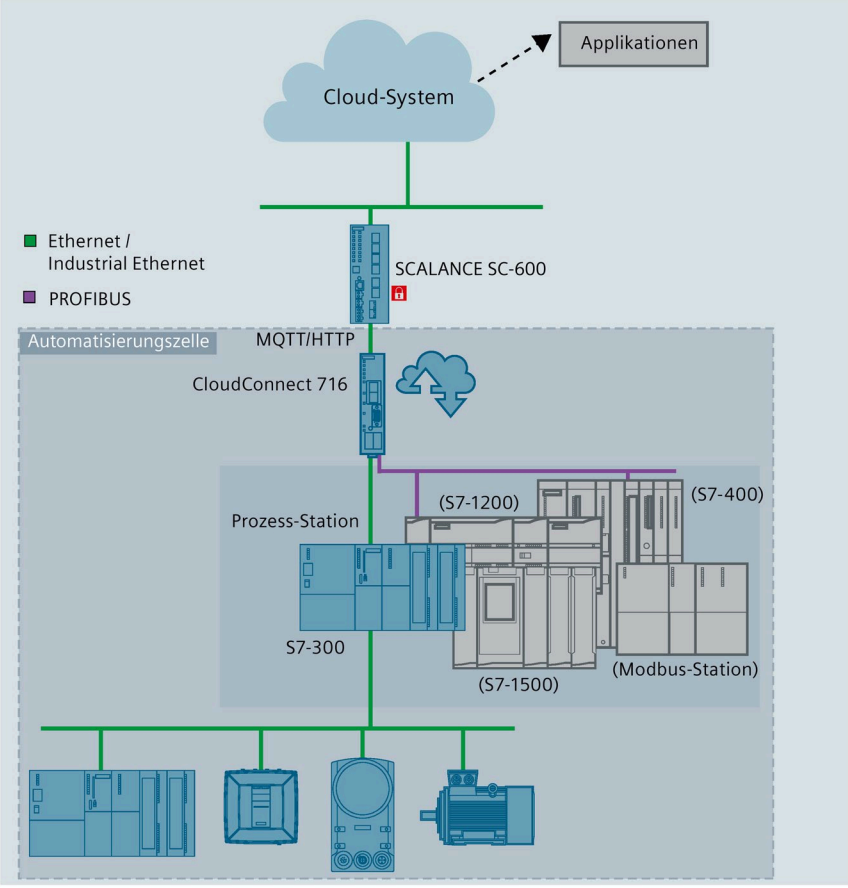


Bild 2-2 CloudConnect 716: Anbindung von Stationen an die Cloud

Anschluss von Prozess-Stationen an externe OPC UA-Clients

Konfiguration eines CC712

In der abgebildeten Konfiguration überträgt das Gateway CC712 Prozessdaten einer S7-Station über OPC UA an eine Zentrale oder an einen oder mehrere OPC UA-Clients.

Das Gateway liest Prozessdaten aus der S7-Station aus und stellt sie als OPC UA-Server einem oder mehreren OPC UA-Clients zur Verfügung.

Die Prozess-Stationen in der Automatisierungszelle sind dabei an der Prozess-Schnittstelle (P2) des Gateways angeschlossen.
Die Zentrale bzw. die OPC UA-Clients werden über einen SCALANCE-S/M an der Cloud-Schnittstelle (P1) angebunden.

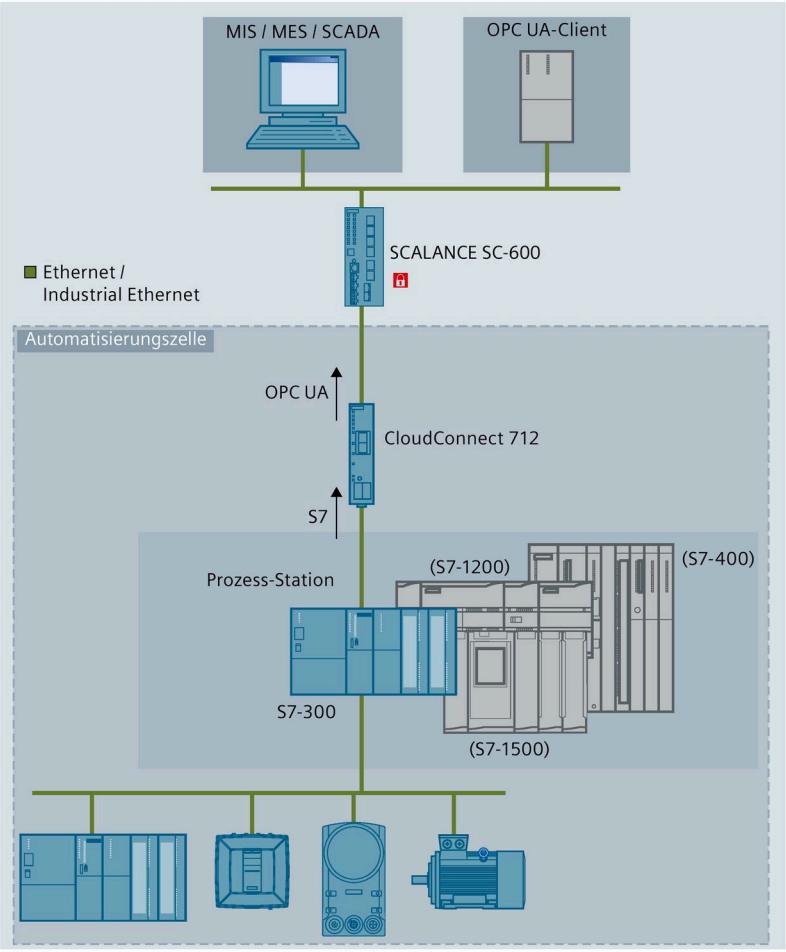


Bild 2-3 CloudConnect 712: Anbindung einer Station an OPC UA-Clients

Über das Gateway CC716 können folgende Stationen über Ethernet oder PROFIBUS angeschlossen und die Daten mit den externen OPC UA-Clients ausgetauscht werden.

- bis zu 7 SIMATIC S7-Stationen und OPC UA-Stationen
- zusätzlich bis zu 10 Modbus-Stationen

Funktionsübersicht

3

3.1 Weitere Dienste und Eigenschaften

Weitere Dienste und Eigenschaften

- **IP-Konfiguration**
  - Das Gateway unterstützt IP-Adressen gemäß IPv4 und IPv6. Zu Details siehe Kapitel Ethernet (Seite 76).
  - Adressvergabe:

    Die IP-Adresse, die Subnetzmaske und die Adresse des Default-Routers können in der Projektierung eingestellt werden.
  - DHCP: Alternativ kann die IP-Adresse an jeder Schnittstelle unabhängig von einem DHCP-Server bezogen werden.
  - DNS: Optional können auch DNS-Server eingestellt werden, über die eine Auflösung der Host-Namen von Kommunikationspartnern möglich ist.
- **Uhrzeitsynchronisation über Industrial Ethernet**

  Die Uhrzeitsynchronisation des Gateways ist nach folgenden NTP-Verfahren (Network Time Protocol) projektierbar:
  - NTP
  - NTP (secure)

  Weitere Informationen finden Sie im Kapitel Systemzeit (Seite 162).
- **CLP (Wechselmedium)**

  Das Gateway besitzt die Möglichkeit, die Konfigurationsdaten auf einem CLP zu speichern. Der CLP ist ein externes Speichermedium und nicht Teil des Lieferumfangs.

  Zum CLP-Schacht siehe Kapitel CLP-Schacht (Seite 39).

  Zu den Funktionen des CLP siehe Kapitel Nutzung eines CLP (Seite 56).

  Zu den Bestelldaten der verfügbaren CLPs siehe Anhang CLPs (Seite 197).
- **Diagnose**

  Über folgende Mittel und Wege erhalten Sie Diagnosedaten zum Gateway:
  - LEDs
  - Webdiagnose

  Weitere Informationen zur Diagnose finden Sie im Kapitel Diagnose (Seite 177).

3.2 Mengengerüst - Kommunikation

Das Gateway unterstützt das folgende maximale Mengengerüst.

Verbindungsressourcen über die Prozess-Schnittstelle

- **Anzahl der Verbindungen über S7-Protokoll**
  - CC712: Max. 1 S7-Verbindung mit einer S7-Station über Ethernet
  - CC716: Max. 7 S7-Verbindungen mit S7-Stationen über Ethernet oder PROFIBUS
- **Anzahl der Verbindungen über UPC UA-Client**
  - CC712: Max. 1 OPC UA-Client-Verbindung mit einem externen OPC UA-Server
  - CC716: Max. 7 OPC UA-Client-Verbindungen mit externen OPC UA-Servern
- **Anzahl der Verbindungen über Modbus/TCP**

  Max. 10 Verbindungen mit Modbus-Stationen
- **Anzahl der Verbindungen mit dem Projektierungs-PC**

  Max. 2 HTTPS-Verbindung

Maximale Anzahl an Verbindungen

S7-Verbindungen und OPC UA-Client-Verbindungen werden zusammengezählt. Die maximale Anzahl beträgt:

- CC712: 1 Verbindung
- CC716: 7 Verbindungen

Anzahl der Prozessdaten

- **Variablen im Datenbereich von S7- oder OPC UA-Stationen**
  - CC712: Insgesamt max. 500 Variablen
  - CC716: Insgesamt max. 3500 Variablen

    Sie können mehrere Stationen anlegen, die das gleiche pysikalische Gerät repräsentieren. Dadurch erhöht sich die Menge der Prozessdaten, die von diesem Gerät gelesen werden können. Die Stationen, von denen die Prozessdaten ausgelesen werden, projektieren Sie im Kapitel Prozess-Zugang (Seite 84).
- **Variablen pro S7- oder OPC UA-Stationen**

  Max. 500 Variablen
- **Arrays pro S7- / OPC-UA Client-Station**

  Max. 100 Arrays
- **Strings pro S7- / OPC-UA Client-Station**

  Max. 100 Strings
- **Variablen im Datenbereich von Modbus-Stationen**

  Max. 100 Variablen pro Modbus-Station

Verbindungen über die Cloud-Schnittstelle

- **Anzahl der Verbindungen zu einem Cloud-Profil**

  Max. 3 aktive Cloud-Profile

- **Anzahl der Verbindungen des integrierten OPC UA-Servers mit externen OPC UA-Clients**

  Max. 10 Sitzungen mit OPC UA-Clients gleichzeitig

OPC UA-Server

Als OPC UA-Server unterstützt das Gateway das folgende Mengengerüst:

- **Anzahl der Variablen**
  - CC712: Insgesamt max. 1500 Variablen; 500 für S7/OPC + 10 * 100 für Modbus
  - CC716: Insgesamt max. 4500 Variablen; 7 * 500 für S7/OPC + 10 * 100 für Modbus
- **Anzahl der unterstützten Subscriptions**

  Max. 5 Subscriptions pro Sitzung

  Insgesamt maximal 50 Subscriptions gleichzeitig
- **Anzahl der Items pro Subscription**

  Max. 1000 Variablen pro Subscription

  Max. 4500 Variablen über alle Subscriptions

3.3 Funktionsumfang des WBM

Web Based Management (WBM)

Sie projektieren das Gateway über dessen Web Based Management (WBM). Das WBM besteht aus Webseiten, die sich im Webbrowser eines angeschlossenen PC aufrufen lassen. Von Ihrem PC aus verbinden Sie sich über HTTPS mit dem WBM. Zusätzlich können Sie über die HTTP-basierte AP-Schnittstelle als API-Client auf das WBM des Gateways zugreifen und ihn mit API-Anfragen konfigurieren. Weitere Informationen siehe Kapitel API (Seite 68).

Zu den einsetzbaren Webbrowsern für den PC siehe Kapitel Lieferumfang und Voraussetzungen (Seite 28).

Zugriff auf das WBM

Für den Aufruf des WBM müssen Sie eine Verbindung zwischen PC und dem Gateway über LAN herstellen, siehe Kapitel Verbindung mit dem WBM aufbauen (Seite 68).

Funktionen des WBM in der Übersicht

Das WBM stellt folgende Funktionen zur Verfügung:

- **Benutzerverwaltung**

  Im geöffneten WBM legen Sie für die Rolle "Administrator" den Benutzernamen und das Passwort fest. Nur mit diesen Administratordaten können Sie auf das WBM zugreifen und Änderungen durchführen.Sie können bis zu 6 weitere Benutzer hinzufügen und der gewünschten Rolle zuweisen. Benutzer mit der Rolle "GUEST" können nur auf Diagnosedaten zugreifen, ohne Änderungen an der Konfiguration durchzuführen.

- **Projektierung**

  Über das WBM projektieren Sie folgende Funktionsbereiche:

  - Basisfunktionen wie Uhrzeit oder IP-Adresse
  - Anschluss der Prozess-Station
  - Anschluss an das übergeordnete Netzwerk (Cloud, OPC-Clients)
  - Kommunikationsfunktionen

- **Instandhaltungs- und Diagnosefunktionen**
  - Diagnose
  - Laden und Speichern der Projektierungsdaten
  - Laden neuer Firmware-Versionen

Konfigurationsdatei wiederverwenden

Die Projektierungsdaten, die Sie im WBM erstellen, werden im Gateway gespeichert. Wenn Sie einen CLP gesteckt haben, werden die Projektierungsdaten des Gateways zusätzlich nach dem Klicken auf die Schaltfläche "Übernehmen" auf den CLP geschrieben.

Wenn Sie mehrere Gateways mit teilweise identischen Projektierungsdaten verwenden, können Sie die Konfigurationsdatei eines Gateways exportieren und in weitere Gateways laden und dort jeweils anpassen.

3.4 Lieferumfang und Voraussetzungen

Lieferumfang

Folgende Positionen gehören zum Lieferumfang des Gateways:

- Gateway "CloudConnect 7"
- Klemmenblock für die Spannungsversorgung des Gateways
- Klemmenblock für den Digitaleingang und den Digitalausgang (CC716)

Erforderliches Zubehör

Das folgende Zubehör (nicht Teil des Lieferumfangs) ist für den Betrieb des Gateways erforderlich:

- Spannungsversorgung

  Sie benötigen eine externe Spannungsquelle DC 24 V

- PC

  Für die Projektierung des Gateways benötigen Sie einen Projektierungs-PC mit geeignetem Webbrowser (siehe unten).

- LAN-Kabel

  Für die Verbindung des Projektierungs-PC mit der LAN-Schnittstelle X2 des Gateways benötigen Sie ein ITP-Kabel Cat-5 oder höher.

- Kabel für die Prozessanschlüsse

  Für die Verbindung der Prozess-Station bzw. Stationen mit dem Gateway benötigen Sie das entsprechende LAN- bzw. PROFIBUS-Kabel.

Kommunikationspartner

- **Prozess-Zugang**

  Für den Zugang zum Prozess benötigen Sie eine Station im Produktivbetrieb, alternativ:

  - S7-Station
  - OPC UA-Station mit OPC UA-Server
  - Modbus-Station

- **Cloud-Zugang / Externe OPC-Clients**

  - Für den Zugang zur Cloud benötigen Sie den eingerichteten Zugang zu einem Cloud-Broker.
  - Für die Anbindung externer OPC UA-Clients benötigen Sie mindestens einen eingerichteten OPC UA-Client.

  Wenn Sie als Cloud-System einen Dienst im Internet verwenden, müssen Sie die Automatisierungszelle nach außen mit zusätzlichen Security-Komponenten (z. B. SCALANCE S/M) absichern.

Voraussetzungen in S7-Stationen

⚠ WARNUNG

Schreiben von Werten in Ausgänge

Beachten Sie bei Referenzierung auf Ausgänge, dass bei schreibendem Zugriff die Werte sofort in die Ausgänge der CPU geschrieben werden, ohne zuvor vom Anwenderprogramm bearbeitet zu werden.

Das Schreiben von Werten hat unmittelbaren Einfluss auf den Prozess.

Folgende Voraussetzungen müssen in Ihrem STEP 7-Projekt bzw. den angeschlossenen S7-Stationen erfüllt sein.

- Variablen / Symbole

  Für den Zugriff auf die Prozessdaten über Referenzierung auf Variablen der CPU müssen Variablen bzw. Symbole in der jeweiligen CPU angelegt sein.

  Der schreibende Zugriff über die MQTT-Subscriber-Funktion des Gateways ist nur möglich in DB-Variablen der CPU.

  STEP 7 Professional: Bei DBs und Zugriff über eine S7-Verbindung muss die Option "Optimierter Bausteinzugriff" deaktiviert sein. Bei Zugriff über den OPC UA-Server der CPU muss die Option nicht deaktiviert sein.

  Für die Nutzung durch OPC UA-Dienste müssen die Variablen der CPU wie folgt ausgezeichnet sein (Optionen aktiviert):

  – "Erreichbar aus HMI/OPC UA"

  – "Schreibbar aus HMI/OPC UA"

    Erforderlich für schreibenden Zugriff

  Zu weiteren Details siehe Kapitel Datenpunkte (Seite 142).

- OPC UA: Bestandteile des Identifiers

  Beachten Sie bei der Projektierung, dass folgende Namen als Bestandteil des Identifiers in die NodeID einer Variable eingehen:

  – CPU-Name

  – Name der DB-Variable

- CPU 1200/1500 über S7-Verbindung

  – Bei der CPU darf unter "Schutz & Security" kein Leseschutz projektiert sein.

  – Bei der CPU muss unter "Schutz & Security" der Zugriff über PUT/GET projektiert sein.

- CPU 300/400 über S7-Verbindung

  Bei der CPU darf unter "Schutz" kein Leseschutz projektiert sein.

- CP 300/400 über S7-Verbindung

  Bei Zugriff auf die Station über einen CP müssen beim CP folgende Voraussetzungen erfüllt sein:

  – Bei projektiertem "IP-Zugriffsschutz" muss die IP-Adresse des Gateways mit dem Recht "A" projektiert sein.

- CP 1200 über S7-Verbindung

  Bei Zugriff auf die Station über einen Telecontrol-CP muss beim CP unter "Kommunikationsarten" die S7-Kommunikation aktiviert sein.

Webbrowser für den Projektierungs-PC

Zum Zugriff auf das WBM des Gateways benötigt der Projektierungs-PC einen der folgenden Webbrowser.

- Apple Safari
- Firefox Quantum
- Google Chrome
- Microsoft Edge

Der Webbrowser muss Cookies akzeptieren. Die Applikation verwendet ein Cookie.

Im Webbrowser muss JavaScript aktiviert sein.

Empfehlung: Verwenden Sie möglichst eine aktuelle Version des Webbrowsers.

Optional

- CLP

  Wechselmedium zur Aufnahme von Konfigurationsdaten
- NTP-Server - erreichbar über Schnittstelle P1 / P2
- DHCP-Server - erreichbar über die Schnittstelle P1 / P2
- DNS-Server - erreichbar über die Schnittstelle P1 / P2

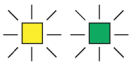
LEDs, Anschlüsse, Taster, CLP

4

4.1 LED-Anzeigen

Die LEDs auf der Frontseite zeigen die Baugruppenzustände des Moduls an.

Die LED-Symbole in der folgenden Tabelle bedeuten folgende Zustände der LEDs:

LED-Symbol			
LED-Zustand	AUS	EIN (Ruhelicht) *	Blinkend

* : Gelb blinkend bei grünem Ruhelicht

Bedeutung der LED-Anzeigen

LED-Bezeichnung (Farben)	**LED-Bild**	**Bedeutung / Baugruppenzustand**
Power (Grün)	**Spannungsversorgung**	
		Spannung AUS
		Heruntergefahren
		Spannung EIN
Device Connection (Grün / gelb)	**Verbindung mit Prozess-Stationen**	
		Keine Prozess-Station projektiert
		Heruntergefahren
		Bestehende Verbindung mit allen projektierten Prozess-Stationen
		Keine Kommunikation mit mindestens einer Prozess-Station. Mögliche Ursachen: • Verbindungsaufbau läuft • Fehlerhafte Projektierung
		Stop der Kommunikation über: • WBM: "Instandhaltung > Kommunikation / Neustart" • CC716: Digitaleingang
Cloud Connection (Grün / gelb)	**Verbindung mit Cloud**	
		Keine Verbindung mit Cloud-Server projektiert
		Heruntergefahren
		Bestehende Verbindung mit allen projektierten Cloud-Servern
		Keine Kommunikation mit mindestens einem Cloud-Server. Mögliche Ursachen: • Verbindungsaufbau läuft • Cloud-Server nicht bereit • Fehlerhafte Projektierung
Diagnosis (Grün / gelb)	**Diagnose**	
		Kein Fehler

LED-Bezeichnung (Farben)	LED-Bild	Bedeutung / Baugruppenzustand
		Heruntergefahren
		Diagnosemeldung bezüglich NTP oder DHCP liegt vor, siehe WBM "Instandhaltung > Diagnose".
		Rücksetzen wird eingeleitet (Taster beim Anlauf gedrückt).
		Rücksetzen wird durchgeführt (Taster kann losgelassen werden).
P1 / P2 (Grün / gelb)	**Verbindung mit Ethernet an Schnittstelle P1 bzw. P2**	
		Keine Verbindung mit Ethernet
		Bestehende Verbindung mit Ethernet
		Bestehende Verbindung mit Datenverkehr
LEDs nur von CC716		
MPI/DP (Grün / gelb)	**Verbindung mit PROFIBUS/MPI**	
		Keine Verbindung mit PROFIBUS/MPI projektiert
		Keine Kommunikation mit PROFIBUS/MPI. Mögliche Ursachen: • Leitungsbruch, Kurzschluss • Fehlerhafte Projektierung, z. B. falsche Übertragungsgeschwindigkeit
		Bestehende Verbindung mit PROFIBUS/MPI
DI (Gelb)	**Digitaleingang**	
		Digitaleingang EIN (1)
		Digitaleingang AUS (0)
DO (Gelb)	**Digitalausgang**	
		Digitalausgang EIN (1)
		Digitalausgang AUS (0)

4.2 Anschlüsse

4.2.1 Ethernet-Schnittstellen P1/P2

Ethernet-Schnittstellen

Das Gateway besitzt zwei Ethernet-Schnittstellen gemäß Gigabit-Standard IEEE 802.3ab, ausgeführt als RJ45-Buchse.

- P1

  Cloud-Schnittstelle für den Anschluss eines Cloud-Brokers und von externen OPC-Clients

- P2

  Prozess-Schnittstelle für den Anschluss der Stationen der Automatisierungsanlage

Hinweis

Verbindung mit Subnetzen

Die zwei Ethernet-Schnittstellen sind nicht als Switch ausgelegt, sondern sind für den Anschluss an unterschiedliche Netze vorgesehen.

Wenn sich der Anschluss zur Cloud im selben Subnetz befindet wie der Prozessanschluss, dann deaktivieren Sie bei der Projektierung die Cloud Schnittstelle P1. Damit wird die Schnittstelle physikalisch abgeschaltet.

Die Eigenschaften der Ethernet-Schnittstellen finden Sie im Kapitel Technische Daten (Seite 185).

4.2.2 PROFIBUS/MPI-Schnittstelle (CC716)

9-polige Sub-D-Buchse (MPI/DP)

Der PROFIBUS/MPI-Anschluss ist eine 9-polige Sub-D-Buchse und arbeitet nach der Übertragungstechnik RS-485.

Optische PROFIBUS-Netze können Sie optional über ein Optical Bus Terminal OBT oder ein Optical Link Module OLM anschließen.

Die Eigenschaften der PROFIBUS-Schnittstelle finden Sie im Kapitel Technische Daten (Seite 185).

4.2.3 Digitaler Eingang / Ausgang (CC716)

Das Gateway CC716 besitzt einen digitalen Eingang und einen digitalen Ausgang. Sie können folgendermaßen genutzt werden:

- Digitaler Eingang

  Der Eingang kann alternativ als Trigger für folgende Funktionen genutzt werden:

  - Externer Trigger für die Übertragung von Datenpunkten
  - Stop-/Start-Trigger für die Prozesskommunikation

- Digitaler Ausgang

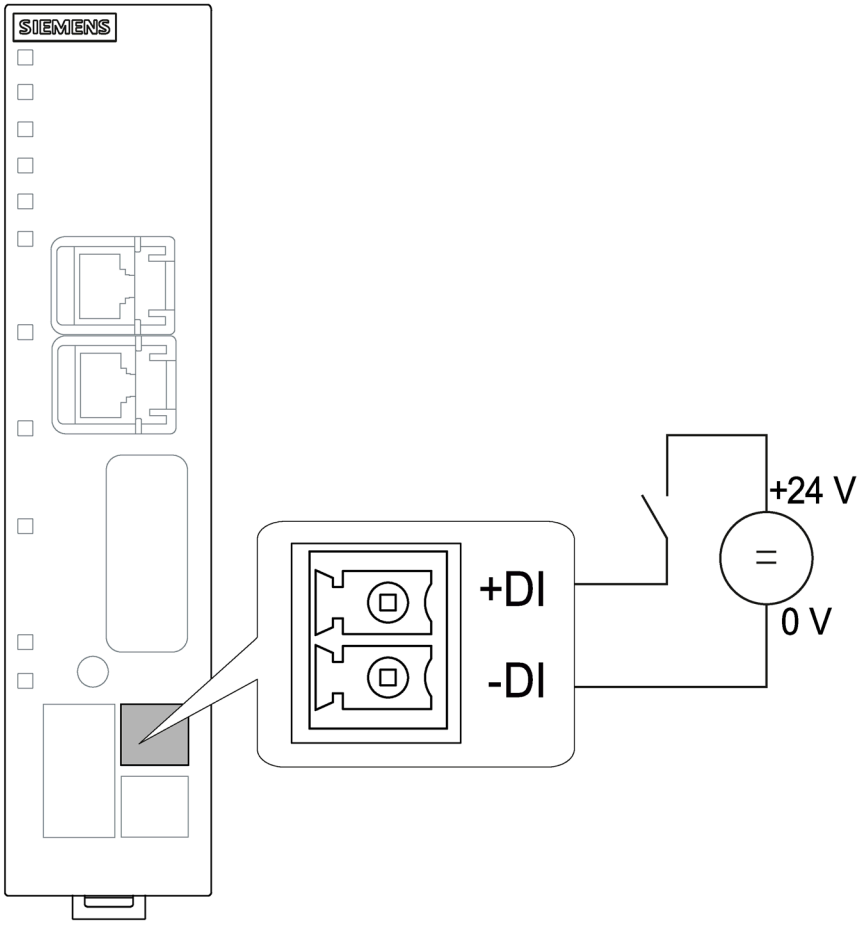
  Der Ausgang ist ein Schalter und kann zur Erzeugung eines Statussignals genutzt werden:

  - Verbindungszustand mit der Cloud

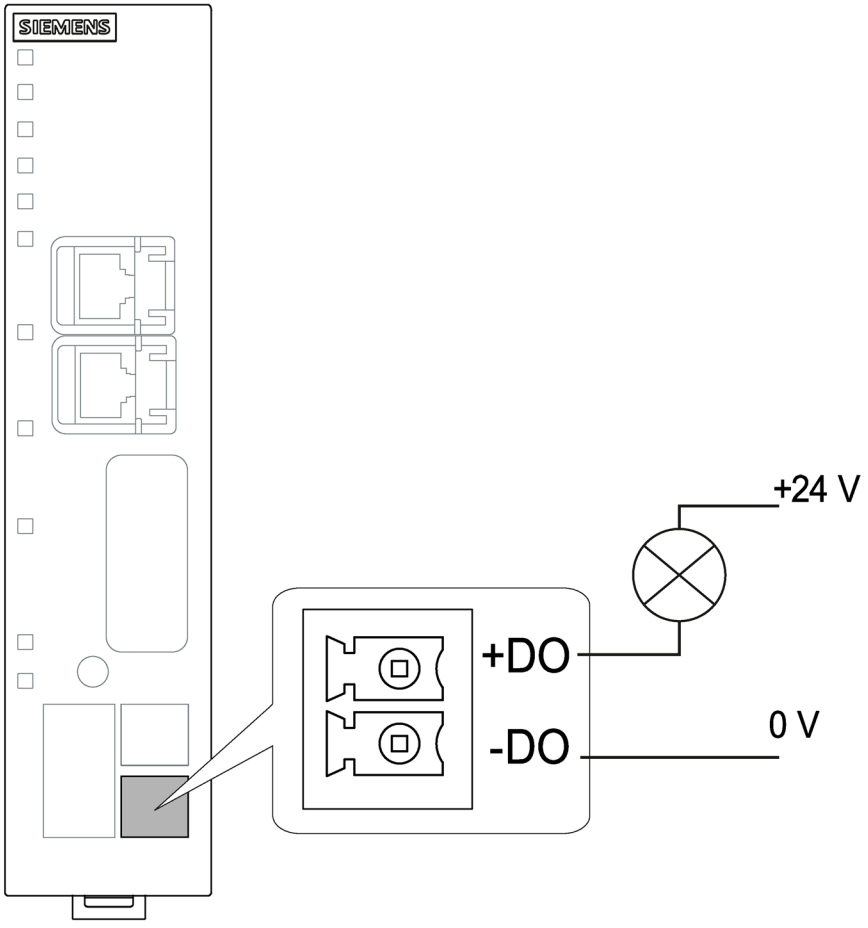
Die Funktionen sind projektierbar, siehe Kapitel DI/DO (CC716) (Seite 82).

Zur Belegung der Klemmenblöcke siehe Kapitel Anschließen (Seite 50).

Digitaler Eingang



Digitaler Ausgang



Der Ausgang ist ein Schalter, der das Signal an +DO auf -DO durchschaltet.

4.2.4 Externe Spannungsversorgung

Externe Spannungsversorgung

Der Anschluss (Buchse) für die externe Spannungsversorgung DC 24 V befindet sich unten auf der Frontseite des Gateways. Die externe Spannungsversorgung ist redundant aufgebaut (optional zu verwenden).

Die Spannungsversorgung wird an den mit dem Gateway mitgelieferten 5-poligen, steckbaren Klemmenblock angeschlossen.

Der Anschluss besitzt einen mechanischen Verpolschutz. Der Klemmenblock ist so ausgeführt, dass er nur in einer Position in die Buchse des Gateways gesteckt werden kann.

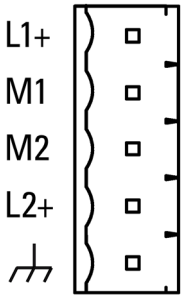


Bild 4-1 Buchse der externen Spannungsversorgung

Zur Belegung der Buchse und zum Anschluss siehe Kapitel Anschließen (Seite 50).

Weitere Daten zur Spannungsversorgung finden Sie im Kapitel Technische Daten (Seite 185).

4.3 Der Taster "SET"

Funktionen des Tasters

⚠ WARNUNG
EXPLOSIONSGEFAHR
Drücken Sie den Taster nicht, wenn eine explosionsgefährdete Atmosphäre besteht.

Der Taster "SET" hat folgende Funktionen:

- **Rücksetzen auf Werkseinstellungen**

  Hinweis

  Projektierungsdaten werden gelöscht

  Durch das Rücksetzen auf Werkseinstellungen wird das Gateway in den Zustand bei Auslieferung vom Werk zurückgesetzt. Hierdurch werden alle projektierten Einstellungen gelöscht.

  Auch die Daten auf einem optionalen CLP werden gelöscht.

  Die genauen Auswirkungen des Rücksetzens finden Sie im Kapitel Neustart und Zurücksetzen (Seite 182).

Bedienung des Tasters

Dauer der Tasterbetätigung (Sekunden)	Funktion und Bedienung
≥ 5 s	**Rücksetzen auf Werkseinstellungen** 1. Schalten Sie die Spannungsversorgung aus. 2. Schalten Sie die Spannungsversorgung bei gedrücktem Taster wieder ein. Halten Sie den Taster während des Anlaufs für mindestens 5 Sekunden gedrückt. Während die LED "Diagnosis" blinkt, wird das Rücksetzen vorbereitet. 3. Lassen Sie den Taster los, wenn die LED aufhört zu blinken. Während die LED mit grünem Ruhelicht leuchtet, führt das Gateway das Rücksetzen durch. Nach Abschluss des Rücksetzens führt das Gateway einen Neustart durch und ist über die werkseitig voreingestellte IP-Adresse erreichbar.

4.4 CLP-Schacht

Der Schacht für einen optionalen CLP befindet sich auf der Rückseite des Moduls.

Zum Stecken und Ziehen des CLP siehe Kapitel Nutzung eines CLP (Seite 56).

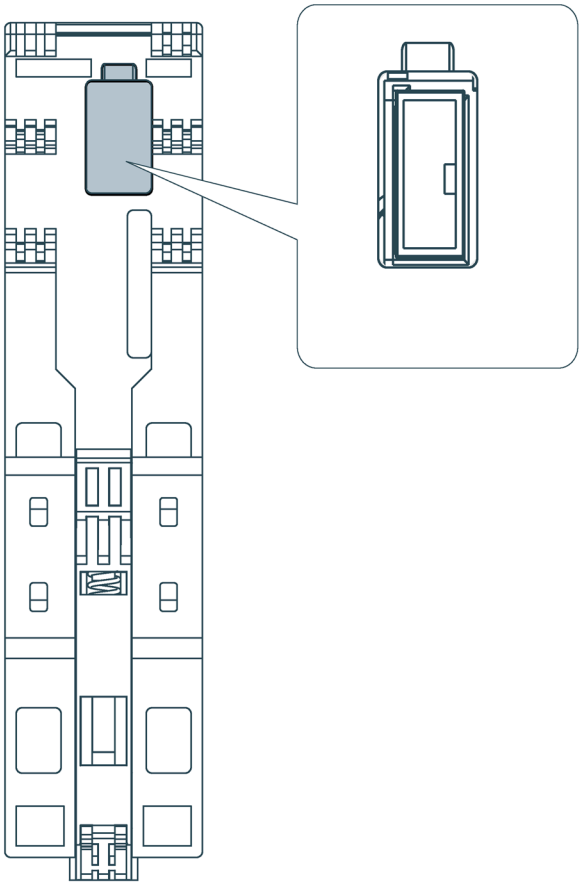


Bild 4-2 Schacht für optionalen CLP auf der Geräterückseite

Montage, Anschluss, Inbetriebnahme, Demontage 5

5.1 Wichtige Hinweise zum Einsatz des Geräts

Sicherheitshinweise für den Geräteeinsatz

Beachten Sie die folgenden Sicherheitshinweise für Aufstellung und Betrieb des Geräts und alle damit zusammenhängenden Arbeiten wie Montieren und Anschließen des Geräts oder Geräteaustausch.

⚠ WARNUNG
Wenn das Gerät in einen Schaltschrank eingebaut ist, entspricht die Innentemperatur des Schaltschranks der Umgebungstemperatur des Geräts.

5.1.1 Hinweise für den Einsatz im Ex-Bereich

⚠ WARNUNG
EXPLOSIONSGEFAHR
ÖFFNEN SIE DAS GERÄT NICHT BEI EINGESCHALTETER VERSORGUNGSSPANNUNG.

⚠ WARNUNG
EXPLOSIONSGEFAHR
Der Austausch von Komponenten kann die Eignung für Class I, Division 2 oder Zone 2 beeinträchtigen.

⚠ WARNUNG
Das Gerät darf nur in einer Umgebung mit Verschmutzungsgrad 1 oder 2 gemäß EN/IEC 60664-1, GB/T 16935.1 betrieben werden.

⚠ WARNUNG

EXPLOSIONSGEFAHR

In einer leicht entzündlichen oder brennbaren Umgebung dürfen keine Leitungen an das Gerät angeschlossen oder vom Gerät getrennt werden.

⚠ WARNUNG

Bei Einsatz in explosionsgefährdeter Umgebung entsprechend Class I, Division 2 oder Class I, Zone 2 muss das Gerät in einen Schaltschrank oder in ein Gehäuse eingebaut werden.

⚠ WARNUNG

Wird ein Gerät bei einer Umgebungstemperatur von mehr als 60 bis 70 °C betrieben, kann die Gehäusetemperatur des Gerätes über 70 °C liegen. Der Montageort des Geräts muss deshalb in einem zugangsbeschränkten Bereich liegen, der nur für Service-Personal oder Benutzer zugänglich ist, die über den Grund der Zugangsbeschränkung und die notwendigen Sicherheitsmaßnahmen bei einer Umgebungstemperatur von mehr als 60 °C informiert wurden.

5.1.2 Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / UKEX / IECEx / CCC-Ex

⚠ WARNUNG

Anforderungen an den Schaltschrank

Um die EU-Richtlinie 2014/34 EU (ATEX 114), die UK-Regulierung SI 2016/1107 oder die Bedingungen von IECEx bzw. CCC-Ex zu erfüllen, muss das Gehäuse oder der Schaltschrank mindestens die Anforderungen von IP54 (gemäß EN/IEC 60529, GB/T 4208) nach EN IEC/IEC 60079-7, GB 3836.8 erfüllen.

⚠ WARNUNG

Kabel

Wenn am Kabel oder an der Gehäusebuchse Temperaturen über 70 °C auftreten oder die Temperatur an den Adernverzweigungsstellen der Leitungen über 80 °C liegt, müssen besondere Vorkehrungen getroffen werden. Wenn das Gerät bei Umgebungstemperaturen von über 50 °C betrieben wird, müssen Sie Kabel mit einer zulässigen Betriebstemperatur von mindesten 80 °C verwenden.

⚠ WARNUNG

Geeignete Kabel bei hoher Temperatur im explosionsgefährdeten Bereich

Setzen Sie bei einer Umgebungstemperatur von ≥ 60 °C hitzebeständige Leitungen ein, die für eine mindestens 20 °C höhere Umgebungstemperatur ausgelegt sind. Die eingesetzten Kabeleinführungen am Gehäuse müssen der gemäß EN IEC / IEC 60079-0, GB 3836.1 geforderten IP-Schutzart entsprechen.

⚠ WARNUNG

Transiente Überspannungen

Treffen Sie Maßnahmen, um transiente Überspannungen von mehr als 40% der Nennspannung (bzw. mehr als 119V) zu verhindern. Das ist gewährleistet, wenn Sie die Geräte ausschließlich mit SELV (Sicherheitskleinspannung) betreiben.

⚠ WARNUNG

EXPLOSIONSGEFAHR

Drücken Sie den SET-Taster nicht, wenn eine explosionsgefährdete Atmosphäre besteht.

5.1.3 Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc / FM

Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Division 2, Groups A, B, C und D und in nicht explosionsgefährdeten Bereichen geeignet.

Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Zone 2, Group IIC und in nicht explosionsgefährdeten Bereichen geeignet.

⚠ WARNUNG

EXPLOSIONSGEFAHR

Sie dürfen spannungsführende Leitungen nur trennen oder anschließen, wenn die Spannungsversorgung ausgeschaltet ist oder wenn sich das Gerät in einem Bereich ohne entflammbare Gas-Konzentrationen befindet.

⚠ WARNUNG

EXPLOSIONSGEFAHR

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

⚠ WARNUNG

Die Wandmontage ist nur zugelassen, wenn die Anforderungen an das Gehäuse, die Montagevorschriften, die Abstände und die Trennvorschriften des Schaltschranks oder Gehäuses eingehalten werden. Die Abdeckung des Schaltschranks oder Gehäuses darf nur mithilfe eines Werkzeugs zu öffnen sein. Eine geeignete Zugentlastung für die Kabel muss vorhanden sein.

⚠ WARNUNG

Der Austausch von Komponenten kann die Eignung für Division 2 beeinträchtigen.

5.2 Montieren

ACHTUNG

Unsachgemäße Montage

Durch unsachgemäße Montage kann das Gerät beschädigt oder die Funktionsweise beeinträchtigt werden.

- Vergewissern Sie sich vor jedem Einbau des Geräts, dass dieses keine sichtbaren Schäden aufweist.
- Montieren Sie das Gerät mit geeignetem Werkzeug. Beachten Sie die Angaben in dem jeweiligen Montage-Kapitel.

⚠ WARNUNG

Offene Betriebsmittel

Bei dem Gerät handelt es sich um "offene Betriebsmittel" (open equipment) nach Standard UL 61010-2-201. Um den Vorgaben für einen sicheren Betrieb bezüglich mechanischer Festigkeit, Flammwidrigkeit, Stabilität und Berührschutz Genüge zu tun, sind folgende alternative Einbauarten vorgeschrieben:

- Einbau in einen geeigneten Schaltschrank
- Einbau in ein geeignetes Gehäuse
- Einbau in einen entsprechend ausgestatteten geschlossenen Betriebsraum

Hinweis

In explosionsgefährdeten Bereichen dürfen Sie das Gerät nicht an einer Wand montieren.

⚠ WARNUNG

Die Wandmontage außerhalb eines Schaltschranks oder eines Gehäuses erfüllt nicht die Anforderungen der FM-Zulassung.

⚠ WARNUNG

Kabel-Temperaturen

Wenn die Temperatur der Kabel oder der Gehäusebuchse 70 °C übersteigt oder die Temperatur der Adernverzweigungsstellen der Leitungen 60 °C übersteigt, müssen besondere Vorkehrungen getroffen werden. Wenn das Gerät bei Umgebungstemperaturen von über 40 °C betrieben wird, müssen Sie Kabel mit einer zulässigen Betriebstemperatur von mindesten 80 °C verwenden.

ACHTUNG

Montage und Demontage des Geräts nur im spannungslosen Zustand!

Schalten Sie die Spannungsversorgung des Geräts aus, bevor Sie das Gerät montieren oder demontieren. Montage oder Demontage bei eingeschalteter Versorgungsspannung kann zu einer Beschädigung der Geräte und zu Datenverlust führen.

