

# Lern-/Lehrunterlagen

Siemens Automation Cooperates with Education (SCE) | Ab Version V15.1

**TIA Portal Modul 142-200** Industrial Security mit SIMATIC S7-1500 und SCALANCE S615

siemens.de/sce



## Passende SCE Trainer Pakete zu dieser Lern-/Lehrunterlage

### Industrielle Kommunikation SIMATIC NET

- IE SCALANCE S615 mit Software SINEMA RC Basis Bestellnr.: 6GK1950-0BB13
- IE SCALANCE S615 LAN-Router Bestellnr.: 6GK1950-0BB23

## SIMATIC Steuerungen

- SIMATIC CPU 1516F PN/DP Safety Bestellnr.: 6ES7516-3FN00-4AB2
- SIMATIC ET 200SP Open Controller CPU 1515SP PC F und HMI RT SW Bestellnr.: 6ES7677-2SB42-4AB1
- SIMATIC ET 200SP Distributed Controller CPU 1512SP F-1 PN Safety Bestellnr.: 6ES7512-1SK00-4AB2
- SIMATIC S7 CPU 1516-3 PN/DP Bestellnr.: 6ES7516-3AN00-4AB3
- SIMATIC CPU 1512C PN mit Software und PM 1507 Bestellnr.: 6ES7512-1CK00-4AB1
- SIMATIC CPU 1512C PN mit Software, PM 1507 und CP 1542-5 (PROFIBUS) Bestellnr.: 6ES7512-1CK00-4AB2
- SIMATIC CPU 1512C PN mit Software Bestellnr.: 6ES7512-1CK00-4AB6
- SIMATIC CPU 1512C PN mit Software und CP 1542-5 (PROFIBUS) Bestellnr.: 6ES7512-1CK00-4AB7

### SIMATIC STEP 7 Software for Training

- SIMATIC STEP 7 Professional V15.1 Einzel-Lizenz Bestellnr.: 6ES7822-1AA05-4YA5
- SIMATIC STEP 7 Professional V15.1 6+20er Klassenraum-Lizenz Bestellnr.: 6ES7822-1BA05-4YA5
- SIMATIC STEP 7 Professional V15.1 6+20er Upgrade-Lizenz Bestellnr.: 6ES7822-1AA05-4YE5
- SIMATIC STEP 7 Professional V15.1 20er Studenten-Lizenz Bestellnr.: 6ES7822-1AC05-4YA5

Bitte beachten Sie, dass diese Trainer Pakete ggf. durch Nachfolge-Pakete ersetzt werden. Eine Übersicht über die aktuell verfügbaren SCE Pakete finden Sie unter: <u>siemens.de/sce/tp</u>

## Fortbildungen

Für regionale Siemens SCE Fortbildungen kontaktieren Sie Ihren regionalen SCE Kontaktpartner: siemens.de/sce/contact

## Weitere Informationen rund um SCE

siemens.de/sce

## Verwendungshinweis

Die SCE Lern-/Lehrunterlage für die durchgängige Automatisierungslösung Totally Integrated Automation (TIA) wurde für das Programm "Siemens Automation Cooperates with Education (SCE)" speziell zu Ausbildungszwecken für öffentliche Bildungs- und F&E-Einrichtungen erstellt. Siemens übernimmt bezüglich des Inhalts keine Gewähr.

Diese Unterlage darf nur für die Erstausbildung an Siemens Produkten/Systemen verwendet werden. D. h. Sie kann ganz oder teilweise kopiert und an die Auszubildenden/Studierenden zur Nutzung im Rahmen deren Ausbildung/Studiums ausgehändigt werden. Die Weitergabe sowie Vervielfältigung dieser Unterlage und Mitteilung Ihres Inhalts ist innerhalb öffentlicher Aus- und Weiterbildungsstätten für Zwecke der Ausbildung oder im Rahmen des Studiums gestattet.

Ausnahmen bedürfen der schriftlichen Genehmigung durch Siemens<u>mailto</u>:. Alle Anfragen hierzu an <u>scesupportfinder.i-ia@siemens.com</u>.

Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte auch der Übersetzung sind vorbehalten, insbesondere für den Fall der Patentierung oder GM-Eintragung.

Der Einsatz für Industriekunden-Kurse ist explizit nicht erlaubt. Einer kommerziellen Nutzung der Unterlagen stimmen wir nicht zu.

Wir danken der TU Dresden, der Fa. Michael Dziallas Engineering und allen weiteren Beteiligten für die Unterstützung bei der Erstellung dieser SCE Lern-/Lehrunterlage.

# Inhaltsverzeichnis

| 1 | Zielstellung |       | ng     | . 6                                     |     |
|---|--------------|-------|--------|---|-----|
| 2 |              | Vora  | ausse  | tzung                                   | . 6 |
| 3 |              | Beni  | ötigte | Hardware und Software                   | . 7 |
| 4 |              | Theo  | orie   |   | . 8 |
|   | 4.           | 1     | Aufb   | au und Bedienung des SCALANCE S615      | . 8 |
|   |              | 4.1.1 | 1      | Industrial Ethernet Security S615       | . 8 |
|   |              | 4.1.2 | 2      | Taster SET                              | . 9 |
|   |              | 4.1.3 | 3      | LED Meldeleuchten                       | 10  |
|   |              | 4.1.4 | 1      | Netzwerk Ports                          | 11  |
|   | 4.           | 2     | VLA    | N: Virtuelle Netzwerke                  | 12  |
|   | 4.           | 3     | Rout   | er                                      | 12  |
|   | 4.           | 4     | Firev  | vall                                    | 13  |
|   |              | 4.4.1 | 1      | Implizite Regel                         | 14  |
|   |              | 4.4.2 | 2      | Stateful Inspection                     | 14  |
|   | 4.           | 5     | CIDF   | R Notation                              | 14  |
|   | 4.           | 6     | IP-A   | dresse einstellen am Programmiergerät   | 16  |
| 5 |              | Aufg  | jaben  | stellung                                | 19  |
| 6 |              | Plan  | ung    |   | 19  |
| 7 |              | Strul | kturie | rte Schritt-für-Schritt-Anleitung       | 20  |
|   | 7.           | 1     | Dear   | chivieren eines vorhandenen Projekts    | 20  |
|   | 7.           | 2     | Eins   | tellen der IP-Adresse des SCALANCE S615 | 22  |
|   | 7.           | 3     | Grur   | ndkonfiguration des SCALANCE S615       | 24  |
|   | 7.           | 4     | Konf   | iguration des DHCP-Servers              | 32  |
|   | 7.           | 5     | Einri  | chten der Firewall                      | 38  |
|   | 7.           | 6     | Einri  | chten des Service Benutzers             | 42  |
|   | 7.           | 7     | Konf   | iguration der CPU 1516F                 | 47  |
|   | 7.           | 8     | Test   | en des Regelwerkes                      | 51  |
|   | 7.9          | 9     | Che    | ckliste – Schritt-für-Schritt-Anleitung | 56  |
| 8 |              | Übu   | ng     |   | 57  |

## Lern-/Lehrunterlagen | TIA Portal Modul 142-200, Edition 09/2019 | Digital Industries, FA

|   | 8.1 | Aufgabenstellung – Übung | 57 |
|---|-----|--------------------------|----|
|   | 8.2 | Planung                  | 57 |
|   | 8.3 | Checkliste – Übung       | 57 |
| 9 | Wei | terführende Information  | 58 |

# Industrial Security mit S7-1500 und SCALANCE S615

# 1 Zielstellung

In diesem Kapitel lernen Sie Industrial Ethernet Security SCALANCE S615 zu konfigurieren und eine S7-1500 Steuerung sicher mit anderen Netzen zu verbinden.

Es können die unter Kapitel 3 aufgeführten SIMATIC S7-Steuerungen eingesetzt werden.

# 2 Voraussetzung

Dieses Kapitel baut auf das Kapitel OPC UA mit SIMATIC S7-1500 als OPC-Server auf. Zur Durchführung dieses Kapitels können Sie z. B. auf das folgende Projekt zurückgreifen: "SCE\_DE\_092-300\_OPC\_UA\_S7-1500\_R1807.zap15".

