Table of contents

Editor – Netzwerkschnittstellen

Editor – *„Netzwerkschnittstellen“*

Im Editor können detaillierte Einstellungen der Netzwerkverbindung vorgenommen werden.

Aufruf:

ctrlX CORE Seitennavigation *Einstellungen ➔ Netzwerkschnittstellen ➔ Doppelklick auf eine der angezeigte Netzwerksverbindungen*

Beschreibung

Der Editor ist in folgende Registerkarten unterteilt:

Registerkarte *„Allgemeines“*

Die Registerkarte zeigt allgemeine Informationen einer Schnittstelle. Außerdem können Sie hier die Schnittstelle aktivieren und deaktivieren.

ACHTUNG!

Durch die Deaktivierung einer Schnittstelle geht die Verbindung zur Steuerung über diese Schnittstelle verloren.

- Verbindungszustand
- Verbindungsgeschwindigkeit
- gesendete und empfangene Daten

Durch Klick auf "Erweiterte Einstellungen einblenden" erhalten Sie weitere Informationen und Optionseinstellungen:, , , . Zudem können Sie hier:

- MAC-Adresse
- Gateway
- DNS-Server
- IP-Adressen
- Optionseinstellungen:
  - MTU konfigurieren (Maximum Transmission Unit)
  - Externe Einstellungen verwenden
    Bei aktivierter Option wird die Schnittstellenkonfiguration einer anderen Instanz überlassen (z.B. einer App).
  - IP-Weiterleitung aktivieren
    Hinweis:
    Die IP-Weiterleitung ist standardmäßig deaktiviert.
    Durch die Aktivierung der IP-Weiterleitung wird das ctrlX-Gerät zu einem unsicheren Netzwerkteilnehmer!
    Die Aktivierung erfordert daher eine zusätzliche Bestätigung per Dialog / Sicherheitsabfrage.

Die IP-Weiterleitung wird nur dann benötigt, wenn eine externe Standard-Ethernet-Kommunikation über den „virtuellen Ethernet-Switch“ des ctrlX EtherCAT-Masters an das EtherCAT-Netzwerk weitergeleitet werden soll. Dies ist beispielsweise der Fall, wenn EtherCAT-Slaves mittels Drittanbieter-Engineering-Programmen über EoE konfiguriert werden sollen. Dabei ermöglicht die IP-Weiterleitung dem ctrlX-Betriebssystem Datenpakete wie ein Router weiterzuleiten. Siehe auch EtherCAT Master-Dokumentation: Web-Dokumentation

Registerkarte *„IPv4“* und *„IPv6“*

Einstellmöglichkeiten:

- Link-local (an/aus)
  Die Option aktiviert eine zusätzliche IP-Adresse im Bereich 169.254.0.0/16.
  Die Adresse wird automatisch zugeordnet und sollte nur für Ad-hoc- oder isolierte Netzwerke verwendet werden.
- DHCP (an/aus)
  Adressbezug über Dynamic Host Configuration Protocol
- IP-Adressen konfigurieren
- DNS-Adressen konfigurieren
  - DNS-Suffixes konfigurieren:
    Durch Klick auf die Schaltfläche [⚙] öffnet sich ein Dialog zur Konfiguration von DNS-Suffixes.
    Die Reihenfolge der Einträge unter DNS-Suffixes ergeben die Suchreihenfolge für die Namensauflösung.
    Für DNS-Clients kann eine DNS-Domänensuffix-Suchliste konfiguriert werden, die DNS-Suchfunktionen erweitert oder überarbeitet. Durch Hinzufügen von Suffixen zur Liste kann nach kurzen, nicht qualifizierten Computernamen in mehreren angegebenen DNS-Domänen gesucht werden. Wenn eine DNS-Abfrage fehlschlägt, kann der DNS-Clientdienst diese Liste verwenden, um andere Namenssuffixenden an Ihren ursprünglichen Namen anzufügen und DNS-Abfragen für diese alternativen, vollqualifizierten Domänennamen zu wiederholen.
    Wenn die Suffixsuchliste leer oder nicht angegeben ist, wird das primäre DNS-Suffix des Computers an kurze, nicht qualifizierte Namen angefügt und eine DNS-Abfrage zum Auflösen des resultierenden vollqualifizierten Domänennamens verwendet. Wenn diese Abfrage fehlschlägt, kann der Computer zusätzliche Abfragen für alternative vollqualifizierte Domänennamen ausprobieren, indem ein verbindungsspezifisches DNS-Suffix angefügt wird, das für Netzwerkverbindungen konfiguriert ist.
    Der Begriff "DNS-Suffix" wird im wesentlichen in einem Windows-Umfeld im Zusammenhang mit einer Windows-Domäne verwendet. Das DNS-Suffix ist im Prinzip der Domänen-Name. Der Name des Rechners (Hostname) zusammen mit dem DNS-Suffix ergibt den Fully-Qualified Domain Name.
    Beispiel:
    DNS-Suffix: mydomain.com
    Fully-Qualified Domain Name: mycomputer.mydomain.com
    Das DNS-Suffix wird beim Beitritt in die Domäne auf dem Rechner eingetragen. Es können mehrere DNS-Suffixes eingegeben werden. Die Reihenfolge der DNS-Suffixes ist relevant
- Gateway-Verbindungen konfigurieren