Montagemöglichkeiten

Zur Montage des Gateways stehen folgende Möglichkeiten zur Verfügung:

- Wandmontage
- Montage auf folgenden Schienentypen (Baugruppenträger):
  - DIN-Hutschiene
  - Profilschiene S7-1500
  - Profilschiene S7-300

  Geeignete Profilschienen finden Sie im Siemens-Zubehörprogramm für Automatisierungstechnik, zum Beispiel:

  Normprofilschiene 35 mm für 19"-Schränke, Artikelnummern 6ES5710-8MA11
- Montage auf Standfuß

  Hierzu steht der SCALANCE M-Standfuß 6GK5898-8MD00 für die Tischmontage zur Verfügung (nicht Teil des Lieferumfangs).

Einbaulage

ACHTUNG
Einbaulage - Abhängigkeit des Temperaturbereichs Beachten Sie die Abhängigkeit des zulässigen Temperaturbereichs von der Einbaulage: • Waagerechter Aufbau des Baugruppenträgers (Hutschiene) bedeutet senkrechte Lage der Module. • Senkrechter Aufbau des Baugruppenträgers (Hutschiene) bedeutet waagerechte Lage der Module. Die zulässigen Temperaturbereiche finden Sie im Kapitel Technische Daten (Seite 185).

Aufbau des Baugruppenträgers	**Einbaulage der Module**
Waagerechter Aufbau des Baugruppenträgers	
Senkrechter Aufbau des Baugruppenträgers	

Mindestabstände

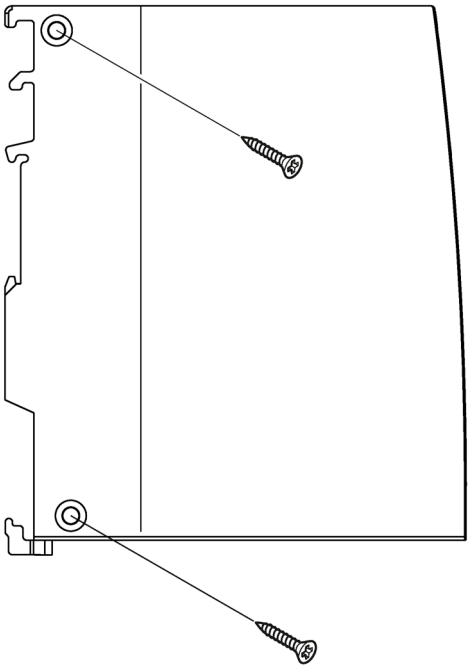
Montieren Sie das Gerät so, dass seine oberen und unteren Lüftungsschlitze nicht verdeckt werden und eine gute Durchlüftung als Schutz vor Überhitzung möglich ist.

Beachten Sie bei waagerechtem Aufbau des Baugruppenträgers folgende Mindestabstände für die Luftzirkulation:

- Oberhalb des Geräts: Mindestens 33 mm
- Unterhalb des Geräts: Mindestens 25 mm

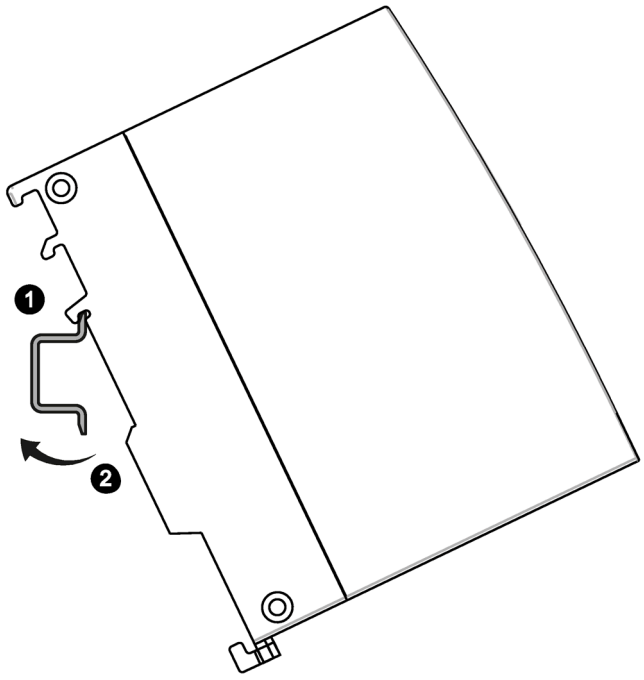
Wandmontage

1. Bereiten Sie die Bohrungen für die Wandmontage vor. Die Abmessungen finden Sie im Kapitel Maßzeichnungen (Seite 195).
2. Befestigen Sie das Gerät mit zwei Schrauben (4 mm) an der Wand.



Hutschienenmontage

1. Hängen Sie das Gerät mit der jeweiligen Führung ① in die Profilschiene ein:
   - Obere Führung für Profilschiene S7-1500
   - Mittlere Führung für Profilschiene S7-300
   - Untere Führung für DIN-Hutschiene
2. Schwenken Sie das Gerät nach hinten, bis die Profilschienenentriegelung hörbar einrastet ②.



3. Erden Sie die Profilschiene.

ACHTUNG
Erdung Die Hutschiene muss aus Gründen der elektrischen Sicherheit an das Schutzleitersystem (PE) der elektrischen Anlage angeschlossen sein.

Hinweis

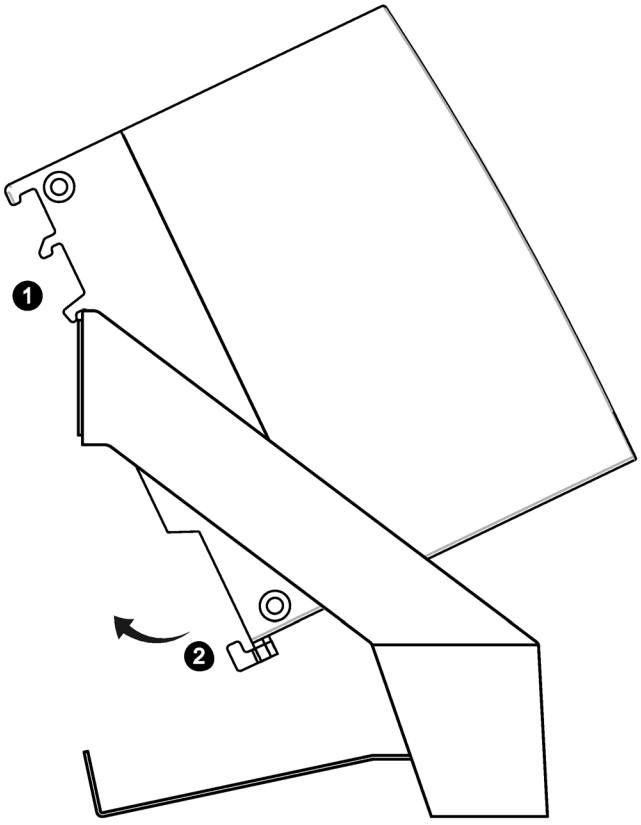
Sicherung der Module vor Verrutschen auf der Hutschiene

Wenn Sie die Module in einem Bereich mit mechanischer Belastung montieren, dann verwenden Sie zur Sicherung der Module auf der Hutschiene geeignete Klemmvorrichtungen an beiden Enden der Gerätegruppe, z. B. Siemens-Endhalter 8WA1808.

Die Endhalter verhindern, dass die Module bei mechanischer Belastung auseinanderrutschen.

Montage auf Standfuß

1. Hängen Sie das Gerät mit der unteren Gehäuseführung auf der Oberkante des Standfußes ① ein.
2. Drücken Sie das Gerät gegen den Standfuß, bis die Profilschienenentriegelung hörbar einrastet ②.



Demontage

Führen Sie die folgenden Schritte durch, um das Gerät von der Schiene zu demontieren:

1. Schalten Sie die Versorgungsspannung des Geräts aus.
2. Ziehen Sie den Stecker der Spannungsversorgung und die Leitungen der Kommunikationsnetze ab.
3. Ziehen Sie die Profilschienenentriegelung auf der Rückseite des Geräts nach unten.
4. Schwenken Sie das Gerät aus der Profilschiene heraus.

5.3 Anschließen

⚠WARNUNG

Ungeeignete Kabel oder Steckverbinder

Explosionsgefahr in explosionsgefährdeten Bereichen

- Verwenden Sie ausschließlich Steckverbinder, die den Anforderungen der relevanten Zündschutzart entsprechen.
- Ziehen Sie ggf. die Steckerverschraubungen, Gerätebefestigungsschrauben, Erdungsschrauben usw. entsprechend den angegebenen Drehmomenten an.
- Schließen Sie ungenutzte Kabelöffnungen für die elektrischen Anschlüsse.
- Überprüfen Sie die Kabel nach dem Einbau auf festen Sitz.

⚠WARNUNG

Ungeschützte Leitungsenden

Durch ungeschützte Leitungsenden in explosionsgefährdeten Bereichen besteht Explosionsgefahr.

- Schützen Sie nicht benutzte Leitungsenden gemäß IEC/EN 60079-14.

⚠WARNUNG

Fehlender Potenzialausgleich

Bei fehlendem Potenzialausgleich in explosionsgefährdeten Bereichen besteht Explosionsgefahr durch Ausgleichsstrom oder Zündfunken.

- Stellen Sie sicher, dass für das Gerät ein Potenzialausgleich vorhanden ist.

⚠WARNUNG

Unsachgemäße Verlegung geschirmter Leitungen

Durch Ausgleichsströme zwischen dem explosionsgefährdeten Bereich und dem nicht explosionsgefährdeten Bereich besteht Explosionsgefahr.

- Erden Sie geschirmte Kabel, die explosionsgefährdete Bereiche kreuzen, nur an einem Ende.
- Verlegen Sie bei beidseitiger Erdung einen Potenzialausgleichsleiter.

⚠WARNUNG

Ungenügende Trennung von eigensicheren und nicht eigensicheren Stromkreisen

Explosionsgefahr in explosionsgefährdeten Bereichen

- Stellen Sie beim Anschluss von eigensicheren und nicht eigensicheren Stromkreisen sicher, dass die galvanische Trennung ordnungsgemäß unter Einhaltung örtlicher Vorschriften ausgeführt wird (z. B. IEC 60079-14).
- Beachten Sie die für Ihr Land geltenden Gerätezulassungen.

⚠WARNUNG

Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS)

Das Gerät ist für den Betrieb mit einer direkt anschließbaren Sicherheitskleinspannung (Safety Extra Low Voltage, SELV) durch eine Spannungsversorgung mit begrenzter Leistung (Limited Power Source, LPS) ausgelegt.

Deshalb dürfen nur Sicherheitskleinspannungen (SELV) mit begrenzter Leistung (Limited Power Source, LPS) nach IEC 60950-1 / EN 60950-1 / VDE 0805-1 mit den Versorgungsanschlüssen verbunden werden. Das Netzteil für die Versorgung des Geräts muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

Wenn das Gerät an eine redundante Spannungsversorgung angeschlossen wird (zwei getrennte Spannungsversorgungen), müssen beide die genannten Anforderungen erfüllen.

ACHTUNG

Geeignete Sicherungen für die Spannungsversorgungskabel (entspricht "Limited Energy")

Die Stromstärke an der Anschlussklemme darf 3 A nicht überschreiten. Verwenden Sie eine Sicherung für die Spannungsversorgung, die gegen Stromstärken > 3 A absichert.

Die Sicherung muss geeignet sein für den Schutz von DC-Spannungsversorgungskreisen und die nachfolgenden Anforderungen erfüllen.

- Im Geltungsbereich von NEC oder CEC muss die Sicherung folgende Anforderungen erfüllen:
  - Geeignet für DC (min. 60 V / max. 3 A)
  - Abschaltstrom min. 10 kA
  - UL/CSA listet (UL 248-1 / CSA 22.2 No. 248.1)
  - Classes R, J, L, T or CC
- In anderen Bereichen:
  - Geeignet für DC (min. 60 V / max. 3 A)
  - Abschaltstrom min. 10 kA
  - Zugelassen für Stromkreise (branch circuits) gemäß lokalen Bestimmungen (bspw. IEC 60127-1, EN 60947-1)
  - Abschaltcharakteristik: B oder C bei Leistungsschaltern und Schmelzsicherungen

Wenn die Eigenschaften der versorgenden Stromquelle bekannt sind, ist auch folgende Absicherung möglich:

- Im Geltungsbereich von NEC oder CEC muss die Sicherung folgende Anforderungen erfüllen:
  - Geeignet für DC (min. 60 V / max. 3 A)
  - Abschaltstrom > höchstmöglicher Strom der Stromquelle (inkl. Kurzschlussstrom und Fehlerfall)
  - Zulassung nach UL 1077 bzw. CSA C22.2 No. 235
- In sonstigen Bereichen muss die Sicherung folgende Anforderungen erfüllen:
  - Geeignet für DC (min. 60 V / max. 3 A)
  - Abschaltstrom > höchstmöglicher Strom der Stromquelle (inkl. Kurzschlussstrom und Fehlerfall)
  - Zulassung nach IEC/EN 60934
  - Abschaltcharakteristik: Max. 120 s bei 2 x I_n

Sie benötigen keine Sicherung für die Versorgungsleitung, wenn Sie eine Spannungsquelle gemäß NEC Class 2 oder eine Spannungsversorgung aus dem Zubehörprogramm verwenden, siehe Anhang Stromversorgung (Seite 197).

Empfehlung: Verwenden Sie die Spannungsversorgung einer Prozess-Station, wenn sich diese in räumlicher Nähe des Gateways befindet.

Hinweis

Schutzerdung

Ein PELV-Stromkreis enthält eine Verbindung zur Schutzerdung. Ohne Verbindung zur Schutzerdung oder im Fall, dass ein Fehler in der Verbindung zur Schutzerdung auftritt, werden die Spannungen des Stromkreises nicht geregelt.

ACHTUNG
Sicherungen für die Kabel des Digitalausgangs (entspricht "Limited Energy") Die Stromstärke an der Anschlussklemme darf 1 A nicht überschreiten. Verwenden Sie eine Sicherung für die Spannungsversorgung, die gegen Stromstärken > 1 A absichert. Die Sicherung muss geeignet sein für den Schutz von DC-Spannungsversorgungskreisen und die nachfolgenden Anforderungen erfüllen. • Im Geltungsbereich von NEC oder CEC muss die Sicherung folgende Anforderungen erfüllen: – Geeignet für DC (min. 60 V / max. 1 A) – Abschaltstrom min. 10 kA – UL/CSA listet (UL 248-1 / CSA 22.2 No. 248.1) – Classes R, J, L, T or CC • In anderen Bereichen: – Geeignet für DC (min. 60 V / max. 1 A) – Abschaltstrom min. 10 kA – Zugelassen für Stromkreise (branch circuits) gemäß lokalen Bestimmungen (bspw. IEC 60127-1, EN 60947-1) – Abschaltcharakteristik: B oder C bei Leistungsschaltern und Schmelzsicherungen

Für den Digitalausgang ist auch folgende Absicherung möglich:

- Im Geltungsbereich von NEC oder CEC muss die Sicherung folgende Anforderungen erfüllen:
  - Geeignet für DC (min. 60 V / max. 1 A)
  - Abschaltstrom > höchstmöglicher Strom der Stromquelle (inkl. Kurzschlussstrom und Fehlerfall)
  - Zulassung nach UL 1077 bzw. CSA C22.2 No. 235
- In sonstigen Bereichen muss die Sicherung folgende Anforderungen erfüllen:
  - Geeignet für DC (min. 60 V / max. 1 A)
  - Abschaltstrom > höchstmöglicher Strom der Stromquelle (inkl. Kurzschlussstrom und Fehlerfall)
  - Zulassung nach IEC/EN 60934
  - Abschaltcharakteristik: max. 120s bei 2 x I_n

Reihenfolge der Arbeiten

ACHTUNG
Anschluss nur im spannungslosen Zustand Schließen Sie das Gerät nur im spannungslosen Zustand an. Das Gerät kann mit dem Klemmenblock von der Spannungsversorgung getrennt werden.

Voraussetzung: Das Gerät ist montiert.

1. Schließen Sie die externe Spannungsversorgung am Klemmenblock des Geräts an.

   Verwenden Sie die Funktionserdung (siehe unten) für die Erdung des Gateways.

2. Verbinden Sie die Leitungen der beiden Ethernet-Netze mit den Schnittstellen des Geräts.

   Beachten Sie den Hinweis im Kapitel Ethernet-Schnittstellen P1/P2 (Seite 34).

3. CC716:

   Schließen Sie das Gateway an der RS485-Buchse über eine Steckleitung an PROFIBUS an.

ACHTUNG
Auflegen der Schirmung des Kabels am Stecker Der Schirm des Kabels muss aufgelegt werden. Isolieren Sie hierzu das Kabel am Ende ein Stück ab und verbinden Sie den Schirm mit der Funktionserdung.

4. CC716:

   Schließen Sie bei Bedarf die Kabel für den digitalen Eingang / Ausgang am Klemmenblock des Geräts an.

   - Verdrahten Sie den digitalen Eingang und Ausgang immer paarweise.
   - Die maximal zulässige Leitungslänge beträgt 30 m.

   Zur Lage der Klemmen siehe Kapitel Digitaler Eingang / Ausgang (CC716) (Seite 35).

5. Schalten Sie die Spannungsversorgung erst ein, nachdem das Gerät komplett verdrahtet und angeschlossen ist.

Das weitere Vorgehen ist im Kapitel Inbetriebnehmen (Seite 55) beschrieben.

Klemmenblöcke für digitalen Eingang/Ausgang und Spannungsversorgung

Die steckbaren Klemmenblöcke für die Buchsen haben einen mechanischen Verpolschutz.

Weitere technische Details finden Sie im Kapitel Technische Daten (Seite 185).

Digitaler Eingang / Ausgang (CC716)

Tabelle 5- 1 Belegung der Buchsen für den Digitaleingang (DI) und Digitalausgang (DO)

Klemme	Belegung
DI+	DC 24 V
DI- (Masse)	-
DO+	max. DC 24 V / max. 1 A
DO-	-

Spannungsversorgung

Hinweis

Das Netzteil des Geräts ist nicht potenzialgetrennt.

Verwenden Sie für die Spannungsversorgung nur Kupferleitungen.

Tabelle 5- 2 Belegung der Buchse für die Spannungsversorgung

Klemme	Belegung
L1+	DC 24 V
M1	Bezugsmasse
M2	Bezugsmasse für redundanten Anschluss (optional)
L2+	DC 24 V für redundanten Anschluss (optional)
⏚	Funktionserdung

5.4 Inbetriebnehmen

5.4.1 Inbetriebnahme

Inbetriebnahme

1. Schalten Sie nach dem Anschluss der Spannungsversorgung an das Gateway die Spannungsversorgung ein.
2. Verbinden Sie den Projektierungs-PC zur Konfiguration mit dem Gateway, siehe Kapitel Verbindung mit dem WBM aufbauen (Seite 68).

Wenn Sie einen CLP verwenden möchten, dann schalten Sie vor Beginn der Projektierung die Spannungsversorgung aus, stecken den CLP und schalten die Spannungsversorgung wieder ein.

Zur Erleichterung der Projektierungsarbeiten bei der Inbetriebnahme mehrerer Gateways siehe Kapitel Konfiguration (Seite 172).

Voraussetzungen für den Betrieb

Mindestens die folgenden Voraussetzungen sind erforderlich für den Betrieb des Gateways:

- Projektierung des Geräts
- Mindestens eine laufende Prozess-Station
- Ein eingerichteter Cloud-Dienst oder externer OPC UA-Client am internen OPC UA-Server
- Anschluss des Gateways an die Netze der Kommunikationspartner

Übernahme von Projektierungsdaten während der Inbetriebnahme

Zu den Schaltflächen des WBM siehe Kapitel Allgemeine Funktionen des WBM (Seite 63).

Die Schaltfläche "Speichern"

Bestätigen Sie alle Ihre Eingaben durch Klicken auf die Schaltfläche "Speichern". Dadurch werden die Einstellungen in den Zwischenspeicher, aber noch nicht vom Gerät übernommen. Dadurch wird vermieden, dass inkonsistente Änderungen bei einem Wechsel der WBM-Seite in das Laufzeitsystem geladen werden.

Die Schaltfläche "Übernehmen"

Alle gespeicherten Konfigurationsdaten werden mit Klicken auf das Symbol "Übernehmen" in das Laufzeitsystem übernommen.

5.4.2 Nutzung eines CLP

Wechselmedium CLP

Das Gateway kann mit einem austauschbaren CLP betrieben werden. Auf diesem Wechselmedium können die Projektierungsdaten spannungsausfallsicher gespeichert werden.

Durch dieses Wechselmedium wird der Ersatzteilfall des Gateways vereinfacht. Durch einfachen Austausch können alle Daten ohne erneute Projektierung übernommen werden.

Der CLP wird vom Gateway mit Spannung versorgt. Der CLP behält in stromlosem Zustand alle Daten dauerhaft.

Hinweis

Verwendung fabrikneuer CLPs

Wenn Sie einen fabrikneuen CLP verwenden, dann gehen Sie folgendermaßen vor:

1. Stecken Sie den CLP in das ausgeschaltete Gateway.
2. Schalten Sie die Spannung des Gateways ein.
3. Formatieren Sie den CLP.
   Siehe hierzu Kapitel Konfiguration (Seite 172).

Nach dem Klicken auf die Schaltfläche "Übernehmen" werden ab jetzt die Projektierungsdaten des Gateways automatisch auf den CLP geschrieben.

Anlauf des Gateways mit Konfigurationsdatei auf CLP

Wenn eine Konfigurationsdatei auf dem CLP gespeichert ist und Sie stecken den CLP in ein Gateway, dann wird diese Konfiguration durch Klicken auf die Schaltfläche "Übernehmen" überschrieben.

Durch Einsetzen eines CLP mit gültigen Projektierungsdaten in ein fabrikneues oder auf Werkseinstellungen zurückgesetztes Gateway können Sie bewirken, dass das Gateway mit der im CLP gespeicherten Konfigurationsdatei anläuft.

Funktion

Auf dem CLP wird die Konfiguration des Gateways automatisch gespeichert, wenn Sie die Projektierung im WBM übernehmen.

Ein Gerät mit gestecktem CLP verwendet beim Anlauf die Konfigurationsdaten auf dem CLP nur, wenn der Zustand auf Werkseinstellungen zurückgesetzt ist. Voraussetzung hierfür ist, dass die Daten von einem kompatiblen Gerätetyp geschrieben wurden.

Somit wird im Fehlerfall ein schneller und einfacher Austausch des Grundgerätes ermöglicht. Im Ersatzteilfall wird der CLP aus dem ausgefallenen Gerät entnommen und in das Ersatzteil gesteckt. Das Ersatzgerät übernimmt beim Erstanlauf automatisch die gleiche Gerätekonfiguration wie das ausgefallene Gerät.

Einsetzen des CLP und Anlaufverhalten

Hinweis

Ziehen und Stecken nur im spannungslosen Zustand

Der CLP darf nur im spannungslosen Zustand gesteckt oder gezogen werden!

Der Steckplatz für den CLP befindet sich auf der Geräterückseite, siehe Kapitel CLP-Schacht (Seite 39).

Gehen Sie zum Einsetzen des CLP folgendermaßen vor:

1. Schalten Sie das Gateway spannungslos.
2. Setzen Sie den CLP in den Steckplatz.

   Der CLP kann nur in einer Position gesteckt werden.
3. Schalten Sie die Spannung wieder ein.

   Das Verhalten des Gateways hängt vom Zustand des Gateways und des CLP ab:

- Gateway ist auf Werkseinstellungen zurückgesetzt (z. B. fabrikneu)
  - CLP unformatiert (Werkszustand) oder zuvor in anderem Gerätetyp verwendet:

    Gateway läuft ohne Projektierungsdaten an, CLP bleibt unformatiert.
  - CLP durch ein kompatibles Gateway formatiert - CLP ohne Projektierungsdaten:

    Gateway läuft ohne Projektierungsdaten an.
  - CLP durch ein kompatibles Gateway formatiert - CLP mit gültigen Projektierungsdaten:

    Gateway läuft mit den Projektierungsdaten des CLPs an.
- Gateway mit intern gespeicherten Projektierungsdaten
  - CLP unformatiert (Werkszustand) oder zuvor in anderem Gerätetyp verwendet:

    Gateway läuft mit interner Projektierung an, CLP bleibt unformatiert.
  - CLP durch ein kompatibles Gateway formatiert - CLP ohne Projektierungsdaten

    Gateway läuft mit interner Projektierung an. Durch Änderung und Übernehmen der Konfiguration wird die Projektierung auf den CLP geschrieben.
  - CLP durch ein kompatibles Gateway formatiert - CLP mit gültigen Projektierungsdaten:

    Gateway läuft mit interner Projektierung an. Durch Änderung und Übernehmen der Konfiguration wird die Projektierung auf den CLP geschrieben.

Entnehmen des CLP

1. Schalten Sie das Gerät spannungslos.
2. Setzen Sie einen Schraubendreher zwischen die Vorderkante des CLP und den Steckplatz und entnehmen Sie den CLP.

Diagnose

Fehlfunktionen des CLP werden über Diagnosemeldungen signalisiert.

5.5 Demontage

⚠WARNUNG

Unsachgemäße Demontage

Durch unsachgemäße Demontage kann in explosionsgefährdetem Bereich Explosionsgefahr entstehen.

Für eine sachgemäße Demontage beachten Sie Folgendes:

- Stellen Sie vor Beginn der Arbeiten sicher, dass die Elektrizität abgeschaltet ist.
- Sichern Sie verbleibende Anschlüsse so, dass bei versehentlichem Hochfahren der Anlage kein Schaden als Folge der Demontage entstehen kann.

5.6 Wartung und Reinigung

⚠VORSICHT

Heiße Oberflächen

Verbrennungsgefahr bei Wartungsarbeiten an Teilen, die Oberflächentemperaturen über 70 °C (158 °F) aufweisen.

- Ergreifen Sie entsprechende Schutzmaßnahmen, z. B. Tragen von Schutzhandschuhen.
- Stellen Sie nach Wartungsarbeiten die Berührungsschutzmaßnahmen wieder her.

⚠WARNUNG

Unzulässige Reparatur von Geräten in explosionsgeschützter Ausführung

Explosionsgefahr in explosionsgefährdeten Bereichen

- Reparaturarbeiten dürfen nur durch von Siemens autorisiertes Personal durchgeführt werden.

⚠WARNUNG

Unzulässiges Zubehör und Ersatzteile

Explosionsgefahr in explosionsgefährdeten Bereichen

- Verwenden Sie ausschließlich Originalzubehör und Originalersatzteile.
- Beachten Sie alle relevanten Installations- und Sicherheitsanweisungen, die in den Anleitungen zum Gerät beschrieben sind oder mit dem Zubehör oder Ersatzteil mitgeliefert werden.

⚠WARNUNG

Gehäuse reinigen

- **Im explosionsgefährdeten Bereich**
  Reinigen Sie die äußeren Gehäuseteile nur mit einem feuchten, aber nicht nassen Tuch.
- **Im Nicht-Ex-Bereich**
  Reinigen Sie die äußeren Gehäuseteile nur mit einem trockenen Tuch.

Verwenden Sie keine Flüssigkeiten oder Lösungsmittel.

Projektierung

6

HTTPS-Verbindung über die Prozess-Schnittstelle

Aus Security-Gründen können Sie von Ihrem PC aus einer Verbindung mit dem WBM in Werkseinstellungen nur über die Prozess-Schnittstelle des Gateways aufbauen.

Hinweis

Stellen Sie sicher, dass PC und Gateway in einem geschützten Netzwerk liegen.

Die Cloud-Schnittstelle ist für den Zugang zum WBM in Werkseinstellungen gesperrt. Auf der Seite "Instandhaltung" > "HTTP-Server" kann die Schnittstelle für den WBM Betrieb aktiviert werden.

6.1 Übersicht der WBM-Seiten

Öffnen der WBM-Seiten

Oben auf jeder WBM-Seite finden Sie alle Seitentitel, die Sie für die Navigation durch das WBM benötigen.

Öffnen Sie eine WBM-Seite durch Klicken auf den Seitentitel.

Die Register des WBM

Die folgende Liste gibt einen Überblick über die WBM-Seiten und deren Funktionen.

- Info (Seite 71)
  - Info
  - Kommunikation
  - Systemüberwachung
  - Netzwerk

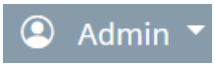
  Diese Seiten geben einen Überblick über wichtige Zustands- und Projektierungsdaten des Gateways.
- Schnittstellen-Konfiguration (Seite 76)
  - Projektierung der Gateway Ethernet-Schnittstellen
  - Projektierung der PROFIBUS / MPI Schnittstelle (CC716)
  - Projektierung des digitalen Eingangs/Ausgangs (CC716)
- Prozess-Zugang (Seite 84)
  - Projektierung S7-Station (S7 Ethernet / S7 PROFIBUS/MPI (CC716))
  - Projektierung Modbus-Station
  - Projektierung OPC UA-Station
- OPC UA-Server (Seite 95)
  - Projektierung des OPC UA-Servers
  - Projektierung und Verwaltung des XML Nodesets
- Cloud-Konfiguration (Seite 106)
  - Projektierung der MQTT-Einstellungen
  - Projektierung der HTTP-Einstellungen
  - Publisher: Projektierung der Topics/Gruppen, des Nutzdatenformats und Zuweisung der Datenpunkte
  - Subscriber: Projektierung der Topics/Gruppen und Zuweisung der Datenpunkte

- Datenpunkte (Seite 141)
  - Projektierung der Datenpunkte der Prozess-Stationen
- Instandhaltung (Seite 160)
  - Verwalten der Webserver Einstellungen
  - Uhrzeitsynchronisation / Stellen der Uhrzeit
  - Zertifikate erstellen und verwalten
  - Benutzerverwaltung
  - Firmware-Aktualisierung
  - Sicherung und Wiederherstellung der Konfiguration
  - Prozess-Kommunikation, Neustart
  - Diagnosemeldungen
  - Export von Protokollierungsdaten

6.2 Allgemeine Funktionen des WBM

Symbole der Funktionsleiste

Über die Anzeigen und Symbole in der Funktionsleiste erreichen Sie folgende Funktionen:

Symbol	Funktion
	Uhrzeit und Datum des Laufzeitsystems
	Profil: Benutzerprofil bearbeiten Sprache: Umstellen der WBM-Sprache Abmelden: Beendet die Verbindung mit dem WBM.
	Übernehmen Alle gespeicherten Daten sind in das Laufzeitsystem übernommen.
	Öffnet die Online-Hilfe des WBM.
	Zeigt die Anzahl der aktiven Sitzungen an.

Menüleiste

Die Menüleiste zeigt die Register des WBM an, durch welche Sie die verschiedenen Seiten des WBM erreichen.

Wenn Sie Ihr Browser-Fenster verkleinern, verschwindet die Anzeige der Register und das folgende Symbol erscheint:

Symbol	Funktion
☰	Blendet die Registertitel bei verkleinertem Browser-Fenster als Navigation ein.

Eingabefelder mit Filter

Eingabefelder, die wie folgt abgebildet sind, haben eine Filterfunktion. Wenn Sie ein Zeichen oder eine Zeichenfolge eingeben und auf das Filter-Symbol klicken, dann werden alle vorhandenen Elemente eingeblendet, welche diese Zeichenfolge enthalten. Folgende Platzhalter können Sie beim Filtern verwenden:

- %

  Das Prozentzeichen dient als Platzhalter für eine beliebige Zeichenfolge.

- _

  Der Unterstrich dient als Platzhalter für exakt ein beliebiges Zeichen.

Wollen Sie das Prozentzeichen oder den Unterstrich als Zeichen und nicht als Platzhalter benutzen, schreiben Sie ein Backslash "\" vor das Zeichen.

Sie finden diese Eingabefelder beispielsweise bei der Zuordnung von Datenpunkten zu Topics.

Bild 6-1 Leeres Eingabefeld mit Cursor

Speichern

Bestätigen Sie alle Ihre Eingaben durch Klicken auf die Schaltfläche "Speichern". Ihre Einstellungen werden dadurch in den Zwischenspeicher übernommen.

Die gespeicherten Konfigurationsdaten werden durch das Speichern noch nicht vom Gerät übernommen. Dadurch wird vermieden, dass inkonsistente Änderungen bei einem Wechsel der WBM-Seite in das Laufzeitsystem geladen werden.

Übernahme in das Laufzeitsystem 

Alle gespeicherten Konfigurationsdaten werden mit Klicken auf das Symbol "Übernehmen" in das Laufzeitsystem übernommen.

Fehleingaben bei der Projektierung

Die Eingabefelder des WBM werden bei der Eingabe auf fehlerhafte Inhalte und Konsistenz geprüft. Zu Feldern mit erkannten Fehlern werden beim Speichern Hinweise ausgegeben. Die Einstellungen können erst nach erfolgreicher Korrektur gespeichert werden.

Ausgegraute Felder können nicht editiert werden.

6.3 Zugelassene Zeichen und Parameter-Längen

6.3.1 Zugelassene Zeichen- und Parameterlängen

Bei der Projektierung von Benutzerdaten, Passwörtern, Geräteparametern etc. sind häufig ASCII-Zeichensätze angegeben. Nachfolgend finden Sie die ASCII-Zeichensätze mit ihrem hexadezimalen Code und den dazugehörenden Zeichen.

Standardzeichen

- **0x30 .. 0x39**

  0 1 2 3 4 5 6 7 8 9
- **0x41 .. 0x5A**

  A B C D E F G H I J KL M N O P Q R S T U V W X Y Z
- **0x61 .. 0x7A**

  a b c d e f g h i j k l m n o p q r s t u v w x y z

Sonderzeichen

- **0x21 .. 0x2F**

  ! " # $ % & ' ( ) * + , - . /
- **0x3A .. 0x40**

  : ; < = > ? @
- **0x5B .. 0x60**

  [\ ] ^ _ `
- **0x7B .. 0x7E**

  { | } ~

Sonderzeichen ≥ 0x80

- **0x80, 0xA3, 0x8A, 0x9A, 0x8E, 0x9E, 0xB5**

  € £ Š š Ž ž µ
- **0xC0 .. 0xFF**

  À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

Hinweis

Zeichenbegrenzung

Eingabefelder haben eine definierte maximale String-Größe, z.B. 1024 Byte. Bei Eingabe werden die Bytes gezählt, nicht die Zeichen. Somit können Sie beispielsweise folgende Werte in Abhängigkeit des Datentyps speichern.

Datentypen:

- 1024 ASCII-Zeichen
- 1024 x Byte Daten
- 512 x Sondersymbole nach UTF-8
- oder eine Mischung verschiedener Datentypen mit einer Gesamtgröße bis zu 1024 Byte.

Tabelle 6- 1 **Zeichen und Formate der im WBM eingebbaren Strings**

Parameter	String min.	String max.	**Zugelassene Zeichen / Format**
Name, Topic	1	1024	**Standardzeichen** **0x20 Leerzeichen** / + - _ . : ; @
Hostname	0	255	Entsprechend den Regeln für DNS-Namen mit einer Kombination aus: • 0x2D .. 0x2E • 0x30 .. 0x39 (keine Ziffern alleine) • 0x41 .. 0x5A • 0x61 .. 0x7A
Benutzername (Benutzer, OPC, Cloud)	2	1024	Alle oben angegebenen Zeichen
Passwort (Benutzer, OPC, Cloud, Zertifikat, privater Schlüssel)	0	1024	Alle oben angegebenen Zeichen
OPC Server / Client			
Application URI	1	1024	**Standardzeichen** / + - _ . : ; @
Applikationsname	1	1024	**Standardzeichen** / + - _ . : ; @
URL-Pfad (optional)	1	1024	**Standardzeichen** & / = ? # - _
Namensraum-URI	0	1024	**Standardzeichen** / + - _ . : ; @
Name des Wurzelverzeichnisses	0	1024	**Standardzeichen** / + - _ . : ; @
NodeID des Wurzelverzeichnisses	0	1024	**Standardzeichen** / + - _ . : ; @
Cloud connection			
Client ID	1	254	Alle oben angegebenen Zeichen
Topic-Präfix	0	1024	Alle oben angegebenen Zeichen
Topic-Suffix	0	1024	Alle oben angegebenen Zeichen
Letzter-Wille-Topic	1	65535	Alle oben angegebenen Zeichen
Letzter Wille / Testament	0	65535	Alle oben angegebenen Zeichen

Device Name	0	1024	Alle oben angegebenen Zeichen
Device Typ	0	1024	Alle oben angegebenen Zeichen
Nutzdaten-Vorlagen			
Version	0	2	**0x30 .. 0x39**
Zertifikate			
Name der Organisation (O)	0	64	**Standardzeichen** / + - _ . : , ; @
Organisationseinheit (OU)	0	64	**Standardzeichen** / + - _ . : , ; @
Stadt (L)	0	128	**Standardzeichen** / + - _ . : , ; @
Staat oder Bundesland (ST)	0	128	**Standardzeichen** / + - _ . : , ; @
Land (C)	0	2	Zwei-Buchstaben Ländercode (nach ISO 3166)
Common name (CN)	0	64	**Standardzeichen** / + - _ . : , ; @
Domain-Komponente (DC)	0	16	**Standardzeichen** / + - _ . : , ; @
URI	0	1024	Entsprechend den Regeln für DNS-Namen mit einer Kombination aus: • 0x2D .. 0x2E • 0x30 .. 0x39 (keine Ziffern alleine) • 0x41 .. 0x5A • 0x61 .. 0x7A
DNS-Name	0	255	Entsprechend den Regeln für DNS-Namen mit einer Kombination aus: • 0x2D .. 0x2E • 0x30 .. 0x39 (keine Ziffern alleine) • 0x41 .. 0x5A • 0x61 .. 0x7A
E-Mail	3	254	Die E-Mail-Adresse ist folgendermaßen aufgebaut: Teil1@Teil2.Teil3 Teil 1@: Standardzeichen + Sonderzeichen (< 0x80; es ist nur ein "@" Zeichen erlaubt) Teil 2+3: Standardzeichen

6.4 Aufrufen des WBM

6.4.1 API

Der API-Server des Gateways ist permanent aktiv.

Über die HTTP basierte Schnittstelle kann das Gateway automatisiert konfiguriert und diagnostiziert werden.

Weiterführende Informationen zur Konfiguration des WBMs des Gateways mit der API-Schnittstelle finden Sie im Getting Started "SIMATIC CC7 API-Server". Siehe Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621/man)

6.4.2 Verbindung mit dem WBM aufbauen

Voraussetzungen

Sie können eine Verbindung zwischen einem PC und dem Gateway ausschließlich über HTTPS aufbauen.

Sie können eine Verbindung über die Schnittstelle P2 des Gateways aufbauen.

Voraussetzung für den Zugriff auf das Gateway ist, dass der PC im selben Subnetz liegt und das Gateway erreichbar ist.

Erster Verbindungsaufbau mit vorbelegter IPv4-Adresse

Verwenden Sie beim ersten Verbindungsaufbau folgende vorbelegte IPv4-Adresse des Gateways:

- Adresse Schnittstelle P2: 192.168.0.55 / 24

Hinweis

IP-Adresse des PC

In der Voreinstellung ist der DHCP-Client des Gateways deaktiviert. Achten Sie beim ersten Verbindungsaufbau darauf, dass der PC eine feste IP-Adresse hat und im gleichen Subnetz liegt wie die angeschlossene Schnittstelle des Gateways.

Bei Nutzung eines DHCP-Servers sind Sie mit der Adressierung des anzuschließenden PC frei. Beim Anschluss des PC an das Netz wird dem PC eine Adresse vergeben.

Verbindung mit dem Webserver des Gateways

Gehen Sie folgendermaßen vor, um sich von dem PC mit dem Webserver des Gateways zu verbinden:

1. Öffnen Sie den Webbrowser.
2. Geben Sie die IP-Adresse des Gateways in die Adresszeile des Webbrowsers ein:
   - https://<Adresse>

   Wenn Sie über HTTP zugreifen, wird die Adresse automatisch auf HTTPS umgeleitet.

   Bei HTTPS-Verbindungen kann beim Anmelden eine Warnmeldung erscheinen, dass die Webseite unsicher ist oder das Zertifikat nicht vertrauenswürdig. Wenn Sie sicher sind, dass Sie die richtige Adresse eingegeben haben, dann ignorieren Sie die Meldung. Fügen Sie die Verbindung gegebenenfalls zu den Ausnahmen hinzu (abhängig vom Webbrowser).

Bei erfolgreichem Verbindungsaufbau öffnet sich das Anmeldefenster des WBM.

6.4.3 Benutzerdaten für das erste Anmelden am WBM

HTTPS-Verbindung

Es werden nur HTTPS-Verbindungen unterstützt.

Es kann maximal eine Verbindung zwischen einem PC und dem WBM des Geräts aufgebaut werden.

Ändern der Standard-Benutzerdaten

Nach dem Aufbau einer Verbindung zwischen PC und dem Gerät öffnet sich das WBM mit der Anmeldeseite.

Hinweis

Ändern der Standard-Benutzerdaten

Aus Sicherheitsgründen müssen die werkseitig voreingestellten Benutzerdaten (Benutzername, Passwort) des Standardbenutzers nach dem ersten Anmelden geändert werden, siehe Kapitel Benutzer (Seite 168).

Systemseitig sind folgende Standard-Benutzerdaten für das erste Anmelden am WBM vorbelegt:

Benutzerdaten	Werkseitig voreingestellte Werte
Benutzername	admin
Passwort	admin

Für die Bedienung des WBM kann ein Administrator mit allen verfügbaren Rechten eingerichtet werden.

6.4.4 Anmelden

Anmelden

Nach dem Aufbau einer Verbindung zwischen PC und dem Gerät öffnet sich das WBM mit der Anmeldeseite.

Hinweis

Fehleingabe von Benutzername oder Passwort

Nach dreimaliger Eingabe eines falschen Benutzernamens oder eines falschen Passworts beginnt eine Sperrzeit von einer Minute. Erst nach Ablauf der Sperrzeit können Sie erneut versuchen, sich anzumelden.

- **Benutzername**

  Geben Sie hier den Benutzernamen ein.