# 3 Benötigte Hardware und Software

- Engineering Station: Voraussetzungen sind Hardware und Betriebssystem (weitere Informationen siehe Readme/Liesmich auf den TIA Portal Installations-DVDs)
- 2 Software SIMATIC STEP 7 Professional im TIA Portal ab V15.1
- 3 Steuerung SIMATIC S7-1500, z. B. CPU 1516F-3 PN/DP ab Firmware V2.1 mit Memory Card
- 4 Industrial Ethernet Security SCALANCE S615
- 5 Ethernet-Verbindung zwischen Engineering Station und SCALANCE S615 und zwischen Steuerung und SCALANCE S615





2 SIMATIC STEP 7 Professional (TIA Portal) ab V15.1

3 Steuerung SIMATIC S7-1500

# 4 Theorie

## 4.1 Aufbau und Bedienung des SCALANCE S615

Im folgenden Abschnitt finden Sie eine kurze Beschreibung des SCALANCE S615. Weiterführende Details und Informationen finden Sie in den Handbüchern, die unter <u>support.automation.siemens.com</u> heruntergeladen werden können.

## 4.1.1 Industrial Ethernet Security S615

Der SCALANCE S615 ist ein industrieller Ethernet Router und Firewall für die Prozessautomatisierung.



- (1) Netzwerk Ports
- (2) SET-Taster
- (3) Digitaler Eingang
- (4) Digitaler Ausgang
- (5) Netzeingang für die Spannungsversorgung
- (6) LED-Anzeige

## 4.1.2 Taster SET

Der SET-Taster ist bei einem SCALANCE S615 auf der Gehäusevorderseite angebracht.



Der SET-Taster hat mehrere Funktionen. Bei kurzem Tasten unter 3 Sekunden führt das Gerät einen Neustart durch. Durch langes Drücken über 10 Sekunden setzt sich das Gerät auf die Werkseinstellungen zurück.

Der Taster kann auch genutzt werden, um das Gerät in den Bootloader zu bringen. Im Falle einer defekten Firmware kann mit Hilfe des Bootloaders eine neue Firmware aufgespielt werden. Genauere Informationen zu dem Thema finden Sie im Handbuch.

## 4.1.3 LED Meldeleuchten

Auf dem SCALANCE S615 befinden sich verschiedene LEDs, die einen Überblick über den Zustand des Systems bieten.



| F  | LED zur Anzeige des Fehlerstatus        |
|----|---|
| L  | LED zur Anzeige der Spannungsversorgung |
| 8  | LED zur Anzeige der VPN-Verbindungen    |
| DI | LED zur Anzeige des digitalen Eingangs  |
| DO | LED zur Anzeige des digitalen Ausgangs  |
| Р  | LEDs zur Anzeige des Portstatus         |

Eine genaue Beschreibung zu jeder LED können Sie dem Handbuch des Geräts entnehmen.

## 4.1.4 Netzwerk Ports

Der SCALANCE S615 verfügt über fünf Netzwerk Ports. Davon sind die ersten vier werksseitig als VLAN 1 (INT) und der fünfte als VLAN 2 (EXT) konfiguriert.



Diese Verschaltung kann beliebig verändert werden. Standardmäßig ist das VLAN 2 als unsicheres externes Netz konfiguriert und das VLAN 1 als zu schützendes internes Netz.

Das VLAN 1 ist in den Werkseinstellungen mit der IP 192.168.1.1/24 konfiguriert. Das Gerät im VLAN 2 besitzt hingegen keine feste IP-Adresse, sondern mit Hilfe von DHCP kann eine dynamische IP-Adresse einstellt werden.

## 4.2 VLAN: Virtuelle Netzwerke

Geräte wie z. B. Switche verfügen meist über mehrere Netzwerk Ports, die alle zum Netzwerk gehören. Ein Teilnehmer an Port A kann also ungehindert mit einem Teilnehmer an Port B kommunizieren. Um einzelne Teilnehmer voneinander zu trennen, müssten entsprechend pro Netzwerk eigene physikalische Geräte eingesetzt werden.

Mit Hilfe von Virtual Local Area Networks (VLANs) kann ein physikalisches Netzwerkgerät in virtuelle Netzwerke unterteilt werden. Jeder Port wird dabei einem VLAN fest zugewiesen. Ein Teilnehmer an einem Port im VLAN 1 kann jetzt nur noch mit Teilnehmern im VLAN 1 kommunizieren. Dabei wird jedes VLAN mit einer eindeutigen ID im Gerät konfiguriert. Diese ID ist in der Regel 12 Bit lang und wird dezimal dargestellt.

Es besteht die Option einem Port auch mehrere VLANs zuzuweisen. Pakete, die einen solchen Port verlassen, werden mit einem Tag versehen, welcher die ID des VLANs enthält. Eingehende Pakete werden auf einen vorhandenen Tag untersucht und das Paket dem VLAN mit der im Tag enthaltenen ID zugewiesen. Die Gegenstelle an einem solchen Port muss natürlich auch entsprechend konfiguriert sein, um die Tags korrekt auszuwerten.

So kann dieselbe physikalische Netzwerkstruktur kostengünstig genutzt werden, um einzelne Teilnehmergruppen voneinander zu separieren.

Der SCALANCE S615 ist werksseitig in zwei separate Netzwerke unterteilt. Ein sicheres Netzwerk mit der VLAN ID 1 und ein unsicheres mit der VLAN ID 2 (siehe Abschnitt 4.1.4).

## 4.3 Router

Im Gegensatz zu einem Switch ist ein Router in der Lage verschiedene Netze miteinander zu koppeln. Dazu besitzt er eine physikalische Verbindung und eine passende IP-Adresse zu jedem Netz. Dadurch ist er für andere Teilnehmer im Netz erreichbar und kann Pakete zwischen den angeschlossenen Netzen vermitteln.



## 4.4 Firewall

Eine Firewall kann, Pakete, welche sie passieren, filtern. Dafür kann das Gerät unterschiedliche Kriterien nutzen, z. B. Quell- und Zieladressen oder TCP-Ports. Leistungsstärkere Geräte sind auch in der Lage, komplexere Dinge zu verstehen, z. B. welche Daten der Benutzer gerade an eine Webseite sendet.

Der SCALANCE S615 ist Router und Firewall zugleich und kann Pakete überprüfen, die durch ihn von einem VLAN in ein anderes geroutet werden (Layer 3). D. h. er kann keine Pakete kontrollieren, die innerhalb eines VLAN durch ihn weitergeleitet werden (Layer 2).

Die Firewall im S615 kann Informationen bis zum Layer 4 verarbeiten. Das beinhaltet IP-Adressen und das genutzte Protokoll z. B. TCP oder UDP und die dabei genutzten Ports.

Das Filtern selbst geschieht mit Hilfe eines Regelwerks, das in Form einer Tabelle vorliegt. Jede Zeile entspricht dabei einer Regel.

| Quell-IP        | Ziel-IP        | Protokoll | Quell-Port | Ziel-Port | Aktion |
|-----------------|----------------|-----------|------------|-----------|--------|
| 192.168.1.24/32 | 192.168.2.5/32 | any       |            |           | Accept |
| 192.168.1.0/24  | 0.0.0/0        | tcp       | *          | 443       | Accept |
| 0.0.0/0         | 0.0.0/0        | any       |            |           | Drop   |

Dieses Regelwerk wird von oben nach unten abgearbeitet und die erste passende Regel wird genutzt. Im obigen Beispiel wäre der Teilnehmer mit der IP 192.168.1.24 in der Lage, jegliche Art von Kommunikation mit dem Teilnehmer 192.168.2.5 aufzubauen.

Teilnehmer aus dem Netz 192.168.1.x können jede andere Adresse über TCP und Port 443 (HTTPS) kontaktieren. Die letzte Regel sorgt dafür, dass alle anderen Pakete verworfen werden.

In der Regel bietet es sich an eine von drei Aktionen auszuführen.

- Pakete können akzeptiert (Accept) und damit weitergeleitet werden.
- Es besteht ebenfalls die Möglichkeit sie zu verwerfen bzw. wegzuwerfen (Drop). Der Absender wird dabei über den Verbleib des Pakets nicht informiert.
- Zuletzt bietet sich die Option an, die Pakete zur
  ückzuweisen (Reject). Hierbei bekommt der Absender eine passende R
  ückmeldung, dass seine Pakete abgelehnt wurden.

In den meisten Fällen werden Accept und Drop genutzt und Reject nur für spezielle Fälle verwendet.

## 4.4.1 Implizite Regel

Was passiert mit Paketen, die auf keine konfigurierte Regel passen? Die Antwort ist abhängig vom Hersteller des Filters. Die meisten Hersteller haben am Ende des Regelwerks eine implizite Regel, die entweder alles zulässt oder alles fallen lässt. Meist kann dieses Verhalten angepasst werden.

Im Falle des SCALANCE S615 verwirft (Drop) die implizite Regel alle Pakete.

## 4.4.2 Stateful Inspection

Die meisten Firewalls filtern nicht einfach nur einkommende Pakete, sondern merken sich auch, welcher Computer welche Verbindung aufgebaut hat. Ein Computer der z. B. eine Webseite aufruft, bekommt vom Server Antwortpakete. Damit diese Antwortpakete nicht auch in den Filterregeln definiert werden müssen, überprüfen moderne Firewalls Pakete nur während des Verbindungsaufbaus.