Detailinformationen betreffend IPv4 und IPv6

- Die IP-Adressen werden im Classless Inter-Domain Routing (CIDR) numerischen Format angegeben. Diese Information erhalten Sie, wenn Sie mit der Maus über dem IP-Adressfeld stehen. Beispielsweise 192.168.1.1/16
- Die einzelnen DNS-Adressen zeigen auf Server des mehrstufigen Domain-Name-Systems. Dieses System ist für die Auflösung von Domänennamen in IP-Adressen sowie umgekehrt zuständig. Die Anfrage wird so lange an den überlagerten DNS-Server weitergeleitet, bis der Domänenname aufgelöst werden kann, der für die Top-Level Domain (z. B. .com) zuständige DNS-Server erreicht wurde und der Domänenname nicht aufgelöst werden kann
- Die Antwort wird an den ursprünglichen Anfragensteller zurückgegeben, so dass dieser sie für die weitere Netzwerkkommunikation verwenden kann. Über der richtigen Konfigurationssyntax erhalten Sie mehr Informationen, wenn Sie mit der Maus über einem DNS-Adressfeld stehen
- "Gateway" signalisiert den Endpunkt, über den die Netzwerkkommunikation in ein anderes Subnetz weitergereicht wird. Geben Sie den erforderlichen Endpunkt ein

Registerkarte *„Routing“*

Mittels "Routing" kann die Kommunikation zu den eingestellten Netzsegmenten über ein definiertes Gateway geleitet werden.

Wenn für einen IP-Adressbereich (IPv4 oder IPv6) Routen definiert sind, dann sollte in den IPv4 oder IPv6 Einstellungen kein Gateway eingetragen sein. Dies könnte zu Routing-Konflikten führen.

"Routing" erfordert folgende Eingaben:

- **Ziel**:
  Das Netzsegment für diesen Routing-Eintrag.
  Tragen Sie immer die erste Netzwerkadresse des Netzsegmentes ein.
  Die Schreibweise erfolgt in CIDR-Notation (Beispielsweise 192.168.0.0/24).
- **Gateway**:
  Die erforderliche IP-Adresse, zu der kommuniziert werden soll.
  Bei dieser Adresse handelt es sich um den Endpunkt, über den die Kommunikation zum definierten Netzsegment geleitet wird.
  Die richtige Schreibweise wird angezeigt, wenn Sie mit der Maus über dem IP-Adressfeld stehen.
- **Metrik**:
  "Metrik" definiert die Priorität, mit der die einzelnen Routen verwendet werden.
  Umso kleiner die Zahl, um so höher ist die Priorität.

Bei bereits vorhandenen Routing-Einträgen sollten die jeweiligen IP-Adresskonfigurationen (IPv4/IPv6) vorhanden sein.

Registerkarte *„Security“*

Mittels Netzwerksicherheit besteht die Möglichkeit nur authentifizierte Verbindungen auf die Ethernet-Schnittstelle zuzulassen.

Wireless Interfaces bieten diese Option nicht!

Über den Schiebeschalter können Sie die Netzwerksicherheit aktivieren.

Dabei wird geprüft ob die Konfiguration gültige Einträge enthält.

Als Zugriffskontrolle wird zum aktuellen Zeitpunkt nur IEEE 802.1X mit der Authentifizierungsmethode EAP-TLS unterstützt.

