Table of contents

Kommunikation verschlüsseln, Security-Einstellungen verändern

Kommunikation verschlüsseln, Security-Einstellungen verändern

ACHTUNG!

Empfehlungen zur Datensicherheit

Um das Risiko von Datensicherheitsverletzungen zu minimieren, empfehlen wir die folgenden organisatorischen und technischen Maßnahmen für das System, auf dem Ihre Applikationen laufen: Vermeiden Sie soweit als möglich, die SPS und die Steuerungsnetzwerke offenen Netzwerken und dem Internet auszusetzen. Verwenden Sie zum Schutz zusätzliche Sicherungsschichten, wie ein VPN für Remote-Zugriffe. Installieren Sie Firewall-Mechanismen. Beschränken Sie den Zugriff auf autorisierte Personen. Verwenden Sie Passwörter mit hoher Stärke. Ändern Sie eventuell vorhandene Standard-Passwörter bei der ersten Inbetriebnahme und auch danach regelmäßig.

Verwenden Sie die von PLC Engineering und dem betreffenden Steuerungsgerät unterstützten Security-Funktionalitäten, wie Verschlüsselung der Kommunikation mit dem Steuerungsgerät und gezielt eingeschränkten Benutzerzugriff.

Die Kommunikation mit dem Gerät kann über Verschlüsselung und über eine Benutzerverwaltung auf dem Gerät geschützt werden. Wenn Sie die aktuelle Security-Voreinstellung ändern wollen, können Sie dies auf der Registerkarte *„Kommunikation“* des Geräteeditors tun.

▼ Verbindung zur Steuerung herstellen, anmelden, vertrauenswürdiges Zertifikat für verschlüsselte Kommunikation installieren

Voraussetzung: Eine verschlüsselte Kommunikation mit der Steuerung und eine Benutzerverwaltung auf der Steuerung sind erzwungen. Es gibt jedoch noch kein individuelles Passwort. Auf Ihrem Computer ist noch kein entsprechendes Zertifikat installiert und die Verbindung zur Steuerung ist noch nicht konfiguriert.

1. Doppelklicken Sie im Gerätebaum auf die Steuerung.
   ⇒ Der Geräteeditor öffnet sich.
2. Wählen Sie die Registerkarte *„Kommunikation“*.
3. Klicken Sie auf die Schaltfläche *„Netzwerk durchsuchen“*.
4. Selektieren Sie die gewünschte Steuerung.
   ⇒ Eine Meldungsbox erscheint mit der Info, dass das Zertifikat des Geräts für die Kommunikation nicht vertrauenswürdig signiert wurde. Sie werden gefragt, ob Sie dieses Zertifikat als vertrauenswürdig im lokalen 'Controller Certificates'-Store auf Ihrem Computer installieren wollen, oder nur für diese eine Sitzung akzeptieren.

   ACHTUNG!

   Ein auf diese Weise installiertes Steuerungszertifikat erhält eine Laufzeit von nur 30 Tagen! Damit haben Sie Zeit für folgende längerfristige Lösungen:

   - Erzeugen eines weiteren selbst signierten Zertifikats mit längerer Laufzeit (beispielsweise 365 Tage). Dies können Sie im Security-Screen tun, wenn Sie den CODESYS Security Agent installiert haben, auch wenn ein Zertifikat bereits vorhanden ist. Die Verwendung der PLC-Shell des Geräteeditors ist eine nicht komfortable Ersatzvorgehensweise.
     Sehen Sie dazu weiter unten: "Verschlüsselte Kommunikation mit einem längerfristig gültigen Steuerungszertifikat konfigurieren..."
   - Einspielen eines CA-signierten Zertifikats. Dies ist aktuell nur über die PLC-Shell-Kommandos des Laufzeitsystems möglich. Daher empfehlen wir erstmal selbst signierte Zertifikate zu verwenden.

5. Wenn Sie das Zertifikat installieren wollen, wählen Sie die erste Option und bestätigen Sie die Meldungsbox mit *„OK“*.
   ⇒ Das Zertifikat wird als vertrauenswürdig eingetragen. Nach diesem erstmaligen Akzeptieren des selbst signierten Zertifikats können Sie sich ohne weitere Abfrage immer wieder mit der Steuerung verschlüsselt verbinden.

   Sie erhalten eine Meldungsbox mit dem Hinweis, dass für das Gerät eine Benutzerverwaltung obligatorisch ist, diese aber noch nicht aktiviert ist. Sie werden gefragt, ob Sie die Benutzerverwaltung jetzt aktivieren wollen. Sie erhalten den Hinweis, dass Sie in diesem Fall einen neuen Administrator-Benutzer anlegen müssen und sich dann als dieser Benutzer einloggen müssen.

6. Schließen Sie die Abfrage mit *„Ja“*.
   ⇒ Der Dialog *„Gerätebenutzer hinzufügen“* öffnet sich zum Anlegen eines initialen Geräteadministrators.

7. Legen Sie einen Gerätebenutzer an, um als dieser Benutzer die Benutzerverwaltung bearbeiten zu können. In diesem Fall steht nur die Gruppe *„Administrator“* zur Verfügung. Definierten Sie für den Benutzer *„Name“* und *„Passwort“*. Die Passwortstärke wird angezeigt. Beachten Sie auch die eingestellten Optionen bezüglich einer Passwortänderung. Standardmäßig kann das Passwort vom Benutzer zu einer beliebigen Zeit geändert werden. Bestätigen Sie mit *„OK“*.
   ⇒ Der Dialog *„Gerätebenutzeranmeldung“* öffnet sich.
8. Geben Sie die im vorigen Schritt definierten Zugangsdaten für den Geräteadministrator ein.
   ⇒ Sie sind auf der Steuerung eingeloggt. Auf der Registerkarte *„Benutzer und Gruppen“* können Sie mit Hilfe der Schaltfläche  in den synchronisierten Betrieb wechseln. Darin wird die Gerätebenutzerverwaltung angezeigt und Sie können sie bearbeiten.

   Nach Bestätigung mit *„OK“* wird die Gerätebenutzerverwaltung im Editorfenster dargestellt. Sie enthält den gerade definierten Benutzer der Gruppe *„Administrator“*. Dessen Name erscheint auch in der Taskleiste des Fensters als *„Gerätebenutzer“*.
9. Alle gespeicherten Steuerungszertifikate (aus Schritt 5) werden unter Windows im lokalen Zertifikatsspeicher auf Ihrem Computer gespeichert. Diesen Speicher erreichen Sie über *„Ausführen“*, Befehl certmgr.msc.
   ⇒ Alle registrierten Zertifikate für verschlüsselte Kommunkation mit Steuerungen finden Sie hier unter *„Controller Certificates/Zertifikate“*.

▶ Längerfristig gültiges Steuerungszertifikat für die verschlüsselte Kommunikation mit Hilfe des CODESYS Security Agent installieren (Empfohlen!)

▶ Steuerungszertifikat für die verschlüsselte Kommunikation über die SPS-Shell des Geräteeditors installieren

Siehe auch

- ↘ „Gerätebenutzerverwaltung handhaben“
- ↘ „Applikation verschlüsseln“
- ↘ „Projektverschlüsselung mit Zertifikaten“