- **Passwort**

  Geben Sie hier das Passwort ein.

- **Anmelden**

  Klicken Sie auf die Schaltfläche, um die Verbindung mit dem WBM aufzubauen.

Beim ersten Anmelden werden Sie aufgefordert, die Standard-Benutzerdaten zu ändern. Die Regeln zur Passwortvergabe finden Sie im Kapitel Benutzer (Seite 168).

Open Source Software und Links zu weiteren Informationen

Unten auf der Anmeldeseite finden Sie folgende Links:

- **Online help**

  Öffnet die Online-Hilfe des WBM.

- **Open Source Software**

  Öffnet das Dokument der Lizenzbedingungen zu Open Source Software.

  Das Dokument können Sie bei Bedarf auf Ihrem PC speichern.

- **Siemens Industry Online Support**

  Öffnet die Seite des Gateways im Internet-Portal des Siemens Industry Online Support.

6.4.5 Abmelden

Manuelles Abmelden über das WBM

Um sich vom WBM abzumelden, klicken Sie in der Funktionsleiste auf den Benutzer und wählen Sie in der Auswahlliste die Option "Abmelden".

Die Verbindung mit dem Gerät wird abgebaut. Alle nicht zuvor gespeicherten Änderungen an den Projektierungsdaten gehen verloren.

Automatisches Abmelden nach Zeitüberschreitung

Nach Ablauf des eingestellten Timeouts (default 600 Sekunden), ohne Speichern oder Wechsel der WBM-Seite, werden Sie abgemeldet und die Verbindung zum WBM wird abgebaut. In diesem Fall müssen Sie sich erneut anmelden.

6.5 Info

6.5.1 Info

Die Seite gibt einen Überblick über wichtige Zustands- und Projektierungs-Daten des Geräts.

Status

- **Betriebszustand**

  Betriebszustand des Geräts
- **Prozess-Kommunikation**

  Zeigt den Zustand der Kommunikation mit den Prozess-Stationen an.
- **Systemlaufzeit (dd-hh-mm-ss)**

  Zeit seit dem letzten Anlauf (dd-hh-mm-ss)
- **Seriennummer**

  Seriennummer des Geräts
- **Artikelnummer**

  Artikelnummer des Geräts
- **Hardware-Erzeugnisstand**

  Hardware-Erzeugnisstand des Geräts
- **U-Boot-Version**

  Aktuelle U-Boot-Version für den Firmware-Boot-Loader

- **Firmware-Version**

  Aktuelle Firmware-Version des Geräts
- **CLP**

  Zeigt an, ob aktuell ein CLP gesteckt ist.
- **Applikations-Prüfsumme**

  Prüfsumme für die aktuelle Firmware Version
- **Konfigurations-Prüfsumme**

  Prüfsumme für die aktuelle Konfiguration des CC7
- **Stromversorgung**

  Zeigt an, ob die Baugruppe über Buchse L1+, L2+ oder über beide versorgt wird.

Prozess-Schnittstelle (P2)

Die Parametergruppe zeigt die aktuellen Adressdaten der Schnittstelle P2 an.

- **MAC-Adresse**
- **IPv4 / IPv6**

  Adressparameter, Default-Router

Cloud-Schnittstelle (P1)

Die Parametergruppe zeigt die aktuellen Adressdaten der Schnittstelle P1 an.

- **MAC-Adresse**
- **IPv4 / IPv6**

  Adressparameter, Default-Router

DNS

- **Hostname**

  Zeigt den lokalen Hostnamen an.
- **DNS-Server**

  Die Parametergruppe zeigt die Adressen von bis zu zwei projektierten oder per DHCP zugewiesenen DNS-Servern an.

6.5.2 Kommunikation

Auf dieser Seite erhalten Sie eine Übersicht zu allen projektierten Prozess-Stationen, der Cloud-Verbindung und dem OPC UA-Server.

Aktualisierung

Hier stellen Sie ein, ob und in welchem Zyklus das WBM die angezeigten Diagnosemeldungen aktualisiert**.**

Prozess-Kommunikation

Zeigt den Zustand der Kommunikation mit den Prozess-Stationen an.

- **Protokoll**

  Zeigt das Protokoll der Prozess-Station an (S7 Ethernet, S7 PROFIBUS / MPI, OPC UA, Modbus / TCP, MQTT, HTTP).

- **Name**

  Zeigt den projektierten Stationsnamen an.

- **Adresse**
  - Bei S7 Ethernet: Anzeige der projektierten IP-Adresse und TSAP
  - Bei S7 PROFIBUS / MPI: Anzeige der projektierten PROFIBUS- / MPI-Adresse und TSAP
  - Bei OPC UA-Client und Modbus: Anzeige der projektierten IP-Adresse und der Portnummer
  - Nur bei OPC UA: Anzeige der verwendeten Security Policy
- **Verbindung**

  Zeigt über ein Symbol den Verbindungsstatus zur Station an:
  - ?: Noch keine Informationen erhalten, Aktualisierung der Seite notwendig, kein Datenpunkt zugewiesen
  - zwei grüne Pfeile: Station verbunden
  - drehender orangener Pfeil: Verbindungsaufbau
- **Polling-Zyklus**

  Zeigt die durchschnittliche Dauer der letzten 100 Lesezyklen für jede S7 Ethernet-, S7 PROFIBUS- und Modbus-Station. Die Dauer kann mit der projektierten Zykluszeit verglichen werden.

  Keine Zeit "--" wird angezeigt:
  - Wenn noch keine 100 Werte ermittelt wurden
  - Bei OPC UA Client-Stationen

Cloud-Kommunikation

Zeigt den Zustand der Kommunikation mit dem aktiven Cloud-Profil an.

- **Adresse**
  - Anzeige der projektierten IP-Adresse und der Portnummer
- **Verbindung**

  Zeigt über ein Symbol den Verbindungsstatus zur Cloud an:
  - ?: Noch keine Informationen erhalten, Aktualisierung der Seite notwendig
  - zwei grüne Pfeile: Station verbunden
  - drehender orangener Pfeil: Verbindungsaufbau

OPC UA-Server

- **Security Policies**

  Alle erlaubten Policies des Servers.
- **Adresse**

  Alle Adressen des OPC UA-Servers.
- **Sitzungen**

  Anzahl der verbundenen OPC UA-Clients mit dem Server. Wenn Sie auf das Feld klicken, werden die IP-Adressen / Port / Security-Pofile der verbundenen Clients angezeigt.

Lesefehler/Schreibfehler

Die Felder sind grau hinterlegt, wenn keine Verbindung besteht. Sobald eine Verbindung aufgebaut ist, werden die Lese- und Schreibfehler gesammelt und angezeigt.

- grün: kein Fehler
- gelb: es liegt mind. 1 Fehler vor

Für eine schnelle Diagnose kann der Fehlertyp (z. B. BadTypeMismatch) über die Auswahlliste ausgelesen werden.

Die Lese- und Schreibfehler werden bei jedem Neustart bzw. Speichern und Bestätigen zurückgesetzt.

6.5.3 Systemüberwachung

Auf dieser Seite erhalten Sie eine Übersicht zur CPU-Auslastung und Speicherauslastung.

Aktualisierung

Hier stellen Sie ein, ob und in welchem Zyklus das WBM die angezeigten Diagnosemeldungen aktualisiert.

Aufgaben

6.5.4 Netzwerk

Auf dieser Seite erhalten Sie eine Übersicht zu den offenen Ports und den aufgebauten Verbindungen der Baugruppe.

Aktualisierung

Hier stellen Sie ein, ob und in welchem Zyklus das WBM die angezeigten Diagnosemeldungen aktualisiert.

Offene Ports

Zeigt den Zustand der Kommunikation mit den Prozess-Stationen an.

- **Applikation**

  Gibt an, um welchen Dienst es sich beim CC7 handelt.

- **Transport**

  UDP oder TCP

- **Adresse**

  IP-Adresse und Portnummer.

- **Status**

  Hörend: Der Port ist offen und wartet auf die Verbindung.

  Verbunden: Die Verbindung ist aufgebaut.

6.6 Schnittstellen-Konfiguration

6.6.1 Ethernet

In diesem Register projektieren Sie die Adressdaten der Ethernet-Schnittstellen des Geräts.

Hinweis

Änderungen an Einstellungen zu P1/P2 oder Hostname

Wenn Sie Änderungen an den Einstellungen zu den Schnittstellen P1/P2 oder dem Hostnamen vornehmen, wird eventuell der interne Netzwerkservice neu gestartet. Sie müssen sich dann erneut am WBM anmelden bzw. die Seite erneut aufrufen.

Schnittstellen und werkseitig vorbelegte Adressen

Auf der Webseite projektieren Sie folgende Schnittstellen:

- Prozess-Schnittstelle (P2)

  Die Schnittstelle (P2) dient dem Anschluss an das Subnetz der Prozess-Stationen und dem Zugriff auf das WBM der Baugruppe zur Projektierung.

- Cloud-Schnittstelle (P1)

  Die Schnittstelle (P1) dient dem Anschluss an das Internet oder an einen Router, über den der Broker oder das Netz mit externen OPC UA-Clients erreichbar ist.

Das Gerät unterstützt IPv4- und IPv6-Adressen.

Werkseitig sind folgende Adressdaten vorbelegt:

Tabelle 6- 2 Voreingestellte Adressdaten

	Werkseitig vorbelegte Adressdaten	
	Prozess-Schnittstelle (P2)	**Cloud-Schnittstelle (P1)**
IPv4-Adresse	192.168.0.55	192.168.121.55
IPv6-Adresse	-	-
Subnetzmaske	255.255.255.0	255.255.255.0

Prozess-Schnittstelle (P2) / Cloud-Schnittstelle (P1)

Hinweis

Keine Adressprüfung / Projektierungsregeln

Es wird keine automatische Prüfung der Adressbänder durchgeführt.

Achten Sie darauf, dass sich die Subnetze der beiden Schnittstellen unterscheiden.

Für die IPv6-Adresse ist die Projektierung von Link Local-, Multicast- und Broadcast-Adressen nicht zulässig.

Die Projektierung nehmen Sie für die beiden Schnittstellen separat vor.

Die nachfolgenden Parameter gelten für beide Schnittstellen.

- **IPv4 / IPv6**
  - **Aktiv**

    Aktivieren der jeweiligen IPv4- bzw. IPv6-Adresse

    Hinweis

    Nicht-Erreichbarkeit bei Übernahme der IP-Adressdaten der Prozess-Schnittstelle

    Die IP-Parameter der Prozess-Schnittstelle müssen zu den Einstellungen der IP-Adressdaten Ihres PC passen.

- **IP-Adresse über DHCP**

  Aktivieren Sie die Option, wenn Sie die Adressdaten der ausgewählten Schnittstelle von einem DHCP-Server beziehen möchten.

  Bei aktivierter Option sind die Felder der Adressdaten ausgegraut und die vom DHCP-Server bezogenen Werte werden angezeigt.

  Hinweis

  DHCP-Server

  Für die Nutzung der Funktion muss sich ein DHCP-Server im Subnetz befinden.

- **IP-Adresse**

  Zeigt die voreingestellte oder die zuletzt projektierte IP-Adresse an. Die tatsächliche IP-Adresse wird auf der Startseite "Info" angezeigt.

  Bei der Erst-Projektierung: Vergeben Sie die IP-Adresse der jeweiligen Schnittstelle oder aktivieren Sie die Adressvergabe durch einen DHCP-Server.

- **Subnetzmaske (nur IPv4)**

  Zeigt die voreingestellte, die zuletzt projektierte oder die vom DHCP-Server bezogene Subnetzmaske an.

  Bei der Erst-Projektierung: Vergeben Sie die Subnetzmaske der jeweiligen Schnittstelle.

- **Präfix-Länge** (nur IPv6)

  Zeigt den voreingestellten, den zuletzt projektierten oder den vom DHCP-Server bezogenen IPv6-Präfix an.

  Bei der Erst-Projektierung: Vergeben Sie den Präfix der jeweiligen Schnittstelle.

  Wertebereich: 0...128, default: 64

- **Default-Router**

  Zeigt die projektierte oder per DHCP bezogene IP-Adresse des verwendeten Routers an.

  Bei der Erst-Projektierung: Vergeben Sie die IP-Adresse des Routers.

- **Hostname**

  Bei aktivierter DHCP-Client-Funktion wird der projektierte Hostname über die DHCP-Option 12 an den DHCP-Server übertragen.

  Vorbelegung: cc7-device

DNS-Server

- **DNS-Server**

  Optional können Sie die IP-Adressen von bis zu zwei DNS-Servern projektieren.

  Bei aktiviertem DHCP-Server werden die bezogenen IP-Adressen der DNS-Server angezeigt.

  Wenn kein DNS-Server verwendet wird, ist das Adressfeld leer.

Routing-Tabelle

Hier legen Sie fest, über welche Routen, die nicht über den Default-Router erreicht werden können, ein Datenaustausch zwischen den verschiedenen Subnetzen stattfinden kann.

Sie können bis zu 20 statische Routen eingetragen.

- **Anlegen**

  Es kann eine weitere Route erzeugt werden. Sie werden auf eine separate Seite weitergeleitet.

- **Löschen**

  Die ausgewählte Tabellenzeile wird gelöscht.

- **Aktiv**

  Aktivieren und deaktivieren von bereits definierten Routen

- **Zieladresse**

  Geben Sie die IP-Adresse und dazugehörige Subnetzmaske des Ziels ein, das über diese Route erreichbar ist. Verwenden Sie die CIDR-Schreibweise, z. B. 192.168.28.0/24 oder 120.12.0.0/16.

- **Gateway-Adresse**

  Tragen Sie die IP-Adresse des Gateways ein, über das diese Netzwerkadresse erreichbar ist.

- **Schnittstelle**

  Angabe, ob die Route über Schnittstelle P1 oder P2 erreicht werden kann.

6.6.2 PROFIBUS / MPI (CC716)

In diesem Register projektieren Sie die Adressdaten der PROFIBUS-Schnittstelle und die Busparameter für den Netzanschluss des Gateways.

Berücksichtigen Sie bei manueller Projektierung ("Automatische Konfiguration" deaktiviert) die Adressbelegung durch bereits vorhandene Busteilnehmer, die am Bus eingestellte Übertragungsgeschwindigkeit sowie das Profil des angeschlossenen PROFIBUS-Netzes.

PROFIBUS-Konfiguration

- **Adresse**

  Eindeutige PROFIBUS/MPI-Adresse des Gateways im Bussystem

  Wertebereich: 0...126

  Anmerkung:
  Die Adresse des Kommunikationspartners des Gateways projektieren Sie im Register "Prozesszugang > Stations-Konfiguration".

- **Automatische Konfiguration**
  - Option aktiviert

    Das Gateway liest alle relevanten Projektierungsdaten vom angeschlossenen PROFIBUS-Netz. Die nachfolgenden Parameter werden für die Projektierung ausgeblendet.

  - Option deaktiviert

    Sie projektieren die PROFIBUS-Parameter selbst.

- **Übertragungsgeschwindigkeit**

  Übertragungsgeschwindigkeit am Bus, Wertebereich - abhängig vom Profil:

  9,6 kbit/s, 19,2 kbit/s, 45,45 kbit/s, 93,75 kbit/s, 187,5 kbit/s, 500 kbit/s, 1,5 Mbit/s, 3 Mbit/s, 6 Mbit/s, 12 Mbit/s

  Beim Profil "Universell" max. 1,5 Mbit/s

- **Höchste Adresse**

  Höchst mögliche PROFIBUS-Adresse eines Teilnehmers im PROFIBUS-Bussystem

  Wertebereich: 1...126

- **Profil**

  Hier legen Sie fest, nach welchem Verfahren (Algorithmus) die für den PROFIBUS-Betrieb maßgeblichen Busparameter berechnet werden sollen. Die verschiedenen Verfahren sind

an die jeweilige Betriebsart des Subnetzes optimal angepasst und führen zu einem stabilen Netzbetrieb.

- Standard/DP

  Das DP-Profil ist geeignet für die Verwendung des DP-Protokolls. Für ein homogenes DP-Netz mit maximal einem DP-Master der Klasse 1 und keinen weiteren DP-Mastern (PG zusätzlich ist möglich).

  Das Standard-Profil ist geeignet für den Multiprotokoll- und Multimasterbetrieb mit schnellen Busteilnehmern, beispielsweise allen SIMATIC NET S7-PROFIBUS-CPs.

- Universell

  Für den Betrieb mit Teilnehmern, die nicht in der Kategorie DP oder Standard betrieben werden können.

  Die Option ist nur bei einer Übertragungsgeschwindigkeit ≤ 1,5 Mbit/s auswählbar.

- Benutzerdefiniert

  In dieser Einstellung können Sie einige der Busparameter projektieren.

  Dieses Profil sollte nur von geschultem Fachpersonal gewählt werden. Ändern Sie die voreingestellten Werte nur, wenn Sie mit der Projektierung des Busprofils für PROFIBUS vertraut sind.

- **Anzahl Master / Anzahl Slaves**

  Bei Verwendung der Profile "Standard/DP" und "Universell" können Sie in diese beiden Eingabefelder die Anzahl der Master und Slaves im Netz angeben. Die Anzahl der Master und Slaves wird für die Berechnung der Busparameter im Netz verwendet.

  Zulässige Wertebereiche bei diesen Profilen:

  - Anzahl Master: 0..126
  - Anzahl Slaves: 0..126

  Bei Verwendung des Profils "Benutzerdefiniert" sind die beiden Eingabefelder gesperrt. In diesem Fall werden die Felder fest vorbelegt:

  - Anzahl Master: 1
  - Anzahl Slaves: 126

Busparameter

Die Parameter (siehe Tabelle), welche die Eigenschaften des PROFIBUS-Subnetzes beschreiben, sind weitgehend vorbelegt:

- Bei Verwendung der Profile "Standard/DP" und "Universell" sind die Busparameter fest vorgegeben bzw. werden aus diesen berechnet.
- Bei Verwendung des Profils "Benutzerdefiniert" können Sie einige der Busparameter projektieren.

Hinweis

Projektierung der Busparameter

Es wird empfohlen, die bereits im angeschlossenen PROFIBUS-Netz eingestellten Werte für die Busparameter zu übernehmen.

Busparameter	Wertebereich [1] (Vorbelegung) [2]	Bedeutung [3]
Tslot	815/995...16383 [1] (100...3000)	Slot time [t_Bit] Die Warte-auf-Empfang-Zeit legt fest, wie lange der Sender maximal wartet, um vom angesprochenen Partner eine Antwort zu erhalten. Bei der Berechnung werden folgende Parameter zugrunde gelegt, die Einfluss auf die Busphysik haben: • Leitungslänge: 1...1100 m • Anzahl Repeater: 0...10
Max. Tsdr	76...1023 [1] (55...980)	Maximale Protokoll-Bearbeitungszeit [t_Bit] Die maximale Protokoll-Bearbeitungszeit legt fest, nach welcher Zeit der antwortende Teilnehmer spätestens geantwortet haben muss. Max. Tsdr muss kleiner sein als die slot time.
Min. Tsdr	11...75 [1] (11...150)	Minimale Protokoll-Bearbeitungszeit [t_Bit] Die minimale Protokoll-Bearbeitungszeit legt fest, nach welcher Zeit der antwortende Teilnehmer frühestens antworten darf.
Tset	1...255 [1] (1...240)	Auslösezeit [t_Bit] Die Auslösezeit ist die Zeit, die zwischen dem Empfang eines Datentelegramms und der Reaktion darauf im Teilnehmer verstreichen darf.
Tqui	0...10 [1] (0...9)	Modulator-Ausklingzeit [t_Bit] Die Modulator-Ausklingzeit ist die Zeit, die ein sendender Teilnehmer nach Telegrammende für das Umstellen von Senden auf Empfangen benötigt.
GAP Factor	1...100 [1] (10...1000)	Der GAP-Aktualisierungsfaktor legt fest, nach wie vielen Token-Umläufen ein neu hinzugekommener aktiver Teilnehmer in den logischen Token-Ring aufgenommen werden kann.
Retry limit	1...15 [1] (1...10)	Mit dem Parameter wird festgelegt, wie viele Versuche (Telegrammwiederholungen) maximal unternommen werden, um einen Teilnehmer zu erreichen.
Tid2	55...980 Berechneter Wert	Ruhezeit 2 [t_Bit] Die Ruhezeit 2 legt fest, nach welcher Zeit ein sendender Teilnehmer nach der Versendung eines nicht quittierten Telegramms frühestens das nächste Telegramm versenden darf.
Trdy	11...150 Berechneter Wert	Bereitschaftszeit [t_Bit] Die Bereitschaftszeit gibt an, nach welcher Zeit ein sendender Teilnehmer frühestens ein Antworttelegramm empfangen kann.
Tid1	37...515 Berechneter Wert	Ruhezeit 1 [t_Bit] Die Ruhezeit 1 legt fest, nach welcher Zeit ein sendender Teilnehmer nach dem Empfang einer Antwort frühestens das nächste Telegramm versenden darf.

Busparameter	**Wertebereich [1] (Vorbelegung) [2]**	**Bedeutung [3]**
Ttr	256...16777960 [1] (0...49888)	Target Rotation Time [t_Bit] Die Soll-Token-Umlaufzeit ist die maximal zur Verfügung gestellte Zeit für einen Token-Umlauf. In dieser Zeit erhalten alle aktiven Teilnehmer (DP-Master etc.) einmal das Senderecht (Token). Die Differenz zwischen der Soll-Token-Umlaufzeit und der tatsächlichen Token-Haltezeit eines Teilnehmers bestimmt, wie viel Zeit den anderen aktiven Teilnehmern (PG, weitere DP-Master etc.) für das Senden von Telegrammen übrig bleibt. Empfehlung für den Wert: 5000 * "Höchste PROFIBUS-Adresse"
Ttr (ms)	Berechneter Wert	Target Rotation Time [Millisekunden], berechnet aus "Ttr".

[1] Wert nur unter Profil "Benutzerdefiniert" projektierbar; Wertebereich abhängig von Übertragungsgeschwindigkeit.

[2] Vorbelegung: Werte abhängig von Profil und Übertragungsgeschwindigkeit.

[3] Die Werte der Parameter werden in t_Bit angegeben. Ausnahme: Ttr (ms)

Bit-Zeit (t_Bit)

Die Bit-Zeit ist die Zeit, die beim Senden eines Bits vergeht. Sie wird berechnet aus dem Kehrwert der Übertragungsgeschwindigkeit.

Die Verwendung der Einheit "Bit-Zeit" hat den Vorteil, dass die Busparameter unabhängig von der verwendeten Übertragungsgeschwindigkeit angegeben werden können.

Um aus der Anzahl der Bit-Zeit-Einheiten die Zeit in Millisekunden zu berechnen, benutzen Sie folgende Formel:

$$\text{Zeit (ms)} = \frac{\text{Anzahl Bit-Zeit-Einheiten}}{\text{Übertragungsgeschwindigkeit (kbit/s)}}$$

6.6.3 DI/DO (CC716)

Hier stellen Sie für das CC716 die Funktion des digitalen Eingangs und Ausgangs ein.

Wenn Sie den Eingang oder Ausgang nicht benötigen, dann wählen Sie die Option "Keine Funktion".

Digitaler Eingang

Konfiguration

Der Eingang kann deaktiviert oder alternativ als Trigger für folgende Funktionen genutzt werden:

- **Keine Funktion**

  Der Eingang ist deaktiviert.

- **Als Datenpunkt-Trigger nutzen**

  – 1 → 0

  Bei fallender Flanke am Eingang wird die Übertragung der Topics mit den zugewiesen Datenpunkten mit der Triggerbedingung 1 → 0 einmalig ausgelöst.

  – 0 → 1

  Bei steigender Flanke am Eingang wird die Übertragung der Topics mit den zugewiesen Datenpunkten mit der Triggerbedingung 0 → 1 einmalig ausgelöst.

- **Prozess-Kommunikation steuern**

  Ein Flankenwechsel am Eingang bewirkt Folgendes:

  – 1 → 0: anhalten

  Bei fallender Flanke am Eingang wird die Kommunikation mit allen Prozess-Stationen angehalten.

  – 0 → 1: starten

  Bei steigender Flanke am Eingang wird die Kommunikation mit allen Prozess-Stationen gestartet.

Digitaler Ausgang

Konfiguration

Der Ausgang kann deaktiviert oder alternativ als Anzeige folgender Funktionen genutzt werden:

- **Keine Funktion**

  Der Ausgang ist deaktiviert.

- **Verbindung zur Cloud**

  Das Ausgangssignal zeigt Folgendes an:

  – 0: getrennt

  Das Ausgangssignal 0 zeigt an, dass die Verbindung des Gateways mit mindestens einem aktivem Cloud Profil abgebaut ist.

  – 1: verbunden

  Das Ausgangssignal 1 zeigt an, dass die Verbindung des Gateways mit allen aktiven Cloud Profilen aufgebaut ist.

6.7 Prozess-Zugang

Über die Auswahlliste gelangen Sie auf die Übersichtsseite des jeweiligen Stationstyp.

- S7 Stationen
- Modbus Stationen
- OPC-UA Stationen

Die Übersichtsseite zeigt eine Auflistung der bereits angelegten Stationen und ihrer Eigenschaften.

Die angezeigten Eigenschaften können direkt auf der Übersichtseite editiert werden.

Anlegen

Die Schaltfläche führt auf eine neue Seite, auf der alle Paramater der neuen Station eingestellt werden können. Durch Klicken auf die Schaltfläche "Speichern" werden die Einstellungen übernommen und die neue Station erscheint auf der in der Tabelle auf der Übersichtseite.

Löschen

Durch Klicken auf die Schaltfläche wird die selektierte Station gelöscht.

Hinweis

Versehentliches Löschen

Bei versehentlichem Entfernen von Stationen können Sie das Löschen nicht rückgängig machen.

6.7.1 S7-Stationen

6.7.1.1 S7 Ethernet

Die Kommunikation zwischen dem Gateway und der SIMATIC S7-Station läuft über S7-Verbindungen. Verbindungstyp ist TCP. Aktiver Partner beim Verbindungsaufbau ist das Gateway.

Voraussetzungen:

- In der S7-CPU muss die PUT/GET-Kommunikation aktiviert sein.
- STEP 7: Bei den Datenbausteinen der CPU, auf welche das Gateway mittels S7-Verbindung zugreift, muss die Option "Optimierter Zugriff" deaktiviert sein.

Für die Kommunikation des Gateways mit der S7-Station müssen Sie auf Stationsseite nicht unbedingt eine Verbindung anlegen. Die CPU hält Verbindungsressourcen zu unspezifizierten Partnern vor.

Wenn Sie dennoch feste Verbindungen anlegen möchten, dann deaktivieren Sie in den Verbindungseigenschaften der CPU die Option "Aktiver Verbindungsaufbau". Notieren Sie in diesem Fall für jede Station den von STEP 7 vergebenen TSAP der Verbindung.

Parameter:

- **Aktiv**

  Nur zu aktiven Stationen wird eine Verbindung aufgebaut. Der Station muss mindestens ein Datenpunkt mit einem Ziel zugewiesen sein.

- **Name**

  Vergeben Sie einen Namen für das Profil.

- **Controller-Familie**

  Wählen Sie aus der Klappliste die Controller-Familie der verbundenen Station aus:

  - S7-1200/1500
  - S7-300/400
  - LOGO!

- **IP-Adresse**

  IP-Adresse der Schnittstelle der Station (CPU oder CP)

- **Standard-TSAPs**

  Bei aktivierter Option verwendet das Gerät die Standard-TSAPs für seinen lokalen TSAP und den fernen TSAP (S7-CPU). Die Standard-Einstellungen für den fernen TSAP sind vorgesehen für den Fall, dass Sie im STEP 7-Projekt in der CPU keine Verbindung mit dem Gateway projektiert haben.

  TSAPs werden hexadezimal angegeben. Bei der S7-300/400 referenziert der TSAP den Baugruppenträger, den Steckplatz und den Typ der Verbindungsressource der CPU.

  Beispiele für eine S7-300-CPU:

  – TSAP: 11.02

    Baugruppenträger 0, Steckplatz 2, Verbindungsressource 11

  – TSAP: 03.02

    Baugruppenträger 0, Steckplatz 2, Verbindungsressource 03

    Einseitige Verbindung (Lokaler Endpunkt "Einseitig") Verbindungspartner "unspezifiziert"; das Gateway als Verbindungspartner ist nicht projektiert.

    Eine Verbindungsressource für eine einseitige Verbindung mit unspezifiziertem Partner hat den Wert 03.

    Eine Verbindungsressource für eine zweiseitige Verbindung mit unspezifiziertem Partner hat den Wertebereich 0x10...0xDF.

    Empfehlung für den Stationsaufbau:
    Verwenden Sie für Baugruppenträge/Steckplatz die Konfiguration 0/0 oder 0/1.

  Folgende Standard-TSAP-IDs werden verwendet:

  – Lokaler TSAP des Gateways: 01.01

  – Ferner TSAP der Controller-Familie:

    - S7-1200/1500: 02.01

    - S7-300/400: 03.02

    - LOGO!: 20.00

  Deaktivieren Sie die Option, wenn die fernen TSAPs nicht den vorbelegten Standard-TSAPs entsprechen. Projektieren Sie in diesem Fall denjenigen TSAP, der im STEP 7-Projekt vergeben ist.

- **Lokaler TSAP**

  Wertebereich: 01.01 ... 7E.7E

  Es wird empfohlen, den vorbelegten TSAP (01.01) zu verwenden.

- **Ferner TSAP**

  Tragen Sie den in STEP 7 vergebenen TSAP der S7-Verbindung auf Stationsseite ein, wenn Sie in der CPU für das Gateway eine Verbindung mit unspezifiziertem Partner projektiert haben.

  Deaktivieren Sie in STEP 7 bei Verwendung einer projektierten unspezifischen Verbindung die Option "Aktiver Verbindungsaufbau".

- **Polling-Zyklus (ms)**

  Zyklusdauer in Millisekunden, in dem das Gateway die Daten aus der Station liest.

  Wertebereich: 50...100 000 000

  Beachten Sie: Wenn Sie größere Datenmengen übertragen, kann die tatsächliche Zykluszeit größer sein als projektiert.

6.7.1.2 S7 PROFIBUS / MPI

Nur bei CC716

Die Kommunikation zwischen dem Gateway und der SIMATIC S7-Station läuft über S7-PROFIBUS-Verbindungen. Das Gateway ist aktiver Teilnehmer.

Voraussetzungen:

Es gelten die gleichen Voraussetzungen wie im Abschnitt "S7 Ethernet" oben.

Parameter:

- **PROFIBUS / MPI-Adresse**

  PROFIBUS-Adresse der S7-Station (Kommunikationspartner des Gateways)

- **Controller-Familie**

  Wählen Sie aus der Klappliste die Controller-Familie der verbundenen Station aus:

  - S7-300
  - S7-400
  - S7-1200
  - S7-1500

- **Standard-TSAPs**

  Bei aktivierter Option verwendet das Gerät die Standard-TSAPs für seinen lokalen TSAP und den fernen TSAP (S7-CPU). Die Standard-Einstellungen für den fernen TSAP sind vorgesehen für den Fall, dass Sie im STEP 7-Projekt in der CPU keine Verbindung mit dem Gateway projektiert haben.

  TSAPs werden hexadezimal angegeben. Bei der S7-300/400 referenziert der TSAP den Baugruppenträger, den Steckplatz und den Typ der Verbindungsressource der CPU.

  Beispiele für eine S7-300-CPU:

  – TSAP: 11.02

    Baugruppenträger 0, Steckplatz 2, Verbindungsressource 11

  – TSAP: 03.02

    Baugruppenträger 0, Steckplatz 2, Verbindungsressource 03

    Einseitige Verbindung (Lokaler Endpunkt "Einseitig") Verbindungspartner "unspezifiziert"; das Gateway als Verbindungspartner ist nicht projektiert.

    Eine Verbindungsressource für eine einseitige Verbindung mit unspezifiziertem Partner hat den Wert 03.

    Eine Verbindungsressource für eine zweiseitige Verbindung mit unspezifiziertem Partner hat den Wertebereich 0x10...0xDF.

  Folgende Standard-TSAP-IDs werden verwendet:

  – Lokaler TSAP des Gateways: 01.01

  – Ferner TSAP der Controller-Familie:

    - S7-1200/1500: 01.01

    - S7-300: 03.02

    - S7-400: 03.03

  Deaktivieren Sie die Option, wenn die fernen TSAPs nicht den vorbelegten Standard-TSAPs entsprechen. Projektieren Sie in diesem Fall denjenigen TSAP, der im STEP 7-Projekt vergeben ist.

- **Lokaler TSAP**

  Wertebereich: 01.01 ... 7E.7E

  Es wird empfohlen, den vorbelegten TSAP (01.01) zu verwenden.

- **Ferner TSAP**

  Tragen Sie den in STEP 7 vergebenen TSAP der S7-Verbindung auf Stationsseite ein, wenn Sie in der CPU für das Gateway eine Verbindung mit unspezifiziertem Partner projektiert haben.

- **Polling-Zyklus (ms)**

  Zyklusdauer in Millisekunden, in dem das Gateway die Daten aus der Station liest.

  Wertebereich: 50...1 000 000 00

  Beachten Sie: Wenn Sie größere Datenmengen übertragen, kann die tatsächliche Zykluszeit größer sein als projektiert.

Die Übertragungsgeschwindigkeit und die weiteren Netzparameter projektieren Sie im Register "Schnittstellen-Konfiguration > PROFIBUS".

6.7.2 Modbus-Stationen

Die Kommunikation zwischen Gateway und der Modbus-Station läuft über Modbus/TCP-Verbindungen. Aktiver Partner beim Verbindungsaufbau ist das Gateway.

Parameter:

- **RTU-Nummer**

  RTU-Nummer des Modbus-Slave

  Wertebereich: 1...254

- **IP-Adresse**

  Adresse der Schnittstelle der Station.

  IPv4, IPv6

- **Portnummer**

  Portnummer der Schnittstelle der Station. Vorbelegung: 502

  Wertebereich für Modbus-Station: 1...65535

- **Verbindungsaufbauversuche**

  Maximale Anzahl an Versuchen, die Verbindung mit einer Station aufzubauen.

  Nach Erreichen der projektierten Anzahl werden so lange keine weiteren Verbindungsaufbauversuche vorgenommen, bis das Gateway neu gestartet wird.

  Wertebereich: -1...32767

  Bei "-1" ist die Anzahl der Verbindungsaufbauversuche unbegrenzt.

- **Polling-Intervall (ms)**

  Zyklusdauer in Millisekunden, in dem das Gateway die Daten aus der Station liest.

  Wertebereich: 50...65535000

  Hinweis
  Zeitverzögerung bei größeren Datenmengen

  Wenn Sie größere Datenmengen übertragen, kann die tatsächliche Zykluszeit größer sein als projektiert.

- **Verbindungsaufbau-Verzögerung (ms)**

  Wartezeit (Sekunden) vor einem neuen Verbindungsaufbauversuch, wenn die Station nicht erreichbar oder die Verbindung abgebrochen ist.

  Eine Wartezeit kann sinnvoll sein, um beispielsweise die Behebung von kurzfristigen Netzstörungen oder den Neustart einer Station abzuwarten.

  Wertebereich: 1000...100000

- **Timeout (ms)**

  Wenn das Gateway innerhalb der projektierten Zeit (Millisekunden) keine Antwort von der Station empfängt, wird die Verbindung abgebrochen und als fehlerhaft gewertet. Ob die Anfrage erneut gesendet wird, hängt von den Einstellungen innerhalb der Parameter "Wiederholungsversuche" bzw. "Max. Anzahl fehlerhafter Antworten" ab.

  Wertebereich: 100...65535

- **Max. Anzahl fehlerhafter Antworten**

  Maximale Anzahl an ausbleibenden oder fehlerhaften Antworten der Station über alle Datenpunkte.

  Bei Erreichen der max. Anzahl stuft das Gateway die Station als gestört ein und baut die Verbindung ab. Nach einem Verbindungsabbau versucht das Gateway, die Verbindung neu aufzubauen.

  Wertebereich: 1...32

- **Wiederholungsversuche**

  Maximale Anzahl an Wiederholungen der Stationsabfrage pro Datenpunkt.

  Wenn das Gateway von der Station bei einem Timeout keine oder eine fehlerhafte Antwort empfängt, wird die Abfrage des einzelnen Datenpunkts so oft wiederholt, bis zum nächsten Datenpunkt gewechselt wird.

  Die Anzahl der Anfragen ist durch die eingestellten Wiederholungsversuche beim Parameter "Max. Anzahl fehlerhafter Antworten" limitiert. Wird der dort eingestellte Wert erreicht, erfolgt danach der Versuch, die Verbindung neu aufzubauen.

  Wertebereich: 0...10

- **Endianness**

  Die Einstellung hat nur Auswirkung auf Datentypen, die aus mehr als einem Wort bestehen.

  Über die Option legen Sie fest, in welcher Ordnung die wortweise gelesenen Daten der Station gespeichert werden.

  – Big Endian

    Das höherwertige Wort 1 wird zuerst gespeichert. (Modbus-Standard)

  – Little Endian

    Das niederwertige Wort 0 wird zuerst gespeichert.

6.7.3 OPC UA-Stationen

OPC UA-Stationen

Parameter:

- **Aktiv**

  Nur zu aktiven Stationen wird eine Verbindung aufgebaut. Der Station muss mindestens ein Datenpunkt zugewiesen sein.

- **Stationsname**

  Geben Sie zum Anlegen einer neuen Station einen eindeutigen Namen in das Eingabefeld ein.

- **Applikations-URI**

  Eindeutiger URI der Station mit folgenden vorbelegten Bestandteilen:

  <Scheme (Protokoll)>:<Authority (Station)>:<Path>

  Vorbelegung:

  – urn:cc7-device:Siemens:OPCStation1@cc7-device

- **Applikationsname**

  Name der OPC UA-Applikation des Gateways. Der Applikationsname wird für die Anzeige der Station bei dem Server benötigt.

  Vorbelegung:

  – OPCStation1@cc7-device

- **Server-Adresse**

  Stellen Sie die IPv4/IPv6-Adresse oder den DNS-Namen des OPC UA-Servers ein, mit dem sich die Station verbinden soll.

- **Portnummer**

  Hier können Sie die Portnummer der Station verändern. In der Voreinstellung wird die Portnummer 4840 verwendet, der Standard-TCP-Port für das OPC UA-Binärprotokoll. Zulässige Portnummern sind:

  – 1...65535

- **URL-Pfad**

  Geben Sie optional einen URL-Pfad innerhalb der Server-Adresse des OPC UA-Clients ein.

- **Dienstaufruf-Timeout (ms)**

  Geben Sie die gewünschte Zeitspanne in Millisekunden ein. Wenn nach Ablauf dieser Zeitspanne kein Dienstaufrufe zu dem unterlagerten OPC UA-Server stattfindet, wird der Dienstaufrufe automatisch unterbrochen.

  Wertebereich: 1000...60000

- **Verbindungs-Timeout (ms)**

  Geben Sie die gewünschte Zeitspanne in Millisekunden ein. Wenn nach Ablauf dieser Zeitspanne kein Verbindungsaufbau zu dem unterlagerten OPC UA-Server stattfindet, wird die Verbindung automatisch getrennt.

  Wertebereich: 1000...60000

- **Watchdog-Zeit (ms)**

  Geben Sie die gewünschte Zeitspanne in Millisekunden ein. Im Fall einer Verbindungsstörung ist dies das Zeitintervall zwischen den Verbindungsüberprüfungen oder den Versuchen, die Verbindung wiederherzustellen.

  Wertebereich: 1000...600000

- **Watchdog-Timeout (ms)**

  Geben Sie die gewünschte Zeitspanne in Millisekunden ein. Wenn nach Ablauf dieser Zeitspanne die Überprüfung der Verbindung zu dem unterlagerten OPC UA-Server nicht erfolgreich war, wird die Überprüfung automatisch abgebrochen.

  Wertebereich: 1000...60000

- **Discover**

  Beim Verwenden von "Discover" wird mit der oben angegebenen Server-Adresse und der Portnummer eine Verbindung aufgebaut. Wird ein OPC UA-Server gefunden, werden der Applikationsname, der Applikations-URI und die Discovery-URLs des OPC UA-Servers angezeigt.

  Beim Klick auf eine der Discovery-URLs werden die verfügbaren Endpunkte der OPC UA-Server-Verbindung angezeigt. Wird einer der verfügbaren Endpunkte mit der gewünschten Verschlüsselung ausgewählt und mit "Speichern" übernommen, wird diese Security Policy eingestellt, automatisch das OPC UA-Server Zertifikat gespeichert, ein optionaler URL-Pfad und die gewählte IP Adresse gesetzt.

  Beachten Sie, dass zunächst ein OPC UA-Client-Zertifikat erzeugt bzw. importiert werden muss, bevor ein Endpunkt != None – None gespeichert werden kann.

Hinweis

Aktualisierungsintervall der Daten

Der OPC UA-Client arbeitet mit Subscriptions statt mit Polling. Damit kann die Last auf der CPU-Seite soweit wie möglich reduziert und trotzdem die Aktualität der Daten im Gateway gesteigert werden. Eine Angabe des Polling-Zyklus wie bei S7- oder Modbus-Stationen ist aus diesem Grund nicht notwendig.

6.7.3.1 OPC UA-Security

OPC UA-Security

Sie können Zertifikat und Schlüssel aus dem globalen Zertifikatsspeicher auswählen oder ein selbst signiertes Zertifikat anlegen. Nach dem Speichern wird das Zertifikat und der private Schlüssel automatisch in die passenden Felder eingetragen. Zum Verwalten von Zertifikaten und Schlüsseln siehe Kapitel Zertifikats-Management (Seite 164).

- **Security Policy**

  Aktivieren Sie in der Tabelle die gewünschte Option.