Versucht der Teilnehmer 192.168.1.5 eine verschlüsselte Webseite auf dem Teilnehmer 192.168.3.25 über Port 443 zu erreichen, so wird dieser Verbindungsaufbau anhand des Regelwerks überprüft. Akzeptiert das Regelwerk diese Verbindung so merkt sich die Firewall, in einer speziellen Sitzungstabelle, die Gültigkeit dieser Verbindung. Jedes nachfolgende Paket, welches zu dieser Verbindung gehört, egal ob vom Client oder Webserver, egal auf welchem Quell- oder Zielport, wird jetzt durch die Firewall akzeptiert.

Durch diese Technik muss der Administrator nur das für den Verbindungsaufbau nötige Regelwerk erstellen.

## 4.5 CIDR Notation

Um eine möglichst effiziente Nutzung der vorhanden IP-Adressen zu gewährleisten, werden diese heutzutage mit der Subnetzmaske klassifiziert und nicht durch die IP-Adresse selbst.

Die Subnetzmaske wird häufig in Form eines Suffixes an der eigentlichen Adresse dargestellt. Diese Darstellung wird auch als CIDR (Classless Inter-Domain Routing) Notation bezeichnet.

→ Beispiel: 192.168.0.1/24

Das Suffix /24 gibt die Anzahl der gesetzten Bits in der Subnetzmaske an. Im Beispiel wären also die ersten 24 Bit der Subnetzmaske gesetzt.

- → Binär: 11111111.1111111.1111111.00000000
- → Dezimal: 255.255.255.0

Im Regelwerk der Firewall wird diese Notation genutzt, um bei den Quell- und Zieladressen Bereiche zu definieren. Das Suffix gibt hier also an, bis zu welchem Bit die Adresse am Paket mit der Adresse in der Regel übereinstimmen muss.

| Adresse im Regelwerk | Beschreibung   |
|----------------------|--|
| 192.168.1.1/32       | Alle Bits müssen übereinstimmen.   |
|                      | Nur die Adresse 192.106.1.1 deckt sich mit der Reger                                 |
| 192.168.1.0/24       | Die ersten 3 Oktette müssen übereinstimmen.  |
|                      | Alle Adressen, die mit 192.168.1.x beginnen decken sich mit der Regel.               |
| 0.0.0.0/0            | Kein Bit muss übereinstimmen.  |
|                      | Alle Adressen decken sich mit der Regel  |
| 192.168.1.0/25       | Die ersten 3 Oktette und das höchste Bit des 4 Oktettes müssen übereinstimmen.       |
|                      | Hier decken sich nur noch die Adresse 192.168.1.0 bis<br>192.168.1.127 mit der Regel |

Für komplexere Bereiche wie im letzten Beispiel können entsprechende Tools hilfreich sein. Eine einfache Internetsuche nach "Subnetz Rechner" oder "CIDR Rechner" sollte genügend Online Tools hervorbringen.

Ein hilfreiches intuitives Tool finden Sie zum Beispiel hier:

heise.de/netze/tools/netzwerkrechner/

## 4.6 IP-Adresse einstellen am Programmiergerät

Um vom PC, dem PG oder einem Laptop aus SIMATIC S7-1500 programmieren zu können, wird eine TCP/IP-Verbindung oder optional eine PROFIBUS-Verbindung benötigt.

Damit PC und SIMATIC S7-1500 über TCP/IP miteinander kommunizieren können, ist es wichtig, dass die IP-Adressen der beiden Geräte zusammenpassen.

Zuerst wird hier gezeigt, wie die IP-Adresse eines Rechners mit dem Betriebssystem Windows 10 eingestellt werden kann.

 $\rightarrow$  Lokalisieren Sie das Netzwerksymbol unten in der Taskleiste und klicken Sie anschließend auf  $\rightarrow$  "Netzwerkeinstellungen".



 $\rightarrow$  Im geöffneten Fenster der Netzwerkeinstellungen klicken Sie auf  $\rightarrow$  "Ethernet" und anschließend auf  $\rightarrow$  "Adapteroptionen ändern".

| Einstellungen                  |   | - | × |
|--------------------------------|---|---|---|
| Startseite                     | Ethernet  |   |   |
| Einstellung suchen             | Ethernet  |   |   |
| Netzwerk und Internet          | Nicht identifiziertes Netzwerk<br>Kein Internet   |   |   |
| 🗇 Status                       |   |   |   |
| 🖫 Ethernet                     | Verwandte Einstellungen<br>Adapteroptionen ändern |   |   |
| ଳ DFÜ                          | Erweiterte Freigabeoptionen ändern                |   |   |
| ∞ VPN                          | Netzwerk- und Freigabecenter                      |   |   |
| ₽ <sup>3</sup> > Flugzeugmodus | Heimnetzgruppe                                    |   |   |
| 🕒 Datennutzung                 | Windows-Firewall                                  |   |   |
| Proxy                          | Haben Sie eine Frage?<br>Hilfe anfordern          |   |   |
|                                | Machen Sie Windows besser.<br>Feedback senden     |   |   |
|                                |   |   |   |

→ Wählen Sie die gewünschte → "LAN-Verbindung" aus, mit der Sie sich mit der Steuerung verbinden möchten und klicken auf → "Eigenschaften".

| 😨 Netzwerkverbindungen – 🗆 🗙                        |   |                       |                  |            |  |  |  |
|---|---|-----------------------|------------------|------------|--|--|--|
| ← → ∨ ↑ 👰 « Netzwerk                                | und Internet > Netzwerkverbindungen   | ✓ Ö "Netzv            | verkverbindungen | " dur 🔎    |  |  |  |
| Organisieren 🔻 Netzwerkger                          | it deaktivieren Verbindung untersuchen  | Verbindung umbenennen | > ∎= ▼           | •          |  |  |  |
| LAN-Verbindung<br>Nicht identifiz<br>Intel(R) PRO/1 | <ul> <li>Deaktivieren<br/>Status<br/>Diagnose</li> <li>Verbindungen überbrücken</li> <li>Verknüpfung erstellen</li> <li>Löschen</li> <li>Umbenennen</li> <li>Eigenschaften</li> </ul> |                       |                  |            |  |  |  |
| 1 Element   1 Element ausgewähl                     | t   |                       |                  | · <b>F</b> |  |  |  |

 $\rightarrow$  Wählen Sie anschließend zum  $\rightarrow$  "Internetprotokoll Version 4 (TCP/IP)" die  $\rightarrow$  "Eigenschaften".

| Eigenschaften von LAN-Verbindung  | ×  |  |  |  |  |
|---|----|--|--|--|--|
| Netzwerk  |    |  |  |  |  |
| Verbindung herstellen über:   |    |  |  |  |  |
| Intel(R) PRO/1000 MT Desktop Adapter  |    |  |  |  |  |
| Konfigurieren   |    |  |  |  |  |
| Diese Verbindung verwendet folgende Elemente:   |    |  |  |  |  |
| <ul> <li>Client für Microsoft-Netzwerke</li> <li>Datei- und Druckerfreigabe für Microsoft-Netzwerke</li> <li>QoS-Paketplaner</li> <li>Internetprotokoll, Version 4 (TCP/IPv4)</li> <li>Microsoft-Multiplexorprotokoll für Netzwerkadapter</li> <li>PROFINET IO protocol (DCP/LLDP)</li> <li>Microsoft-LLDP-Treiber</li> </ul> |    |  |  |  |  |
| Installieren Deinstallieren Eigenschaften   | Ц  |  |  |  |  |
| Beschreibung<br>TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den<br>Datenaustausch über verschiedene, miteinander verbundene<br>Netzwerke emöglicht.<br>OK Abbreche   | 'n |  |  |  |  |

→ Jetzt können Sie z. B. die IP-Adresse: 192.168.1.99 mit der Subnetzmaske 255.255.255.0 verwenden und die Einstellungen übernehmen. (→ "OK")

| Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)  |                    |  |  |  |  |  |  |
|--|--------------------|--|--|--|--|--|--|
| Allgemein  |                    |  |  |  |  |  |  |
| IP-Einstellungen können automatisch zugewiesen werden, wenn das<br>Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den<br>Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen. |                    |  |  |  |  |  |  |
| O IP-Adresse automatisch beziehen  |                    |  |  |  |  |  |  |
| Folgende IP-Adresse verwenden:   |                    |  |  |  |  |  |  |
| IP-Adresse:  | 192 . 168 . 1 . 99 |  |  |  |  |  |  |
| Subnetzmaske:  | 255.255.255.0      |  |  |  |  |  |  |
| Standardgateway:   |                    |  |  |  |  |  |  |
| ODNS-Serveradresse automatisch b   | peziehen           |  |  |  |  |  |  |
| Folgende DNS-Serveradressen ve   | rwenden:           |  |  |  |  |  |  |
| Bevorzugter DNS-Server:  |                    |  |  |  |  |  |  |
| Alternativer DNS-Server:   |                    |  |  |  |  |  |  |
| Einstellungen beim Beenden über  | prüfen             |  |  |  |  |  |  |
| Erweitert  |                    |  |  |  |  |  |  |
|  | OK Abbrechen       |  |  |  |  |  |  |

# 5 Aufgabenstellung

In diesem Kapitel soll die Hardware und das Programm aus Kapitel "SCE\_DE\_092-300\_OPC\_UA\_S7-1500", um den SCALANCE S615 erweitert werden.