Erforderliche Einstellungen bei aktivierter Netzwerksicherheit:

- **Zugriffssteuerung**
  IEEE 802.1X (voreingestellt)
- **Authentifizierungsmethode**
  EAP-TLS (voreingestellt)
- **Identität**
  Auswahl eines, auf dem remote Server registrierten Accounts

Unterstützte Zertifikate (muss zuvor auf die ctrlX CORE Steuerung hochgeladen werden, siehe oben)

- **CA-Zertifikat**
  Auswahl des Zertifikats (Kategorie "CA-Zertifikat")
- **Client-Zertifikat**
  Auswahl des Zertifikats (Kategorie "Vertrauenswürdig" oder "Eigenes")
- **Privater Client-Schlüssel**
  Auswahl des Zertifikats (Kategorie "Vertrauenswürdig" oder "Eigenes")
- **Passwort für privaten Client-Schlüssel**
  Wenn "Privater Client-Schlüssel" mittels Passwort geschützt ist, tragen Sie das Passwort im Eingabefeld ein.

Registerkarte *„Konfiguration“*

Hier können Sie das Ethernet Interface der Steuerung deaktivieren/aktivieren und konfigurieren.

ACHTUNG!

Mit der Deaktivierung der Optionen geht die Ethernet-Verbindung zur Steuerung verloren.

Einstellbare Optionen:

- Externe Einstellungen verwenden (aktivieren/deaktivieren)
- Netzwerkschnittstelle aktivieren (aktivieren/deaktivieren)
- IP-Weiterleitung aktivieren (aktivieren/deaktivieren)
  Hinweis:

Die IP-Weiterleitung ist standardmäßig deaktiviert.
Durch die Aktivierung der IP-Weiterleitung wird das ctrlX-Gerät zu einem unsicheren Netzwerkteilnehmer!
Die Aktivierung erfordert daher eine zusätzliche Bestätigung per Dialog / Sicherheitsabfrage.

Die IP-Weiterleitung wird nur dann benötigt, wenn eine externe Standard-Ethernet-Kommunikation über den „virtuellen Ethernet-Switch“ des ctrlX EtherCAT-Masters an das EtherCAT-Netzwerk weitergeleitet werden soll. Dies ist beispielsweise der Fall, wenn EtherCAT-Slaves mittels Drittanbieter-Engineering-Programmen über EoE konfiguriert werden sollen. Dabei ermöglicht die IP-Weiterleitung dem ctrlX-Betriebssystem Datenpakete wie ein Router weiterzuleiten.

Siehe auch EtherCAT Master-Dokumentation: Azyklische Kommunikation (Mailbox)

Registerkarte *„Wi-Fi“* (nur bei vorhandenem WiFi-Interface)

Hier haben Sie die Möglichkeit Wireless Interfaces zu konfigurieren und Funknetze hinzufügen, mit denen sich die Steuerung verbinden soll.

Funknetze werden nicht unterstützt, wenn im Netz-Namen das Sonderzeichen "**/**" enthalten ist.

Unterstützte Verschlüsselungsarten für Funknetze:

- **Ohne Verschlüsselung**
  Einzustellender Wert:
  - Security-Modus: "Keine"
- **Verschlüsselung WPA2/PreShared Key**
  Einzustellende Werte:
  - Security-Modus: WPA/WPA2 Personal
  - Passwort: <password>
- **Verschlüsselung WPA2/EAP-TLS**
  Einzustellende Werte:
  - Security-Modus: WPA/WPA2 Enterprise (TLS)
  - Identität: Auswahl eines, auf dem remote Server registrierten Accounts

  Unterstützte Zertifikate
  (muss zuvor auf die ctrlX CORE Steuerung hochgeladen werden, siehe oben)
  - **CA-Zertifikat**:
    Auswahl des Zertifikats Kategorie "CA-Zertifikat"
  - **Client-Zertifikat**:
    Auswahl des Zertifikats Kategorie "Vertrauenswürdig" oder "Eigenes"
  - **Privater Client-Schlüssel**:
    Auswahl des Zertifikats Kategorie "Vertrauenswürdig" oder "Eigenes"
  - **Passwort für privaten Client-Schlüssel**:
    Wenn "Privater Client-Schlüssel" mittels Passwort geschützt ist, tragen Sie das Passwort in das Eingabefeld ein.

Die Steuerung verbindet sich immer mit dem stärksten Netz!

Wenn sich die Steuerung mit einem bestimmten Netz verbinden soll, müssen alle anderen eingetragenen Netze gelöscht werden.

In der Liste der bekannten Netzwerke wird nach der SSID der Status "Verbunden" angezeigt, sofern die Steuerung mit diesem Funknetz verbunden ist.