  Die Station unterstützt folgende Optionen der "SecurityPolicy":

  - Keine (nicht empfohlen)
  - Basic128Rsa15 (nicht empfohlen)

    Signierung und 128-Bit-Verschlüsselung
  - Basic256 (nicht empfohlen)

    Signierung und 256-Bit-Verschlüsselung
  - Basic256Sha256 (SecurityPolicy [B])

    Signierung und 256-Bit-Verschlüsselung (SHA-256)
  - Aes128_Sha256_RsaOaep

    Signierung und 256-Bit-Verschlüsselung
  - Aes256_Sha256_RsaPss

    Signierung und 256-Bit-Verschlüsselung

  Die ergänzenden Conformance Units (Signing / Encryption) bedeuten:

  - Signieren

    Die Station erlaubt nur Kommunikation mit signierten Telegrammen.
  - Signieren und verschlüsseln

    Die Station erlaubt nur Kommunikation mit signierten und verschlüsselten Telegrammen.

- **Vertrauenswürdige Server**
  - **Keine Zertifikatsvalidierung**

    Über diese Option deaktivieren Sie die Prüfung der Partnerzertifikate.

    Bei aktivierter Option lässt der Client Kommunikation generell zu, auch wenn die unten genannten Kriterien der Zertifikatsvalidierung nicht erfüllt werden oder wenn das Server-Zertifikat nicht in der Liste der vertrauenswürdigen Server vorhanden ist.

    Bei deaktivierter Option prüft die Station die Zertifikate seiner Partner, außer bei ausgewählter "SecurityPolicy - None".

    Zu den Prüfmechanismen siehe Abschnitt "Zertifikatsvalidierung" unten.
  - **Server-Zertifikat importieren**

Über diese Option können Client Zertifikate aus dem globalen Zertifikatsspeicher ausgewählt werden.

Zertifikatsvalidierung

Der UA-Server der Station prüft bei deaktivierter Option "Keine Zertifikatsvalidierung" die Zertifikate seiner Kommunikationspartner, außer bei projektierter "SecurityPolicy - None".

Falls ein Partnerzertifikat ungültig oder nicht vertrauenswürdig ist, wird die Kommunikation abgebrochen. Die Kommunikation wird in folgenden Fällen abgebrochen:

- Die IP-Adresse des Kommunikationspartners ist nicht identisch mit der IP-Adresse in dessen Zertifikat.
- Die im Zertifikat hinterlegte Verwendung (OPC UA-Client/Server) unterscheidet sich von der Funktion (OPC UA-Client/Server) des Kommunikationspartners.
- Der aktuelle Zeitpunkt der Station liegt außerhalb der Gültigkeitsdauer des Partnerzertifikats.

Voraussetzungen für den Verbindungsaufbau

Unabhängig von der Zertifikatsvalidierung müssen für einen Verbindungsaufbau folgende Voraussetzungen erfüllt sein:

- Der von der anfragenden Station mitgeschickte Applikations-URI muss mit dem URI der Server-Applikation der Station übereinstimmen.
- Wenn das Partnerzertifikat nicht vertrauenswürdig ist, muss die Station zumindest ein selbstsigniertes Zertifikat des Partners gespeichert haben.
- Mindestens eine Option der Authentifizierung ist aktiviert (siehe unten).

Partnerzertifikate, die von mehreren CAs ausgestellt wurden (Zertifikatsketten), werden von der Station nicht unterstützt.

6.7.3.2 Benutzer-Authentifizierung

Über die Option stellen Sie die Zugriffsberechtigung der OPC UA Station ein:

- **Anonymer Zugriff**

  Wenn Sie die Option aktivieren, werden Benutzername und Passwort ausgegraut. Die Station kann ohne Authentifizierung auf die OPC UA-Daten zugreifen.

- **Authentifizierung mit Benutzername und Passwort**

  Wenn Sie die Option aktivieren, öffnen sich die Eingabefelder für den Benutzer der OPC UA-Station. Die Station kann nur mit Benutzer-Authentifizierung auf die OPC UA-Daten zugreifen.

- **Benutzername**

  Benutzername des Kommunikationspartners

- **Passwort**

  Passwort des Kommunikationspartners

Die Benutzerdaten müssen beim jeweiligen Server projektiert sein.

6.8 OPC UA-Server

6.8.1 Konfiguration

Voraussetzungen

Variablen der CPU

Die Prozessdaten, welche das Gateway den OPC UA-Diensten zur Verfügung stellt, entstammen den verbundenen Prozess-Stationen. Die zulässigen Speicherbereiche der verschiedenen Stations-Typen und die unterstützten Datentypen finden Sie im Kapitel Datenpunkte (Seite 142).

Die bei der Datenpunktprojektierung vergebenen Datenpunktnamen gehen als Bestandteil des Identifiers in die NodeID eines Items ein, vgl. Kapitel Eigenschaften des OPC UA-Servers (Seite 100).

Anmerkung:
Lesen Sie Variablen in Datenbausteinen möglichst blockweise pro DB, um eine höhere Geschwindigkeit zu erreichen.

Security-Einstellungen: Server-Zertifikat

Wenn Sie den OPC UA-Server des Gateways aktivieren, dann müssen Sie ein selbst signiertes Server-Zertifikat erstellen oder importieren.

OPC UA-Server

- **OPC UA-Server aktivieren**

  Aktivieren Sie die Option, um die OPC UA-Server-Funktion des Gateways zu aktivieren.

- **Applikations-URI**

  Eindeutiger OPC UA-Server-URI des Gateways mit folgenden vorbelegten Bestandteilen:

  <Scheme (Protokoll)>:<Authority (Server)>:<Path>

  Vorbelegung:

  – urn:cc7-device:Siemens:OpcUaServer@cc7-device

  Der Protokollteil (urn) darf nicht verändert werden, die übrigen Bestandteile sind projektierbar.

- **Applikationsname**

  Name der OPC UA-Applikation des Gateways. Der Applikationsname wird für die Anzeige des OPC UA-Servers bei den Clients benötigt.

  Vorbelegung:

  – OpcUaServer@cc7-device

- **Host-Name (optional)**

  Optionales Eingabefeld für einen Host-Namen, der statt der IP-Adresse des UA-Endpunkts des Gateways verwendet werden kann.

  Wenn Sie keinen Host-Namen verwenden möchten, lassen Sie das Feld frei.

- **Portnummer**

  Hier können Sie die Portnummer der Server-Applikation verändern. In der Voreinstellung wird die Portnummer 4840 verwendet, der Standard-TCP-Port für das OPC UA-Binärprotokoll.

  Zulässige Portnummern sind:

  – 1024 .. 65535

- **URL-Pfad (optional)**

  Geben Sie optional einen URL-Pfad innerhalb der Server-Adresse des OPC-UA Servers ein.

- **Gebietsschema-ID**

  Geben Sie eine Gebietsschema-ID für den OPC UA-Server ein, z. B. en-US.

  Die ID wird benötigt, wenn bei Nodeset ein String auf einen LocalizedText gemappt wird.

- **Namensraum-URI**

  Tragen Sie die Adresse (Namensraum-URI) des Ziel-Servers ein.

  Voreinstellung: urn:Siemens:OpcUaServer:CC7

- **Name Wurzelverzeichnis**

  Geben Sie einen Namen für das Verzeichnis ein.

  Voreinstellung: CC7

- **NodeID Wurzelverzeichnis**

  Ändern Sie die NodeID des CC7-Ordners;

  Voreinstellung: ns=2;s=CC7; setzt sich zusammen aus Namensraum-Index des aktiven Node-Managers (2) und einem String-Identifier mit Namen des Wurzelverzeichnisses (CC7).

- **Min. Publishing-Intervall (ms)**

  Hier stellen Sie das minimale Publishing-Intervall ein, welches die Server-Applikation des Gateways unterstützen soll. Von OPC UA-Clients geforderte kleinere Werte werden nicht berücksichtigt.

  Der OPC UA-Server stellt den Clients die UA-Daten im Zyklus des Publishing-Intervalls zur Verfügung.

  Wertebereich: 100 .. 10000 ms

  Voreinstellung: 500 ms

- **Min. Sampling-Intervall (ms)**

  Hier stellen Sie das minimale Sampling-Intervall ein, welches die Server-Applikation des Gateways unterstützen soll. Von OPC UA-Clients geforderte kleinere Werte werden nicht berücksichtigt.

  Der OPC UA-Server des Gateways tastet mit dem Sampling-Intervall sein internes Prozessabbild ab.

  Das Lesen aus der Station legen Sie über den Polling-Zyklus fest, siehe Kapitel Prozess-Zugang (Seite 84).

  Die Voreinstellung ist für die meistens Anwendungsfälle geeignet. Ein kleineres Sampling-Intervall kann für das Lesen weniger Datenpunkte gewählt werden, wenn auch der Polling-Zyklus mit einem entsprechend kleinen Wert projektiert ist.

  Wertebereich: 100 .. 10000 ms

  Voreinstellung: 500 ms

6.8.1.1 OPC UA-Security

Security-Mechanismen

Entsprechend der OPC UA-Spezifikation unterstützt das Gateway folgende Security-Profile:

- **SecurityPolicy**

  Sie bestimmt die Signierung und Verschlüsselung der übertragenen Daten.

- **UserToken**

  Ermöglicht Authentifizierung über Zertifikate.

- **Authentifizierung der Kommunikationspartner über Benutzername und Passwort**

  Siehe hierzu Kapitel Authentifizierung (Seite 99).

Zu den OPC UA-Profilen der OPC Foundation siehe:
Profiles (https://apps.opcfoundation.org/ProfileReporting)

- **Selbst signiertes Zertifikat**

  Klicken Sie auf die Schaltfläche "Anlegen", um ein selbst signiertes Zertifikat zu erstellen. Erforderliche Felder werden dabei mit den benötigten Parametern vorausgefüllt. Nach dem Speichern wird das Zertifikat und der private Schlüssel automatisch in die folgenden Felder eingetragen und im globalen Zertifikatsspeicher gespeichert.

- **Server-Zertifikat**

  Über die Auswahlliste wählen Sie ein Server-Zertifikat aus dem globalen Zertifikatsspeicher.

- **Privater Schlüssel**

  Über die Auswahlliste wählen Sie einen privaten Server-Schlüssel aus dem globalen Zertifikatsspeicher.

- **Keine Zertifikatsvalidierung**

  Über diese Option deaktivieren Sie die Prüfung der Partnerzertifikate.

  Bei aktivierter Option lässt das Gateway Kommunikation generell zu, auch wenn die unten genannten Kriterien der Zertifikatsvalidierung nicht erfüllt werden oder wenn das Client-Zertifikat nicht in der Liste der vertrauenswürdigen Clients vorhanden ist.

  Bei deaktivierter Option prüft das Gateway die Zertifikate seiner Partner, außer bei ausgewählter "SecurityPolicy - None".

  Zu den Prüfmechanismen siehe Abschnitt "Zertifikatsvalidierung" unten.

- **Vertrauenswürdige Clients**

  Über diese Option können Sie Client-Zertifikate aus dem globalen Zertifikatsspeicher auswählen.

Zertifikatsvalidierung

Der UA-Server des Gateways prüft bei deaktivierter Option "Keine Zertifikatsvalidierung" die Zertifikate seiner Kommunikationspartner, außer bei projektierter "SecurityPolicy - None".

Falls ein Partnerzertifikat ungültig oder nicht vertrauenswürdig ist, wird die Kommunikation abgebrochen. Die Kommunikation wird in folgenden Fällen abgebrochen:

- Die IP-Adresse des Kommunikationspartners ist nicht identisch mit der IP-Adresse in dessen Zertifikat.
- Die im Zertifikat hinterlegte Verwendung (OPC UA-Client/Server) unterscheidet sich von der Funktion (OPC UA-Client/Server) des Kommunikationspartners.
- Der aktuelle Zeitpunkt im Gateway liegt außerhalb der Gültigkeitsdauer des Partnerzertifikats.

Voraussetzungen für den Verbindungsaufbau

Unabhängig von der Zertifikatsvalidierung müssen für einen Verbindungsaufbau folgende Voraussetzungen erfüllt sein:

- Der vom anfragenden Client mitgeschickte Applikations-URI muss mit dem URI der Server-Applikation des Gateways übereinstimmen.
- Wenn das Partnerzertifikat nicht vertrauenswürdig ist, muss das Gateway zumindest ein selbstsigniertes Zertifikat des Partners gespeichert haben.
- Mindestens eine Option der Authentifizierung ist aktiviert (siehe unten).

Partnerzertifikate, die von mehreren CAs ausgestellt wurden (Zertifikatsketten), werden vom Gateway nicht unterstützt.

Siehe auch

Konfiguration (Seite 95)

6.8.1.2 Authentifizierung

Benutzer-Authentifizierung

Über die beiden Optionen stellen Sie die Zugriffsberechtigung der Kommunikationspartner (Clients) auf die OPC UA-Daten des Gateways ein. Aktivieren Sie eine oder beide (Parallelbetrieb möglich) Optionen.

- **Anonymen Zugriff aktivieren**

  Clients können bei aktivierter Funktion ohne Benutzer-Authentifizierung auf die OPC UA-Daten zugreifen.

- **Authentifizierung mit Benutzername und Passwort**

  Clients können bei aktivierter Funktion nur mit Benutzer-Authentifizierung auf die OPC UA-Daten zugreifen.

- **Benutzer hinzufügen**

  Bei aktivierter Option "Authentifizierung mit Benutzername und Passwort" öffnen Sie über diese Schaltfläche die Eingabefelder für einen neuen Benutzer.

- **Benutzername**

  Benutzername des Kommunikationspartners

- **Passwort**

  Passwort des Kommunikationspartners

Die Benutzerdaten müssen beim jeweiligen Client projektiert sein.

6.8.1.3 Eigenschaften des OPC UA-Servers

Identifizierung und Adressierung

Es gelten folgende Adressierungs- und Identifizierungsmerkmale des OPC UA-Servers des Gateways.

- Applikationsname, Applikations-URI, Server-URL, Portnummer der Applikation:
  - Siehe Kapitel Konfiguration (Seite 95).
- Namensraum der Datenpunkte des Gateways:
  - CC7
- Namensraum-URI:
  - urn:Siemens:OpcUaServer:CC7
- NodeID - Identifier:

  Der Identifier der NodeIDs der Datenpunkte des Namensraums "CC7" wird von der Server-Applikation des Gateways aus dem Namen der CPU, ggf. des Datenbausteins und der Struktur und dem Datenpunktnamen gebildet:
  - *<CPU-Name>.<DB-Name>__<Datenpunktname>*
- Unterstütze Sampling-Intervalle

  100, 250, 500, 1000, 2000, 5000, 10000 ms

Subscriptions

Zur Anzahl der vom Gateway als OPC UA-Server unterstützten Subscriptions für MonitoredItems siehe Kapitel Mengengerüst - Kommunikation (Seite 26).

Der Datenhaushalt der Subscriptions wird im RAM des Gateways hinterlegt.

Bei Spannungsausfall gehen alle Daten und Verbindungsinformationen von Subscriptions verloren. Nach dem Neustart des Servers muss der Client die Verbindung neu aufbauen und die Subscriptions neu einrichten.

Deadband

Der OPC UA-Server des Gateways unterstützt bei der Überwachung von Items im "DataChangeFilter" den Filter "AbsoluteDeadband".

6.8.2 Nodeset

Nodeset-Dateien

Die OPC Foundation hat ein Standard-Format, basierend auf XML, zum Beschreiben von Informationsmodellen spezifiziert. Damit kann einem Client vorab das Informationsmodell eines OPC UA-Servers zur Verfügung gestellt werden oder es können Informationsmodelle auf einen OPC UA-Server geladen werden. Eine Datei in diesem Format wird Nodeset-Datei genannt, weil es ein Informationsmodell als Menge (Set) von Knoten (Nodes) beschreibt.

Alle Variablen, unabhängig von der Quelle (Prozess-Stationen), haben einen definierten Wert und eine definierte NodeID.

OPC UA-Exportdatei erzeugen

Sie können Nodeset-Dateien entweder manuell oder mit OPC-konformer Software erzeugen.

Siemens bietet zur Erzeugung von Nodeset-Dateien folgende Software an:

- Mit STEP 7 (TIA Portal) können Sie das Standard-SIMATIC-Informationsmodell in eine OPC UA-XML-Datei (Nodeset-Datei) exportieren; inklusive aller PLC-Variablen, NodeIDs und Methoden, die Sie für OPC UA freigegeben haben.
- Mit dem "Siemens OPC UA Modeling Editor" (SiOME) können Sie Modelle erstellen und als Nodeset-Datei exportieren.

OPC UA-Nodeset importieren

Beim Import findet ein Mapping zwischen den Prozess-Variablen und den Variablen in der geladenen Nodset-Datei statt. Damit präsentiert der CC7 auf dem eigenen OPC UA-Server die gewünschten standardisierten OPC UA-Werte und nicht die eigene Struktur.

- **Nodeset-XML**

  Klicken Sie auf die Schaltfläche "Durchsuchen".

  Der Browser zum Durchsuchen des Dateisystems Ihres PC öffnet sich.

  Wählen Sie gewünschte XML-Datei und klicken Sie auf "Öffnen".

  Der Dateiname wird im Ausgabefeld des WBM angezeigt.

  Wenn Sie die Datei verwenden möchten, klicken Sie auf "Hochladen".

  Ist die falsche Datei gewählt, klicken Sie das Löschen-Symbol.

- **Aktiv**

  Wenn aktiviert, verwendet CC7 die Struktur und die Daten der geladene Nodeset-XML-Datei, und nicht die eigenen Prozessdaten.

- **Parsen**

  Das Parsen wird beim Laden einer neuen Nodset-XML-Datei automatisch durchgeführt.

  Ergebnis: Die Nodset-XML-Datei wird gelesen und die Oberfläche des WBMs wird in zwei Bereiche geteilt:

  – Auf der linken Seite wird das geladene Nodeset-XML mit den zugehörigen Variablen angezeigt. Sie können nun durch die einzelnen Ordner oder Variablen browsen.

  – Auf der rechten Seite sind alle Prozess-Stationen des CC7 aufgelistet. Browsen Sie durch die Ordner der Prozess-Station, werden alle Datenpunkte, die dem Ziel "OPC" zugeordnet sind, angezeigt.

6.8.2.1 Mapping

Variablen zuweisen (Mapping)

Beim Mapping werden die Prozessdaten der CC7-Stationen den Variablen des Nodeset-XML zugewiesen. Eine Variable der CC7-Station kann dabei mehreren Variablen der Nodeset-XML-Datei zugewiesen werden.

Ziehen Sie dazu per Drag&Drop die Datenpunkte der CC7-Stationen im rechten Bereich auf die entsprechenden Nodeset XML-Variablen im linken Bereich.

Ergebnis:

- Eine zugewiesene Variable wird im Nodeset-XML fett markiert und der entsprechende CC7-Datenpunkt dahinter geschrieben.
- Die Anzahl der Verlinkungen wird auf CC7-Seite hinter der zugewiesenen Variable angezeigt.
- Die vollständige NodeID wird im Tooltip angezeigt, wenn Sie mit der Maus über den Datenpunkt-Namen fahren.

- Über das schwarze Kreuz-Symbol hinter dem Datenpunkt können Sie die Verbindung wieder auflösen.
- Nicht zugewiesene Datenpunkte des XML werden mit dem QualityCode "BadNotImplemented" an den CC7 OPC UA-Server übertragen.

6.8.2.2 Casting

Variablen umwandeln (Casting)

Beim Zuweisen der Variablen zu den OPC UA XML-Datenpunkte ist es möglich, den Zugriff und/oder den Datentyp der CC7-Prozessvariablen umzuwandeln.

CC7-Datenpunkte mit der OPC-Berechtigung "ReadWrite" können in XML-Datenpunkte "Read", "Write" und "ReadWrite" umgewandelt werden.

Umgekehrt ist es nicht möglich, eine CC7-Variable "Read" in eine XML-Variable "ReadWrite" umzuwandeln.

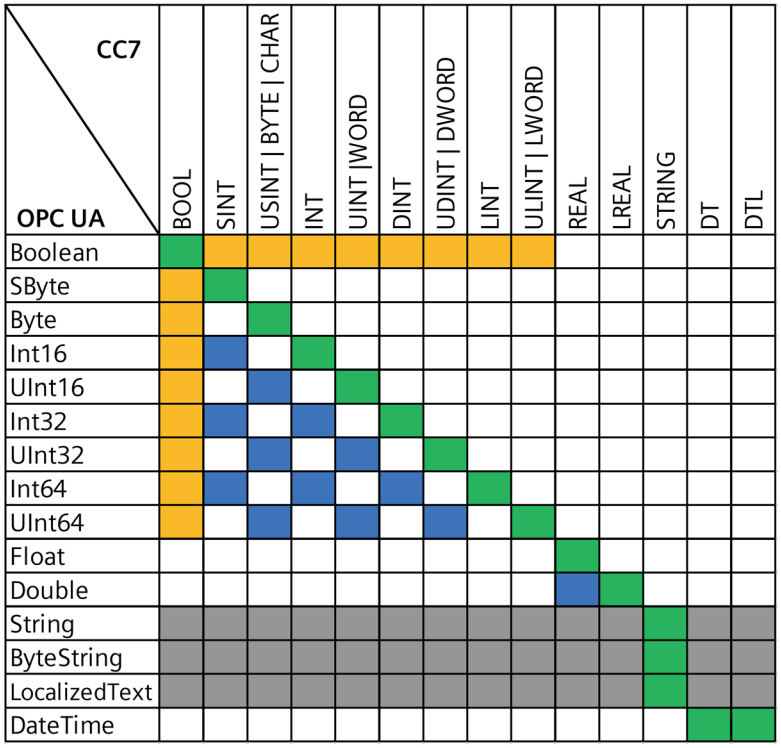
OPC UA XML-Datenpunkte	**CC7-Prozessvariablen**		
Zugriffsrecht	Read	Write	ReadWrite
Read	x	-	x
Write	-	x	x
ReadWrite	-	-	x

Übersicht nach OPC UA-Datentypen

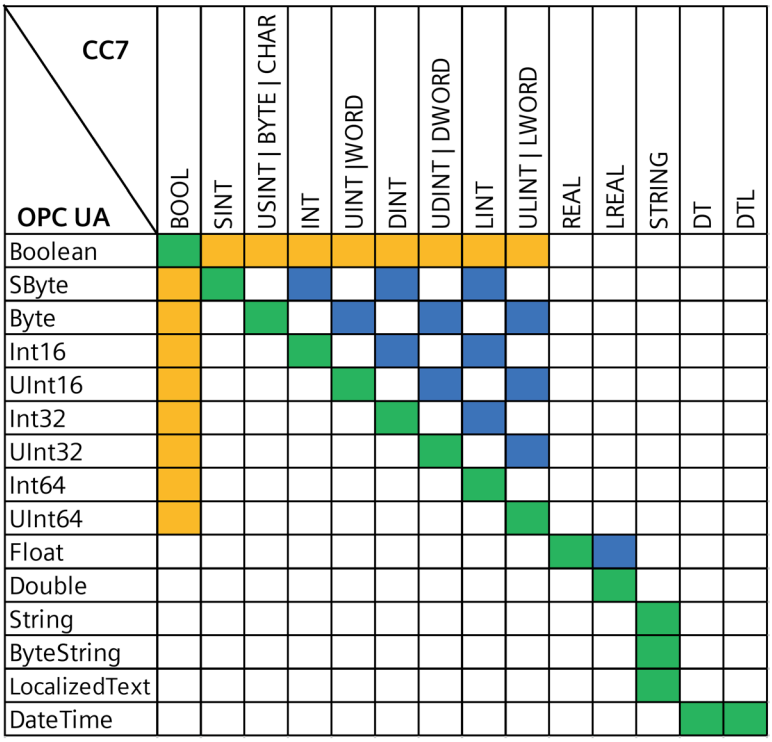
In den nachfolgenden Grafiken erhalten Sie eine Übersicht, welche ein- und ausgehenden Datentypen der CC7-Prozessvariablen, abhängig von dem OPC-Zugriffsrecht, in welche ein- und ausgehenden OPC UA XML-Datenpunkte umgewandelt werden können. Dabei haben die Felder die folgende Bedeutung:

Feld	**Beschreibung**
CC7	CC7-Prozessvariablen
OPC UA	OPC UA XML-Datenpunkte / Nodeset
	Zuweisung nach Datentypen
	Umwandeln von Datentypen Bei "ReadWrite" müssen die Datentypen genau passen, es ist kein Up- bzw. Down-Casting möglich wie bei "Read" bzw. "Write".
	Die Variable kann einer XML-Bool-Variablen zugewiesen werden. Folgende Werte der Prozess-Station entsprechen dann auf dem OPC UA-Server den folgenden XML-Bool-Variablen: Wert "0" entspricht dem Wert "false" Wert "!= 0" entspricht dem Wert "true"
	Umwandeln von Strings Jeder Datenpunkt kann in einen String umgewandelt und somit als String dargestellt werden.

XML-Daten "Read"



XML-Daten "Write"



XML-Daten "ReadWrite"

CC7 / OPC UA	BOOL	SINT	USINT | BYTE | CHAR	INT	UINT |WORD	DINT	UDINT | DWORD	LINT	ULINT | LWORD	REAL	LREAL	STRING	DT	DTL
Boolean	■													
SByte		■												
Byte			■											
Int16				■										
UInt16					■									
Int32						■								
UInt32							■							
Int64								■						
UInt64									■					
Float										■				
Double											■			
String												■		
ByteString												■		
LocalizedText												■		
DateTime													■	■

6.9 Cloud-Konfiguration

6.9.1 Hinweise zur Datenstrukturierung und Projektierung

⚠ WARNUNG

Schreiben von Werten in Ausgänge

Beachten Sie bei Referenzierung auf Ausgänge, dass bei schreibendem Zugriff die Werte sofort in die Ausgänge der CPU geschrieben werden, ohne zuvor vom Anwenderprogramm bearbeitet zu werden.

Das Schreiben von Werten hat unmittelbaren Einfluss auf den Prozess.

Datenstrukturen

Abhängig vom Cloud-Betreiber werden die Daten für die Übertragung an den Broker unterschiedlich strukturiert:

- AWS / Azure / IBM Cloud
  - Topics

    Ein Topic ist der Kanal für die Übertragung der Werte eines oder mehrerer Datenpunkte.

    Sie können mehrere Topics anlegen.

    Es können keine Gruppen projektiert werden.
- MindConnect IoT Extension / Andere Cloud
  - Gruppen

    Eine Gruppe kann einen oder mehrere Datenpunkte enthalten.

    Sie können eine oder mehrere Gruppen anlegen.
  - Topic

    Sie können den Gruppen verschiedene Topics zuordnen.

    MindConnect IoT Extension: Die Gruppen werden in der Voreinstellung dem Standard-Topic "s/us" der MindConnect IoT Extension zugewiesen.

Aufbau der Topic-Namen

Da die Anforderungen an das Format der Topics je nach Empfänger (Broker, Cloud) unterschiedlich sein können, wird ein Topic-Name aus unterschiedlichen Teilen zusammengesetzt.

Präfix und Suffix gelten grundsätzlich für alle Topics.

Präfix und Suffix sind nicht relevant für Gruppen.

Aufbau der Topic-Namen:

- **Präfix**

  Das Präfix des Namens ist ein Adressierungs- und Strukturierungs-String.
- **Topic-Name**
  - Für den Cloud-Betreiber MindConnect IoT Extension ist der Topic-Name "s/us" fest vorgegeben.
  - Für alle anderen Cloud-Betreiber sind die Topic-Namen projektierbar.

    Durch Einfügen mehrerer Namenskomponenten, getrennt durch Schrägstriche (/), können Sie Hierarchie-Ebenen für die spätere Auswertung durch die Subscriber erzeugen.
- **Suffix**

  Das Suffix des Namens ist ein Format-String.

Namensvergabe für Topics und Gruppen

Da die Topic- bzw. Gruppennamen in die Struktur der Datenhaltung des Brokers einfließen, wird die spätere Zuordnung und Auswertung der veröffentlichten Daten erleichtert, wenn die Namen einen Bezug zu den Prozessdaten der Stationen haben.

Beispiel:

Sie möchten eine Gruppe oder ein Topic "Motor5" benennen und der Station mit dem Namen "Station1" zuordnen. Sinnvoll wäre für diesen Fall beispielsweise folgende Eingabe für den Topic-Namen bzw. Gruppennamen:

Station1/Motor5

Projektierungsregeln

Beachten Sie folgende Regeln für die Projektierung:

- Topic-Name

  Innerhalb einer Cloud-Anwendung muss der Name eines Topics eindeutig sein.

  Dies gilt für alle beteiligten Publisher und Subscriber.

- Datenpunktname

  Innerhalb eines Topics muss der Name eines Datenpunkts eindeutig sein.

Hinweis

Konsistenzprüfung von Parametern bei Publisher und Subscriber

Wenn das Gateway als Subscriber zur Laufzeit Daten von einem Publisher empfängt, dann prüft der Subscriber bei jedem empfangenen Wert die folgenden vom Publisher in den Nutzdaten mitgelieferten Parameter:

- Topic-Name
- Datenpunktname
- Datentyp

Wenn diese drei Parameter des Publishers identisch sind mit den im Subscriber projektierten Parametern und wenn der QualityCode der Nachricht "GOOD" ist, schreibt der Subscriber die empfangenen Daten in den Datenbaustein seiner CPU.

Wenn diese drei Parameter des Publishers nicht identisch sind mit den im Subscriber projektierten Parametern, dann verwirft der Subscriber die Daten.

Der Stationsname eines Publishers wird vom Gateway als Subscriber nicht ausgewertet.

Empfehlungen für die Projektierung

Generell ist bei der Übertragung von Daten in einem hierarchisch aufgebauten System eine Benennung der Komponenten entsprechend dieses hierarchischen Aufbaus empfehlenswert.

Beispiel für den Namen eines zu übertragenden Datenpunkts:
"Anlage_1/Anlagenteil_1/Aggregat_1/DB_1_Signal_1"

Für den Zugriff auf die Prozessdaten einer S7-Station kann das Gateway direkt auf Ein- und Ausgänge zugreifen oder auf Variablen der CPU.

Innerhalb einer Cloud-Anwendung können einzelne Publisher Daten für mehrere Subscriber veröffentlichen. Einzelne Subscriber können Daten von mehreren Publishern abonnieren.

Um die Übersichtlichkeit der Daten zu erhöhen und gleichzeitig die Möglichkeit identischer Namen zu reduzieren, empfiehlt sich die folgende Vorgehensweise bei der Projektierung:

- Datenpunktname / DB-Nummer

  Verwenden Sie die Nummer des Datenbausteins (DB), auf den der Datenpunkt zugreift, als Bestandteil des Datenpunktnamens.

- Publisher

  Nehmen Sie den Stationsnamen als Bestandteil der Datenpunktnamen auf, beispielsweise als Präfix. Damit erreichen Sie die Eindeutigkeit der Datenpunktnamen.

- Subscriber

  Legen Sie in der zugeordneten CPU einen separaten DB für jeden Publisher an.

Projektierungsfehler - Diagnosemeldungen

Wenn Sie nach der Inbetriebnahme des Gateways ein anderes Verhalten vorfinden als erwartet, dann nutzen Sie die Diagnosemeldungen des Gateways, die Sie im WBM unter "Instandhaltung > Diagnose" finden.

6.9.2 Profil

Die Einstellungen, die Sie für den Cloud-Zugang des Gateways projektieren, werden in einem Profil hinterlegt. Dies erleichtert die Verwendung des Geräts für verschiedene Einsatzfälle. Individuelle Einstellungen für verschiedene Einsatzfälle können so in verschiedenen Profilen zusammengefasst werden, ohne dass Sie bei einem Wechsel der Cloud die Projektierung ändern müssen.

Für die vorbelegten Cloud-Betreiber sind bereits bestimmte Parameter gemäß den unterschiedlichen Anforderungen der jeweiligen Cloud hinterlegt.

Über das Register wechseln Sie zwischen der Übersichtsseite der MQTT Profile und der HTTP Profile. Alle gespeicherten Profile werden in der Übersichtstabelle dargestellt. Sie können die angezeigten Informationen direkt auf der Übersichtsseite editieren.

Profil hinzufügen / bearbeiten

Legen Sie mindestens ein Profil an, in dem Sie Ihre Einstellungen für den Cloud-Zugang speichern. Sie können bis zu 10 Profile anlegen.

Einstellungen

- **Aktiv**

  Aktiviert das ausgewählte Profil zur Verwendung im Produktivbetrieb.

- **Name**

  Vergeben Sie einen Namen für das Profil.

- **Cloud-Betreiber**

  Wählen Sie den von Ihnen genutzten Dienstbetreiber aus.

  Die Auswahl des Cloud-Betreibers wirkt sich auf die Parameter der Topic-Projektierung aus, siehe auch Kapitel Publish-Gruppen (Seite 117).

  Mit der Auswahl des Cloud-Betreibers legen Sie fest, ob für die Datenübertragung Topics oder Gruppen projektiert werden:

  – AWS / Azure / IBM Cloud

    Sie können mehrere Topics anlegen. Ein Topic kann mehrere Datenpunkte enthalten.

  – MindConnect IoT Extension

    Sie können mehrere Gruppen anlegen. Eine Gruppe kann mehrere Datenpunkte enthalten.

    Eine Gruppe entspricht in der IoT Extension dem Strukturmerkmal "Series".

    In der Voreinstellung werden alle Gruppen dem vorbelegten Standard-Topic "s/us" zugeordnet.

    Hinweis

    Namensänderung des zugeordneten Topics "s/us"

    Wenn Sie dem zugeordneten Topic in der Projektierung einen anderen Namen geben, dann beachten Sie, dass die Daten möglicherweise nicht von der IoT Extension ausgewertet werden können.

  – Andere Cloud

    Sie können mehrere Gruppen anlegen. Eine Gruppe kann mehrere Datenpunkte enthalten.

    In der Voreinstellung werden alle Gruppen einem Topic zugeordnet. Sie können verschiedene Gruppen auch verschiedenen Topics zuordnen.

    Wenn Sie keine Gruppen verwenden möchten, dann legen Sie nur eine Standardgruppe an und löschen im Nutzdaten-Editor den Eintrag "<GROUP_NAME>".

In den weiteren Registern dieser Seite projektieren Sie den Zugang des Geräts zur Cloud.

6.9.2.1 MQTT-Konfiguration

MQTT-Profil hinzufügen

- **Aktiv**

  Aktivieren Sie das Profil für die Verwendung im Produktivbetrieb.

- **Name**

  Vergeben Sie einen Namen für das Profil.

- **Cloud-Betreiber**

  Wählen Sie einen Cloud-Betreiber aus der Klappliste.

- **Adresse**

  Geben Sie die IP-Adresse oder den Host-Namen des Brokers ein.

  Diese Information erhalten Sie von Ihrem Dienstbetreiber.

- **Portnummer**

  Geben Sie die Portnummer des Brokers ein.

MQTT-Security

- **TLS**
  - Option aktiviert

    Die Daten werden über das gesicherte Verfahren TLS übertragen. Für die verschlüsselte Übertragung ist Port 8883 voreingestellt.
  - Option deaktiviert

    Die Daten werden unverschlüsselt übertragen. Für die unverschlüsselte Übertragung ist Port 1883 voreingestellt.

- **TLS-Version**

  Wählen Sie aus der Klappliste die von Ihnen gewünschte und vom Broker unterstützte Version des TLS-Protokolls aus.

- **Nur Secure Ciphers verwenden**

  Hier können Sie die Kommunikation mit Geräten erlauben, die Verfahren für die verschlüsselte Kommunikation verwenden, die aufgrund bekannter Schwachstellen nicht mehr empfohlen werden.
  - Option aktiviert

    Ermöglicht Kommunikation nur mit Geräten, welche empfohlene Verschlüsselungsverfahren unterstützen (Secure Ciphers).
  - Option deaktiviert

    Ermöglicht Kommunikation auch mit Geräten, welche nicht mehr empfohlene Verschlüsselungsverfahren unterstützen (Legacy-Ciphers).

- **Client-Zertifikat**
  Wählen Sie über die Auswahlliste das passende Zertifikat aus dem globalen Zertifikatsspeicher**.**
- **Client-Private key**
  Wählen Sie über die Auswahlliste den passenden private key aus dem globalen Zertifikatsspeicher.
- **Server Zertifikate**
  Über das Add Zeichen können Sie ein Server-Zertifikat hinzufügen. Wählen Sie über die Auswahlliste das passende Server-Zertifikat aus dem globalen Zertifikatsspeicher.
- **Authentifizierung mit Benutzername und Passwort**
  - Aktivieren Sie die Option, wenn Sie einen Verbindungsaufbau mit Authentifizierung nutzen möchten. Die Authentifizierung wird über Benutzername und Passwort durchgeführt.
  - Bei deaktivierter Option wird die Verbindung anonym aufgebaut.
- **Benutzername**

  Geben Sie den von Ihrem Dienstbetreiber zugewiesenen bzw. den selbst festgelegten Benutzernamen ein.
- **Passwort**

  Geben Sie das von Ihrem Dienstbetreiber zugewiesene bzw. das selbst festgelegte Passwort ein.

MQTT-Einstellungen

- **MQTT-Version**

  Wählen Sie die genutzte Protokollversion aus.
- **Client-ID**

  Geben Sie die von Ihrem Dienstbetreiber zugewiesene bzw. die selbst festgelegte Client-ID des Geräts ein.
- **Sitzung bereinigen**
  - Bei aktivierter Option werden die Sitzungsinformationen bei einem Verbindungsabbau gelöscht.
  - Bei deaktivierter Option werden die Sitzungsinformationen bei einem Verbindungsabbau beibehalten.
- **Keepalive-Intervall (s)**

  Vergeben Sie für die Überwachung der Verbindung zum Broker einen Wert (Sekunden). Wenn nach dem Senden von Daten innerhalb der projektierten Zeit keine weiteren Daten zur Übertragung an den Broker anstehen, sendet das Gerät ein Keepalive-Telegramm an den Broker.

  Zulässiger Bereich: 0 oder 5...65535

  Bei 0 (null) wird der maximale Wert (65535 Sekunden) verwendet.

  Voreinstellung: 10

- **Topic Präfix**

  Vergeben Sie optional ein Präfix, das dem Topic-Namen vorangestellt wird.

  Durch gleiche Präfix-Bestandteile können verschiedene Topics in Topic-Ebenen gruppiert werden.

  Das Präfix kann auch Komponenten enthalten, die für den Empfänger des Topics als Bestandteil des Topic-Namens erforderlich sind.

- **Topic Suffix**

  Vergeben Sie optional ein Suffix, das dem Topic-Namen angefügt wird.

  Durch gleiche Suffix-Bestandteile können Sie verschiedene Topics für den gleichen Empfänger vorsehen.

  Das Suffix kann auch Komponenten enthalten, die für den Empfänger erforderlich sind.

Letzter Wille / Testament

- **Letzter Wille / Testament**
  - Bei aktivierter Option werden die Funktionen "Letzter Wille" und "Testament" freigegeben.
  - Bei deaktivierter Option ist die Nutzung beider Funktionen deaktiviert.

  Die Funktionen haben folgende Bedeutung:

  - Letzter Wille

    Im Fall eines Verbindungsabbruchs zwischen Gerät und Broker wird das Versenden einer Nachricht an die Subscriber ermöglicht.

    Sobald der Broker (Server) einen Abbruch der Verbindung mit dem Gerät (Client) feststellt, versendet er eine Nachricht (Testament) an alle Subscriber, die sich am Broker für dieses Topic angemeldet haben.

  - Testament

    Das Testament ist der Inhalt der Nachricht, die beim Verbindungsabbruch an diejenigen Subscriber gesendet wird, die sich am Broker für dieses Topic angemeldet haben.

    Die Testament-Nachricht wird beim Broker gespeichert.

- **Letzter-Wille-Topic**

  Geben Sie hier den Namen des Topics an, welches das Testament überträgt.

  Die weiteren Parameter des Topics projektieren Sie im Topic-Editor, siehe Kapitel Publish-Gruppen (Seite 117).

- **Testament**

  Geben Sie hier den Inhalt der zu übertragende Nachricht ein.

  Max. Anzahl an Zeichen: 65535

- **QoS - Letzter Wille**

  Wählen Sie aus der Klappliste die Quality of Service, mit der das Letzter Wille-Topic übertragen wird.

  – QoS 0 / QoS 1 / QoS 2

  Zur Bedeutung der drei Optionen siehe Kapitel Publish-Gruppen (Seite 117).

- **Retain - Letzter Wille**

  – Bei aktivierter Option wird das Testament mit dem Flag "Retain" an den Broker gesendet.

    Das Testament wird für die dauerhafte Speicherung im Broker aktiviert.

    Bei einem Verbindungsabbau zwischen Gerät und dem Broker veröffentlicht der Broker das Testament für jeden angemeldeten Subscriber.

    Wenn ein Subscriber während eines Verbindungsabbruchs zwischen Gerät und Broker selbst keine Verbindung zum Broker hat, geht das "Testament" für den Subscriber verloren. Beim Wiederaufbau der Verbindung mit dem Broker empfängt der Subscriber dann als erstes das "Testament" mit dem Flag "Retain".

    Weitere Details zum Flag "Retain" finden Sie im Kapitel Publish-Gruppen (Seite 117).

  – Bei deaktivierter Option wird das Testament nicht dauerhaft im Broker gespeichert.

Device-Parameter

Die Paramtergruppe ist nur relevant für die Anbindung an MindConnect IoT Extension. Die Felder können nur editiert werden, wenn als Cloud-Betreiber MindConnect IoT Extension ausgewählt ist.

Die beiden Parameter werden nach dem Verbindungsaufbau zwischen Gerät und MindConnect IoT Extension für die Identifikation Ihres Geräts und für den Austausch von Schlüsselmaterial beim Onboarding-Prozess verwendet.