Mit Hilfe des SCALANCE S615 soll ein gesicherter Zugriff auf die Steuerung aus dem Firmennetzwerk ermöglicht werden. Der Webserver auf der CPU soll dabei zu Diagnosezwecken frei zugänglich sein, während der Zugang zur Programmierung mittels des TIA Portals nur authentifizierten Benutzern erlaubt sein soll.

# 6 Planung

Als Erstes muss der SCALANCE S615 mit einer neuen IP-Adresse konfiguriert und die Grundkonfiguration vorgenommen werden.

Anschließend kann in der CPU 1516F der S615 als Router eingetragen und die Konfiguration auf die CPU übertragen werden.

Nach erfolgreicher Grundkonfiguration beider Geräte kann die physikalische Vernetzung der Komponenten wie folgt aufgebaut werden.



Als Letztes werden die Zugriffsregeln im SCALANCE S615 angelegt und getestet.

### WICHTIG:

Da sich das Programmiergerät während der Inbetriebnahme in verschiedenen Subnetzen befinden wird, dürfen Sie auf keinen Fall eine projektspezifische IP-Adresse durch das TIA Portal anlegen lassen. Konfigurieren Sie stattdessen die korrekten IP-Einstellungen statisch in das Programmiergerät. Später wird der S615 die korrekten IP-Adressen dynamisch vergeben.

# 7 Strukturierte Schritt-für-Schritt-Anleitung

Im Folgenden finden Sie eine Anleitung wie Sie die Planung umsetzen können. Sollten Sie schon bereits entsprechende Vorkenntnisse haben, so reichen Ihnen die nummerierten Schritte zur Bearbeitung aus. Ansonsten folgen Sie einfach den folgenden bebilderten Schritten der Anleitung.

## 7.1 Dearchivieren eines vorhandenen Projekts

- → Bevor Sie das Projekt "SCE\_DE\_092-300 OPC UA S7-1500\_R1807.zap15" aus dem Kapitel "SCE\_DE\_092-300 OPC UA S7-1500" erweitern können, müssen Sie dieses dearchivieren.
- → Zum Dearchivieren eines vorhandenen Projekts müssen Sie aus der Projektansicht heraus unter → Projekt → Dearchivieren das jeweilige Archiv aussuchen. Bestätigen Sie Ihre Auswahl anschließend mit Öffnen. (→ Projekt → Dearchivieren → Auswahl eines .zap-Archivs ... → Öffnen)



→ Wählen Sie als Nächstes das Zielverzeichnis, in welches das dearchivierte Projekt gespeichert werden soll. Bestätigen Sie Ihre Auswahl mit "OK". (→ Zielverzeichnis … → Ordner auswählen) → Das dearchivierte und geöffnete Projekt speichern Sie unter dem Namen 142-200\_Industrial\_Security\_mit\_S615. (→ Projekt → Speichern unter ... → 142-200\_Industrial\_Security\_mit\_S615 → Speichern)

| K Siemens - C:\00_TIA_Portal\092 300_OPC UA  | 57-1500_V15.1\092 300_OPC UA \$7-1500_V15.1                                   | _ 🗆 🗙                          |
|--|---|--------------------------------|
| Projekt Bearbeiten Ansicht Einfügen Online   | Extras Werkzeuge Fenster Hilfe  | otally Integrated Automation   |
| B Neu  | 🖙 ± (4 ± 🐁 🔃 🛐 🖳 🖉 Online verbinden 🖉 Online-Verbindung trennen 🐰 🖪 🖪 🛠 🖃 🔲 * | PORTAL                         |
| Coffnen Strg+O                               |   | Aufgaben 🗐 🛙 🕨                 |
| Schließen Stra+W                             |   | Ontingen                       |
|  |   | Optionen 🚽                     |
| Speichern unter Stra+Shift+S                 | - 04  | 5                              |
| Projekt Jöschen Strauß                       |   | ✓ Suchen und ersetzen          |
| Archivieren                                  |   | - Cushana                      |
| Dearchivieren                                |   | Suchen:                        |
| Multiuser                                    |   |                                |
| Projekt aus Teamcenter öffnen                |   | Nur ganzes wort suchen         |
| Tard Beader/USB-Speicher                     |   | GroB-/Kleinschreibung          |
| Memory Card-Datei                            |   | Suchen in untergeordneten Stru |
| Basis-Integritätsprüfung starten             |   | Suchen in ausgeblendeten Texte |
| E Drucken Stroug                             |   | Platzhalterzeichen verwenden   |
| A Druckvorschau                              |   | Reguläre Ausdrücke verwenden   |
| Beschriftungsstreifen für Module exportieren |   | Nach unten                     |
| C:\00 TIA\092 300 OPC UA \$7-1500 V15.1      |   | O Nach oben                    |
| C:\\140-100_Industrial_Ethernet_mit_XC2      |   | Suchen                         |
| C:\00_TIA\SCL_Leitfaden_Aufbaukurs_V15.1     |   |                                |
| C:\\032-600_Globale_Datenbausteine_V1        |   | Ersetzen:                      |
| C:\1032-600_Globale_Datenbausteine_V1        |   |                                |
| C:\Users\schulung\Documents\\Safety Test     |   | Gesamtes Dokument              |
| C:\Users\schulung\Documen\Sortieranlage      | 🖳 Eigenschaften 🚺 Info 🔒 🗓 Diagnose 📄 🖃 🥆                                     | O Von der aktuellen Position   |
| Beenden Alt+F4                               | Allgemein (1) Querverweise Übersetzen   | O Auswahl                      |
| ✓ Detailansicht                              | 🔁 🛕 🕕 Alle Meldungen anzeigen 💌   | Ersetzen Alle ersetzen         |
| Module                                       |   |                                |
|  | Pfad Beschreibung Gehe zu ? Fehler  |                                |
| Name   |   |                                |
| Gerätekonfiguration                          |   |                                |
| 🖳 Online & Diagnose 📃                        |   |                                |
| Rogrammbausteine                             |   | < III >                        |
| lecnnologieobjekte                           |   | > Sprachen & Ressourcen        |
| Portalansicht Übersicht                      | 🔛 🗹 Projekt 092 300.  | _OPC UA \$7-1500_V15 🎾         |

## 7.2 Einstellen der IP-Adresse des SCALANCE S615

- → Verbinden Sie das Programmiergerät mit dem Port 4 des SCALANCE S615.
- → Trennen Sie alle anderen Verbindungen zum SCALANCE S615
- → Stellen Sie sicher, dass Ihr Programmiergerät sich im Subnetz 192.168.1.0/24 befindet. Folgen Sie den Anweisungen in Abschnitt 4.6.
- $\rightarrow$  Öffnen Sie die Suche nach Erreichbaren Teilnehmern. ( $\rightarrow$  **b**?)
- $\rightarrow$  Wählen Sie Ihre PN/IE Schnittstelle aus und starten Sie die Suche. ( $\rightarrow$  <u>Suche starten</u>)
- → Wählen Sie den SCALANCE S-600 aus und klicken Sie auf "Anzeigen". (→ Anzeigen

| Erreichbare Teilnehme         | r                     |                          |                   |                   | ×                                   |
|-------------------------------|-----------------------|--------------------------|-------------------|-------------------|-------------------------------------|
|                               |                       | Tun der PG/PC-Schnittste | lle: Ph/IE        |                   |                                     |
|                               |                       | PG/PC-Schnittste         | lle: Intel(B) PB  | O/1000 MT Desktor | n Adapter 🔍 🗑 🔯                     |
| a7                            |                       |                          |                   |                   |                                     |
|                               | Erreichbare Teilnehm  | er der ausgewählten Sch  | nittstelle:       | A deserve         | MAG Advance                         |
|                               | Gerat                 | Geratetyp                | Schnittstellentyp | Adresse           | MAC-Adresse                         |
| LED blinken                   |                       |                          |                   |                   |                                     |
|                               |                       |                          |                   |                   | Suche starten                       |
| Online-Statusinformation      | :                     |                          |                   | 📃 Nur Fehlerm     | neldungen anzeigen                  |
| A Gefundenes erreichb         | ares Gerät Teilnehmer |                          |                   |                   | <b>^</b>                            |
| 🚹 Suche beendet. 1 Tei        | ilnehmer gefunden.    |                          |                   |                   |                                     |
| <b>"?</b> Geräteinformationen | werden eingeholt      |                          |                   |                   |                                     |
|                               |                       |                          |                   |                   | An <u>z</u> eigen <u>A</u> bbrechen |

→ Öffnen Sie unter "Online-Zugänge" den Punkt "Online&Diagnose" des angezeigten Teilnehmers.

| 🐘 Siemens - C:00_TIA_Portal\140-100_Industrial_Ethernet_mit_XC208\140-100_Industrial_Ethernet_mit_XC208 🖉 🗆 🛛 🗙 |   |                                    |                           |                                |          |  |  |  |
|---|---|------------------------------------|---------------------------|--------------------------------|----------|--|--|--|
| Projekt Bearbeiten Ansicht Einfügen Onlin   | Projekt Bearbeiten Ansicht Einfügen Online Extras Werkzeuge Fenster Hilfe Totally Integrated Automation   |                                    |                           |                                |          |  |  |  |
| 📑 🛅 🔚 Projekt speichern 🔳 🐰 🗐 🗎 🕽   | < う き ( ) ) ( ) き ( ) き ( ) き ( ) ) ( ) ( | 🛔 🚿 Online verbinden 🚀 Online-Verb | indung trennen  🏦 🖪 🖪 🖓 ' | , , ,                          | PORTAL   |  |  |  |
| Projektnavigation 🔲 🖣   | line-Zugänge > Intel(R) PRO   |                                    |                           |                                | -∎≡×∢    |  |  |  |
| Geräte  |   |                                    |                           |                                | <b>U</b> |  |  |  |
|   | ▼ Diagnose<br>Allgemein   | Algemein                           |                           |                                | Onlin    |  |  |  |
| Nicht gruppierte Geräte   | Funktionen  | Modul                              |                           |                                | -        |  |  |  |
| Security-Einstellungen  |   | Kurzbezeichnung:                   | SCALANCE XC-200           |                                |          |  |  |  |
| Dokumentationseinstellungen   |   |                                    |                           |                                |          |  |  |  |
| Sprachen & Ressourcen   |   | Baugruppeninformation              |                           |                                | A L      |  |  |  |
| Schnittstellen anzeigen/verber  |   | Gerätename:                        |                           |                                | gabe     |  |  |  |
| <ul> <li>Intel(R) PRO/1000 MT Desktop</li> <li>Erreichbare Teilnehmer akt</li> </ul>                            |   | Herstellerinformation              |                           |                                | 2        |  |  |  |
| Weitere Informationen anze.   |   |                                    |                           |                                |          |  |  |  |
| cpu_1516f.profinet-schnitt  |   | Herstellerbeschreibung:            | SIEMENS AG                |                                | Bibl     |  |  |  |
| L leinenmer [20-87-56-80-2  |   | Rolle des Moduls:                  | Device                    |                                | it       |  |  |  |
| PC internal [Lokal]   |   | -                                  |                           |                                | ek       |  |  |  |
| PLCSIM [PN/IE]  |   |                                    |                           |                                | en       |  |  |  |
| USB [S7USB]   |   |                                    |                           |                                |          |  |  |  |
| TeleService [Automatische Prot.]  |   |                                    |                           |                                |          |  |  |  |
|   |   | -                                  |                           |                                |          |  |  |  |
| ✓ Detailansicht   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
| Name  |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    |                           |                                |          |  |  |  |
|   |   |                                    | G Figenschaften           | 1 Info Diagnose                |          |  |  |  |
| A Portalansicht   | Q Online & Dia  |                                    |                           | he pack Tailachmann in der Sch | รีย      |  |  |  |
| Pontaliansion:  | omine a bia   |                                    | 🔤 🚺 Die Su                | ne nach Teilnehmern in der Sch | 2        |  |  |  |

 $\rightarrow$  Stellen Sie die IP-Adresse auf 192.168.1.254/24. ( $\rightarrow$  Funktionen  $\rightarrow$  IP-Adresse zuweisen  $\rightarrow$ 

| IP-Adresse: 192.168.1.254 $\rightarrow$ Subnetzmaske: 255.255.255.0 $\rightarrow$ | IP-Adresse zuweisen |
|---|---------------------|
|   |                     |

| Zugänge 🕨 Intel(R) PRO/100 | 0 MT Desktop Adapter 🔸 Teilnehmer [192.168.1.1] 🔸 Teilnehmer [192.168.1.1] 💦 💶 🗮 🗮 🗙  |
|----------------------------|---|
|                            |   |
| ✓ Diagnose<br>Allgemein    | IP-Adresse zuweisen   |
| ▼ Funktionen               |   |
| IP-Adresse zuweisen        | IP-Adresse dem Gerät zuweisen   |
| PROFINET-Gerätename verg   | Corëta dia an ain Eirmannatzwark adar an dar Internet annarshlarran wardan, miissan aga   |
| Rücksetzen auf Werkseins   | Zugiff angemessen geschützt sein, z. B. durch die Verwendung von Firewalls und Netzwerk<br>Weiterführende Informationen über Industrial Security finden Sie unter<br><u>http://www.siemens.com/industrialsecurity</u> |
|                            |   |
| •                          | MAC-Adresse: 20 - 87 - 56 - 76 - CD - 3F Erreichbare Teilnehmer   |
|                            | IP-Adresse: 192.168.1 .254  |
|                            | Subnetzmaske: 255 . 255 . 0   |
|                            | Router verwenden  |
|                            | Router-Adresse: 0.0.0.0   |
|                            | IP-Adresse zuweisen   |
|                            |   |
|                            |   |
| < III >                    |   |

## 7.3 Grundkonfiguration des SCALANCE S615

- → Öffnen Sie im Browser die Weboberfläche des SCALANCE S615. (→ https://192.168.1.254)
- → Die Weboberfläche des SCALANCE S615 ist mit einem selbstsignierten Zertifikat geschützt. Bestätigen Sie die Ausnahme, um fortzufahren.



#### Hinweis:

Je nach Browser sieht das Bestätigen des Zertifikats etwas anders aus.



 $\rightarrow$  Wechseln Sie als Erstes die Sprache der Oberfläche auf Deutsch. ( $\rightarrow$  Deutsch  $\rightarrow$  Go)

|  |   | _                        |                      | ×           |
|--|---|--------------------------|----------------------|-------------|
|  | ☆ | 9.0                      | Θ                    | 0<br>0<br>0 |
|  |   | Deuts<br>Englis<br>Deuts | sch ▼ ⊆<br>sh<br>sch | <u>io</u>   |
|  |   |                          | ?                    | ÷.          |
|  |   |                          |                      |             |
| Name:  |   |                          |                      |             |
| Password:<br>Login   |   |                          |                      |             |
| Switch to firewall login<br>Switch to insecure HTTP                    |   |                          |                      |             |
| For information about browser compatibility please refer to the manual |   |                          |                      |             |

→ Als Nächstes können Sie sich mit dem Benutzer "admin" und dem Passwort "admin" einloggen. (→ Name: admin → Password: admin → Login)

| SIEMENS   | Deutsch V Go |
|---|--------------|
| Name English<br>Passwort Anneder<br>Anneder   | ? 🗄          |
| Amedian<br>Annexian<br>Annexian<br>Annexian<br>Annexian<br>Annexian<br>Machael zur Frewall-Annexidung<br>Wechsel zu unsicherer HTTP-Verbindungs<br>Informationen zur Kompatibilität des Browsers finden Sie in der Dokumentation. |              |
|   |              |

 $\rightarrow$  Der Standardzugang muss vor dem ersten Login geändert werden. ( $\rightarrow$  OK)



- → Geben Sie zuerst das alte Passwort ein "admin" und anschließend zweimal ein neues Passwort.
  - → Aktuelles Benutzerpasswort: admin
  - → Neues Passwort: \*\*\*
  - → Passwort bestätigen: \*\*\*
  - $\rightarrow$  Einstellungen übernehmen

| Name Passwort Anmelden | Passwörter von Benut                               | tzern          |  |
|------------------------|--|----------------|--|
|                        | Aktueller Benutzer:<br>Aktuelles Benutzerpasswort: | admin<br>••••• |  |
|                        | Benutzerkonto:<br>Passwortrichtlinie:              | admin •        |  |
|                        | Neues Passwort:                                    | ••••••         |  |
|                        | Passwort bestätigen:                               | •••••          |  |
|                        | Einstellungen übernehmen                           | Aktualisieren  |  |