- **Device-Name**

  Vergeben Sie den Namen, unter dem das Gerät beim Onboarding-Prozess registriert wird.

  Der Device-Name erscheint in MindConnect IoT Extension an folgender Stelle:
  Device > Device profile > "NAME"

- **Device-Typ**

  Der Parameter wird in MindConnect IoT Extension zur Feststellung des Gerätetyps benötigt. Geben Sie folgenden String ein:

  – c8y_MQTTDevice

  Der Device-Typ erscheint in MindConnect IoT Extension an folgender Stelle:
  Device > Device profile > "Type"

Weitere Informationen zum Einrichten der IoT Extension finden Sie im Internet unter:

Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621)

6.9.2.2 HTTP-Profile

HTTP-Profil hinzufügen

- **HTTP aktiv**

  Aktivieren Sie das Profil für die Verwendung für den Produktivbetrieb.

- **Name**

  Vergeben Sie einen Namen für das Profil.

- **Cloud-Betreiber**

  Wählen Sie einen Cloud-Betreiber aus der Klappliste.

- **Adresse**

  Geben Sie die IP-Adresse oder den Host-Namen des Servers ein.

- **HTTP-Port**

  Geben Sie die Portnummer des Servers ein.

TLS

- **TLS**
  - Option aktiviert

    Die Daten werden über das gesicherte Protokoll TLS übertragen. Für die verschlüsselte Übertragung ist Port 443 voreingestellt.
  - Option deaktiviert

    Die Daten werden unverschlüsselt übertragen. Für die unverschlüsselte Übertragung ist Port 80 voreingestellt.

- **TLS-Version**

  Wählen Sie aus der Klappliste die von Ihnen gewünschte und vom Server unterstützte Version des TLS-Protokolls.

- **Nur Secure Ciphers verwenden**

  Hier können Sie die Kommunikation mit Geräten erlauben, die Verfahren für die verschlüsselte Kommunikation verwenden, die aufgrund bekannter Schwachstellen nicht mehr empfohlen
  werden.
  - Option aktiviert

    Ermöglicht Kommunikation nur mit Geräten, welche empfohlene Verschlüsselungsverfahren unterstützen (Secure Ciphers).
  - Option deaktiviert

    Ermöglicht Kommunikation auch mit Geräten, welche nicht mehr empfohlene Verschlüsselungsverfahren unterstützen (Legacy-Cipher).

- **Zertifikat**

  Wählen Sie über die Auswahlliste ein Zertifikat aus dem globalen Zertifikatsspeicher.

- **Privater Schlüssel**

  Wählen Sie über die Auswahlliste einen Schlüssel aus dem globalen Zertifikatsspeicher.

- **Vertrauenswürdiger Server**

  Über das Hinzufügen-Zeichen können Sie ein Server-Zertifikat hinzufügen. Wählen Sie über die Auswahllliste einen vertrauenswürdigen Server.

HTTP-Einstellungen

- **HTTP-Version**

  Wählen Sie die gewünschte Protokollversion.

- **Zielpfad-Präfix**

- **Zielpfad-Suffix**

6.9.3 Publisher

Übersicht

In diesem Register legen Sie für alle projektierten Profile die Topics bzw. Gruppen für die Übertragung an den Broker / HTTP-Server an. Zur Projektierung des Profils siehe Kapitel Profil (Seite 109).

Informationen zur Strukturierung der Daten in Topics bzw. Gruppen bei verschiedenen Cloud-Betreibern und zur Projektierung der Topic-Namen finden Sie im Kapitel Hinweise zur Datenstrukturierung und Projektierung (Seite 106).

6.9.3.1 Publish-Gruppen

Topic hinzufügen / Gruppe hinzufügen

- **Profil wählen**

  Wählen Sie eines der zuvor angelegten Profile aus der Auswahlliste.

Für das ausgewählte Profil werden alle projektierten Gruppen / Topics angezeigt.

- **Hinzufügen**

  Ein neues editierbares Topic wird der Tabelle hinzugefügt.

  Maximale Anzahl Publish- und Subscriber-Topics bzw. Gruppen

  CC712: 500

  CC716: 3500

- **Kopieren**

  Die ausgewählten Topics werden kopiert und ein weiteres Mal der Tabelle hinzugefügt.

- **Löschen**

  Alle ausgewählten Topics werden gelöscht.

Topic-/Gruppen-Tabelle

In der Tabelle sehen Sie die angelegten Topics bzw. Gruppen und projektieren deren Eigenschaften.

Sie können die Anzeige alphabetisch nach Name oder Topic sortieren, indem Sie in der Kopfzeile der Tabelle auf das Symbol neben der Bezeichnung klicken.

- **Name**

  Die Namen der projektierten Gruppen werden angezeigt.

- **Topic**

  – ⇒ Gültigkeit: MindConnect IoT Extension

    Der vorbelegte Topic-Name "s/us" wird eingefügt.

    Verwenden Sie diesen Standard-Namen bei Anbindung an MindSphere über IoT Extension.

    Passen Sie den Namen bei Anbindung an eine andere Cloud nach Vorgaben des Cloud-Betreibers an.

  – ⇒ Gültigkeit: AWS / Azure / IBM Cloud / Andere Cloud

    Geben Sie den Namen des Topics an.

  – Gültigkeit: HTTP

    Geben Sie den auf <Servername>:<Port> folgenden Teil der URL an.

  Der projektierte Namen mit allen Bestandteilen wird im Tooltip angezeigt, wenn Sie mit der Maus über das Topic fahren.

- **QoS**

  Nur bei Auswahl von Profil "MQTT".

  Legen Sie über den Parameter "Quality of Service" das Übertragungsverhalten der Nachrichten dieses Topics fest:

  – QoS 0

    Übertragung höchstens einmal

    Das Gerät sendet das Topic einmal an den Broker. Das Gerät erwartet keine Quittung. Wenn das Topic vom Broker nicht empfangen wird, dann ist es verloren.

  – QoS 1

    Übertragung mindestens einmal

    Das Gerät sendet das Topic so lange an den Broker, bis es ein PUBACK-Paket als Quittung vom Broker empfängt.

  – QoS 2

    Übertragung genau einmal

    Das Gerät sendet das Topic und wartet, bis es die spezifikationsgemäße zweistufige Quittung vom Broker empfängt.

    Diese Variante stellt die höchste Qualitätsstufe dar, ist aber mit dem höchsten Verwaltungsaufwand sowohl beim Client als auch beim Server verbunden.

  Bei Verbindungsabbrüchen werden die Daten-Telegramme bei QoS 1 und QoS 2 zwischengespeichert. Siehe hierzu Abschnitt "Verbindungsabbruch" unten.

- **Retain**

  Nur bei Auswahl von Profil "MQTT".

  Aus Topics/Gruppen mit dem Flag "Retain" speichert der Broker die jeweils letzte Nachricht.

  Wenn ein Subscriber ein neues Topic abonniert oder wenn die Verbindung mit einem Subscriber nach einem Abbruch wiederkehrt, versendet der Broker zu jedem Topic mit Retain-Flag die letzte Nachricht an den Subscriber.

  Das Retain-Flag können Sie für alle oder für einzelne Topics/Gruppen setzen (Option in einzelner Zeile aktiviert).

  Das übergeordnete Optionskästchen aktiviert die Funktion für alle Topics/Gruppen der Tabelle.

  Beachten Sie:
  Wenn Sie nach Aufnahme des Produktivbetriebs das Versenden der letzten Nachricht durch den Broker an neu verbundene Subscriber zurücknehmen möchten, bewirken Sie dies nicht durch die nachträgliche Deaktivierung des Retain-Flags am Topic. Der Broker schickt weiterhin die letzte gültige Nachricht des Publishers an neu verbundene Subscriber. Um das Versenden dieser Nachrichten durch den Broker zu verhindern, senden Sie z. B. eine leere Nachricht (0 Bytes) an den Broker.

- **Nutzdaten-Format**

  Zeigt das derzeit ausgewählte Nutzdaten-Format an.

  Über die erste Schaltfläche öffnen Sie den Nutzdaten-Editor zur Festlegung des Formats der übertragenen Nutzdaten. Zur Beschreibung siehe Kapitel Nutzdaten-Format (Seite 123).

  Über die zweite Schaltfläche öffnen Sie die Nutzdaten-Vorschau zur Überprüfung und Anzeige der festgelegten Nutzdaten mit dem gewünschten Format. Wird ein neues Nutzdaten-Format ausgewählt, muss die Seite mit den Publish-Gruppen zuerst gespeichert werden. Erst dann wird die Vorschau an das neu ausgewählte Format angepasst.

  Hinweis

  Nutzdaten-Format älterer Firmware-Versionen nicht veränderbar

  Ein Nutzdaten-Format älterer Firmware-Versionen wird als veraltet angezeigt. Es wird von der aktuellen Firmware-Version zwar zur Laufzeit noch unterstützt, kann aber ohne die Umstellung auf ein aktuelles Format nicht mehr verändert werden.

  Zukünftige Firmware-Versionen werden veraltete Formate nicht mehr unterstützen und eine entsprechende Konfiguration kann dann nicht mehr geladen werden.

- **Verb**

  Nur bei Auswahl von Profil "HTTP".
  Wählen sie eine der HTTP-Methoden aus: POST, PUT, PATCH, DELETE

- **HTTP-Header**
  Nur bei Auswahl von Profil "HTTP".
  Ergänzen Sie den vom HTTP-Server benötigte HTTP-Header.
  Für das Senden von Nutzdaten im JSON-Format sollte beispielsweise der HTTP-Header "Content-Type" mit dem Wert "application/json" ergänzt werden.
  Den HTTP Header "Content-Length" ergänzt die Baugruppe intern.

- **Trigger**

  Mit den Triggern legen Sie die Bedingungen fest, bei deren Eintreten die Übertragung des im Gerät gespeicherten Werts an den Broker ausgelöst wird.

  Pro Topic kann ein Trigger ausgewählt werden. Folgende Trigger-Klassen sind projektierbar:

  Zeit-Trigger

  – Zyklisch

    Der Wert des Datenpunkts wird zyklisch übertragen. Wertebereiche:
    100 .. 100 000 000 ms
    1 .. 100 000 s
    1 .. 1666 min
    1 .. 27 h

  – Einmal täglich

    Der Wert wird einmal täglich zur projektierten Zeit übertragen.

  – Einmal wöchentlich

    Der Wert wird einmal in der Woche übertragen.

  – Einmal monatlich

    Der Wert wird einmal im Monat übertragen.

    Wenn ein Monat weniger Tage hat als der in der Projektierung angegebene Tag, wird der Wert des Datenpunkts am Monatsende übertragen.

  Eingangs-Trigger

  – Digitaler Eingang

    Erscheint nur in Auswahlliste, wenn der digitale Eingang in der Schnittstellen-Konfiguration als Trigger definiert wurde, siehe Kapitel DI/DO (CC716) (Seite 82).

    Übertragung einmalig bei Flankenwechsel am digitalen Eingang.

    Alternativ bei Flankenwechsel 1 → 0 oder 0 → 1

  – Cloud-Verbindung

    Übertragung beim Flankenwechsel des Cloud-Verbindungsstatus.

- **Nachrichten-Pufferung**

  Im Fall eines Verbindungsabbruchs zwischen Gateway und Cloud-Server speichert das Gateway auflaufende Nachrichten bis zu der im Feld "Nachrichten-Pufferung" eingegebenen Anzahl in seinem Nachrichtenspeicher. Die Gesamtgröße des Nachrichtenspeichers kann auf die einzelnen Topics bzw. Gruppen verteilt werden. Beim Speichern der Einstellung wird überprüft, ob die projektierte Anzahl für dieses Topic bzw. Gruppe noch in den Nachrichtenspeicher passt. Der benötigte Platz im Nachrichtenspeicher hängt auch von der Anzahl der zum Topic bzw. Gruppe zugeordneten Datenpunkte und deren maximalen Datenbreite ab. Außerdem wirkt sich das Sammeln von Werten auf den benötigten Platz im Nachrichtenspeicher aus.

  Der Nachrichtenspeicher arbeitet chronologisch, das heißt, die ältesten Nachrichten werden zuerst gesendet (FIFO-Prinzip). Sobald die projektierten Pufferplätze für ein Topic bzw. Gruppe belegt sind, wird die jeweils älteste Nachricht wieder überschrieben.

- **Sammeln**

  Sammelt Werte, die aufgrund von erfüllten Trigger-Bedingungen (Wert- oder Zeit-Trigger) ausgelöst wurden. Sobald die eingegebene Anzahl an Werten erreicht ist, werden sie gesammelt als eine Nachricht an den Broker versendet.

  Die gesammelten Werte können alternativ folgendermaßen in den Nutzdaten angezeigt werden:

  - Als Array, durch Kommas getrennt in einer Liste.
  - Als gesammelte Einzelwerte, jeweils mit Qualitätsstatus und Zeitstempel. Verwenden Sie dazu den Code-Schlüssel `TIME_SERIES` innerhalb des Nutzdaten-Formats.

- **Löschen**

  Durch Klicken auf die Schaltfläche werden die Topics der markierten Zeilen gelöscht. Sind keine Zeilen markiert, werden Sie gefragt ob Sie alle Topics löschen möchten.

Hinweis
Löschen

Beachten Sie, dass Sie das versehentliche Entfernen eines Topics oder einer Gruppe nicht rückgängig machen können.

Datenpunkt-Zuordnung

Auf dieser Seite ordnen Sie die projektierten Datenpunkte einem zuvor angelegten Topic bzw. einer Gruppe zu. Zur Beschreibung siehe Kapitel Datenpunkt-Zuordnung (Seite 136).

Die übertragenen Nutzdaten ordnen Sie den Topics in der Datenpunktprojektierung zu.

6.9.3.2 Publish-Einstellungen

Empfehlungen für die Projektierung

- **Profil wählen**

  Wählen Sie eines der zuvor angelegten Profile aus der Auswahlliste.

- **Zeitstempel-Format**

  Einstellung, in welchem Format die Platzhalter `PUBLISH_TIMESTAMP` und `SOURCE_TIMESTAMP` der Topics übertragen werden.

  - **ISO 8601 String**

    Angabe im Format 2021-10-26T10:35:06.248716825+00:00

  - **Unix-Zeit**

    Angabe als Unix-Wert, z. B. 1635238284.356

  - **Benutzerdefiniert**
    Definition eines selbst definierten Zeitstempel Formats. Das Format wird im Textfeld darunter eingegeben

- **Zeitstempel-String**

  Textfeld zur Eingabe eines benutzerdefinierten Zeitstempels. Nur bei Auswahl des Zeitstempel-Formats "Benutzerdefiniert" möglich.

  Folgende Platzhalter können dabei genutzt werden Link (https://cplusplus.com/reference/ctime/strftime/).

  Zusätzlich sind folgende Platzhalter definiert:

Platzhalter	Darstellung
{{ms}}	Sekunden-Anteil mit 3 Nachkommastellen (Millisekunden)
{{us}}	Sekunden-Anteil mit 6 Nachkommastellen (Mikrosekunden)
{{ns}}	Sekunden-Anteil mit 9 Nachkommastellen (Nanosekunden)

  Bei Auswahl von "ISO 8601 String" ist das Textfeld ausgegraut und belegt mit dem Format "%FT%T.{{ns}}+00:00"

- **QualityCode-Format**

  Einstellung, in welchem Format und mit welchem Wert der Platzhalter `QUALITY_CODE` übertragen werden soll.

  Vorbelegt sind:

  Good = String "GOOD"

  Bad = String "BAD"

- **Boolesche-Werte-Format**

  Einstellung, in welchem Format und mit welchem Wert der Platzhalter `VALUE` bei BOOL-Variablen übertragen werden soll.

  Vorbelegt sind:

  True = Integer 1

  False = Integer 0

Hinweis

Benutzerdefinierten Nutzdaten-Formaten nach Firmware-Aktualisierung prüfen

Nach der Firmware-Aktualisierung wird für benutzerdefinierte Nutzdaten-Formate die den Platzhalter "`{{QUALITY_CODE}}`" verwenden, der Status ""GOOD"" statt wie bisher "GOOD" ausgeben.

Prüfen Sie, ob die benutzerdefinierten Nutzdaten-Formate nach der Aktualisierung die korrekte JSON-Syntax haben und passen Sie diese ggf. an.

Bei Verwendung der CloudConnect 7-Vorlagen für die Nutzdaten-Formate, werden die Daten konvertiert und können ohne Anpassungen verwendet werden.

Siehe auch

Profil (Seite 109)

Link: (https://www.unixtimestamp.com)

6.9.3.3 Nutzdaten-Format

Da verschiedene Cloud-Systeme ein unterschiedliches Nutzdaten-Format erwarten, müssen Sie das Format an die Anforderungen der weiterverarbeitenden Systeme anpassen.

Auf dieser Seite finden Sie Syntax-Vorlagen, von denen Sie die passende auswählen und bei Bedarf an die Anforderungen des Cloud-Systems anpassen können. Den Code verändern Sie im Textfeld "Nutzdaten-Format".

Automatische Datenpunkt-Zuordnung zum Nutzdaten-Format

Wenn der Code den Anforderungen entspricht, dann lassen Sie ihn unverändert. Damit werden alle dem Topic/Gruppe zugeordneten Datenpunkte vor dem Versenden immer gemäß der ausgewählten Vorlage aufbereitet. Das heißt, wenn Sie bereits zugeordnete Datenpunkte aus diesem Topic/Gruppe entfernen oder weitere Datenpunkte zuordnen, so werden die Nutzdaten immer die letztendlich zugeordneten Datenpunkte enthalten.

Manuelle Datenpunkt-Zuordnung zum Nutzdaten-Format

Wenn Sie das Nutzdaten-Format im Textfeld verändern, dann wird durch den Dialog die Vorlage "Benutzerdefiniert" ausgewählt. Damit legen Sie den Inhalt und das Format der Nutzdaten fest und das Gateway verändert dieses Format und die Zuordnung der Datenpunkte danach nicht mehr. Auch nicht, wenn Sie bereits zugeordnete Datenpunkte aus dem Topic oder der Gruppe entfernen oder weitere Datenpunkte dem Topic zuordnen. Explizite Referenzierung von Datenpunkten, die dem Topic oder der Gruppe nicht zugeordnet sind, werden in den Nutzdaten als leere Zeichenkette dargestellt.

Für die Formatierung der Nutzdaten wird die Zeichen-Kodierung UTF-8 verwendet.

Nutzdaten-Vorlagen

Hier sind die wichtigsten Informationen aufgelistet und können direkt editiert werden. Für die jeweiligen Erklärungen der Parameter sind die folgenden Seiten beim Anlegen neuer Stationen.

- **Hinzufügen**

  Leitet auf eine neue Seite weiter, auf der Nutzdaten-Vorlagen erstellt werden können.

- **Löschen**

  Die selektierten Nutzdaten-Vorlagen werden gelöscht. Vom CC7 verwaltete Default Vorlagen können nicht gelöscht werden.

Syntax-Vorlagen

Folgende Vorlagen stehen zur Verfügung:

- **Hinzufügen**

  Über das "Hinzufügen"-Symbol können eigene Nutzdaten-Vorlagen erstellt werden.

- **JSON generisch v2 / JSON spezifisch v2**
  - Es wird die Syntax des JSON-Formats gemäß ECMA-404 und ISO/IEC 21778:2017 verwendet.
  - Die Werte werden nicht als String, sondern als native Datentypen verwendet und können somit Datenpunkte vom Typ "Array" übertragen.

- **JSON generisch v3 / JSON spezifisch v3**
  - Es wird die Syntax des JSON-Formats gemäß ECMA-404 und ISO/IEC 21778:2017 verwendet.
  - Die Werte werden nicht als String, sondern als native Datentypen verwendet und können somit Datenpunkte vom Typ "Array" übertragen.
  - Bei Aktivierung der Funktion "Sammeln" werden über die Schleife "TIME_SERIES" alle Datenpunkte gesammelt in einem Topic übertragen.

  Alle Vorlagen sind geeignet für die Anbindung an:
  - AWS (Amazon) / IoT Core
  - Azure (Microsoft) / IoT Hub
  - IBM Cloud (IBM) / Watson IoT Platform

- **XML generisch v1 / XML spezifisch v1**

  Vorlagen für die Anbindung an Cloud-Dienste, die das XML-Format erwarten.

- **CSV generisch v1**

  Vorlage für die Anbindung an MindSphere (Siemens) / MindConnect IoT Extension

Nutzdaten-Editor

Über die Schalfläche "Nutzdaten-Format" öffnen Sie den Nutzdaten-Editor.

- **Vorlage für Nutzdaten-Format**

  In der Voreinstellung wird im Textfeld "Nutzdaten-Format" das Format "JSON generisch v2" angezeigt.

  Über die Klappliste können Sie eine der oben beschriebenen Syntax-Vorlagen auswählen. Nach Auswahl einer Syntax-Vorlage können Sie durch Klicken auf das Stift-Symbol in die benutzerdefinierte Bearbeitung wechseln.

- **Nutzdaten-Format**

  In dem Textfeld können Sie das zu verwendende Nutzdaten-Format verändern oder ein Format nach Ihren eigenen Bedürfnissen erstellen.

  Mit Auswahl einer Syntax-Vorlage (siehe oben) wird die Syntax der oben ausgewählten Vorlage angezeigt und verwendet.

  Hinweis

  Einstellungen zum Nutzdaten-Format

  - Wenn Sie die "Vorlage für Nutzdaten-Format" ändern (z. B. von "Benutzerdefiniert" auf "JSON spezifisch"), dann geht ein manuell angepasstes Nutzdaten-Format verloren. Damit können Sie aber auch die automatische Datenpunkt-Zuordnung zum Nutzdaten-Format wiederherstellen.
  - Das Nutzdaten-Format darf nicht mehr als 65.535 Bytes an UTF-8-Text enthalten, ansonsten kann es nicht übernommen werden.

- **Automatisch Anführungszeichen um Werte hinzufügen**

  Option kann nur bei der Syntax-Vorlage "Benutzerdefiniert" angepasst werden. Bei den anderen Syntax-Vorlagen ist die Option entsprechend der Auswahl gesetzt.

  Wenn aktiviert, wird bei Datenpunkten vom Typ "String" und "DateTime" automatisch ein String um den Wert {{VALUE}} gesetzt, falls notwendig.

- **Escape-Sequenzen**

  Für die Umwandlung bestimmter Sonderzeichen können Escape-Sequenzen angewendet werden, die den Code gemäß dem verwendeten Protokoll anpassen.

  Sonderzeichen können beispielsweise innerhalb der folgenden Namens-Komponenten auftreten:

  - Stationsname
  - Topic-Name
  - Gruppenname

  Folgende Escape-Sequenzen stehen für die Anwendung zur Auswahl:

  - JSON

    Standard-JSON-Escape-Sequenzen
  - XML

    Standard-XML-Escape-Sequenzen
  - CSV

    Standard-CSV-Escape-Sequenzen

  Bei Auswahl einer Option werden die jeweiligen Sonderzeichen beim Publisher in Escape-Sequenzen umgewandelt.

  Beim Subscriber werden die Escape-Sequenzen in umgekehrter Richtung umgewandelt.

  Zu den beim JSON-Format verwendeten Escape-Sequenzen siehe Anhang JSON-Escape-Sequenzen (Seite 199).

- **Dieses Nutzdaten-Format für alle Topics verwenden**

  Bei aktivierter Option wird das im Textfeld angezeigte Nutzdaten-Format für alle zu veröffentlichenden Gruppen bzw. Topics übernommen.

  Nach dem Speichern wird das Häkchen der Option aus dem Topic-Editor entfernt.

  Beachten Sie:
  Bei späteren Änderungen werden die Änderungen beim Klicken auf "Übernehmen" nur für das jeweilige Topic bzw. die jeweilige Gruppe übernommen, nicht für alle.

- **Abbrechen**

  Der Nutzdaten-Editor wird geschlossen, ohne dass die getätigten Änderungen gespeichert werden.

- **Speichern**

  Die vorgenommenen Änderungen im Nutzdaten-Editor werden gespeichert und der Nutzdaten-Editor wird geschlossen.

Nutzdaten-Vorschau

Die Vorschau zeigt an, wie die projektierten Nutzdaten des ausgewählten Topics, gefüllt mit Beispielwerten, an den Broker versendet werden.

Die Anzeige ist auf 65535 Zeichen begrenzt.

- **Exportieren**

  Das gesamte Nutzdaten-Format kann zur Analyse als Datei "cc_plrender.txt" heruntergeladen werden (auch bei mehr als 65535 Zeichen).

- **Schließen**

  Die Nutzdaten-Vorschau wird geschlossen.

Nutzdaten-Format - JSON generisch v3

Es werden alle dem Topic zugeordneten Datenpunkte über ein Schleifenkonstrukt mit den angegebenen Eigenschaften und Formatierungen in den Nutzdaten abgebildet.

```
{"Timestamp":"{{PUBLISH_TIMESTAMP}}","DataItems":[{{#DATA_POINT_ARRAY}}{"Variable":"{{NAME}}","Type":"{{TYPE}}","TimeSeries":[{{#TIME_SERIES}}{"Value":{{VALUE}},"QualityCode":{{QUALITY_CODE}},"SourceTimestamp":"{{SOURCE_TIMESTAMP}}"}{{^LAST_ITEM}},{{/LAST_ITEM}}{{/TIME_SERIES}}]}{{^LAST_DATA_POINT}},{{/LAST_DATA_POINT}}{{/DATA_POINT_ARRAY}}]}
```

Anwendungsfälle:

- Einfaches JSON-Nutzdatenformat mit vielen Datenpunkten und möglichst hoher Performance bei möglichst niedrigem Datenaufkommen.
- Unterstützung Datenpunkte vom Typ "Array".
- Unterstützung der Funktion "Sammeln".

Nutzdaten-Format - JSON generisch v2

Es werden alle dem Topic zugeordneten Datenpunkte über ein Schleifenkonstrukt mit den angegebenen Eigenschaften und Formatierungen in den Nutzdaten abgebildet.

```
{"Timestamp":"{{PUBLISH_TIMESTAMP}}","DataItems":[{{#DATA_POINT_ARRAY}}{"Variable":"{{NAME}}","Type":"{{TYPE}}","Value":{{VALUE}},"QualityCode":{{QUALITY_CODE}}}{{^LAST_DATA_POINT}},{{/LAST_DATA_POINT}}{{/DATA_POINT_ARRAY}}]}
```

Anwendungsfälle:

- Einfaches JSON-Nutzdatenformat mit vielen Datenpunkten und möglichst hoher Performance bei möglichst niedrigem Datenaufkommen.
- Unterstützung Datenpunkte vom Typ "Array".

Nutzdaten-Format - JSON spezifisch v3

Bei Auswahl dieses Formats werden alle zugeordneten Datenpunkte mit ihren verfügbaren Eigenschaften einzeln aufgelistet. Beispiel für 3 Datenpunkte der Station "ST1" mit den Namen "DP1", "DP2" und "DP3":

```
{
 "Timestamp": "{{PUBLISH_TIMESTAMP}}",
 "DataItems":
 [
 {
 "Variable":"{{ST1.DP1.NAME}}",
 "Type":"{{ST1.DP1.TYPE}}",
 "TimeSeries":
 [{{#ST1.DP1.TIME_SERIES}}
 {
 "Value":{{VALUE}},
 "QualityCode":{{QUALITY_CODE}},
 "SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
 }{{^LAST_ITEM}},{{/LAST_ITEM}}
 {{/ST1.DP1.TIME_SERIES}}]
 },
 {
 "Variable":"{{ST1.DP2.NAME}}",
 "Type":"{{ST1.DP2.TYPE}}",
 "TimeSeries":
 [{{#ST1.DP2.TIME_SERIES}}
 {
 "Value":{{VALUE}},
 "QualityCode":"{{QUALITY_CODE}}",
 "SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
 }{{^LAST_ITEM}},{{/LAST_ITEM}}
 {{/ST1.DP2.TIME_SERIES}}]
 },
 {
 "Variable":"{{ST1.DP3.NAME}}",
 "Type":"{{ST1.DP3.TYPE}}",
 "TimeSeries":
```

```
 [{{#ST1.DP3.TIME_SERIES}}
 {
 "Value":{{VALUE}},
 "QualityCode":"{{QUALITY_CODE}}",
 "SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
 }{{^LAST_ITEM}},{{/LAST_ITEM}}
 {{/ST1.DP3.TIME_SERIES}}]
 }
 ]
}
```

Umschaltung von "JSON spezifisch" auf "Benutzerdefiniert"

Jeder Datenpunkt kann dabei individuell formatiert und mit ausgesuchten Eigenschaften in den Nutzdaten abgebildet werden. Nicht benötigte Eigenschaften einzelner Datenpunkte können einfach gelöscht werden. Zusätzliche (z. B. auch statische) Inhalte können ergänzt werden. Die Eigenschaften ausgesuchter Datenpunkte können auch mehrfach referenziert werden. Die Referenzen auf die Datenpunkte müssen aber immer innerhalb der eckigen Klammer "DataItems" [...] stehen.

Anwendungsfälle:

- Komplexes JSON-Nutzdatenformat mit wenigen Datenpunkten.
- Unterstützung Datenpunkte vom Typ "Array".
- Unterstützung der Funktion "Sammeln"

Nutzdaten-Format - JSON spezifisch v2

Bei Auswahl dieses Formats werden alle zugeordneten Datenpunkte mit ihren verfügbaren Eigenschaften einzeln aufgelistet. Beispiel für 3 Datenpunkte der Station "ST1" mit den Namen "DP1", "DP2" und "DP3":

```
{
 "Timestamp": "{{PUBLISH_TIMESTAMP}}",
 "DataItems":
 [
  {
   "Variable": "{{ST1.DP1.NAME}}",
   "Type": "{{ST1.DP1.TYPE}}",
   "Value": {{ST1.DP1.VALUE}},
   "QualityCode": {{ST1.DP1.QUALITY_CODE}},
   "StationName": "{{ST1.DP1.STATION_NAME}}",
   "Timestamp": "{{ST1.DP1.SOURCE_TIMESTAMP}}"
```

```
  },
  {
   "Variable": "{{ST1.DP2.NAME}}",
   "Type": "{{ST1.DP2.TYPE}}",
   "Value": {{ST1.DP2.VALUE}},
   "QualityCode": {{ST1.DP2.QUALITY_CODE}},
   "StationName": "{{ST1.DP2.STATION_NAME}}",
   "Timestamp": "{{ST1.DP2.SOURCE_TIMESTAMP}}"
  },
  {
   "Variable": "{{ST1.DP3.NAME}}",
   "Type": "{{S1.DP3.TYPE}}",
   "Value": {{ST1.DP3.VALUE}},
   "QualityCode": {{ST1.DP3.QUALITY_CODE}},
   "StationName": "{{ST1.DP3.STATION_NAME}}",
   "Timestamp": "{{ST1.DP3.SOURCE_TIMESTAMP}}"
  }
 ]
}
```

Umschaltung von "JSON spezifisch" auf "Benutzerdefiniert"

Jeder Datenpunkt kann dabei individuell formatiert und mit ausgesuchten Eigenschaften in den Nutzdaten abgebildet werden. Nicht benötigte Eigenschaften einzelner Datenpunkte können einfach gelöscht werden. Zusätzliche (z. B. auch statische) Inhalte können ergänzt werden. Die Eigenschaften ausgesuchter Datenpunkte können auch mehrfach referenziert werden. Die Referenzen auf die Datenpunkte müssen aber immer innerhalb der eckigen Klammer "DataItems" [...] stehen.

Anwendungsfälle:

- Komplexes JSON-Nutzdatenformat mit wenigen Datenpunkten.
- Unterstützung Datenpunkte vom Typ "Array".

Nutzdaten-Format - XML generisch

Es werden alle dem Topic zugeordneten Datenpunkte über ein Schleifenkonstrukt mit den angegebenen Eigenschaften und Formatierungen in den Nutzdaten abgebildet.

```
<?xml version="1.0" encoding="UTF-
8"?><root><Timestamp>{{PUBLISH_TIMESTAMP}}</Timestamp><DataItems>{{#
DATA_POINT_ARRAY}}<DataItem><Variable>{{NAME}}</Variable><Type>{{TYP
E}}</Type><Value>{{VALUE}}</Value><QualityCode>{{QUALITY_CODE}}</Qua
lityCode></DataItem>{{/DATA_POINT_ARRAY}}</DataItems></root>
```

Anwendungsfälle:

- Einfaches XML-Nutzdatenformat mit vielen Datenpunkten und möglichst hoher Performance bei möglichst niedrigem Datenaufkommen.

Nutzdaten-Format: XML spezifisch

Bei Auswahl dieses Formats werden alle zugeordneten Datenpunkte mit ihren verfügbaren Eigenschaften einzeln aufgelistet. Beispiel für 3 Datenpunkte der Station "ST1" mit den Namen "DP1", "DP2" und "DP3":

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
 <Timestamp>{{PUBLISH_TIMESTAMP}}</Timestamp>
 <DataItems>
  <DataItem>
   <Var>{{ST1.DP1.NAME}}</Var>
   <Type>{{ST1.DP1.TYPE}}</Type>
   <Value>{{ST1.DP1.VALUE}}</Value>
   <QualityCode>{{ST1.DP1.QUALITY_CODE}}</QualityCode>
   <StationName>{{ST1.DP1.STATION_NAME}}</StationName>
   <Timestamp>{{ST1.DP1.SOURCE_TIMESTAMP}}</Timestamp>
  </DataItem>
  <DataItem>
   <Var>{{ST1.DP2.NAME}}</Var>
   <Type>{{ST1.DP2.TYPE}}</Type>
   <Value>{{ST1.DP2.VALUE}}</Value>
   <QualityCode>{{ST1.DP2.QUALITY_CODE}}</QualityCode>
   <StationName>{{ST1.DP2.STATION_NAME}}</StationName>
   <Timestamp>{{ST1.DP2.SOURCE_TIMESTAMP}}</Timestamp>
  </DataItem>
  <DataItem>
   <Var>{{ST1.DP3.NAME}}</Var>
   <Type>{{ST1.DP3.TYPE}}</Type>
   <Value>{{ST1.DP3.VALUE}}</Value>
   <QualityCode>{{ST1.DP3.QUALITY_CODE}}</QualityCode>
   <StationName>{{ST1.DP3.STATION_NAME}}</StationName>
   <Timestamp>{{ST1.DP3.SOURCE_TIMESTAMP}}</Timestamp>
  </DataItem>
```

```
 </DataItems>
</root>
```

Umschaltung von "XML spezifisch" auf "Benutzerdefiniert"

Jeder Datenpunkt kann dabei individuell formatiert und mit ausgesuchten Eigenschaften in den Nutzdaten abgebildet werden. Nicht benötigte Eigenschaften einzelner Datenpunkte können einfach gelöscht werden. Zusätzliche (z. B. auch statische) Inhalte können ergänzt werden. Die Eigenschaften ausgesuchter Datenpunkte können auch mehrfach referenziert werden. Die Referenzen auf die Datenpunkte müssen aber immer innerhalb der XML-Klammer <DataItems> ... </DataItems> stehen.

Anwendungsfälle:

- Komplexes XML-Nutzdatenformat mit eher wenigen Datenpunkten.
- Spezielle Anpassung der Nutzdaten an Vorgaben Dritter.

Nutzdaten-Format - MindConnect IoT Extension

```
{{#DATA_POINT_ARRAY}}200,{{NAME}},{{GROUP}},{{VALUE}},{{ADDITIONAL_A
TTRIBUTE}},{{PUBLISH_TIMESTAMP}}\n{{/DATA_POINT_ARRAY}}
```

Code: Syntax und Bedeutung

Beschreibung der Syntax

Die Beschreibung der einzelnen Schlüssel ist folgendermaßen aufgebaut:

- **Name**

  `<Syntax>`

  Bedeutung

Code-Schlüssel

Der Code für die Formatierung der Nutzdaten kann aus den nachfolgend aufgelisteten Schlüsseln bestehen.

Wenn Sie nicht nur die Schlüssel für die Übertragung der Nutzdaten verwenden möchten, sondern Text ergänzen möchten, können Sie den Text vor oder nach einem Schlüssel ergänzen.

Der Code der formatierten Nutzdaten kann je nach Format die nachfolgenden Schlüssel enthalten.

- **Zeitstempel**

  `{{PUBLISH_TIMESTAMP}}`

  Zeitpunkt der Veröffentlichung

  – Beispiel für die Kodierung des Zeitstempels mit ergänztem Text "sent at":

    Syntax: "`sent at {{PUBLISH_TIMESTAMP}}`"
    Ergibt Zeichenkette: "`sent at 2019-04-20T13:58:16.192313634+00:00`"

- **Beginn und Ende der Schleife über alle zugeordneten Datenpunkte**

  `{{#DATA_POINT_ARRAY}}`

  `{{/DATA_POINT_ARRAY}}`

- **Beginn und Ende der Schleife über alle gesammelten Werte**

  `{{#TIME_SERIES}}`

  `{{/TIME_SERIES}}`

- **200**

  `200`

  Funktionscode (MindConnect IoT Extension)

- **Station**

  Hinweis
  Korrekte Benennung der Station / Variable

  Die direkte Referenzierung mittels {{Station.Variable.xxx}} bei benutzerdefinierten Nutzdaten kann nur mit Stationen bzw. Variablen verwendet werden, in denen kein Punkt im Namen vorkommt. Mit einem Punkt werden die Werte nicht mehr korrekt ersetzt.

  `{{STATION_NAME}} /`

  `{{Station.Variable.STATION_NAME}}`

  Stationsname des Datenpunkts

  Projektierung nur beim Publisher

- **Datenpunkt / Variable**

  `{{NAME}} /`

  `{{Station.Variable.NAME}}`

  Name des Datenpunkts

- **Gruppe**

  `{{GROUP}} /`

  `{{Station.Variable.GROUP}}`

  Gruppenname

- **Wert**

  `{{VALUE}} /`

  `{{Station.Variable.VALUE}}`

  Wert des Datenpunkts

  Ist die Funktion "Sammeln" aktiviert und enthält das Nutzdaten-Format keine TIME_SERIES-Schleife, dann werden die gesammelten Werte innerhalb der Nutzdaten durch Kommas getrennt in einer Liste angezeigt.

- **Attribut**

  `{{ADDITIONAL_ATTRIBUTE}} /`

  `{{Station.Variable.ADDITIONAL_ATTRIBUTE}}`

  Zusätzliches Attribut, das individuell für jeden Datenpunkt manuell konfiguriert werden kann (bei MindConnect IoT Extension zwingend erforderlich, sonst optional).

- **QualityCode**

  `{{QUALITY_CODE}} /`

  `{{Station.Variable.QUALITY_CODE}}`

  Qualitätsstatus des Werts

  Ist die Funktion "Sammeln" aktiviert und enthält das Nutzdaten-Format keine TIME_SERIES-Schleife, dann enstpricht der gemeinsame Qualitätsstatus dem aller gesammelten Werte. Das bedeutet, dass der gemeinsame Qualitätsstaus "GOOD" nur erreicht wird, wenn jeder einzelne Wert den Status hat.

  Zur Bedeutung siehe Kapitel Publish-Gruppen (Seite 117).

- **Datentyp**

  `{{TYPE}} /`

  `{{Station.Variable.TYPE}}`

  Datentyp-Alias: Vom Gerät in den Nutzdaten ausgegebener Datentyp des Datenpunkts

  Zur Ausgabe der Datentypen siehe Kapitel Datenpunkte (Seite 142).

- **Letzter Datenpunkt** (nur in der generischen Variante)

  `{{#LAST_DATA_POINT}} /`

  `{{/LAST_DATA_POINT}}`

  Letzter Datenpunkt

- **Alle außer dem letzten Datenpunkt** (nur in der generischen Variante)

  `{{^LAST_DATA_POINT}} /`

  `{{/LAST_DATA_POINT}}`

  Alle Datenpunkte außer dem letzten Datenpunkt

- **Alle außer dem letzten Datenpunkt der TIME_SERIES**

  ```
  {{^LAST_ITEM}} /
  {{/LAST_ITEM}}
  ```

  "True" für das letzte Item einer TIME_SERIES
- **Quell-Zeitstempel**

  ```
  {{SOURCE_TIMESTAMP}} /
  {{Station.Variable.SOURCE_TIMESTAMP}}
  ```

  Zeitpunkt des letzten Empfangs aus der Quell-Station.

Beispiel für übertragene Nutzdaten auf Basis der unveränderten Vorlage "JSON generisch"

Nachfolgend finden Sie ein Beispiel für die übertragenen Nutzdaten eines Topics.

Das Topic enthält drei Variablen einer S7-Station für die Datenpunkte "DP1", "DP2" und "DP3".

Der Wert des Schlüssels "DataItems" ist ein Array mit den Objekten der drei Variablen.