#### Hinweis:

- Das neue Passwort benötigt mindestens acht Zeichen, eine Zahl, ein groß geschriebenes Zeichen und ein Sonderzeichen!
- → Nach erfolgreicher Änderung der Zugangsdaten und Anmeldung wird der DCP-Zugriff auf das Gerät nur noch lesend zugelassen. (→ OK)



→ Stellen Sie im folgenden Konfigurationsassistenten das VLAN 2 auf die statische Adresse 10.0.0.254/24 und klicken Sie auf "Weiter". (Extern (vlan2) → DHCP → IP-Adresse: 10.0.0.254 → Subnetzmaske: 255.255.255.0 → Weiter)

| IP | Gerät | Zeiteinste  | llung DDN    | SINEMA RO                        | C Zusammenfassung   |
|----|-------|-------------|--------------|----------------------------------|---|
|    |       |             |              |                                  |   |
|    |       |             | Geben Sie    | die IP-Adresse                   | und Subnetzmaske ein, unter der die Management-Funktionen des Geräts erreichbar |
|    |       |             | oder E-Mail  | Sie das Gerat<br>-Server, dann ( | geben Sie auch die IP-Adresse des Standard-Gateways ein.                        |
|    |       |             |              |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             | Intern (vlan | 1)                               |   |
|    |       | IP-Adresse: | 192.168.1.2  | 254                              |   |
|    | Sub   | netzmaske:  | 255.255.25   | 5.0                              |   |
|    |       |             |              |                                  |   |
|    |       |             | Extern (vla  | 12)                              |   |
|    |       |             | DHCP         |                                  |   |
|    |       | IP-Adresse: | 10.0.254     |                                  |   |
|    | Sub   | netzmaske:  | 255.255.25   | 5.0                              |   |
|    | Gatew | ay (DHCP):  | -            |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             | Neuen Gat    | eway anlegen                     |   |
|    |       | IP-Adresse: | 0.0.0.0      |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             |              |                                  |   |
|    |       |             |              |                                  |   |
|    | Ab    | brechen     | Weite        | er                               |   |
|    |       |             |              |                                  |   |

→ Füllen Sie die Identifikationsdaten nach Belieben aus und klicken Sie "Weiter". (→ Systemname: ... → Gerätestandort: ... → Kontaktperson: ... → Weiter)

| IP Gerät Zeiteins | tellung DDNS SINEMA RC Zusammenfassung  |
|-------------------|---|
|                   |   |
|                   | Legen Sie zur besseren Identifikation des Geräts die allgemeinen Geräteinformationen fest. Hier können Sie<br>einen eindeutigen Namen für das Gerät festlegen. Normalerweise ist das der FQDN (Fully Qualified Domain<br>Name). Wenn Sie einen eindeutigen Namen verwenden, können Sie das Gerät im Rahmen einer Anwendung<br>identifizieren. Sie können eine Kontaktperson eingeben, die für die Verwaltung des Geräts zuständig ist und die<br>Ortsbezeichnung des Aufstellungsorts, z.B. die Raumnummer. |
| Systemname:       | s615  |
| Gerätestandort:   | Labor   |
| Kontaktperson:    | Michael Dziallas Engineering  |
|                   |   |
| Zurück            | Abbrechen Weiter  |

 $\rightarrow$  Übernehmen Sie die Zeit vom PC und klicken Sie "Weiter". ( $\rightarrow$  PC-Zeit verwenden  $\rightarrow$  Weiter)

| IP | Gerät Zeit | einstellung [   | DDNS SINEM   | A RC Zusammenfassung   |  |   |
|----|------------|---|--|--|--|---|
|    |            |   |  |  |  |   |
|    |            | Hier stellen S<br>Zeitstempel v<br>einem Zeitse<br>aktuelle Uhrz<br>anderes Verfa | ie das Datum u<br>ion Log-Einträg<br>rver automatisc<br>eit präzise bezo<br>ahren verwende | ind die Zeit zur Überprüfung zeitlichen Gültigkeit<br>en. Sie können die Systemzeit selbst manuell ei<br>h synchronisieren. Im Internet gibt es eine Reih-<br>ogen werden kann. Der Basic Wizard verwendet<br>en wollen, konfigurieren Sie dies nach Beenden | t von Zertifikaten und<br>instellen, oder Sie las<br>e von Zeitservern, vor<br>NTP als Zeitserver. \<br>des Basic Wizards. | für die<br>sen sie mit<br>1 denen die<br>Wenn Sie ein |
|    |            |   |  |  |  |   |
|    |            | Manuelle 2  | Zeiteinstellung  |  |  |   |
|    | Systemzeit | 01/01/2000 0  | 1:10:18  |  |  |   |
|    |            | PC-Zeit verw  | venden   |  |  |   |
|    |            | NTP-Clien   | t  |  |  |   |
|    |            | Nur NTP-O   | Client (gesicher   | t)   |  |   |
|    | Zeitzone:  | +00:00  |  |  |  |   |
|    |            |   |  |  |  |   |
|    |            | Selektieren   | NTP-<br>Serverindex  | NTP-Server-Adresse   | Port des NTP-<br>Servers   | Poll-Intervall  |
|    |            |   | 1  | 0.0.0.0  | 123  | 64  |
|    |            | •   |  |  |  |   |
|    |            |   |  |  |  |   |
|    | Zurüc      | k Ab  | brechen  | Weiter   |  |   |

→ Überspringen Sie die dynamischen DNS Einstellungen mit "Weiter". (→ Weiter)

| IP Gerät Zeiteinstellu  | ng DDNS   | SINEMA RC Zusammenfassung   |  |  |                     |
|---|---|---|--|--|---------------------|
| DDNS steht für 'Dyn<br>das Gerät aus dem i<br>geben Sie den Hostu<br>Daten (Benutzernan<br>Sie das Kontrollkäst | amic Domai<br>externen Ne<br>namen, den<br>ne, Passwor<br>chen 'Aktivie | n Name System'. Wenn Sie das Gerät be<br>tz auch unter einem Hostnamen erreicht<br>Sie mit Ihrem DDNS-Anbieter für das Ge<br>1) für den DDNS-Server. Um den gewün<br>nt'. | ei einem DDNS-Diens<br>par, z. B. 'example.no-<br>arät vereinbart haben i<br>schten Service zu ver | t anmelden, ist<br>ip.com'. Hier<br>und die Login-<br>wenden, aktivieren |                     |
| Dienst  | Aktiviert   | Host  | Benutzername   | Passwort   | Passwort bestätigen |
| No-IP   |   |   |  |  |                     |
| DynDNS  |   |   |  |  |                     |
|   |   |   |  |  |                     |

→ Überspringen Sie die SINEMA RC Einstellungen mit "Weiter". (→ Weiter)

| IP Gerät Zeiteinstellung DDNS SINEMAR        | C Zusammenfassung   |
|--|---|
|  | Hier konfigurieren Sie den Zugriff auf den SINEMA RC-Server. Mit diesen Einstellungen meldet sich das Gerät<br>am Server an. Der VPN-Tunnel zwischen dem Gerät und dem SINEMA RC Server ist erst nach erfolgreicher<br>Authentifizierung eingerichtet. Erst nach erfolgreicher Authentifizierung wird der VPN-Tunnel zwischen dem<br>Gerät und dem SINEMA RC Server aufgebaut. Abhängig von den projektierten Kommunikationsbeziehungen<br>und den Sicherheitseinstellungen verschaltet der SINEMA RC Server die einzelnen VPN-Tunnels. |
|  | SINEMA RC aktivieren  |
|  | Server-Einstellungen  |
| SINEMA RC-Adresse:                           |   |
| SINEMA RC-Port:                              | 443   |
|  |   |
|  | Serverüberprüfung   |
| Prüfungsart:                                 | Fingerabdruck •   |
| Fingerabdruck:                               |   |
| CA-Zertifikat:                               | - Y   |
|  |   |
|  | Geräteanmeldedaten  |
| Geräte-ID:                                   | 0   |
| Geräte-Passwort:                             |   |
| Geräte-Passwort bestätigen:                  |   |
|  |   |
|  | Optionale Einstellungen   |
|  | Auto Firewall/NAT-Regeln  |
| Verbindungsart:                              | Auto 🔻  |
| Proxy verwenden:                             | none 🔻  |
| Automatisches Registrierung-Intervall [min]: | 60  |
|  |   |
| Zurück Abbrechen                             | Weiter  |