```
{ "Timestamp": "2019-05-03T09:13:46.000000000+00:00",
"DataItems": [ { "Variable":"DP1", "Type":"BOOL", "Value":"0",
"QualityCode":"GOOD" }, { "Variable":"DP2", "Type":"DOUBLE_FLOAT",
"Value":"0.496043966059748", "QualityCode":"GOOD" },
{ "Variable":"DP3", "Type":"S7_STRING", "Value":"Abcd99vE",
"QualityCode":"GOOD" } ] }
```

6.9.3.4 Datenpunkt-Zuordnung

In diesem Register ordnen Sie die projektierten Datenpunkte einem zuvor angelegten Topic bzw. einer Gruppe zu. Datenpunkte können mit mehreren Topics / Gruppen von mehreren Cloud Profilen verknüpft werden.

Voraussetzung

Bevor Sie Datenpunkte den Topics bzw. Gruppen zuordnen, müssen Sie die Datenpunkte anlegen, siehe Kapitel Datenpunkte (Seite 142). Dort legen Sie auch Datenpunktname, Datentyp und die weiteren Parameter fest.

Datenpunkt-Zuordnung

Auf der linken Seite sind alle projektierten Topics bzw. Gruppen des ausgewählten Profils zu sehen. Auf der rechten Seite sind alle projektierten Cloud-Datenpunkte der ausgewählten Station zu sehen.

Die Zuordnung funktioniert über Drag&Drop. Wählen Sie die Datenpunkte und ziehen sie mit gedrückter linker Maustaste auf das gewünschte Topic.

Eine Mehrfachauswahl der Datenpunkte ist mit Strg+linke Maustaste möglich.

- **Station selektieren**

  Selektieren Sie über die Auswahlliste das gewünschte Cloud Profil und die gewünschte Station.

  Die Datenpunkttabelle listet alle Datenpunkte auf, die in den oben selektierten Stationen projektiert sind und den Zugriff "Schreiben" oder "Lesen/Schreiben" haben.

  Die Datenpunkte können Sie den Topics / Gruppen einzeln oder gebündelt zuordnen.

  Einzel-Zuordnung:

  Ordnen Sie jeden Datenpunkt in der Datenpunkttabelle einzeln einem Topic bzw. einer Gruppe zu.

  Gebündelte Zuordnung:

  Selektieren Sie vor der gebündelten Zuordnung all diejenigen Datenpunkte in der Tabelle, die Sie einem Topic zuordnen möchten.

  Weisen Sie die Datenpunkte mit der Maus per Drag&Drop einem Topic zu.

  Um alle Datenpunkte einer Station gleichzeitig einem Topic zuzuordnen, weisen Sie mit der Maus per Drag&Drop das übergeordnete Stationsobjekt einem Topic zu. Sie werden gefragt, ob Sie alle untergeordneten Datenpunkte dem Topic zuordnen möchten.

  Die Anzahl der zugewiesenen Datenpunkte wird pro Topic bzw. Gruppe angezeigt.

  Über die Schaltfläche des Topics können die zugewiesenen Datenpunkte betrachtet und die Zuweisung gelöscht werden.

Siehe auch

Nutzdaten-Format (Seite 123)

Prozess-Zugang (Seite 84)

6.9.4 Subscriber

Gültigkeit

⇒ Gültig für MQTT-Profile mit den Cloud-Betreibern: AWS / Azure / IBM Cloud / Other Cloud

In diesem Register legen Sie die Topics für die Subscriber-Funktion des Gateways unter dem aktivierten Profil an.

6.9.4.1 Topics projektieren

Topic hinzufügen

- **Profil wählen**

  Wählen Sie aus der Auswahlliste eines der projektierten Cloud-Profile.

  Für das ausgewählte Profil werden alle projektierten Gruppen / Topics angezeigt.

- **Hinzufügen**

  Ein neues editierbares Topic wird der Tabelle hinzugefügt.

  Maximale Anzahl Publish- und Subscriber-Topics bzw. Gruppen

  CC712: 500

  CC716: 3500

- **Kopieren**

  Die ausgewählten Topics werden kopiert und ein weiteres Mal der Tabelle hinzugefügt.

- **Löschen**

  Alle ausgewählten Topics werden gelöscht.

- **Name**

  Geben Sie den Namen der Gruppe, die Sie anlegen möchten, in das Eingabefeld ein.

  Der Name ist der wesentliche Bestandteil zur Identifikation einer Gruppe.

- **Topic**

  Geben Sie den Namen des Topics in das Eingabefeld ein. Den Namen können Sie später in der Topic-Tabelle unterhalb ändern.

  Innerhalb einer Cloud-Anwendung muss der Name eines Topics eindeutig sein.

Subscribe-Gruppen-Konfiguration

Das Ausgabefeld "Nutzdaten-Format" gibt die Syntax an, die von den empfangenen abonnierten Nachrichten zwingend erwartet wird. Berücksichtigen Sie dies bei der Projektierung der betreffenden Publisher.

Wenn eine Nachricht empfangen wird, deren Nutzdaten-Format nicht genau dieser Syntax entspricht, wird die Nachricht verworfen und das Gateway erzeugt eine Diagnosemeldung.

Die Diagnosemeldungen finden Sie im WBM unter "Instandhaltung > Diagnose".

6.9.4.2 Nutzdaten-Format

Nutzdaten-Format

Verwenden Sie für die Kommunikation zwischen Publisher und Subscriber das JSON Nutzdaten-Format aus der Vorlage:

```
{
   "Timestamp": "PUBLISH_TIMESTAMP",
   "DataItems":
   [
      {
         "Variable": "{{Var1.NAME}}",
         "Type": "{{Var1.TYPE}}",
         "Value": {{Var1.VALUE}},
         "QualityCode": "{{Var1.QUALITY_CODE}}"
      },
      {
         "Variable": "{{Var2.NAME}}",
         "Type": "{{Var2.TYPE}}",
         "Value": {{Var2.VALUE}},
         "QualityCode": "{{Var2.QUALITY_CODE}}"
      },
...

{
         "Variable": "{{VarN.NAME}}",
         "Type": "{{VarN.TYPE}}",
         "Value": {{VarN.VALUE}},
         "QualityCode": "{{VarN.QUALITY_CODE}}"
      },
   ]
}
```

Der Zeitstempel ist optional. Er wird im Nutzdaten-Format nicht ausgewertet.

Nutzdaten-Beispiel

Durch Klicken auf die Schaltfläche finden Sie ein Beispiel für die erwartete Syntax mit unterschiedlichen Datentypen.

Topic-Tabelle

In der Tabelle sehen Sie die angelegten Topics und projektieren deren Parameter "Quality of Service".

Sie können die Anzeige alphabetisch nach Topic-Name sortieren, indem Sie in der Kopfzeile der Tabelle auf das Symbol neben der Bezeichnung klicken.

- **Topic**

  Bei Bedarf können Sie hier den Namen des Topics ändern.

- **QoS**

  Legen Sie über den Parameter "Quality of Service" des Topics das Übertragungsverhalten der Nachrichten zwischen Broker und Subscriber des Gateways fest:

  – QoS 0

    Übertragung höchstens einmal

    Der Broker sendet das Topic einmal an das Gateway. Der Broker erwartet keine Quittung. Wenn das Topic vom Gateway nicht empfangen wird, dann ist es verloren.

  – QoS 1

    Übertragung mindestens einmal

    Der Broker sendet das Topic solange an das Gateway, bis er ein PUBACK-Paket als Quittung vom Gateway empfängt.

  – QoS 2

    Übertragung genau einmal

    Der Broker sendet das Topic und wartet, bis er die spezifikationsgemäße zweistufige Quittung vom Gateway empfängt.

  Bei Verbindungsabbrüchen werden die Daten-Telegramme bei QoS 1 und QoS 2 im Broker zwischengespeichert.

  Wenn beim Subscriber des Gateways ein niedrigerer QoS-Wert projektiert ist als beim Publisher, dann gilt für die Kommunikation zwischen Broker und Subscriber der niedrigere Wert.

- **Löschen**

  Durch Klicken auf die Schaltfläche wird das Topic der jeweiligen Zeile gelöscht.

Hinweis

Löschen

Beachten Sie, dass Sie das versehentliche Entfernen eines Topics nicht rückgängig machen können.

6.9.4.3 Datenpunkt-Zuordnung

Datenpunkt-Zuordnung

Auf der linken Seite sind alle projektierten Topics bzw. Gruppen des ausgewählten Profils zu sehen. Auf der rechten Seite sind alle projektierten Cloud-Datenpunkte der ausgewählten Station zu sehen.

Die Zuordnung funktioniert über Drag&Drop. Wählen Sie die Datenpunkte und ziehen sie mit gedrückter linker Maustaste auf das gewünschte Topic.

Eine Mehrfachauswahl der Datenpunkte ist mit Strg+linke Maustaste möglich.

- **Station selektieren**

  Selektieren Sie über die Auswahlliste das gewünschte Cloud Profil und die gewünschte Station.

  Die Datenpunkttabelle listet alle Datenpunkte auf, die in den oben selektierten Stationen projektiert sind und den Zugriff "Schreiben" oder "Lesen/Schreiben" haben.

  Die Datenpunkte können Sie den Topics / Gruppen einzeln oder gebündelt zuordnen.

  Einzel-Zuordnung:

  Ordnen Sie jeden Datenpunkt in der Datenpunkttabelle einzeln einem Topic bzw. einer Gruppe zu.

  Gebündelte Zuordnung:

  Selektieren Sie vor der gebündelten Zuordnung all diejenigen Datenpunkte in der Tabelle, die Sie einem Topic zuordnen möchten.

  Weisen Sie die Datenpunkte mit der Maus per Drag&Drop einem Topic zu.

  Um alle Datenpunkte einer Station gleichzeitig einem Topic zuzuordnen, weisen Sie mit der Maus per Drag&Drop das übergeordnete Stationsobjekt einem Topic zu. Sie werden gefragt, ob Sie alle untergeordneten Datenpunkte dem Topic zuordnen möchten.

  Die Anzahl der zugewiesenen Datenpunkte wird pro Topic bzw. Gruppe angezeigt.

  Über die Schaltfläche des Topics können die zugewiesenen Datenpunkte betrachtet und die Zuweisung gelöscht werden.

6.10 Datenpunkte

6.10.1 Übertragungszeitpunkt und übertragene Daten

Hinweis

Voraussetzungen für die Übertragung (Cloud)

Für die Übertragung eines Werts müssen folgende Bedingungen erfüllt sein:

- Der Datenpunkt ist in der Projektierung einem Topic zugeordnet.
- Mindestens eine Trigger-Bedingung ist erfüllt.

Zeitpunkt der Datenübertragung und Anzahl der übertragenen Daten

Das Auslösen der Datenübertragung unterscheidet sich bei den beiden Zielsystemen:

- **Cloud**

  Der Zeitpunkt der Übertragung wird über Trigger gesteuert, siehe Kapitel Datenpunkte (Seite 142) und Kapitel Publisher (Seite 116).

  Den Zeitpunkt, wann die Werte von Datenpunkten an den Broker übertragen werden, legen Sie für jeden Datenpunkt und für jedes Topic über den "Trigger" fest.

  Folgende Daten werden gemeinsam an den Broker übertragen:

  – AWS / Azure / IBM Cloud

    Übertragung der Werte aller Datenpunkte des zugeordneten Topics

  – MindConnect IoT Extension / Andere Cloud

    Übertragung der Werte aller Datenpunkte der zugeordneten Gruppe

  Die Übertragung erfolgt, sobald der Wert eines Datenpunkts zur Übertragung ansteht bzw. bei aktivierter Funktion "Sammeln", die Bedingungen zum Sammeln der Daten erfüllt sind.

  Beachten Sie bei allen Wert-Triggern, dass die Daten eines Topics bzw. einer Gruppe so lange übertragen werden, wie die Trigger-Bedingung erfüllt ist. Dies hat Auswirkungen auf die übertragene Datenmenge.

- **OPC UA**

  Der OPC UA-Server des Gateways führt die Lese- und Schreibaufträge der OPC UA-Clients aus.

  Für OPC UA-Clients mit Subscriptions werden die Werte gemäß den Einstellungen im Kapitel Konfiguration (Seite 95) unter "Min. Publishing-Intervall (ms)" und "Min. Polling-Intervall (ms)" vom Server versendet. Der Trigger ist dabei eine Wertänderung oder eine Änderung des QualityCode.

6.10.2 Datenpunkte

Datenpunkt-Konfiguration

In diesem Register legen Sie stationsweise die Datenpunkte als Datenquellen bzw. Datenziel für die Übertragung fest.

Bei S7-Stationen können Sie zusätzlich die Variablen-Informationen der CPU über eine Quelldatei aus STEP 7 exportierten und als Basis für die Datenpunkt-Projektierung importieren, siehe S7-Import (Seite 154).

Bei OPC-UA-Client Stationen können Sie folgendermaßen vorgehen:

- Exportieren Sie die Variablen-Informationen des Servers in eine XML-Quelldatei und importieren Sie diese als Basis für die Datenpunkte, siehe OPC UA-Import (Seite 159).
- Stellen Sie über "OPC UA-Browse" eine Verbindung mit dem OPC-Server her und importieren Sie die Datenpunkte, siehe OPC UA-Browse (Seite 158).

Hinweis

Löschen von projektierten Datenpunkten beim Import

Beim Import von Variablen aus STEP 7-Dateien können Sie auswählen, ob zuvor projektierte Datenpunkte gelöscht werden sollen.

Nach dem Import von Variablen aus STEP 7-Dateien können Sie weitere Datenpunkte auch manuell projektieren.

Ein Datenpunkt im Gateway kann alternativ für eines der beiden Zielsysteme (Cloud / OPC UA) projektiert werden.

Es können aber mehrere Datenpunkte für unterschiedliche Zielsysteme mit Referenz auf die gleiche Adresse in der Station angelegt werden.

- **Station selektieren**

  Wählen Sie aus der Klappliste eine Station aus, deren Datenpunkte Sie für die Übertragung projektieren möchten. Die Klappliste enthält alle Stationen, die unter "Prozess-Zugang" projektiert worden sind, siehe Kapitel Prozess-Zugang (Seite 84).

  Wenn bereits Datenpunkte für eine Station projektiert sind, werden diese bei Selektion der Station in der nachfolgenden Tabelle angezeigt. Sie können dann die Daten nachträglich ändern.

- **Datenpunkt hinzufügen**

  Legt in der Tabelle die Zeile für einen neuen Datenpunkt an.

  Alternativ:

- **Kopieren**

  Sie können neue Datenpunkte auch anlegen, indem Sie vorhandene Datenpunkte kopieren.

  Selektieren Sie hierzu über die Optionskästchen (siehe unten) ein oder mehrere Datenpunkte und klicken Sie auf die Schaltfläche "kopieren".

  Passen Sie anschließend die Eigenschaften der kopierten Datenpunkte an.

- **Mehrfachbearbeitung**

  Über die Schaltfläche öffnen Sie den Dialog "Datenpunkt-Konfiguration". In dem Dialog können Sie in einem Bearbeitungsschritt bestimmte Parameter für alle oder zuvor selektierte Datenpunkte setzen.

  Selektieren Sie für diese Funktion mehrere Datenpunkte über die Optionskästchen in der Auswahlspalte (links) der Datenpunkttabelle.

  Folgende Parameter können Sie in dem Dialog für mehrere Datenpunkte setzen:

  - Ziel
  - Zugriff
  - Trigger
  - Quality-Änderung

  Zur Bedeutung der Parameter siehe unten.

  Die Mehrfachbearbeitung kann insbesondere dann sinnvoll sein, wenn Sie große Mengen an Datenpunkten importieren, die mit gleichen Werten für die genannten Parameter versehen werden sollen.

  Nach der Projektierung der genannten Parameter im Dialog "Datenpunkt-Konfiguration" wählen Sie im Parameter "Setzen für" eine der zwei Optionen aus und klicken sie "speichern".

  - **Für Selektierte setzen**

    Weist die Parameterwerte denjenigen Datenpunkten zu, die Sie vor dem Öffnen des Dialogs selektiert haben.

  - **Für alle setzen**

    Weist die Parameterwerte allen Datenpunkten der Datenpunkttabelle zu.

Selektion von Datenpunkten über die Auswahlspalte

Über die Optionskästchen der Auswahlspalte links in der Tabelle können Sie einzelne Datenpunkte für das Kopieren, das Löschen und für die Mehrfachbearbeitung selektieren.

In den Tabellenspalten können Sie die Datenpunkte sortieren, um die Auswahl zu erleichtern.

Über das oberste Optionskästchen im Tabellenkopf selektieren Sie alle Datenpunkte der Tabelle.

Löschen von Datenpunkten

Hinweis
Löschen

Das Löschen eines Datenpunkts können Sie nicht rückgängig machen.

Datenpunkte können Sie löschen, indem Sie diese über die Auswahlspalte (links) selektieren und anschließend auf die Schaltfläche "Löschen" oberhalb der Tabelle klicken.

Wenn Sie keinen Datenpunkt ausgewählt haben und auf die Schaltfläche "Löschen" klicken, können Sie alle Datenpunkte löschen.

Datenpunkt-Tabelle

Projektieren Sie die Parameter der Datenpunkte in der Tabelle und speichern sie. Fehlerhafte Datenpunkte können Sie in der Tabelle korrigieren oder löschen.

Je nach Übertragungsprotokoll der Datenpunkte unterscheiden sich die Parameter. Die nachfolgende Auflistung enthält alle Parameter, die für S7 und Modbus/TCP projektierbar sind.

- **Auswahlspalte**

  Über die Optionskästchen der linken Spalte können Sie alle, einzelne oder mehrere Zeilen für die Mehrfachbearbeitung, das Kopieren oder das Löschen selektieren.

- **Ziel**

  Wählen Sie für den jeweiligen Datenpunkt das zu verwendende Zielsystem.

  - **-**

    Dem Datenpunkt ist kein Zielsystem zugeordnet. Daten werden nicht gelesen und nicht übertragen.

    Hinweis
    Keine Verbindung ohne zugewiesene Datenpunkte

    Wenn keine Datenpunkte einem Ziel zugewiesen sind, wird keine Verbindung zur jeweiligen Station aufgebaut.

  - Cloud
  - OPC UA

- **Datenpunktname**

  Vergeben Sie dem Datenpunkt einen eindeutigen Namen.

- **Datentyp**

  Projektierter Datentyp des zu lesenden Datenbereichs des Datenpunkts

  Die unterstützten Datentypen finden Sie unten in der Tabelle der Datentypen.

- **Operandenbereich** (nur S7-Stationen)

  Folgende Operandenbereiche der CPU stehen bei S7 zur Auswahl:

  - I - Eingang
  - M - Merker
  - Q - Ausgang
  - DB - Datenbaustein

- **Funktionscode** (nur Modbus-Stationen)

  Folgende Bereiche (tables) des Speicherbereichs der Station stehen bei Modbus/TCP zur Auswahl:

  - 1: Read Coil
  - 2: Read Discret Input
  - 3: Read Holding Registers
  - 4: Read Input Registers
  - 5: Write Single Coil
  - 6: Write Single Holding Registers
  - 16: Write Multiple Holding Registers

- **DB-Nummer** (nur S7-Stationen)

  Nummer des DB der S7-CPU

  Achten Sie darauf, dass die Nummer mit der tatsächlich projektierten Nummer des Datenbausteins übereinstimmt.

- **Offset / Adresse**

  Für S7-Stationen

  Adresse des Operanden in Abhängigkeit des Datenbereichs. Geben Sie den Wert als Dezimalzahl ein:

  - Adresse (Eingang, Merker, Ausgang, DB)

    Angabe für Bool-Operanden in <Byte.bit>. Bsp.: 0.6
    Angabe für Operanden ≥ Byte in <Byte>. Bsp.: 3

  - Offset des Operanden zur Anfangsadresse des Operandenbereichs (Spule, Register)

    Angabe in <Byte>. Bsp.: 12

  Für Modbus-Stationen

  Gibt die Stelle des Registers an, das bzw. ab dem gelesen oder geschrieben wird.

- **NodeID** (nur OPC UA-Stationen)

  ID des Knoten zur eindeutigen Identifizierung des Objektes beim OPC UA-Server.

- **Array-Dimension** (nur S7- und OPC UA-Stationen)

  Die Größe des Arrays.

  - Ein leerer Eintrag bedeutet, dass die Variable kein Array ist.
  - Eindimensionales Array: Eingabe der Zahl, deren Größe das Array entspricht.

    Für Variablen vom Typ "Bool" werden nur Arrays mit einer Dimension unterstützt.
  - Mehrdimensionale Arrays: Eingabe der Zahlen, durch Komma getrennt.

    Max. 3 Dimensionen werden unterstützt.
- **Länge** (nur S7- und Modbus-Stationen)

  Anzahl der Zeichen beim Datentyp "String" (S7-Station: 1 .. 254, Modbus-Station: 64)
- **Zugriff**

  Die Option legt den Zugriff der Kommunikationspartner auf die Daten des Gateways fest.

  - **Lesen**

    Nur lesender Zugriff ist erlaubt.
  - **Lesen/Schreiben**

    Lesender und schreibender Zugriff ist erlaubt.
  - **Schreiben**

    Schreibender Zugriff ist erlaubt.

- **Trigger**

  Mit den Triggern legen Sie die Bedingungen fest, bei deren Eintreten die Übertragung des im Gerät gespeicherten Werts an den Broker ausgelöst wird. Pro Datenpunkt können Sie einen Trigger auswählen.

  Wählen Sie über die Klappliste den Typ für den Wert-Trigger und ergänzen Sie die jeweiligen Werte:

  - Änderung

    Der Wert wird übertragen, sobald er sich gegenüber dem zuvor eingelesenen Wert ändert.

  - Bereich außerhalb

    Der Wert wird übertragen, sobald er sich außerhalb des projektierten Bereichs befindet.

  - Bereich innerhalb

    Der Wert wird übertragen, sobald er sich innerhalb des projektierten Bereichs befindet.

  - Schwellenwert HOCH

    Der Wert wird übertragen, sobald er den projektierten Wert überschreitet.

  - Schwellenwert TIEF

    Der Wert wird übertragen, sobald er den projektierten Wert unterschreitet.

  Beachten Sie:

  - Die Wertebereiche der Wert-Trigger sind abhängig vom Datentyp des Datenpunkts.
  - Der Wertebereich des Datenpunkts in der Station wird auf den Wertebereich des Datenpunkts im Gerät umgerechnet.

- **Quality-Änderung**

  Über den Parameter legen Sie das Übertragungsverhalten der Nachrichten aller Topics bzw. Gruppen fest:

  – Aktiviert

    Übertragung bei Änderung des "QualityCode" (Good → Bad oder Bad → Good)

    Sobald sich die Qualität eines Datenpunkts ändert, wird das Topic übertragen.

  – Deaktiviert

    Keine Übertragung bei Änderung des "QualityCode".

- **Attribut**

  Das Attribut wird als `{{ADDITIONAL_ATTRIBUTE}}` / `{{Station.Variable.ADDITIONAL_ATTRIBUTE}}` in die Nutzdaten übernommen, siehe Kapitel Nutzdaten-Format (Seite 123).

  Geben Sie das Attribut nach Vorgaben des Cloud-Betreibers ein:

  – AWS / Azure / IBM Cloud / Andere Cloud: Optional

    Wenn kein Attribut verlangt oder benötigt wird, lassen Sie das Feld leer.

  – IoT Extension: Zwingend erforderlich

  Bei Anbindung an IoT Extension wird das Attribut als Kennzeichnung der physikalischen Einheiten des jeweiligen Datenpunkts interpretiert. Die Standardeinheiten sind:

  – C = Temperatur in Grad Celsius
  – P = Druck in bar
  – mm = Länge in Millimeter
  – km/h = Geschwindigkeit in km/h
  – m/s2 = Beschleunigung in m/s^2
  – % = Größe in Prozent
  – %RH = Relative Luftfeuchtigkeit in Prozent
  – A = Stromstärke in Ampere
  – V = Spannung in Volt
  – W = Leistung in Watt
  – kWh = Energie in Kilowattstunde
  – VAh = Scheinenergie in Voltamperestunde
  – dBm = Leistungspegel in Dezibel Milliwatt (logarithmisches Verhältnis)
  – lux = Beleuchtungsstärke in Lux (lm/m^2)

  Es können auch weitere zusammengesetzte Einheiten des SI-Systems angegeben werden, beispielsweise:

  m/h, m/s, m, km, mW, kW, mWh, mA, VArh

Trigger

Sie können pro Datenpunkt zwei Trigger kombinieren:

- Einen Trigger mit dem Wert des Datenpunkts.
- Einen zeitlichen Trigger oder Eingangs-Trigger am Topic, welchem der Datenpunkt zugewiesen wird.

Bei Projektierung von zwei Triggern wird die Übertragung ausgelöst, sobald eine der beiden Trigger-Bedingung erfüllt ist.

Weitere Einschränkungen können sich aus den unterstützten Trigger-Typen des jeweiligen Datentyps ergeben, siehe Tabelle "Datentypen" unten.

Übertragung und QualityCode

Mit den Nutzdaten wird auch der Qualitätsstatus "QualityCode" eines Datenpunkts übertragen. Der Status kennzeichnet die Gültigkeit des Werts.

Der Status wird vom Gateway als Publisher gesetzt und hat folgenden Wertebereich:

- GOOD

  Der Wert ist gültig.

- BAD

  Der Wert der Variable ist nicht gültig oder nicht aktuell. Mögliche Ursachen:

  - CPU in STOP
  - Wert nicht aktuell
  - Fehler beim Lesen der Variable

Der Wert des Status hat folgende Auswirkung auf die Übertragung:

- Publisher → Cloud

  Die Veröffentlichung von Nachrichten des Gateways als Publisher ist unabhängig vom Wert des Status.

- Cloud → Subscriber

  Der Empfang von Nachrichten durch das Gateway als Subscriber ist unabhängig vom Wert des Status.

  Beim Empfang einer Nachricht mit dem Status "BAD" wird jedoch der Wert vom Gateway als Subscriber nicht in die Prozess-Station geschrieben.

Verbindungsabbruch und QualityCode

Bei einem Verbindungsabbruch gilt das folgende Verhalten:

- **Verbindungsabbruch zwischen Station und Gateway**
  - Während des Verbindungsabbruchs

    Das Gateway sendet das Topic mit leeren Strings für die Werte und dem QualityCode "Bad".
  - Wiederkehrende Verbindung

    Wenn die Trigger-Bedingung erfüllt ist, sendet das Gateway das Topic mit den aktuellen Werten und dem QualityCode "Good".
- **Verbindungsabbruch zwischen Gateway und Cloud**
  - Während des Verbindungsabbruchs - Kabel am Gateway gezogen oder Cloud-Server nicht erreichbar.

    Das Gateway sendet keine Daten. Abhängig davon, welchen Wert Sie bei den einzelnen Topics bzw. Gruppen zur "Nachrichten-Pufferung" eingetragen haben, werden die Daten im Gateway mit ihrem aktuellen Wert und QualityCode gepuffert.
  - Wiederkehrende Verbindung

    Das Gateway sendet zuerst die gepufferten Nachrichten. Anschließend werden die aktuellen Werte nach Auslösen der Trigger-Bedingungen gesendet.

Datentypen

Nicht jeder Datentyp unterstützt alle Trigger-Typen. Die folgenden Tabellen listen die projektierbaren Datentypen auf und geben für jeden Datentyp die unterstützten Trigger-Typen an.

Tabelle 6- 3 **Datentypen für S7-Station**

S7-Station			Datentyp im Zielsystem		Unterstützte Trigger		Geeignet für Array
Datentyp	**Bitbreite**	**Operanden bereich**	**OPC-Server**	**MQTT/HTTP**	**Zeit**	**Wert**	**(max. 100 Arrays pro Station)**
BOOL	1	I, Q, M, DB	Boolean	BOOL	x	x	x [7]
CHAR	8	I, Q, M, DB	Byte	CHAR	x	x	x
SINT [2]	8	I, Q, M, DB	SByte	INT8	x	x	x
INT	16	I, Q, M, DB	Int16	INT16	x	x	x
DINT	32	I, Q, M, DB	Int32	INT32	x	x	x
LINT [1]	64	I, Q, M, DB	Int64	INT64	x	x	x
USINT [2]	8	I, Q, M, DB	Byte	UINT8	x	x	x
UINT [2]	16	I, Q, M, DB	UInt16	UINT16	x	x	x
UDINT [2]	32	I, Q, M, DB	UInt32	UINT32	x	x	x
ULINT [1]	64	I, Q, M, DB	UInt64	UINT64	x	x	x
BYTE	8	I, Q, M, DB	Byte	UINT8	x	x	x
WORD	16	I, Q, M, DB	UInt16	UINT16	x	x	x
DWORD	32	I, Q, M, DB	UInt32	UINT32	x	x	x
LWORD [1]	64	I, Q, M, DB	UInt64	UINT64	x	x	x

S7-Station			Datentyp im Zielsystem		Unterstützte Trigger		Geeignet für Array
Datentyp	**Bitbreite**	**Operanden bereich**	**OPC-Server**	**MQTT/HTTP**	**Zeit**	**Wert**	**(max. 100 Arrays pro Station)**
REAL	32	I, Q, M, DB	Float	SINGLE_FLOAT	**x**	**x**	**x**
LREAL[2)]	64	I, Q, M, DB	Double	DOUBLE_FLOAT	**x**	**x**	**x**
DATE_AND_TIME [3)]	64	DB	DateTime	S7_DT [5)]	**x**	-	-
DTL [2)]	96	DB	DateTime [4)]	S7_DTL [5)]	**x**	-	-
STRING	2..256 Bytes	DB	String	STRING	**x**	-	**x**
CSTRING [6)]	0..254 Bytes	DB	String	STRING, C_STRING	**x**	-	**x**

1) Nur S7-1500

2) Nur S7-1200/1500

3) Nur S7-300/400/1500

4) Die Genauigkeit des DTL (1 ns, 10^{-9} Sekunden) ist für OPC DateTime auf 100 ns (10^{-7} Sekunden) eingeschränkt.

5) Formatierung nach ISO 8601, z. B. "2020-03-31T08:25:59.1234+02:00".

6) Ein Array vom Typ "CHAR" oder einzelne direkt aufeinanderfolgende Datenpunkte vom Typ "CHAR" können als "CSTRING" definiert werden. Die Länge des Strings setzt sich aus der Anzahl der einzelnen CHAR-Elemente zusammen. Der Datenpunkt wird in beiden Zielsystemen als String dargestellt. Für die korrekte Verarbeitung in einem Subscriber-Topic muss der Datentyp "C_STRING" empfangen werden.

7) Es werden nur eindimensionale Arrays vom Typ "Bool" unterstützt. Mehrdimensionale Arrays vom Typ "Bool" können nicht projektiert werden und werden beim Import nicht angeboten.

Tabelle 6- 4 **Datentypen für Modbus-Client**

Modbus-Client			Datentyp im Zielsystem		Unterstützte Trigger		Geeignet für Array
Datentyp	**Bitbreite**	**Memory Area [1)]**	**OPC-Server**	**MQTT/HTTP**	**Zeit**	**Wert**	
BOOL	1	Coil, Discretes Input	Boolean	BOOL	**x**	**x**	-
UINT16	16	Holding Register, Input Register	UInt16	UINT16	**x**	**x**	-
UINT32	32	Holding Register, Input Register	UInt32	UINT32	**x**	**x**	-
FLOAT	32	Holding Register, Input Register	Float	SINGLE_FLOAT	**x**	**x**	-
STRING	64 Bytes	Holding Register, Input Register	String	STRING	**x**	**-**	-

1) Schreibzugriff wird nicht für "Discrete Inputs" und "Input Register" unterstützt.

Modbus-Datentypen

Der Modbus-Standard kennt nur 1-Bit- und 16-Bit-Datenobjekte. Die erweiterten Datentypen werden als 2 bzw. 4 aufeinander folgende 16-Bit-Datenobjekte übertragen.

Bei Verwendung anderer Datentypen im Gerät und in nachgeschalteten Anwendungen müssen Sie die aus der Station gelesenen Daten anwenderspezifisch abbilden und interpretieren.

Tabelle 6- 5 **Datentypen für OPC-Stationen**

OPC-Server		Datentyp im Zielsystem		Unterstützte Trigger		Geeignet für Array
Datentyp	**Bitbreite**	**OPC-Server**	**MQTT/HTTP**	**Zeit**	**Wert**	**(max. 100 Arrays pro Station)**
Boolean	1	Boolean	BOOL	**x**	**x** (nur Wert 0)	**x**
SByte	8	SByte	INT8	**x**	**x**	**x**
Int16	16	Int16	INT16	**x**	**x**	**x**
Int32	32	Int32	INT32	**x**	**x**	**x**
Int64	64	Int64	INT64	**x**	**x**	**x**
Byte	8	Byte	UINT8	**x**	**x**	**x**
UInt16	16	UInt16	UINT16	**x**	**x**	**x**
UInt32	32	UInt32	UINT32	**x**	**x**	**x**
UInt64	64	UInt64	UINT64	**x**	**x**	**x**
Float	32	Float	SINGLE_FLOAT	**x**	**x**	**x**
Double	64	Double	DOUBLE_FLOAT	**x**	**x**	**x**
DateTime	64	DateTime	DTL [3]	**x**	-	-
String [1]	0..256 Bytes	String	STRING	**x**	-	**x**
S7_DATE_AND_TIME [2]	8 Bytes	DateTime	DT-STRING (ISO 8601)	**x**	-	-

[1] Überschreitet der String im OPC-Server die Länge von 256 Byte, dann kann der String nicht vom OPC UA-Client gelesen werden und der QualityCode wechselt auf BAD.

[2] Eine S7-1500 bildet den internen Datentyp DATE_AND_TIME als Byte-Array mit der Länge 8 in ihrem OPC UA-Server ab. Dieses Array kann über den OPC UA-Client des CC7 als S7-DATE_AND_TIME-Variabe interpretiert und mit dem Datums-Zeit-Wert ans Zielsystem weitergeleitet werden.

[3] Formatierung nach ISO 8601, z. B. "2020-03-31T08:25:59.1234+02:00".

Einschränkungen bei MindConnect IoT Extension

Folgende Daten werden nicht unterstützt:

- Zeitstempel
- Bei S7-LINT / S7-ULINT:

  Ganzzahlen von 2^{63} bis 2^{64}

Folgende Datentypen werden nur unterstützt, wenn sie als Event übertragen werden:

- Bool
- String

6.10.3 S7-Import

Zusätzlich zur manuellen Datenpunkt-Projektierung können Sie bei S7-Stationen die Variablen-Informationen über eine aus STEP 7 exportierte Datei importieren.

Beim Import von Variablen aus STEP 7-Dateien können Sie auswählen, ob zuvor projektierte Datenpunkte gelöscht werden sollen oder nicht.

Nach dem Import von Variablen aus STEP 7-Dateien können Sie weitere Datenpunkte auch manuell projektieren.

Beachten Sie folgende Grenzen beim Import:

- Maximale Anzahl an Variablen pro Datei: 5000
- Maximale Anzahl an Variablen pro Station: 500

  Der Wert gilt auch beim Import mehrerer Dateien.

Voraussetzung: Anlegen von CPU-Variablen in STEP 7

Als Voraussetzung für die Nutzung der Funktion müssen Sie in Ihrem STEP 7-Projekt Variablen bzw. Symbole in der jeweiligen CPU angelegt haben.

- STEP 7 Professional (TIA Portal)
  - DB-Variablen

    Bei DBs muss die Option "Optimierter Bausteinzugriff" deaktiviert sein.
  - PLC-Variablen
- STEP 7 V5.6
  - DB-Variablen
  - Symbole

Export aus STEP 7

Exportieren Sie im STEP 7-Projekt die Variablen in eine Exportdatei.

Empfehlung: Geben Sie den Exportdateien sprechende Namen, aus denen der Stationstyp, der Stationsname und ggf. die DB-Nummer hervorgehen.

Folgende Dateiformate werden unterstützt: *.db, *.awl, *.sdf, *.xml, *.dif, *.asc

- **STEP 7 Professional (TIA Portal)**

  DB-Variablen

  - Selektieren Sie den DB.
  - Klicken Sie auf das Kontextmenü "Quelle aus Bausteinen generieren > Nur selektierte Bausteine".
  - Wählen Sie den Dateityp "DB-Dateien (*.db)" und klicken Sie auf "Speichern".

  PLC-Variablen

  - Öffnen Sie die Variablentabelle
  - Klicken Sie oberhalb der Variablentabelle auf das Symbol "Exportieren".
  - Wählen Sie im folgenden Dialog "Export" die betreffenden Optionen aus.
  - Speichern Sie die PLC-Variablen in einem der folgenden Dateiformate: *.xml, *.sdf

  UDT

  - Selektieren Sie den PLC-Datentyp UDT.
  - Klicken Sie auf das Kontextmenü "Quelle aus Bausteinen generieren > Einschließlich abhängige Bausteine", damit der Programmcode der abhängigen Bausteinen und referenzierten PLC-Datentypen ebenfalls in der externen Quelldatei gespeichert wird.
  - Wählen Sie den Dateityp "DB-Dateien (*.db)" und klicken Sie auf "Speichern".

- **STEP 7 V5.6**

  DB-Variablen

  - Öffnen Sie im SIMATIC Manager im Bausteine-Verzeichnis der CPU den DB.
  - Klicken Sie im Bausteineditor auf "Datei > Quelle generieren".
  - Wählen Sie im Dialog "Neu" die Quellen der CPU aus, vergeben Sie unter "Objektname" einen Namen für die Datei und klicken Sie auf OK.
  - Verschieben Sie im Folgedialog "Quelle generieren" den oder die DBs über das Pfeilsymbol in das Feld "Gewählte Bausteine".

    Aktivieren Sie die Option "Absolut" und klicken Sie auf OK.
  - Schließen Sie das Bausteinfenster.
  - Öffnen Sie im SIMATIC Manager im Quellen-Verzeichnis der CPU, selektieren Sie die neu generierte Quelle und klicken Sie auf das Kontextmenü "Quelle exportieren".
  - Wählen Sie im Dialog "Quelle exportieren" das gewünschte Zielverzeichnis im Dateisystem des PC.
  - Wählen Sie den Dateityp "AWL-Quelle (*.awl)" und klicken Sie auf "Speichern".

  Symbole

  - Selektieren Sie im SIMATIC Manager das S7-Programm der CPU.
  - Öffnen Sie die Symboltabelle.
  - Klicken Sie auf das Menü "Tabelle > Exportieren".

- Speichern Sie die Symboltabelle in einem der folgenden Dateiformate: *.SDF, *.ASC, *.DIF

UDT

- Öffnen Sie im SIMATIC Manager im Bausteine-Verzeichnis der CPU den DB.
- Klicken Sie im Bausteineditor auf "Datei > Quelle generieren".
- Wählen Sie im Dialog "Neu" die Quellen der CPU aus, vergeben Sie unter "Objektname" einen Namen für die Datei und klicken Sie auf OK.
- Verschieben Sie im Folgedialog "Quelle generieren" den oder die DBs über das Pfeilsymbol in das Feld "Gewählte Bausteine".

  Aktivieren Sie die Option "Referenzierte Bausteine einbeziehen" und klicken Sie auf OK.
- Schließen Sie das Bausteinfenster.
- Öffnen Sie im SIMATIC Manager im Quellen-Verzeichnis der CPU, selektieren Sie die neu generierte Quelle und klicken Sie auf das Kontextmenü "Quelle exportieren".
- Wählen Sie im Dialog "Quelle exportieren" das gewünschte Zielverzeichnis im Dateisystem des PC.
- Wählen Sie den Dateityp "AWL-Quelle (*.awl)" und klicken Sie auf "Speichern".

Variablen importieren

1. Speichern Sie die aus STEP 7 exportierte Datei mit den Variablen-Informationen im Dateisystem Ihres PC.
2. Öffnen Sie das WBM-Register "Datenpunkte > S7-Import".
3. Selektieren Sie bei mehreren Stationen die gewünschte Station.
4. Klicken Sie auf "Durchsuchen", wählen Sie die gewünschte STEP 7-Datei aus und klicken Sie auf "Öffnen".

   Im WBM wird der Dateiname angezeigt.
5. Wählen Sie die gewünschte Option für "Arrays als Einzelelemente importieren". Wenn aktiviert, werden Arrays als einzelne Elemente importiert. Wenn deaktiviert, werden Arrays als einziger Datenpunkt importiert.

Hinweis

Struct-Arrays importieren

Struct-Arrays werden immer als Einzelelemente importiert. Die Option "Arrays als Einzelelemente importieren" bezieht sich auf Arrays von unterstützen Datenpunkten innerhalb des Struct-Arrays.

6. Wenn Sie die Datei verwenden möchten, dann klicken Sie auf "Quelldatei importieren".

   Wenn Sie mehrere Dateien importieren möchten, dann wiederholen Sie den Vorgang "Durchsuchen" > "Quelldatei importieren".

   Nach dem Import einer Quelldatei aus einem DB werden in einer Tabelle zunächst folgende Spalten angezeigt:

   - Name
   - DB-Nummer

     Nur dieses Feld ist editierbar.

7. Wenn Sie den Import abbrechen möchten, dann klicken Sie auf "Löschen". Die Datei und die bereits importierten Variablen werden gelöscht.
8. Vergeben Sie die DB-Nummer entsprechend der STEP 7-Projektierung und klicken Sie auf "Speichern".

   Die Daten werden dadurch noch nicht in die Datenpunkliste der Applikation übernommen.

   Nach der Vergabe der DB-Nummer oder nach dem Import einer Quelldatei aus einer Variablenliste werden die Variablen in einer Tabelle mit folgenden Spalten angezeigt.

   - Auswahlspalte

     Dient der Selektion von Datenpunkten für die teilweise Übernahme in die Applikation.

   - Name

     Der Datenpunktname wird aus folgenden beiden Komponenten gebildet und später übernommen:

     - DB-Variable: <DB-Name>__<Variablenname>

     - PLC-Variable/Symbol: <Symbolname>

   - Operandenbereich, DB-Nummer, Adresse, Typ, Länge, Array-Dimensionen

     Die jeweiligen Daten gemäß dem Inhalt der Quelldatei werden angezeigt.

   Über die Schaltfläche "Löschen", entfernen Sie die ausgewählten Datenpunkte. Wenn keine Datenpunkte ausgewählt sind, werden Sie gefragt, ob Sie alle Datenpunkte löschen möchten.
9. Wenn Sie vor dem Import Werte einzelner Datenpunkte anpassen möchten, nehmen Sie die Änderungen vor und bestätigen Sie die Änderung mit "Speichern".

10. Übernehmen Sie die Variablen in die Applikation.
    - Wenn Sie alle Variablen der Tabelle übernehmen möchten, dann selektieren Sie alle Variablen gleichzeitig, indem Sie das Optionskästchen in der Tabellenkopfzeile aktivieren und auf "Importieren" klicken.

      In einem Dialogfenster werden Sie gefragt, ob Sie alle bereits bestehenden Datenpunkte löschen möchten:

      - Wählen Sie "Ja", um alle bestehenden Datenpunkte vor dem Import zu löschen.

      - Wählen Sie "Nein", wenn die Datenpunkte zusätzlich zu den Bestehenden importiert werden sollen.
    - Wenn Sie nur einen Teil der importierten Variablen nutzen möchten, dann selektieren Sie die betreffenden Variablen über das Optionskästchen (linke Spalte) in der jeweiligen Tabellenzeile und klicken auf "Importieren".

    Die übernommenen Variablen werden aus der Tabelle gelöscht.
11. Wechseln Sie abschließend in das WBM-Register "Datenpunkte", prüfen die übernommenen Variablen und klicken Sie auf "Speichern".

Die übernommenen Variablen können Sie im Register "Datenpunkte" weiter bearbeiten.

6.10.4 OPC UA-Browse

- **Station selektieren**

  Wählen Sie eine der angelegten Stationen aus, um die Einstellungen anzuzeigen.

Browse OPC UA-Adressraum

- **Server-Adresse (IPv4) / (IPv6) / DNS-Name**

  Die IPv4- oder gegebenenfalls die IPv6-Adresse oder der DNS-Name der Station werden angezeigt.
- **Security Policy**

  Die für die Station ausgewählte Option wird angezeigt.
- **Verbinden**

  Über die Schaltfläche verbinden Sie sich mit dem Server.

  Bei erfolgreicher Verbindung wird diese Zeile ausgeblendet und der OPC UA Nodeset Baum wird stattdessen angezeigt.
- **Nur unterstützte Variablen anzeigen**

  Wird angezeigt, wenn eine erfolgreiche Verbindung zur Station aufgebaut wurde. Bei Aktivierung werden alle ungültigen Datenpunkte, die nicht unterstützt werden, ausgeblendet.
- **Importieren**

  Beim Importieren werden die ausgewählten Variablen in die Applikation übernommen.

OPC UA-Browsen durchführen

1. Wählen Sie über "Station selektieren" die gewünschte Station aus.
2. Klicken Sie auf die Schaltfläche "Verbinden".
3. Bestätigen Sie die Meldung, dass der Verbindungsaufbau mit dem Server erfolgreich war.

   Ergebnis: Die ausgewählte Station mit den zugehörigen Variablen wird angezeigt. Außerdem ist die Option "Nur unterstützte Variablen anzeigen" aktivierbar.

   Sie können nun durch die einzelnen Ordner oder Variablen browsen und Variablen importieren.

Variablen importieren

Markieren Sie einzelne Variablen oder ganze Ordner, und klicken Sie auf "Importieren". Um einen ganzen Ordner markieren zu können, muss er einmal geöffnet worden sein. Die Variablen werden in das WBM-Register "Datenpunkte" übernommen und können dort weiter bearbeitet werden.

6.10.5 OPC UA-Import

OPC UA-Nodeset importieren

- **Station selektieren**

  Wählen Sie eine der angelegten Stationen aus, um die Einstellungen anzuzeigen.

- **Nodeset-XML**

  Klicken Sie auf die Schaltfläche "Durchsuchen".

  Der Browser zum Durchsuchen des Dateisystems Ihres PC öffnet sich.

  Wählen Sie gewünschte XML-Datei und klicken Sie auf "Öffnen".

  Der Dateiname wird im Ausgabefeld des WBM angezeigt.

  Wenn Sie die Datei verwenden möchten, klicken Sie auf "Importieren" und bestätigen Sie anschließend mit "OK".

  Der Importvorgang wird durch den Laufbalken angezeigt.

  Wenn Sie mehrere Dateien importieren möchten, dann wiederholen Sie den Vorgang "Durchsuchen" > "Importieren".

  Ergebnis: Die Option "Nur unterstützte Variablen anzeigen" ist aktivierbar.

  Wenn Sie die Datei nicht verwenden möchten, dann klicken Sie auf "Löschen".

- **Hochladen**

  Durch das Hochladen wird die ausgewählte Nodeset-XML-Datei in die Applikation übernommen.

- **Nur unterstützte Variablen anzeigen**

  Wird angezeigt, wenn eine Nodeset-XML-Datei erfolgreich geladen wurde. Bei Aktivierung werden alle ungültigen Datenpunkte, die nicht unterstützt werden, ausgeblendet.

OPC UA-Import durchführen

Sie können offline durch die einzelnen Ordner oder Variablen navigieren und Variablen importieren.

- **Variablen importieren**

  Markieren Sie eine einzelne Variable oder einen Ordner. Um einen Ordner markieren zu können, muss er geöffnet sein.

  Klicken Sie auf "Importieren".

  Ergebnis: Die Variablen werden in das WBM-Register "Datenpunkte" übernommen und können dort weiter bearbeitet werden.

6.11 Instandhaltung

6.11.1 HTTP-Server

In diesem Register werden Einstellungen zum Webserver getätigt.

HTTP-Server Einstellungen

- **Schnittstelle**
  Wählen Sie über welches Interface auf das WBM zugegriffen werden kann.
  Optionen:
  - Prozess Schnittstelle (P2)
  - Cloud-Schnittstelle (P1)
  - Alle
- **HTTP aktiv**
  Bei aktivierter Option, kann unverschlüsselt über HTTP auf das WBM zugegriffen werden. Die Option ist in der Voreinstellung deaktiviert.
- **HTTP Port**
  Einstellung des HTTP-Ports. Vorbelegung: 80

- **Weiterleitung HTTP zu HTTPS**
  Bei aktivierter Option, werden Zugriffe über HTTP direkt zu HTTPS weitergeleitet. Der Status Code der Umleitung kann im Folgenden eingestellt werden.
- **Weiterleitung Status**
  Wählen Sie, ob bei der Weiterleitung von HTTP zu HTTPS Anfragen der Status Code "301 Moved Permanently" oder "308 Permanent Redirect" verwendet wird.

HTTP-Security

- **HTTPS aktiv**

  Bei aktivierter Option wird verschlüsselt über HTTPS auf das WBM zugegriffen. Die Option ist in der Voreinstellung aktiviert.
- **HTTPS Port**
  Einstellung des HTTPS-Ports. Vorbelegung: 443

Hinweis

Zertifikate für HTTPS-Kommunikation

Für die HTTPS-Kommunikation mit dem WBM enthält die Applikation ein werkseitig von Siemens ausgestelltes Zertifikat.

Optional können Sie zur Erhöhung der Sicherheit ein eigenes Server-Zertifikat und einen privaten Schlüssel importieren.

- **Webserver Zertifikat**

  Wählen Sie ein Webserver Zertifikat. Das Siemens Werkszertifikat ist mit der Auswahl "Standard" voreingestellt.
- **Webserver privater Schlüssel**
  Auswahl der Webserver Schlüsseldatei. Der Siemens Werkszertifikatsschlüssel ist mit der Auswahl "Standard" voreingestellt.

Schutz vor Brute-Force-Attacken

- **Anzahl fehlgeschlagener Anmeldeversuche**

  Anzahl der fehlgeschlagenen Anmeldeversuche bis zur Sperrung der IP-Adresse

  Wertebereich: 1...100, Default: 3
- **Überwachungszeitraum fehlgeschlagener Anmeldeversuche (s)**

  Zeitbereich in denen die projektierte Anzahl der Fehlversuche überwacht wird.

  Wertebereich: 1...3600, Default: 60 s
- **Sperrzeit (s)**
  Zeitdauer in der das WBM für die IP Adresse gesperrt ist.

  Wertebereich: 1...3600, Default: 60 s

6.11.2 Systemzeit

In diesen Registern setzen Sie die Uhrzeit oder projektieren die Uhrzeitsynchronisation des Gateways.

Hinweis

Projektierter NTP-Server muss beim Anlauf der Baugruppe erreichbar sein

Falls Sie einen NTP-Server projektiert haben, stellen Sie sicher, dass dieser beim Neustart der Baugruppe erreichbar ist. Wenn der projektierte NTP-Server nicht erreichbar ist, läuft die Baugruppe nicht an.

Uhrzeitformat und Zeitstempel

Das Gerät führt die Uhrzeit intern als UTC. Es wird die im WBM projektierte lokale Uhrzeit mit Zeitzone und optionaler Berücksichtigung der Sommer-/Winterzeit angezeigt.

Die Zeitstempel der übertragenen Daten werden im UTC-Format (48 Bit) übertragen.

Synchronisationsverfahren

Sie können die Uhrzeit manuell oder über NTP (Network Time Protocol) synchronisieren.

Hinweis

Uhrzeitsynchronisation

Bei Anwendungen, die eine Uhrzeitsynchronisation erfordern, sollten Sie die Uhrzeit des Geräts synchronisieren. Wenn Sie die Uhrzeit nicht regelmäßig synchronisieren, kann es zu Abweichungen der Uhrzeit zwischen Gerät und Kommunikationspartnern von einigen Sekunden pro Tag kommen.

NTP-Konfiguration

- **Aktiv**

  Aktivieren Sie die Option, wenn die Uhrzeit über NTP synchronisiert werden soll.

  Bei deaktivierter Option können Sie die Uhrzeit des Geräts manuell einstellen.

- **NTP-Server-Adresse**

  Geben Sie die Adresse des NTP-Servers als IPv4/IPv6-Adresse oder als DNS-Name ein.

- **Portnummer**

  Einstellung, über welchen Port der NTP Server erreicht wird. Vorbelegung: 123

- **Synchronisationszyklus (s)**

  Legt den Zyklus der Uhrzeitanfragen am NTP-Server fest.

  Wertebereich in Sekunden: 16..1024

- **NTP (secure)**

  Bei aktivierter Option wird die Uhrzeit über das gesicherte Verfahren NTP (secure) synchronisiert. NTP (secure) nutzt Authentifizierung über symmetrische Schlüssel.

Parameter für das Verfahren NTP (secure)

- **Schlüssel-ID**

  Schlüssel-ID des NTP-Servers. Numerischer Wert.

  Wertebereich: 1..65534

- **Schlüssel**

  Geben Sie den NTP-Schlüssel im ausgewählten Format ein.

  Zulässige Schlüssellänge:

  - ASCII: 5..20
  - Hexadezimal: 10-40

- **Schlüssel-Format**

  Geben Sie an, in welchem Format Sie den Schlüssel eingeben:

  - ASCII
  - HEX (hexadezimal)

- **Hash-Algorithmus**

  Wählen Sie alternativ:

  - SHA-1
  - MD5
  - AES128
  - AES256

Zeitzone

- **Zeitzone**

  Im NTP-Verfahren wird generell UTC (Universal Time Coordinated) übertragen. Dies entspricht GMT (Greenwich Mean Time).

  Durch die Projektierung der lokalen Zeitzone kann der Zeitversatz gegenüber UTC eingestellt werden.

Sommerzeit (DLS)

- **Aktiv**

  Bei aktivierter Option, wird die Systemzeit auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt.

  Wenn deaktiviert, wird die aktuelle Systemzeit nicht verändert.

- **Beginnt am**

  Wählen Sie, wann die Sommerzeit aktiviert werden soll.

- **Endet am**

  Wählen Sie, wann die Sommerzeit deaktiviert werden soll.

Systemzeit

Manuelles Setzen von Datum und Uhrzeit

Hinweis
Uhrzeit läuft im spannungslosen Zustand nicht weiter

Schalten Sie das Gateway spannungslos, läuft die manuell gesetzte Uhrzeit in der spannungslosen Zeit nicht weiter.

Die Eingabefelder für Datum und Uhrzeit sind nur bei deaktivierter Uhrzeitsynchronisation über NTP aktiv.

- **Datum**

  Geben Sie das aktuelle Datum manuell entsprechend dem vorgegebenen Format ein oder nutzen Sie den Kalender, der sich beim Klicken ins Eingabefeld öffnet:

  – DD.MM.YYYY

- **Uhrzeit**

  Geben Sie die aktuelle Uhrzeit manuell entsprechend dem vorgegebenen Format ein:

  – hh:mm:ss

- **Speichern**

  Bei Klicken auf die Schaltfläche übernimmt das Gerät die gespeicherten Zeitdaten.

6.11.3 Zertifikats-Management

Auf dieser Seite werden alle Zertifikate und privaten Schlüssel verwaltet.

Über die Registerkarten wechseln Sie zwischen der Übersicht für Zertifikate und private Schlüssel. Die gespeicherten Zertifikate und Schlüssel werden in der Übersichtstabelle dargestellt. Über die erste Tabellenzeile können Sie die Anzeige filtern.

Zertifikatdetails

Die Tabelle zeigt die Details der gespeicherten Zertifikate mit folgenden Parametern an:

- **Dateiname**

  Name der Zertifikatsdatei wird angezeigt.

- **Aussteller**

  Informationen des Antragsstellers des Zertifikates (CN, OU, O, L, S, C)

- **Gültig ab**

  Anfangsdatum der Gültigkeitsdauer des Zertifikats

- **Gültig bis**

  Enddatum der Gültigkeitsdauer des Zertifikats

- **Fingerabdruck**

  Fingerabdruck (Digest) der Zertifizierungsdaten

- **Herunterladen**

  Das Zertifikat wird auf dem PC gespeichert.

Zertifikate

- **Erzeugen**

  Durch Klicken auf die Schaltfläche, werden Sie auf eine Seite weitergeleitet, auf der Sie ein neues Zertifikat erstellen können.

- **Hochladen**

  Laden Sie bestehende Zertifikate und Client Keys in den Zertifikatsspeicher.

  Voraussetzung für den Import von Zertifikaten und Schlüsseln ist, dass die entsprechenden Dateien auf Ihrem PC gespeichert sind.

  Folgende Typen von Zertifikatsdateien werden unterstützt: *.pem, *.crt, *.cer, *.crl

  Folgende Typen von Schlüsseldateien werden unterstützt: *.pem

  – Klicken Sie auf die Schaltfläche "Datei auswählen".

    Es öffnet sich ein Browser zum Durchsuchen des Inhalts des Dateisystems Ihres PC.

    Wählen Sie die auf Ihrem PC gespeicherte Datei aus.

  – Klicken Sie anschließend auf "Importieren", um das Zertifikat zu laden.

  Nach Import einer Datei wird der Dateiname angezeigt.

- **Löschen**

  Durch Klicken auf die Schaltfläche löschen Sie die jeweiligen Zertifikats- und Schlüssel-Dateien aus dem Zertifikatespeicher.

Zertifikat erzeugen

- **Dateiname**

  Vergeben Sie einen Namen für die Datei.
- **Format**

  Wählen Sie ein Format aus der Auswahlliste.
- **Algorithmus**

  Wählen Sie den gewünschten Algorithmus aus der Auswahlliste.
- **Länge des privaten Schlüssels (Bit)**

  Wählen Sie die Schlüssellänge aus der Auswahlliste.
- **Elliptic Curve Cryptography (ECC)**

  Wählen Sie die gewünschte elliptic curve aus der Auswahlliste.
- **Passwort des privaten Schlüssels (optional)**

  Vergeben Sie optional ein Passwort für den privaten Schlüssel.
- **Gültigkeit (Tage)**

  Legen Sie fest, wieviele Tage das Zertifikat gültig ist. Wertebereich: 1..3650.
- **Signatur-Algorithmus**

  Wählen Sie einen Signatur-Algorithmus aus der Auswahlliste.
- **Name der Organisation (O)**
- **Organisationseinheit (OU)**
- **Stadt (L)**
- **Staat oder Bundesland (ST)**
- **Land (C)**
- **Common Name (CN)**
- **Domain-Komponente (DC)**

Alternativer Name des Zertifikatsinhabers (SAN)

- **URI**
- **DNS-Name**

  Sie können mehrere DNS-Namen mit einem Komma getrennt eintragen.
- **IP-Adresse**

  Sie können mehrere IP-Adressen mit einem Komma getrennt eintragen.
- **E-Mail**

Private Schlüssel

- **Hochladen**

  Laden Sie bestehende private Schlüssel in den Zertifikatsspeicher.

  Voraussetzung für den Import: Der Schlüssel ist auf Ihrem PC gespeichert.

  – Klicken Sie auf die Schaltfläche "Datei auswählen".

    Es öffnet sich ein Browser zum Durchsuchen des Inhalts des Dateisystems Ihres PC.

    Wählen Sie die auf Ihrem PC gespeicherte Datei aus.

  – Klicken Sie anschließend auf "Importieren", um den Schlüssel zu laden.

  Nach Import einer Datei wird der Dateiname angezeigt.

  – Vergeben Sie ein Passwort für den Schlüssel.

- **Löschen**

  Löscht selektierte Schlüssel.

6.11.4 Benutzerverwaltung

6.11.4.1 Passwort-Regeln

In diesem Register können Sie für jede Benutzergruppe die Regeln zur Passworterstellung festlegen.

- **Benutzergruppe**

  Wählen Sie die Benutzergruppe, für welche Sie Passwortregeln festlegen möchten.

- **Min. Passwortlänge**

  Legen Sie die Mindestlänge des Passworts fest. Vorbelegung: 8 Zeichen

- **Maximale Passwortlänge**

  Legen Sie die Maximallänge des Passworts fest. Vorbelegung: 1024 Zeichen

- **Mindestens 1 Kleinbuchstabe**

  Aktivieren Sie das Optionskästchen, um diese Regel anzuwenden.

- **Mindestens 1 Großbuchstabe**

  Aktivieren Sie das Optionskästchen, um diese Regel anzuwenden.

- **Mindestens 1 Ziffer**

  Aktivieren Sie das Optionskästchen, um diese Regel anzuwenden.

- **Mindestens 1 Sonderzeichen**

  Aktivieren Sie das Optionskästchen, um diese Regel anzuwenden. Das Passwort muss mindestens eines der folgenden Sonderzeichen enthalten (ASCII 0x21..0x7E):

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

- **Passwort zurücksetzen erzwingen**

  Aktivieren Sie das Optionskästchen, um beim Ändern der Passwortregeln alle Benutzer-Passwörter zurückzusetzen.

  Benutzer mit der Rolle "ADMIN" müssen bei der nächsten Anmeldung ein neues Passwort eingeben.

  Benutzer mit der Rolle "GUEST" werden deaktiviert, bis ein Benutzer mit der Rolle "ADMIN" dem "GUEST" ein neues Passwort zuweist.

6.11.4.2 Benutzer

Hinweis
Verlust von Benutzerdaten

Notieren Sie geänderte oder neu vergebene Benutzernamen und Passwörter.

Wenn Sie die Benutzerdaten des Administrators verlieren, haben Sie keinen Zugriff mehr auf das WBM.

Bei Verlust der Anmeldedaten erlangen Sie nur noch Zugriff auf das WBM, wenn Sie das Gerät auf Werkseinstellungen zurücksetzen. Dies ist mit Verlust von Daten verbunden.

Zu den voreingestellten Standard-Benutzerdaten für das erstmalige Anmelden siehe Kapitel Benutzerdaten für das erste Anmelden am WBM (Seite 69).

Zulässige Länge des Benutzernamens: 4...64 Zeichen

Hinweis
Ändern des Passworts

Aus Sicherheitsgründen müssen der werkseitig voreingestellte Benutzername und das Passwort beim ersten Anmelden geändert werden.

Übersicht

Alle angelegten Benutzer werden in der Tabelle auf der Übersichtsseite dargestellt.

Über die erste Zeile in der Tabelle können Sie filtern und sortieren.

Einige der angezeigten Eigenschaften können direkt auf der Übersichtsseite editiert werden.

Passwort-Regeln

Neu vergebene Benutzer-Passwörter müssen folgende Bedingungen erfüllen:

- Mindestlänge: 8 Zeichen
- Mindestens 1 Kleinbuchstabe
- Mindestens 1 Großbuchstabe
- Mindestens 1 Ziffer
- Mindestens 1 der folgenden Sonderzeichen (ASCII 0x21..0x7E):

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Rollen und Rechte

SuperUser

Der SuperUser ist der erste Nutzer auf der Baugruppe. Er ist standardmäßig in Gruppe "ADMIN" und kann weder umgruppiert noch gelöscht werden. Es gibt genau einen SuperUser.

Sie können bis zu 6 weitere Benutzer mit den Rollen "ADMIN" oder "GUEST" hinzufügen.

ADMIN

Benutzer mit der Rolle "ADMIN" haben die Rechte zum Ändern sämtlicher Daten, die im WBM zugänglich sind.

GUEST

Benutzer mit der Rolle "GUEST" haben nur Zugriff auf die Diagnosedaten, ohne Änderungen an der Konfiguration durchführen zu können.

Benutzer hinzufügen

Klicken Sie auf die Schaltfläche "Erstellen" um einen neuen Benutzer anzulegen.

- **Aktiv**

  Nur aktive Benutzer können eine Verbindung zum WBM aufbauen. Es muss immer einen aktiven Benutzer mit Administratorenrechten geben.

- **Benutzergruppe**

  Ordnen Sie dem Benutzer die Rolle "ADMIN" oder "GUEST" zu. Die ausgewählte Rolle kann später nicht mehr geändert werden.

- **Neuer Benutzername**

  Geben Sie den Benutzernamen des neuen Benutzers ein.

- **Benutzername wiederholen**

  Wiederholen Sie zur Bestätigung den oben eingegebenen Benutzernamen.

- **Neues Passwort**

  Geben Sie das Passwort für den neuen Benutzer ein.

- **Passwort wiederholen**

  Wiederholen Sie das oben eingegebene Passwort.

- **Sprache**

  Wählen Sie die Standard-Sprache des WBM für den Benutzer.

- **Vorname**

  Geben Sie optional den Vornamen des Benutzers an.

- **Nachname**

  Geben Sie optional den Nachnamen des Benutzers an.

Benutzerdaten bearbeiten

Hinweis
Übernahme geänderter Benutzerdaten

Geänderte Benutzerdaten werden nach dem Speichern unmittelbar übernommen.

Nach dem Ändern von Benutzerdaten müssen Sie diese bei der nächsten Anmeldung verwenden.

Klicken Sie auf das Symbol in der Tabellenspalte "Bearbeiten", um die Benutzerdaten zu editieren.

Parameter:

- **Aktiv**

  Nur aktive Benutzer können eine Verbindung zum WBM aufbauen.

- **Super User**

  Zeigt an, ob der Benutzer Administrator ist.

- **Benutzergruppe**

  Zeigt an, welche Rolle dem Benutzer zugeordnet ist. Die Benutzergruppe kann nicht verändert werden.

- **Benutzername**

  Anzeige des aktuellen Benutzernamen

- **Aktuelles Passwort**

  Geben Sie das aktuelle Passwort ein, bevor Sie Änderungen am Benutzernamen oder am Passwort vornehmen.

- **Neuer Benutzername**

  Geben Sie zum Ändern einen neuen Benutzernamen ein.

- **Benutzername wiederholen**

  Wiederholen Sie zur Bestätigung eines neuen Benutzernamen den oben eingegebenen Benutzernamen.

- **Neues Passwort**

  Geben Sie zum Ändern des Passworts ein neues Passwort ein.

- **Passwort wiederholen**

  Wiederholen Sie das neue Passwort.