→ Überprüfen Sie erneut alle Einstellungen in der Zusammenfassung und Bestätigen Sie die Konfiguration. (→ Einstellungen übernehmen)

| IP Gerät Zeiteinstellung D               | DNS SINEMA RC       | Zusammenfassung     |                  |                      |                    |
|--|---------------------|---------------------|------------------|----------------------|--------------------|
|  |                     |                     |                  |                      |                    |
|  | Intern (vlan1)      |                     |                  |                      |                    |
| IP-Adresse:                              | 192.168.1.254       |                     |                  |                      |                    |
| Subnetzmaske                             | 255.255.255.0       |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  | Extern (vlan2)      |                     |                  |                      |                    |
| IP-Adresse:                              | 10.0.0.254          |                     |                  |                      |                    |
| Subnetzmaske:                            | 255.255.255.0       |                     |                  |                      |                    |
| DHCP:                                    | Deaktiviert         |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  | Neuen Gateway an    | legen               |                  |                      |                    |
| IP-Adresse:                              | 0.0.0.0             |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
| Systemname:                              | s615                |                     |                  |                      |                    |
| Gerätestandort                           | Labor               |                     |                  |                      |                    |
| Kontaktperson:                           | Michael Dziallas En | igineering          |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
| Manuelle Zeiteinstellung:                | Aktiviert           |                     |                  |                      |                    |
| Systemzen:                               | 00/03/2019 18:23:3  | 1                   |                  |                      |                    |
| Nur NTP Client (gesishert):              | Deaktiviert         |                     |                  |                      |                    |
| Nul NTE-Olient (gesichert).<br>Zeitzone: | +00:00              |                     |                  |                      |                    |
| Zenzone.                                 | NTP Serverindex     | NTR Server Ad       |                  | Port doc NTP Sonuoro | Poll Intonial      |
|  | 1                   | 0.000               | 6556             | 123                  | 64                 |
|  |                     | 0.0.0.0             |                  | 120                  |                    |
|  | Diopet              | Aktiviort           | Host             |                      | Poputzornamo       |
|  | No-IP               | Deaktiviert         | HUSI             |                      | Denutzenname       |
|  | DynDNS              | Deaktiviert         |                  |                      | <b>.</b>           |
|  | ,                   |                     |                  |                      |                    |
| SINEMA RC:                               | Deaktiviert         |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  |                     |                     |                  |                      |                    |
|  | Klicken Sie auf die | Schaltfläche 'Finst | ellungen überneh | men'. um die Änderun | gen zu übernehmen! |
|  |                     | Lind                |                  | ,                    | 0                  |
| Zurück Abb                               | rechen Einstellu    | ngen übernehmen     |                  |                      |                    |

→ Nach Übernahme der Einstellungen landen Sie in der endgültigen Weboberfläche des SCALANCE S615.



## 7.4 Konfiguration des DHCP-Servers

Um die Verbindung mit dem Anlagennetz so einfach wie möglich für den Service-Techniker und auch später bei den Tests zu gestalten, wird der SCALANCE S615 sowohl im gesicherten als auch im ungesicherten Bereich dynamische Adressen vergeben.

→ Wechseln Sie im Menü System auf die DHCP-Server Einstellungen. (→ System → DHCP → DHCP-Server)

| Abmelden             | • ? = ×  | • |
|----------------------|--|---|
| ▶Wizards             | DHCP-Client DHCP-Server DHCP-Optione Statische Zuordnung       |   |
| ▶ Information        | DHCP-Server  |   |
| →System              | Auresse vor dem Anmeten mit CAR-Echo primen                    |   |
| ►Konfiguration       | Selektieren Pool-ID Aktivieren Gültigkeitsdauer (Sek)          |   |
| ►Allgemein           | 0 Einträge.  |   |
| ▶Neustart            |  |   |
| Laden &<br>Speichern | Erstellen   Lüschen   Einstellungen übernehmen   Aktualisieren |   |
| ▶Ereignisse          |  |   |
| ▶SMTP-Client         |  |   |
| ▶SNMP                |  |   |
| ▶Systemzeit          |  |   |
| ►Auto-Logout         |  |   |
| ▶Taster              |  |   |
| ▶Syslog-Client       |  |   |
| ▶Fehlerkontrolle     |  |   |
| ▶PLUG                |  |   |
| ▶ Ping               |  |   |
| ►DCP Discovery       |  |   |
| ▶ DNS                |  |   |
| ► DHCP               |  |   |
| ▶cRSP / SRS          |  |   |

→ Erstellen Sie zunächst einen neuen Pool an IP-Adressen. (→ Erstellen)

| DHCP-Client D                                 | HCP-Server  | DHCP-Optionen Statische Z   | uordnung   |         |                    |                  |                        |  |  |  |  |
|---|-------------|-----------------------------|------------|---------|--------------------|------------------|------------------------|--|--|--|--|
|   |             |                             |            |         |                    |                  |                        |  |  |  |  |
| DHCP-Se                                       | rver        |                             |            |         |                    |                  |                        |  |  |  |  |
| Adresse vor dem Anbieten mit ICMP-Echo prüfen |             |                             |            |         |                    |                  |                        |  |  |  |  |
|   |             |                             |            |         |                    |                  |                        |  |  |  |  |
| Sololtioron                                   | Pool ID     | Schnittstollo               | Aktivioron | Subpotz | Lintoro ID Adrosso | Oboro IP Adrosso | Gültigkoitedauar [Sak] |  |  |  |  |
| Selektieren                                   | FUUHD       | Schnittstelle               | Akuvieren  | Subnetz | Unitere IF-Auresse | Obere IF-Auresse | Guiligkeitsuauer [Sek] |  |  |  |  |
|   | 1           | vlan1 (INT)                 |            | 0.0.0/0 | 0.0.0.0            | 0.0.0.0          | 3600                   |  |  |  |  |
| 1 Eintrag                                     |             |                             |            |         |                    |                  |                        |  |  |  |  |
| . Linitagi                                    |             |                             |            |         |                    |                  |                        |  |  |  |  |
| Erstellen Li                                  | Sechon Fine | tellungen übernehmen Aktual | sioron     |         |                    |                  |                        |  |  |  |  |
| Erstelleri                                    | Schen       | ARUan                       | sieren     |         |                    |                  |                        |  |  |  |  |

- → Wählen Sie für die Schnittstelle vlan1 aus. (→ Schnittstelle: vlan1 (INT))
- $\rightarrow$  Stellen Sie das korrekte Subnetz ein. ( $\rightarrow$  Subnetz: 192.168.1.0/24)
- $\rightarrow$  Setzen Sie die erste IP-Adresse. ( $\rightarrow$  Untere IP-Adresse: 192.168.1.208)
- $\rightarrow$  Setzen Sie die letzte IP-Adresse. ( $\rightarrow$  Obere IP-Adresse: 192.168.108.223)
- $\rightarrow$  Übernehmen Sie die Einstellungen. ( $\rightarrow$  Einstellungen übernehmen)

 DHCP-Client
 DHCP-Server
 DHCP-Optionen
 Statische Zuordnung

 DHCP-Server
 Adresse vor dem Anbieten mit ICMP-Echo prüfen

 Selektieren
 Pool-ID
 Schnittstelle
 Aktivieren
 Subnetz
 Untere IP-Adresse
 Obere IP-Adresse
 Gültigkeitsdauer [Sek]

 1
 Vlan1 (INT)
 192.168.1.0/24
 192.168.1.203
 192.168.1.223
 3600

 1 Eintrag.
 Erstellen
 Löschen
 Einstellungen übernehmen
 Aktualisieren

 $\rightarrow$  Erstellen Sie einen weiteren Pool an IP-Adressen ( $\rightarrow$  Erstellen)

DHCP-Client DHCP-Server DHCP-Optionen Statische Zuordnung

| DHCP-Server Adresse vor dem Anbieten mit ICMP-Echo prüfen  |   |             |  |                |               |               |      |  |  |  |  |
|--|---|-------------|--|----------------|---------------|---------------|------|--|--|--|--|
| Selektieren Pool-ID Schnittstelle Aktivieren Subnetz Untere IP-Adresse Obere IP-Adresse Gültigkeitsdauer [Sek] |   |             |  |                |               |               |      |  |  |  |  |
|  | 1 | vlan1 (INT) |  | 192.168.1.0/24 | 192.168.1.203 | 192.168.1.208 | 3600 |  |  |  |  |
|  | 2 | vlan1 (INT) |  | 0.0.0/0        | 0.0.0.0       | 0.0.0.0       | 3600 |  |  |  |  |
| 2 Einträge.  |   |             |  |                |               |               |      |  |  |  |  |
| Erstellen Löschen Einstellungen übernehmen Aktualisieren   |   |             |  |                |               |               |      |  |  |  |  |