- **Sprache**

  Wählen Sie die Standard-Sprache des WBM für den Benutzer.

- **Vorname**

  Ändern Sie optional den Vornamen des Benutzers.

- **Nachname**

  Ändern Sie optional den Nachnamen des Benutzers.

6.11.4.3 Benutzergruppen

In diesem Register können Sie für jede Benutzergruppe festlegen, nach welcher Inaktivitätszeit die laufende Sitzung beendet und der Benutzer abgemeldet wird.

- **Sitzungslebensdauer**

  Wählen Sie, nach welcher Inaktivitätszeit die laufende Sitzung automatisch beendet wird.

  - 10 min
  - 30 min
  - 1 Stunde
  - 1 Tag
  - 1 Woche

  Vorbelegung: 10 min.

6.11.5 Firmware

Die aktuelle Firmware-Version des Geräts finden Sie auf der WBM-Seite Info (Seite 71).

Wenn eine neue Firmware-Version zur Verfügung steht, dann können Sie die Firmware-Datei über diese WBM-Seite vom PC in das Gateway laden.

Zu neuen Firmware-Dateien für das Gateway siehe Kapitel Neue Firmware laden (Seite 181).

Hinweis

Digital signierte und verschlüsselte Firmware

Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Firmware-Aktualisierung

- **Firmware-Datei**

  Nach Auswahl einer auf dem PC gespeicherten Firmware-Datei über die Schaltfläche "Durchsuchen" wird der Dateiname hier angezeigt.

- **Durchsuchen**

  Durchsucht das Dateisystem des PC nach einer dort gespeicherten Firmware-Datei, welche in das Gateway geladen werden soll.

  Firmware-Dateien haben das Dateiformat *.upd.

  Nach Auswahl der Datei wird der Name der selektierten Datei angezeigt, die Firmware wird aber noch nicht verwendet.

- **Laden in Gerät**

  Durch Klicken auf die Schaltfläche laden Sie die selektierte Firmware-Datei in das Gateway.

  Der laufende Aktualisierungsvorgang wird im WBM durch einen Laufbalken angezeigt.

Nach Abschluss der Aktualisierung führt das Gateway einen Neustart durch. Anschließend müssen Sie sich neu anmelden. Prüfen Sie auf der Startseite unter "Info" > "Status" ob die geladene Firmware-Version angezeigt wird.

Hinweis

Firmware-Aktualisierung

Beachten Sie, dass das Aktualisieren der Firmware eine Weile dauern kann.

- **Keine Eingaben während der Aktivierung**

  Während des Aktivierens bis zum Neustart des Gateways ist das WBM nicht gesperrt.

  Wechseln Sie in dieser Zeitspanne nicht die WBM-Seite.

- **Kein Ausschalten des Gateways**

  Schalten Sie das Gateway während des Aktivierungsvorgangs der Firmware nicht aus. Sie vermeiden damit das Auftreten inkonsistenter Zustände.

- **Automatische Übernahme der gespeicherten Konfigurationsänderungen**

  Bereits gespeicherte aber noch nicht übernommene Konfigurationsänderungen werden beim Neustart nach Firmware-Aktualisierung automatisch übernommen.

6.11.6 Sicherung und Wiederherstellung

6.11.6.1 Konfiguration

In diesem Register können Sie die Projektierungsdaten des Gateways über eine Konfigurationsdatei speichern und wieder laden.

Konfigurationsdateien haben den Namen "CC712<Datum und Uhrzeit>.cfg" oder "CC712<Datum und Uhrzeit>.cfgp" bzw. "CC716...".

Sie können verschlüsselte Konfigurationsdateien (*.cfgp) nicht editieren. Wenn verschlüsselte Teile verändert werden, wird die Konfigurationsdatei beim Laden abgelehnt.

Unverschlüsselte Konfigurationsdateien (*.cfg) können Sie manuell editieren. Bei fehlerhaften Veränderungen z. B. Formfehlern wird die Konfigurationsdatei beim Laden abgelehnt.

Das Speichern der Konfigurationsdatei auf dem PC ist in folgenden Fällen sinnvoll:

- Sie möchten die Projektierungsdaten des Gateways für ein anderes Gateway verwenden.
- Sie möchten mehrere Gateways mit ähnlichen Projektierungsdaten einsetzen.
- Im Ersatzteilfall

Sie laden die Projektierungsdaten vom PC in ein weiteres Gateway und projektieren ggf. nur die abweichenden Parameter neu.

Weiterhin können Sie einen gesteckten CLP durch das Gateway formatieren lassen.

Konfiguration exportieren

Hinweis

Optionen beim Exportieren einer Konfiguration

Beim Exportieren einer Konfiguration haben Sie folgende Optionen:

- **Ohne Benutzerdaten und PKI-Speicher**

  Diese Datei mit der Dateiendung *.cfg enthält nur die Gerätekonfiguration mit den projektierten Verbindungen und Datenpunkten. Diese Datei eignet sich für die Übernahme der Konfiguration in weitere Gateways, da in der Regel Zertifikate und Schlüssel angepasst werden müssen.
- **Mit Benutzerdaten und PKI-Speicher**

  Diese Datei mit der Dateiendung *.cfgp enthält neben der Gerätekonfiguration mit den projektierten Verbindungen und Datenpunkten auch noch sämtliche Benutzerdaten, Passwörter, Zertifikate und ggf. zugehörige private Schlüssel. Mit dieser Datei kann ein anderes Gateway, z. B. im Ersatzteilfall, sämtliche Einstellungen übernehmen und sofort den Betrieb wieder fortsetzen.

Hinweis

Automatisches Backup

Sollte bei einem Firmware-Update auf die aktuelle Version eine bestehende Konfiguration des CloudConnect nicht konvertiert werden, wird die Konfiguration automatisch als Backup gespeichert und kann heruntergeladen werden. Dieses Backup können Sie in dringenden Fällen dem Support zusenden.

CC7 startet in dem Fall mit Werkseinstellungen und Standard-Benutzerdaten.

- **Passwort** (optional)

  Die Konfigurationsdatei wird verschlüsselt gespeichert. Zusätzlich können Sie die Konfigurationsdatei durch Angabe eines Passwortes (8-64 Zeichen) gegen unbefugte Benutzung sichern. Die Konfigurationsdatei kann nur unter Angabe dieses Passwortes wieder geladen werden.

- **Exportieren**

  Speichert die aktuell vom Gateway verwendete Konfiguration mit den ausgewählten Optionen in eine Konfigurationsdatei auf dem PC.

Laden einer Konfiguration

- **Legacy-Konfiguration (vor V2.0)**

  Über diese Option können Sie eine Backup-Konfigurationsdatei der V1.9 laden. Bei Legacy-Konfigurationen von früheren Firmware-Versionen kann der Import fehlschlagen.

- **Passwort (optional)**

  Wurde beim Speichern der Konfigurationsdatei ein Passwort angegeben, so muss dieses Passwort beim Laden dieser Konfigurationsdatei auch wieder angegeben werden.

- **Konfigurationsdatei**

  Nach Auswahl einer auf dem PC gespeicherten Konfigurationsdatei über die Schaltfläche "Durchsuchen" wird der Dateiname hier angezeigt.

- **Datei auswählen**

  Durchsucht das Dateisystem des PC nach einer dort gespeicherten Konfigurationsdatei, welche in das Gateway geladen werden soll.

- **Laden in Gerät**

  Lädt die unter "Datei" angezeigte Konfigurationsdatei in das Gateway.

Hinweis
Übernehmen der Konfigurationsdaten

Die Benutzerdaten einer geladenen Konfigurationsdatei vom Typ "cfgp" werden direkt übernommen und bei der nächsten Benutzer-Anmeldung vom Gateway verwendet, auch wenn die restliche Konfiguration noch nicht auf dem CC7 übernommen wurde.

Die Projektierungsdaten der geladenen Konfigurationsdatei werden mit Klicken auf die Schaltfläche "Übernehmen" übernommen und bei der nächsten Benutzer-Anmeldung vom Gateway verwendet.

Hinweis
Gespeicherte Zertifikate

Beim Laden einer Konfigurationsdatei vom Typ "cfg" bleiben alle bereits bestehenden Zertifikate im Zertifikatsspeicher bestehen.

Beim Laden einer Konfigurationsdatei vom Typ "cfgp" werden die bestehenden Zertifikate mit den Zertifikaten aus der geladenen Konfigurationsdatei überschrieben.

6.11.6.2 CLP

In diesem Register erhalten Sie Informationen zum CLP. Außerdem können Sie einen fabrikneuen oder zuvor von einem anderen Gerät verwendeten CLP formatieren. Durch die Formatierung werden die vorhandenen Daten auf dem CLP gelöscht.

- **Status**

  Zeigt, ob ein CLP gesteckt ist oder nicht und ob das Format bekannt ist oder nicht.

- **Dateisystem**
- Zeigt an, wo im Dateisystem. EXT4
- **Speicherkapazität**

  Speichergröße des CLP in Byte.

- **Belegter Speicherplatz**

  Belegten Speicherplatz in Byte.

- **Informationen**

  Anzeige von allgemeinen Informationen, die auf dem CLP gespeichert sind.

- **Speichern**

  Klicken Sie auf die Schaltfläche "Speichern" um die aktuelle Konfiguration auf dem CLP zu speichern.

- **Formatieren**

  Nach Klicken auf die Schaltfläche "Formatieren" wird der gesteckte CLP formatiert.

  Wenn der Formatierungsprozess abgeschlossen ist, wird eine Meldung im WBM eingeblendet. Schalten Sie das Gateway nicht aus, bevor die Meldung erscheint.

6.11.7 Kommunikation / Neustart

Prozess-Kommunikation / Neustart

Auf dieser Seite können Sie die Kommunikation zwischen Gateway und Prozess-Stationen anhalten oder starten und einen Neustart der Applikation veranlassen.

Bei jedem Befehl wird eine Meldung des Systems ausgegeben, der angezeigte Status wird aktualisiert.

Prozess-Kommunikation

Unter "Status" wird der aktuelle Zustand angezeigt.

- **Stop**

  Klicken Sie auf die Schaltfläche, um die Kommunikation anzuhalten.

  Die Beschriftung der Schaltfläche schlägt um.

- **Start**

  Klicken Sie auf die Schaltfläche, um die Kommunikation wieder zu starten.

Neustart

- **Neustart**

  Klicken Sie auf die Schaltfläche, um einen Neustart der Applikation auszulösen.

Rücksetzen auf Werkseinstellungen

Durch Klicken auf die Schaltfläche setzen Sie alle Daten der Applikation auf Werkseinstellungen zurück.

Die MAC-Adressen der Schnittstellen werden durch das Rücksetzen nicht gelöscht.

Nach dem Rücksetzen führt die Applikation einen Neustart durch.

Hinweis

Datenverlust durch Rücksetzen

Beachten Sie vor dem Rücksetzen die nachfolgend beschriebenen Auswirkungen des Rücksetzens.

- Alle Projektierungsdaten, Zertifikate, Schlüssel und Benutzerdaten werden durch das Rücksetzen gelöscht.

  Auch die Daten auf einem optionalen CLP werden gelöscht.
- Die Applikation ist durch das Rücksetzen der IP-Parameter an der jeweiligen Schnittstelle nicht mehr unter den zuvor projektierten Adressdaten erreichbar.

  Die Applikation ist dann über die werkseitig vorbelegte IP-Adresse der jeweiligen Schnittstelle erreichbar. Zu den vorbelegten IP-Parametern siehe Kapitel Neustart und Zurücksetzen (Seite 182).

Betriebssystem

- **Neustarten**

  Klicken Sie auf die Schaltfläche, um den CC7 komplett neu zu starten.
- **Herunterfahren**

  Klicken Sie auf die Schaltfläche, um den CC7 vollständig herunterzufahren.

  Alle LEDs bis auf die LAN LEDs von P1 und P2 werden deaktiviert. Der CC7 kann nun von der Spannung getrennt werden.

  Der CC7 startet erst wieder, wenn die Spannung einmal getrennt und wieder gesteckt wurde.

6.11.8 Diagnose

Diagnosemeldungen

Die Seite enthält Diagnosemeldungen zu internen Ereignissen und Fehlern.

- **Aktualisierung**

  Hier stellen Sie ein, ob und in welchem Zyklus das WBM die angezeigten Diagnosemeldungen aktualisiert.

Die Einträge enthalten einen Zeitstempel und den Meldungstext.

- Benachrichtigungen (NOTIFICATION) werden fett markiert dargestellt.
- Fehler werden rot dargestellt.
- Hinweise werden blau dargestellt.
- Warnungen werden gelb dargestellt.

Beispiele für Ereignisse:

- Anlauf

- Aufbau/Abbruch einer Kommunikationsverbindung

- Änderung der Konfiguration

6.11.9 Protokollierung

6.11.9.1 Protokollierung

Nutzung der Protokollierung

Über die Protokollierungsfunktionen in Log-Dateien können Sie wichtige Ereignisse in eine Datei exportieren.

- **Exportieren**

  Klicken Sie auf die Schaltfläche, um die jeweilige Datei in das Dateisystem des PC zu exportieren.

Die exportierten Dateien werden in der Fußzeile des WBM angezeigt. Sie können die Dateien aus dem Dateisystem des PC oder direkt aus dem WBM-Register öffnen.

Siehe auch

Syslog-Meldungen (Seite 201)

6.11.9.2 Log-Dateien exportieren

- **Trace**

  Zur Laufzeit werden automatisch Informationen zu wichtigen auftretenden Ereignissen abgespeichert. Dies sind Daten zur Konfiguration, zu aktiven Vorgängen und zu Fehlerfällen.

  Die Protokollierung von Ereignissen sollten Sie nur nutzen, wenn Sie vor Problemen mit der Anwendung stehen, die Sie nicht selbst lösen können.

  Über die "Exportieren"-Schaltfläche können Sie diese Daten in einer Protokollierungsdatei "*.enc" speichern.

  Die Informationen in dieser nicht lesbaren Datei sind verschlüsselt und können nur durch den Siemens Industry Online Support gelesen werden. Schicken Sie die Protokollierungsdatei zurück an Ihren Ansprechpartner beim Siemens Industry Online Support.

- **Security-Meldungen**

  Hier können Sie die Security-Ereignisse in einer *.log-Datei speichern.

- **Diagnosemeldungen**

  Hier können Sie die Diagnosemeldungen des Geräts in ein gepacktes Archiv "diagnostic.tqz" speichern.

  Entpacken Sie das *.tqz-Archiv sowie das folgende entpackte *.tar-Archiv. Die Diagnosemeldungen finden Sie in einer *.log-Datei.

- **Netzwerkanalyse**

  Nur Benutzer mit der Rolle "ADMIN" können eine Netzwerkanalyse durchführen.

  Die Ergebnisse der Netzwerkanalyse werden in max. 4 Dateien gespeichert.

  Sie sollten die Netzwerkanalyse nur nutzen, wenn Sie vor Problemen mit der Anwendung stehen, die Sie nicht selbst lösen können.

  Über die "Exportieren"-Schaltfläche können Sie diese Daten in einer Protokollierungsdatei "*.enc" speichern.

  Die Informationen in dieser nicht lesbaren Datei sind verschlüsselt und können nur durch den Siemens Industry Online Support gelesen werden. Schicken Sie die Protokollierungsdatei zurück an Ihren Ansprechpartner beim Siemens Industry Online Support.

- **PROFIBUS/MPI (CC716)**

  Über die "Exportieren"-Schaltfläche können Benutzer mit der Rolle "ADMIN" diese Daten in einer Protokollierungsdatei "profibus.bin" speichern.

6.11.9.3 Datenverkehr aufzeichnen

Zur Diagnose von Netzwerkproblemen können Sie eine Aufzeichnung des Datenverkehrs am CC7 aktivieren. Die Ergebnisse können Sie exportieren und als verschlüsselte Datei an den Siemens Industry Online Support zur Analyse schicken.

Die Parameter können miteinander kombiniert und leer gelassen werden.

- **Aktivieren**

  Aktivieren Sie die Option, um die Aufzeichnung zu starten.

  Bei einem Neustart der Baugruppe wird die Aufzeichnung automatisch beendet. Bei "Speichern" und "Übernehmen" läuft die Aufzeichnung weiter.

- **Netzwerkschnittstelle**

  Wählen Sie die Netzwerkschnittstelle, deren gesendeter oder empfangener Datenverkehr aufgezeichnet wird.

- **Host**

  Wählen Sie die Richtung und die aufzuzeichnende IP-Adresse.

- **Port**

  Wählen Sie die Richtung und die Portnummer.

- **Protokoll**

  Wählen Sie das gewünschte Protokoll.

6.11.9.4 Security-Ereignisse

Das Gateway gibt Syslog-Meldungen gemäß RFC 5424 / RFC 5426 aus. Die Meldungen orientieren sich an der IEC 62443-3-3.

Bei Eingabe der Adressdaten eines Syslog-Servers sendet das Gateway die Meldungen an den Server.

Wenn Sie nicht über einen Syslog-Server verfügen, lassen Sie die Server-Adresse frei.

- **Aktiv**

  Wenn aktiviert werden alle Security-Ereignisse an den projektierten Syslog-Server gesendet.

- **Server-Adresse**

  Geben Sie die IP-Adresse des Syslog-Servers ein.

- **Server-Port**

  Den vorbelegten Server-Port 514 (UDP) können Sie ändern.

Die Beschreibung der Syslog-Meldungen finden Sie im Anhang Syslog-Meldungen (Seite 201).

Diagnose und Instandhaltung 7

7.1 Diagnosemöglichkeiten

Nachfolgende Diagnosemöglichkeiten stehen Ihnen zur Verfügung.

LEDs der Baugruppe

Informationen zu den LED-Anzeigen finden Sie im Kapitel LED-Anzeigen (Seite 33).

Web Based Management (WBM)

Hierfür müssen Sie Ihren PC an das Gateway anschließen.

Auf den folgenden WBM-Seiten erhalten Sie Informationen zum Zustand des Gateways:

- Allgemeine Informationen zum Status des Gateways finden Sie auf der Startseite des WBM, vgl. Kapitel Info (Seite 71).
- Die Diagnosemeldungen finden Sie auf der Diagnoseseite des WBM, vgl. Kapitel Diagnose (Seite 177).

  Bei wichtigen Ereignissen schreibt das Gateway Diagnosemeldungen in den Diagnosepuffer.

7.2 Neue Firmware laden

Die aktuelle Firmware-Version des Geräts finden Sie auf der WBM-Seite Info (Seite 71).

Neue Firmware-Versionen

Wenn für die Baugruppe eine neue Firmware-Version zur Verfügung steht, dann finden Sie diese auf den Internet-Seiten des Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621/dl)

Speichern Sie die Firmware-Datei auf dem Projektierungs-PC.

Laden neuer Firmware-Dateien

Eine neue Firmware-Datei laden Sie vom Projektierungs-PC über das WBM in das Gateway.

Die Beschreibung finden Sie im Kapitel Firmware (Seite 171).

7.3 Neustart und Zurücksetzen

Funktionen und Durchführung

Folgende Funktionen zum Rücksetzen stehen zur Verfügung:

- **Neustart**

  Die Projektierungsdaten bleiben erhalten.

  Das Gateway führt einen Neustart durch.

  Die Funktion können Sie durchführen über:

  – WBM: "Instandhaltung > Kommunikation / Neustart"

- **Rücksetzen auf Werkseinstellungen**

  Die Projektierungsdaten werden gelöscht.

  Auch die Daten auf einem optionalen CLP werden gelöscht.

  Das Gateway führt einen Neustart durch.

  Die Funktion können Sie durchführen über:

  – Taster "SET"

    Zur Betätigung des Tasters siehe Kapitel Der Taster "SET" (Seite 38).

  – WBM: "Instandhaltung > Kommunikation / Neustart"

Neustart

Das Gateway beendet den Produktivbetrieb, läuft automatisch wieder neu an und nimmt den Produktivbetrieb mit den vorhandenen Projektierungsdaten wieder auf.

Rücksetzen auf Werkseinstellungen: Auswirkung

Hinweis

Daten werden gelöscht

Mit dem Rücksetzen auf Werkseinstellungen werden alle Projektierungsdaten und Prozessdaten im Gateway gelöscht!

Beim Rücksetzen auf Werkseinstellungen ist das Gateway nur über die werkseitig voreingestellten Adressdaten erreichbar.

- **Gelöschte Daten**

  Folgende Daten werden durch das Rücksetzen auf Werkseinstellungen im Gateway gelöscht:

  - Anwenderseitig projektierte Adressen der LAN-Schnittstellen

    Sie werden auf die werkseitig voreingestellten Adressdaten zurückgesetzt.
  - Alle weiteren Projektierungsdaten des Gateways
  - Alle Prozessdaten im Speicher des Gateways
  - Benutzernamen und Passwörter
  - Alle importierten Zertifikate
  - Diagnosepuffer

  Weiterhin werden folgende Daten gelöscht:

  - Alle Daten auf einem gesteckten CLP
- **Nicht gelöschte Daten**

  Folgende Daten werden durch das Rücksetzen auf Werkseinstellungen nicht gelöscht:

  - MAC-Adresse der LAN-Schnittstellen

Wiederanlauf nach Rücksetzen

- Das Gateway läuft ohne Projektierungsdaten an.
- Die DHCP-Client-Funktion ist deaktiviert.

Das Gateway ist über die werkseitig vorbelegten Adressdaten erreichbar, siehe Kapitel Verbindung mit dem WBM aufbauen (Seite 68).

7.4 Gerätetausch im Fehlerfall

Gerät defekt

Bitte senden Sie das Gerät im Fehlerfall an Ihre Siemens-Vertretung zur Reparatur ein. Eine Reparatur vor Ort ist nicht möglich.

Tausch des Gateways

⚠ WARNUNG

Vor dem Austausch

- Lesen Sie vor einem Wechsel des Gateways die Sicherheitshinweise im Kapitel Wichtige Hinweise zum Einsatz des Geräts (Seite 41).
- Stellen Sie sicher, dass während der Arbeiten die Spannungsversorgung ausgeschaltet ist.

Gehen Sie beim Austausch des Gateways entsprechend den Beschreibungen im Kapitel Montieren (Seite 44) vor.

Übertragung der Projektierungsdaten auf das neue Gateway

Wenn Sie zuvor die Projektierungsdaten des Gateways in einer Konfigurationsdatei auf einem PC oder einem CLP gespeichert haben, können Sie diese nach dem Verbinden des PC mit dem Gateway bzw. beim Anlauf in das Gateway laden, siehe Kapitel Konfiguration (Seite 172).

Technische Daten

8

8.1 Technische Daten - CloudConnect 712

Technische Daten - CloudConnect 712		
Artikelnummer	6GK1411-1AC00	
Anschluss an Industrial Ethernet		
Anzahl	2 x Gigabit-Schnittstelle (P1, P2)	
Ausführung	RJ45-Buchse, galvanisch getrennt	
Eigenschaften		
• Standard	• 1000BASE-T, IEEE 802.3ab	
• Übertragungsgeschwindigkeiten	• 10 / 100 / 1000 Mbit/s	
• Weitere Eigenschaften	• Halbduplex/Vollduplex, Autocrossover, Autonegotiation, Autosensing	
Spannungsversorgung		
Ausführung	Buchse inklusive fünfpoliger Klemmenblock mit Verpolschutz	
Versorgungsspannung	• Spannungsart	• DC 24 V
	• Zulässige untere Grenze	• 19,2 V
	• Zulässige obere Grenze	• 28,8 V
Klemmenblock	(Spannungsversorgung)	
Klemmschraube	M2	
	Schraubendreherklinge:	0,4 x 2,5 (DIN 5264)
Anzugsdrehmoment	0,2...0,25 Nm	
Anschließbare Leitungsquerschnitte	• Ohne Adernendhülse	• 0,5...2,5 mm^2 / AWG 20...12
	• Mit Adernendhülse	• 0,5....1,5 mm^2 / AWG 20 .. 16
Weitere elektrische Daten		
Stromaufnahme (typisch)	200 mA	
Verlustwirkleistung (typisch)	4,8 W	
Überspannungskategorie gemäß IEC / EN 60664-1	Kategorie II	
Zulässige Umgebungsbedingungen		
Umgebungstemperatur	Während Betrieb bei waagerechtem Aufbau des Baugruppenträgers	0 °C ... +60 °C
	Während Betrieb bei senkrechtem Aufbau des Baugruppenträgers	0 °C ... +50 °C
	Während Lagerung	-40 °C ... +70 °C
	Während Transport	-40 °C ... +70 °C
Relative Luftfeuchte	Während Betrieb	≤ 60 % bei 25 °C, ohne Kondensation
Zulässige Schadstoffkonzentration	Schadgasprüfung gemäß ISA-S71.04 severity level G1, G2, G3:	
	• SO_2	• < 0,5 ppm
	• H_2S	• < 0,1 ppm

Technische Daten - CloudConnect 712	
Bauform, Maße und Gewicht	
Baugruppenformat	Kompaktbaugruppe S7-1500
Schutzart	IP20
Gewicht	300 g
Abmessungen (B x H x T)	35 x 147 x 127 mm
Befestigungsart	• 35 mm DIN-Hutschienenmontage • S7-300-Profilschienenmontage • S7-1500-Profilschienenmontage • Wand-Montage

Weitere Daten finden Sie im Kapitel Vorgesehene Betriebsumgebung (Seite 19).

8.2 Technische Daten - CloudConnect 716

Technische Daten - CloudConnect 716		
Artikelnummer	6GK1411-5AC00	
Anschluss an Industrial Ethernet		
Anzahl	2 x Gigabit-Schnittstelle (P1, P2)	
Ausführung	RJ45-Buchse, galvanisch getrennt	
Eigenschaften		
• Standard	• 1000BASE-T, IEEE 802.3ab	
• Übertragungsgeschwindigkeiten	• 10 / 100 / 1000 Mbit/s	
• Weitere Eigenschaften	• Halbduplex/Vollduplex, Autocrossover, Autonegotiation, Autosensing	
Anschluss an PROFIBUS		
Anzahl	1 x PROFIBUS/MPI-Schnittstelle (MPI/DP)	
Ausführung und Standard	9-polige Sub-D-Buchse, RS-485	
Übertragungsgeschwindigkeiten	9,6 kbit/s, 19,2 kbit/s, 45,45 kbit/s, 93,75 kbit/s, 187,5 kbit/s, 500 kbit/s, 1,5 Mbit/s, 3 Mbit/s, 6 Mbit/s, 12 Mbit/s	
Maximale Stromaufnahme an der PROFIBUS-Schnittstelle beim Anschluss von Netzkomponenten (beispielsweise optische Netzkomponenten)	15 mA bei 5 V (nur für die Bus-Terminierung) *****	
Spannungsversorgung		
Ausführung	Buchse inklusive fünfpoliger Klemmenblock mit Verpolschutz	
Versorgungsspannung	• Spannungsart	• DC 24 V
	• Zulässige untere Grenze	• 19,2 V
	• Zulässige obere Grenze	• 28,8 V
An Klemmenblock anschließbare Leitungsquerschnitte	• Ohne Adernendhülse	• 0,2 .. 2,5 mm^2 / AWG 24 .. 13
	• Mit Adernendhülse	• 0,25 .. 1,5 mm^2 / AWG 24 .. 16
	• Mit TWIN-Adernendhülse	• 0,5 .. 1,0 mm^2 / AWG 20 .. 17

Technische Daten - CloudConnect 716		
Weitere elektrische Daten		
Stromaufnahme (typisch)	250 mA	
Verlustwirkleistung (typisch)	6 W	
Überspannungskategorie gemäß IEC / EN 60664-1	Kategorie II	
Digitaler Eingang		
Anzahl	1 x Klemmenblock (DI)	
Ausführung	2-polig	
Spannung	Nennspannung DC 24 V Sicherheitskleinspannung (SELV) • Für Zustand "1": DC 13 V ... 30 V • Für Zustand "0": DC -30 V ... 3 V	
Weitere Eigenschaften	• Maximaler Eingangsstrom 8 mA • Maximale Leitungslänge < 30 m Leitungen sind paarweise zu führen. • Eingang potentialgetrennt zur Elektronik • Minimale Pulslänge: 100 ms	
Digitaler Ausgang		
Anzahl	1 x Klemmenblock (DO)	
Ausführung	Schalter, 2-polig	
Spannung	Nennspannung DC 24 V Sicherheitskleinspannung (SELV)	
Weitere Eigenschaften	• Intern, nicht strombegrenzt • Maximale Strombelastbarkeit 1 A • Maximale Leitungslänge < 30 m Leitungen sind paarweise zu führen. • Ausgang potentialgetrennt zur Elektronik	
Klemmenblöcke (Spannungsversorgung, Digitaleingang, Digitalausgang)		
Klemmschraube	M2 Schraubendreherklinge:	0,4 x 2,5 (DIN 5264)
Anzugsdrehmoment	0,2...0,25 Nm	
Anschließbare Leitungsquerschnitte	• Ohne Adernendhülse • Mit Adernendhülse	• 0,5...2,5 mm^2 / AWG 20...12 • 0,5....1,5 mm^2 / AWG 20 .. 16
Zulässige Umgebungsbedingungen		
Umgebungstemperatur	Während Betrieb bei waagerechtem Aufbau des Baugruppenträgers	0 °C ... +60 °C
	Während Betrieb bei senkrechtem Aufbau des Baugruppenträgers	0 °C ... +50 °C
	Während Lagerung	-40 °C ... +70 °C
	Während Transport	-40 °C ... +70 °C
Relative Luftfeuchte	Während Betrieb	≤ 60 % bei 25 °C, ohne Kondensation
Zulässige Schadstoffkonzentration	Schadgasprüfung gemäß ISA-S71.04 severity level G1, G2, G3:	
	• SO_2	• < 0,5 ppm
	• H_2S	• < 0,1 ppm

Technische Daten - CloudConnect 716	
Bauform, Maße und Gewicht	
Baugruppenformat	Kompaktbaugruppe S7-1500
Schutzart	IP20
Gewicht	400 g
Abmessungen (B x H x T)	35 x 147 x 127 mm
Befestigungsart	• 35 mm DIN-Hutschienenmontage • S7-300-Profilschienenmontage • S7-1500-Profilschienenmontage • Wand-Montage

***** Die Strombelastung durch einen externen Verbraucher, der zwischen VP (Pin 6) und DGND (Pin 5) angeschlossen wird, darf für die Bus-Terminierung maximal 15 mA betragen (kurzschlussfest).

Weitere Daten finden Sie im Kapitel Vorgesehene Betriebsumgebung (Seite 19).

Zulassungen

9

Erteilte Zulassungen

Hinweis

Erteilte Zulassungen auf dem Typenschild des Geräts

Die angegebenen Zulassungen gelten erst dann als erteilt, wenn auf dem Produkt eine entsprechende Kennzeichnung angebracht ist. Welche der nachfolgenden Zulassungen für Ihr Produkt erteilt wurde, erkennen Sie an den Kennzeichnungen auf dem Typenschild.

Dokumente im Internet

Die nachfolgend aufgeführten Konformitätserklärungen und Zertifikate des Produkts finden Sie im Internet unter folgender Adresse:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/25621/cert)

Die berücksichtigten Normen können Sie im jeweiligen Zertifikat einsehen, das Sie im Internet unter der oben genannten Adresse finden.

Anschrift für Konformitätserklärungen

Die EU- und die UK-Konformitätserklärung stehen allen zuständigen Behörden zur Verfügung bei:

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 Nürnberg
Deutschland

EU-Konformitätserklärung

Das Produkt erfüllt die Anforderungen und sicherheitsrelevanten Ziele der folgenden EU-Richtlinien und entspricht den harmonisierten europäischen Normen (EN) für speicherprogrammierbare Steuerungen, die in den Amtsblättern der EU aufgeführt sind.

- **2014/34/EU (ATEX-Explosionsschutzrichtlinie)**

  Richtlinie des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen; Amtsblatt der EU L96, 29/03/2014, S. 309-356

- **2014/30/EU (EMV)**

  EMV-Richtlinie des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit; Amtsblatt der EU L96, 29/03/2014, S. 79-106

- **2011/65/EU (RoHS)**

  Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten

UK-Konformitätserklärung

Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

Das Produkt erfüllt die Anforderungen folgender Richtlinien:

- UKEX Regulations

  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.

- EMC Regulations

  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

- RoHS Regulations

  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX-, IECEx-, UKEX- und CCC-Ex-Zertifizierung

Beachten Sie die Angaben im Dokument "Use of subassemblies/modules in a Zone 2 Hazardous Area", das Sie hier finden:

- Auf der Dokumentations-DVD, die dem Produkt beiliegt, unter:
  "Alle Dokumente" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- Im Internet unter der folgenden Adresse:
  Link: (Link: (https://support.industry.siemens.com/cs/ww/de/view/78381013))

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / UKEX / IECEx / CCC-Ex (Seite 42) müssen erfüllt sein.

Das Produkt erfüllt die nachfolgenden Anforderungen an den Explosionsschutz.

II 3G Ex ec IIC T4 Gc

- DEKRA 18ATEX0027 X
- DEKRA 21UKEX0003 X
- IECEx DEK 18.0019X

Importer UK:
Siemens plc,
Manchester
M20 2UR
(Ex nA IIC T4 Gc, nicht auf dem Typschild)

Das Produkt erfüllen die Anforderungen der Normen:

EN/IEC 60079-7, GB 3836.8

EN IEC/IEC 60079-0, GB 3836.1

Die berücksichtigten Normen finden Sie in den aktuell gültigen Zertifikaten.

EMV

Das Produkt erfüllt die Anforderungen der folgenden Richtlinien:

- EU-Richtlinie 2014/30/EU "Elektromagnetische Verträglichkeit" (EMV-Richtlinie)
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

Angewandte Normen:

- EN 61000-6-2

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche

- EN 61000-6-4

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche

RoHS

Das Produkt erfüllt die Anforderungen der folgenden Richtlinien:

- EU-Richtlinie 2011/65/EU zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten.
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

Angewandte Norm: EN IEC 63000

c(UL)us

Angewandte Normen:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E 85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

HAZ. LOC.

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Angewandte Normen:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta: Siehe Temperaturklasse auf dem Typenschild des CP

Report / UL file: E223122 (NRAG, NRAG7)

Beachten Sie die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc / FM (Seite 43).

Hinweis

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA

CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM

Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

Entnehmen Sie die Temperaturklasse dem Typenschild auf der Baugruppe.

Australien - RCM

Das Produkt erfüllt die Anforderungen der Normen nach AS/NZS 2064 (Klasse A).

Kanada

Dieses Digitalgerät Klasse A erfüllt die Anforderungen der Norm Canadian ICES-003.

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Beachten Sie, dass dieses Gerät bezüglich der Emission von Funkstörungen der Grenzwertklasse A entspricht. Dieses Gerät ist einsetzbar in allen Bereichen außer dem Wohnbereich.

Aktuelle Zulassungen

SIMATIC NET-Produkte werden regelmäßig für die Zulassungen hinsichtlich bestimmter Märkte und Anwendungen bei Behörden und Zulassungsstellen eingereicht.

Wenden Sie sich an Ihre Siemens-Vertretung, wenn Sie eine Liste mit den aktuellen Zulassungen für die einzelnen Geräte benötigen, oder informieren Sie sich auf den Internet-Seiten des Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/de/ps/15248/cert)

Maßzeichnungen

10

Maßangaben in den Maßzeichnungen in Millimetern.

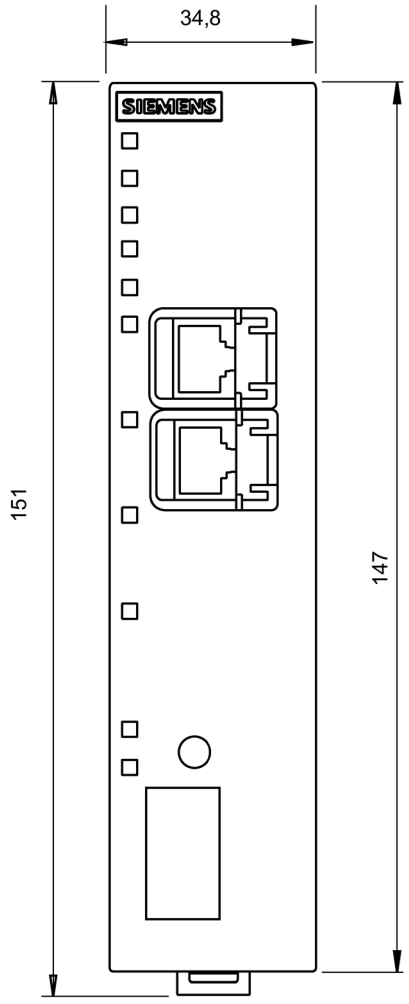


Bild 10-1 Vorderansicht

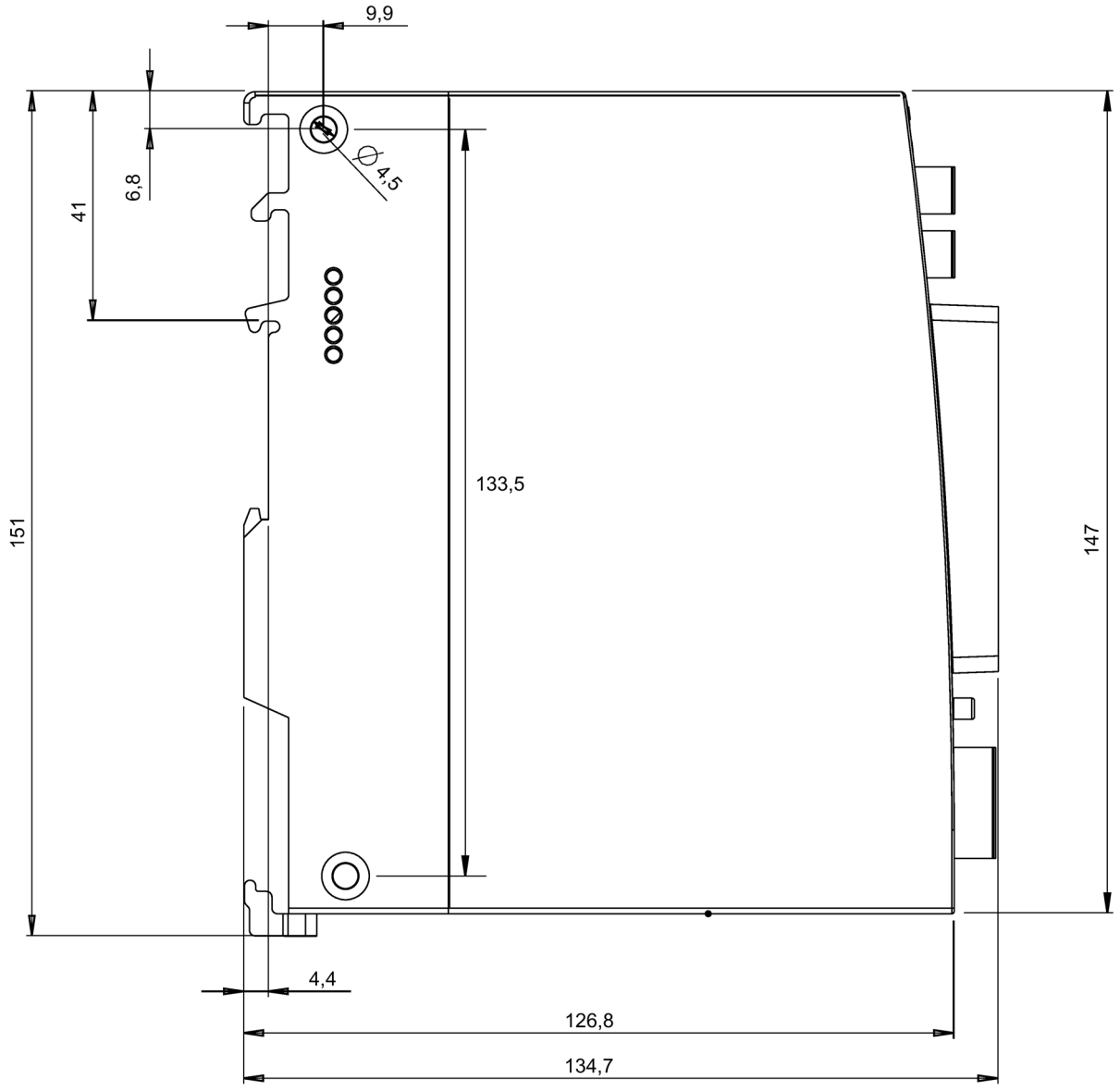


Bild 10-2 Seitenansicht

Zubehör

A

Details und Bestelldaten zu den Produkten des Zubehörprogramms finden Sie in der Siemens Industry Mall, siehe:
Link: (https://mall.industry.siemens.com)

A.1 Stromversorgung

Stromversorgungen für das Gateway

Auszug aus dem Siemens-Programm für Stromversorgungen SITOP und S7-1500:

- SITOP PSU100C

  24 V / 0,6 A, geregelte Stromversorgung, Eingang: AC 120/230 V, Ausgang: DC 24 V / 0,6 A

  Artikelnummer: 6EP1331-5BA00

- SIMATIC PM 1507 24 V / 3 A

  Geregelte Stromversorgung für SIMATIC S7-1500, Eingang: AC 120/230 V, Ausgang: DC 24 V / 3 A

  Artikelnummer: 6EP1332-4BA00

- SIMATIC PM 1507 24 V / 8 A

  Geregelte Stromversorgung für SIMATIC S7-1500, Eingang: AC 120/230 V, Ausgang: DC 24 V / 8 A

  Artikelnummer: 6EP1333-4BA00

A.2 CLPs

Verwendbare CLPs

Das Gerät kann mit einem CLP, einem Wechselmedium zur Aufnahme von Konfigurationsdaten, betrieben werden. Ein CLP ist nicht Teil des Lieferumfangs des Geräts.

Folgende CLPs stehen zur Verfügung:

- SCALANCE CLP 2GB
  Artikelnummer: 6GK1900-0UB00-0AA0
  Wechselmedium zum einfachen Geräte-Tausch
- SCALANCE CLP 32GB
  Artikelnummer: 6GK1900-0UB40-0AA0
  Wechselmedium zum einfachen Geräte-Tausch
- SCALANCE CLP EEC 2GB
  Artikelnummer: 6GK1900-0UQ00-0AA0
  Wechselmedium mit lackierten Leiterplatten zum einfachen Geräte-Tausch

Escape-Sequenzen

B

B.1 JSON-Escape-Sequenzen

JSON-Escape-Sequenzen

Bei der Verwendung des JSON-Formats für die Nutzdaten werden folgende Zeichen beim Publisher in Escape-Sequenzen umgewandelt.

Beim Subscriber werden die Escape-Sequenzen in umgekehrter Richtung umgewandelt.

Zur Übertragung der Nutzdaten siehe Kapitel Nutzdaten-Format (Seite 123).

Zeichen	JSON-Escape-Sequenz	Anmerkung
\n	\\n	Neue Zeile *
\r	\\r	Zeilenumbruch *
\t	\\t	Tabulator *
\"	\\"	Anführungszeichen
\\	\\\\	Doppel-Backslash
\u0000	\\u0000	
\u0001	\\u0001	
\u0002	\\u0002	
\u0003	\\u0003	
\u0004	\\u0004	
\u0005	\\u0005	
\u0006	\\u0006	
\u0007	\\u0007	
\b	\\u0008	
\t	\\u0009	
\n	\\u000A	
\u000b	\\u000B	
\f"	\\u000C	
\r	\\u000D	
\\u000e	\\u000E	
\u000f	\\u000f	
\u0010	\\u0010	
\u0011	\\u0011	
\u0012	\\u0012	
\u0013	\\u0013	
\u0014	\\u0014	
\u0015	\\u0015	
\u0016	\\u0016	
\u0017	\\u0017	
\u0018	\\u0018	

Zeichen	JSON-Escape-Sequenz	Anmerkung
\u0019	\\u0019	
\u001a	\\u001a	
\u001b	\\u001b	
\u001c	\\u001c	
\u001d	\\u001d	
\u001e	\\u001e	
\u001f	\\u001f	
\u007F	\\u007F	

***** Nicht in STEP 7 als Namensbestandteil projektierbar

Syslog-Meldungen

C

Security-Ereignisse

Das Gateway gibt Syslog-Meldungen gemäß RFC 5424 aus. Die Meldungen orientieren sich an der IEC 62443-3-3.

C.1 Aufbau der Meldungen

C.1.1 Aufbau der Syslog-Meldungen

Syslog-Meldungen protokollieren Zustandsänderungen von Geräten als Statusinformation. Syslog-Meldungen gemäß RFC 5424 bzw. RFC 5426 werden von Geräten ausgegeben und über den eingestellten UDP-Port (Standard: 514) an einen Server übertragen. Der Syslog-Server sammelt die Informationen der Geräte und informiert über diese Ereignisse.

Das Syslog-Protokoll schreibt eine festgelegte Reihenfolge und Struktur der möglichen Parameter vor. Syslog-Meldungen gemäß RFC5424 sind folgendermaßen aufgebaut:

Teil / Parameter	Erläuterung
HEADER	
PRI	Priorität der Syslog-Meldung, aufgeteilt in: • Severity (Schweregrad) Mögliche Werte: – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility (Herkunft) Mögliche Werte, bspw.: Subsystem, Dienst, Benutzer
VERSION	Versionsnummer der Syslog-Spezifikation
TIMESTAMP	Zeitstempel des Geräts als lokale Zeit inklusive Zeitzone und Korrektur für Sommer-/Winterzeit Format: YYYY-MM-DDThh:mm:ss.msmsmsms+xx:yy Beispiel: 2010-01-01T02:03:15.0003+02:00

Teil / Parameter	Erläuterung
HOSTNAME	Identifiziert das Quell-Gerät, alternativ über: • FQDN • IPv4-Adresse nach RFC1035: Bytes in dezimaler Darstellung: XXX.XXX.XXX.XXX • IPv6-Adresse nach RFC4291 Section 2.2 • Host-Name Bei fehlenden Angaben wird "-" ausgegeben. Im Produkt: Die projektierte IPv4-Adresse der Prozess-Schnittstelle P2
APP-NAME	Gerät oder Anwendung, von dem die Meldung stammt. Bei fehlenden Angaben wird "-" ausgegeben. Beim Produkt: "-"
PROCID	Die Prozess-ID dient z. B. bei der Analyse und Fehlersuche dazu, die einzelnen Prozesse eindeutig zu identifizieren. Bei fehlenden Angaben wird "-" ausgegeben. Beim Produkt: "-"
MSGID	ID zur Identifizierung der Nachricht. Bei fehlenden Angaben wird "-" ausgegeben. Beim Produkt: "-"
STRUCTURED-DATA	
timeQuality	Das strukturierte Datenelement "timeQuality" liefert Informationen zur Systemzeit mit den beiden Parametern "tzKnown" und "isSynced". Beispiel: [timeQuality tzKnown="0" isSynced="0"] • tzKnown Der Parameter gibt an, ob im Quell-Gerät die Zeitzone bekannt ist. – 1 = bekannt – 0 = unbekannt • isSynced Der Parameter gibt an, ob das Quell-Gerät mit einer zuverlässigen externen Zeitquelle synchronisiert ist, z. B. über NTP. – 1 = synchronisiert – 0 = nicht synchronisiert
MSG	
MESSAGE	Meldungstext als ASCII-String (Englisch)

Weiterführende Informationen zum Aufbau der Syslog-Meldungen und zur Bedeutung der Parameter können Sie in den RFCs nachlesen:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

C.1.2 Variablen in Syslog-Meldungen

Die Variablen werden im Kapitel "Syslog-Meldungen" im Feld "Meldungstext" mit geschweiften Klammern {variable} dargestellt.

Die ausgegebenen Meldungen können folgende Variablen enthalten:

Variable	Beschreibung	Format	Mögliche Werte oder Beispiel
{IP address}	IPv4-Adresse nach RFC1035 IPv6-Adresse nach RFC4291 Abschnitt 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name: Vollständig angegebener Host-Name; Angabe als Domain (FQDN) oder als IPAdresse.	FQDN: host1.com IPv4: %d.%d.%d.%d	server1 192.168.1.105
{Protocol}	Verwendetes Layer-4-Protokoll oder Dienst, der das Ereignis generiert hat.	%s	UDP | TCP | WBM | PB | OPC
{User name}	Zeichenkette (ohne Leerzeichen), die den authentifizierten Benutzer anhand seines Namens identifiziert.	%s	<Admin>
{Time minute} {Timeout}	Anzahl Minuten	%d	1
{Time second}	Anzahl Sekunden	%d	600
{Failed login count}	Anzahl fehlgeschlagener Anmeldeversuche	%d	3
{Max sessions}	Maximale Anzahl der Sitzungen	%d	2
{Version}	Bezeichnung der Version (ohne Leerzeichen)	%s	V1.2.6
{Config detail}	Zeichenkette für die Identifizierung der WBM-Sitzung.	%s	ELXsKPKGzxFey7ap92bqBbbU7uxtazb7QCEaptnpZDGoaO05XK5l6UpbF1HUTFV2

C.2 Syslog-Meldungen

Das Gateway gibt folgende SYSLOG-Meldungen aus, sortiert nach Klassen:

C.2.1 Process communication status

SE_COMMUNICATION_STARTED_(protocol)

Meldungstext	{Protocol}: User {User name} started the process communication.
Beispiel	Console: User Admin started the process communication.
Erläuterung	Der Benutzer hat die Prozess-Kommunikation gestartet.
Severity	Notice
Facility	local0
Norm	-

SE_COMMUNICATION_STOPPED_(protocol)

Meldungstext	{Protocol}: User {User name} stopped the process communication.
Beispiel	Console: User Admin stopped the process communication.
Erläuterung	Der Benutzer hat die Prozess-Kommunikation angehalten.
Severity	Notice
Facility	local0
Norm	-

C.2.2 IACS User identification and authentication

SE_NETWORK_SUCCESSFUL_LOGON_(protocol)

Meldungstext	{Protocol}: User {User name} logged in from {IP address}.
Beispiel	Console: User Admin logged in from 192.168.0.1.
Erläuterung	Anmeldung mit gültigen Anmeldeinformationen
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

SE_NETWORK_UNSUCCESSFUL_LOGON_(protocol)

Meldungstext	{Protocol}: User {User name} failed to log in from {IP address}.
Beispiel	Console: User Admin failed to log in from 192.168.0.1.
Erläuterung	Falscher Benutzername oder falsches Passwort bei der Anmeldung angegeben.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

SE_LOGOFF (protocol)

Meldungstext	{Protocol}: User {User name} logged out from {IP address}.
Beispiel	Console: User Admin logged out from 192.168.0.1.
Erläuterung	Sitzung mit Abmeldung des Benutzers beendet.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

SE_DEFAULT_USER_AUTHENTICATION_USED (protocol)

Meldungstext	{Protocol}: Default user {User name} logged in from {IP address}.
Beispiel	Console: Default user <user name> logged in from 192.168.0.1.
Erläuterung	Standardbenutzer hat sich über die IP-Adresse angemeldet.

Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

C.2.3 Account management

SE_ACCESS_PWD_CHANGED_(protocol)_(own password)

Meldungstext	{Protocol}: User {User name} has changed the password.
Beispiel	Console: User admin has changed the password.
Erläuterung	Benutzer hat sein Passwort geändert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

SE_ACCOUNT_NAME_CHANGE_(protocol)_(user)

Meldungstext	{Protocol}: Default user account was changed to {User name}.
Beispiel	Console: Default user account was changed to <new user>.
Erläuterung	Der Standard-Account wurde geändert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_CREATED_(protocol)

Meldungstext	{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.
Beispiel	WBM: User "ADMIN" created user-account "User1" with role "GUEST".
Erläuterung	Der Administrator hat einen neuen Benutzer "User1" mit der Rolle "GUEST" angelegt.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_CHANGED_(protocol)

Meldungstext	{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.
Beispiel	WBM: User "ADMIN" changed user-account "User1" with role "GUEST".
Erläuterung	Der Administrator hat das vorhandene Benutzerkonto "User1" mit der Rolle "GUEST" geändert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_DELETED_(protocol)

Meldungstext	{Protocol}: User {User name} deleted user-account {Destination user name}.
Beispiel	WBM: User "ADMIN" deleted user-account "User1".
Erläuterung	Der Administrator hat das vorhandene Benutzerkonto "User1" gelöscht.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

C.2.4 Unsuccessful login attempts

SE_ACCOUNT_LOCKED_TEMP_(protocol)_(User)

Meldungstext	{Protocol}: User {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Beispiel	Console: User Admin account is locked for 1 minutes after 3 unsuccessful login attempts.
Erläuterung	Nach zu vielen fehlgeschlagenen Anmeldungen wurde das entsprechende Benutzerkonto für einen bestimmten Zeitraum gesperrt.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.11

C.2.5 Remote session termination

SE_RAS_SESSION_TERMINATED_INACTIVITY_(protocol)

Meldungstext	{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.
Beispiel	WBM: Remote session o1cs3jjKy... was closed after 600 seconds of inactivity.
Erläuterung	Die Sitzung wurde nach Inaktivitätszeit beendet.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.6

C.2.6 Concurrent session control

SE_ACCESS_DENIED_NUMBER_OF_CONCURRENT_SESS_(protocol)

Meldungstext	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Beispiel	WBM: The maximum number of 2 concurrent login session exceeded.
Erläuterung	Die maximale Anzahl gleichzeitiger Sitzungen ist erreicht.

Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.7

C.2.7 Non-repudiation (config change)

SE_CONFIG_CHANGE_(protocol)_(complete configuration)

Meldungstext	{Protocol}: User {User name} has changed configuration.
Beispiel	WBM: User Admin has changed configuration.
Erläuterung	Benutzer hat die Projektierungsdaten durch Laden einer neuen *.cfg-Datei geändert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_(protocol)_(specific configuration)

Meldungstext	{Protocol}: User {User name} has changed {Config detail} configuration.
Beispiel	WBM: User Admin has changed opcua_server configuration
Erläuterung	Benutzer hat spezifische Teile der Konfiguration geändert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_DELETE_(protocol)_(reset to factory)

Meldungstext	{Protocol}: User {User name} has deleted {Config detail} configuration.
Beispiel	WBM: User Admin has deleted opcua_server configuration
Erläuterung	Benutzer hat spezifische Teile der Konfiguration gelöscht.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_RTF_(protocol)_(reset to factory)

Meldungstext	{Protocol}: User {User name} has initiated a reset to factory defaults.
Beispiel	WBM: User Admin has initiated a reset to factory defaults.
Erläuterung	Benutzer hat ein Rücksetzen auf Werkseinstellungen initiiert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

C.2.8 Communication integrity

SE_COMMUNICATION_DATA_INTEGRITY_ERROR_(protocol)

Meldungstext	{Protocol}: Integrity verification failed.
Beispiel	MQTT: Integrity verification failed.
Erläuterung	Integritätsnachweis fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 3.1

C.2.9 Session authenticity

SE_INVALID_SESSION_ID_(protocol)

Meldungstext	{Protocol}: Session ID verification failed.
Beispiel	WBM: Session ID verification failed.
Erläuterung	Die Sitzungs-ID ist ungültig.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 3.8

C.2.10 IACS Backup

SE_BACKUP_SUCCESSFULLY_DONE_(protocol)

Meldungstext	{Protocol}: User {User name} created backup file.
Beispiel	Console: User <Benutzername> created backup file.
Erläuterung	Benutzer hat eine Sicherungsdatei erstellt.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.3

SE_BACKUP_FAILED_(protocol)

Meldungstext	{Protocol}: User {User name} failed to create backup file.
Beispiel	Console: User <Benutzername> failed to create backup file.
Erläuterung	Erstellen einer Sicherungsdatei durch Benutzer fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.3

C.2.11 IACS Recovery and Reconstitution

SE_BACKUP_RESTORE_FAILED_(protocol)

Meldungstext	{Protocol}: User {User name} failed to apply backup file.
Beispiel	Console: User <Benutzername> failed to apply backup file.
Erläuterung	Verwenden einer Sicherungsdatei durch Benutzer fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

SE_BACKUP_RESTORE_SUCCESSFULLY_DONE_(protocol)

Meldungstext	{Protocol}: User {User name} applied backup file.
Beispiel	Console: User <Benutzername> applied backup file.
Erläuterung	Sicherungsdatei durch Benutzer erfolgreich verwendet.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

SE_FW_DEPLOYMENT_SUCCEEDED_(protocol)_(user)

Meldungstext	{Protocol}: User {User name} activated the Firmware {Version}.
Beispiel	Console: User <Benutzername> activated the Firmware V2.
Erläuterung	Firmware durch Benutzer erfolgreich aktiviert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

SE_FW_DEPLOYMENT_FAILED_(protocol)_(user)

Meldungstext	{Protocol}: User {User name} failed to activate Firmware {Version}.
Beispiel	Console: User <Benutzername> failed to activate Firmware V2.
Erläuterung	Firmware-Aktivierung durch Benutzer fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

Verwendete Verschlüsselungsverfahren (Ciphers) D

D.1 Einleitung des Abschnitts "Ciphers"

In den nachfolgenden Tabellen sind die von CC7 verwendeten Verschlüsselungsverfahren (Ciphers) aufgelistet.

Für jede Kommunikationsklasse werden folgende Daten für CC7 angegeben:

- Dienste / Protokolle (Rolle)
  - Dienste / Protokolle: Die von CC7 verwendeten Dienste oder Protokolle
  - (Rolle): Die von CC7 eingenommene Kommunikationsrolle: Client, Server oder beides

In den Tabellen werden folgende Daten angegeben:

- **Kategorie**

  Authentifizierungs-/Verschlüsselungs-Verfahren, Protokollversion oder Cipher Suite

- **Name**

  Name der Kategorie gemäß IANA

  Eine Übersicht der TLS-Parameter und Cipher Suites finden Sie auf folgender Seite: Link: (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4)

- **Wert (hex)**

  Wert (hexadezimal) der Suite gemäß IANA

- **Aktivierung**

  Verwendung in CC7

  - -

    Als sicher eingestufter Cipher, in der Voreinstellung nicht aktiviert.

  - ✓

    Als sicher eingestufter Cipher, in der Voreinstellung aktiviert.

  - Legacy

    Als nicht mehr sicher eingestufter Cipher

    Die Verwendung müssen Sie in CC7 explizit aktivieren.

D.2 SSL

Kommunikation zwischen CC7 und Kommunikationspartnern

Dienste / Protokolle (Rolle):

- WBM/HTTPS (Server) (RSA Zertifikat)

Kategorie	Name	Wert (hex)	Aktivierung
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA8	✓
Cipher Suite	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCCAA	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CCM	0xc09F	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006B	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CCM	0xC09E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Protokollversion	TLSv1.2	-	✓
Protokollversion	TLSv1.3	-	✓

Dienste / Protokolle (Rolle):

- WBM/HTTPS (Server) (ECDH Zertifikat)

Kategorie	Name	Wert (hex)	Aktivierung
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC024	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA9	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC023	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0AC	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0AD	✓

Protokollversion	TLSv1.2	-	✓
Protokollversion	TLSv1.3	-	✓

Dienste / Protokolle (Rolle):

- MQTT (Client)
- HTTP (Client)

Kategorie	Name	Wert (hex)	Aktivierung
Cipher Suite	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x0040	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x006A	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006B	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00A2	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00A3	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC023	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC024	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC027	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC028	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CCM	0xC09E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CCM	0xC09F	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0AC	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0AD	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA8	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCCA9	✓
Cipher Suite	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCCAA	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Cipher Suite	TLS_RSA_WITH_AES_256_CBC_SHA	0x0035	Legacy
Cipher Suite	TLS_RSA_WITH_AES_128_CBC_SHA	0x002F	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0xC00A	Legacy
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xC014	Legacy
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x0039	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xC009	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xC013	Legacy
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x0033	Legacy

Protokollversion	TLSv1.1	-	Legacy
Protokollversion	TLSv1.2	-	✓
Protokollversion	TLSv1.3	-	-

D.3 OPC UA

Dienste / Protokolle (Rolle):

- OPC UA (Server)

Kategorie	Name	Wert (hex)	Aktivierung
Security Policy	Basic256Sha256	-	✓
Security Policy	None	-	Legacy
Security Policy	Basic128Rsa15	-	Legacy
Security Policy	Basic256	-	Legacy
Security Policy	Aes128_Sha256_RsaOaep	-	-
Security Policy	Aes256_Sha256_RsaPss	-	-

Dienste / Protokolle (Rolle):

- OPC UA (Client)

Kategorie	Name	Wert (hex)	Aktivierung
Security Policy	Basic256Sha256	-	✓
Security Policy	None	-	Legacy
Security Policy	Basic128Rsa15	-	Legacy
Security Policy	Basic256	-	Legacy
Security Policy	Aes128_Sha256_RsaOaep	-	-
Security Policy	Aes256_Sha256_RsaPss	-	-

Index

T

U

V

W

Z