- $\rightarrow$  Wählen Sie für die Schnittstelle vlan2 aus. ( $\rightarrow$  Schnittstelle: vlan2 (EXT))
- $\rightarrow$  Stellen Sie das korrekte Subnetz ein. ( $\rightarrow$  Subnetz: 10.0.0/24)
- $\rightarrow$  Setzen Sie die erste IP-Adresse. ( $\rightarrow$  Untere IP-Adresse: 10.0.0.1)
- $\rightarrow$  Setzen Sie die letzte IP-Adresse. ( $\rightarrow$  Obere IP-Adresse: 10.0.0.127)

| □ DHCP-Server         □ Adresse vor dem Anbieten mit ICMP-Echo prüfen         Selektieren       Pool-ID         Schnittstelle       Aktivieren         Subnetz       Untere IP-Adresse         Obere IP-Adresse       Gültigkeitsdaue         1       vlan1 (INT)               | HCP-Client DHCP-Server DHCP-Optionen Statische Zuordnung |  |  |  |  |  |  |  |  |  |  |  |
|---|--|--|--|--|--|--|--|--|--|--|--|--|
| Selektieren       Pool-ID       Schnittstelle       Aktivieren       Subnetz       Untere IP-Adresse       Obere IP-Adresse       Gültigkeitsdaue         1       vlan1 (INT)       192.168.1.0/24       192.168.1.203       192.168.1.208       3600                           | DHCP-Server  |  |  |  |  |  |  |  |  |  |  |  |
| Selektieren       Pool-ID       Schnittstelle       Aktivieren       Subnetz       Untere IP-Adresse       Obere IP-Adresse       Gültigkeitsdaue         1       vlan1 (INT)       •       192.168.1.0/24       192.168.1.203       192.168.1.208       3600                   | DHCP-Server  |  |  |  |  |  |  |  |  |  |  |  |
| Selektieren         Pool-ID         Schnittstelle         Aktivieren         Subnetz         Untere IP-Adresse         Obere IP-Adresse         Gültigkeitsdaue           1         vlan1 (INT)         192.168.1.0/24         192.168.1.203         192.168.1.208         3600 | Adresse vor dem Andieten mit ICMM-Echo pruten            |  |  |  |  |  |  |  |  |  |  |  |
| Selektieren         Pool-ID         Schnittstelle         Aktivieren         Subnetz         Untere IP-Adresse         Obere IP-Adresse         Gültigkeitsdaue           1         vlan1 (INT)         192.168.1.0/24         192.168.1.203         192.168.1.208         3600 |  |  |  |  |  |  |  |  |  |  |  |  |
| □ 1 vlan1 (INT) ▼ □ 192.168.1.203 192.168.1.208 3600  | [Sek]  |  |  |  |  |  |  |  |  |  |  |  |
|   |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 VIan2 (EXT) T 10.0.0/24 10.0.1 10.0.127 3600  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 Einträge  |  |  |  |  |  |  |  |  |  |  |  |  |
|   |  |  |  |  |  |  |  |  |  |  |  |  |
| Erstallan Löschen Einstallungen übergehmen Aktualisieren  |  |  |  |  |  |  |  |  |  |  |  |  |

 $\rightarrow$  Wechseln Sie in den Reiter DHCP-Optionen ( $\rightarrow$  DHCP-Optionen)

| DHCP-Client D | HCP-Server   | DHCP-Opti    | onen Statische | Zuordnung                   |                       |
|---------------|--------------|--------------|----------------|-----------------------------|-----------------------|
|               |              |              |                |                             |                       |
| Pool-ID:      | 1 🔻          |              |                |                             |                       |
| Optionswert:  |              |              |                |                             |                       |
|               | Selektieren  | Pool-ID      | Optionswert    | Schnittstellen-IP verwenden | Wert                  |
|               |              | 1            | 1              |                             | 255.255.255.0         |
|               |              | 1            | 3              |                             | 0.0.0.0               |
|               |              | 1            | 6              |                             | 0.0.0.0               |
|               |              | 1            | 66             |                             |                       |
|               |              | 1            | 67             |                             | Bootfile name not set |
|               |              | 2            | 1              |                             | 255.255.255.0         |
|               |              | 2            | 3              |                             | 0.0.0.0               |
|               |              | 2            | 6              |                             | 0.0.0.0               |
|               |              | 2            | 66             |                             |                       |
|               |              | 2            | 67             |                             | Bootfile name not set |
|               | 10 Einträge. |              |                |                             |                       |
|               | -            |              |                |                             |                       |
| Erstellen Lö  | öschen Einst | tellungen üb | ernehmen Aktu  | alisieren                   |                       |

→ Verwenden Sie in beiden Pools, bei der Option 3 die Schnittstellen-IP und übernehmen Sie die Einstellungen.

 $(\rightarrow$  Pool-ID: 1  $\rightarrow$  Optionswert: 3  $\rightarrow$  Schnittstellen-IP verwenden)

 $(\rightarrow \text{Pool-ID: } 2 \rightarrow \text{Optionswert: } 3 \rightarrow \blacksquare \text{Schnittstellen-IP verwenden})$ 

(→ Einstellungen übernehmen)

DHCP-Client DHCP-Server DHCP-Optionen Statische Zuordnung

| Optionswert: |              |         |             |                             |                       |
|--------------|--------------|---------|-------------|-----------------------------|-----------------------|
|              | Selektieren  | Pool-ID | Optionswert | Schnittstellen-IP verwenden | Wert                  |
|              |              | 1       | 1           |                             | 255.255.255.0         |
|              |              | 1       | 3           | <b></b>                     | 192.168.1.254         |
|              |              | 1       | 6           |                             | 0.0.0.0               |
|              |              | 1       | 66          |                             |                       |
|              |              | 1       | 67          |                             | Bootfile name not set |
|              |              | 2       | 1           |                             | 255.255.255.0         |
|              |              | 2       | 3           | <b></b>                     | 10.0.0.254            |
|              |              | 2       | 6           |                             | 0.0.0.0               |
|              |              | 2       | 66          |                             |                       |
|              |              | 2       | 67          |                             | Bootfile name not set |
|              | 10 Einträge. |         |             |                             |                       |

- → Wechseln Sie zurück auf den DHCP-Server. (→ DHCP-Server)
- $\rightarrow$  Aktivieren Sie den DHCP-Server. ( $\rightarrow$   $\checkmark$  DHCP-Server)
- $\rightarrow$  Aktivieren Sie die beiden Pools. ( $\rightarrow$   $\checkmark$  Aktivieren)
- → Übernehmen Sie die Einstellungen (→ Einstellungen übernehmen)

| DHCP-Client D   | HCP-Server   | DHCP-Optionen Statisci | he Z | uordnung |                |               |               |      |  |  |  |
|---|--|------------------------|------|----------|----------------|---------------|---------------|------|--|--|--|
| DHCP-Server Adresse vor dem Anbieten mit ICMP-Echo prüfen               |  |                        |      |          |                |               |               |      |  |  |  |
| Selektieren   | Selektieren Pool-ID Schnittstelle Aktivieren Subnetz Untere IP-Adresse Obere IP-Adresse Gültigkeitsdauer [Sek] |                        |      |          |                |               |               |      |  |  |  |
|   | 1  | vlan1 (INT)            | Ŧ    | <b></b>  | 192.168.1.0/24 | 192.168.1.203 | 192.168.1.208 | 3600 |  |  |  |
|   | 2  | vlan2 (EXT)            | Ŧ    | <b></b>  | 10.0.0/24      | 10.0.0.1      | 10.0.0.127    | 3600 |  |  |  |
| 2 Einträge.<br>Erstellen Löschen Einstellungen übernehmen Aktualisieren |  |                        |      |          |                |               |               |      |  |  |  |

#### Hinweis:

 Der S615 wird darauffolgend auf den Ports 1 bis 4 Adressen aus dem Subnetz 192.168.1.0/24 verteilen und auf dem Port 5 aus dem Netz 10.0.0.0/24. Dabei wird er jeweils seine eigene IP als Gateway mitliefern.

- → Für die Einstellungen am Programmiergerät folgen Sie den Anweisungen im Abschnitt 4.6 bis zu den Einstellungen des Internetprotokolls, Version 4 (TCP/IP).
- → Beziehen Sie die IP-Adresse automatisch anstelle der statischen Konfiguration. ( $\rightarrow$  IP-Adresse automatisch beziehen  $\rightarrow$  DNS-Serveradresse automatisch beziehen)

| Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|
| Allgemein Alternative Konfiguration  |  |  |  |  |  |  |  |  |  |  |
| IP-Einstellungen können automatisch zugewiesen werden, wenn das<br>Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den<br>Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen. |  |  |  |  |  |  |  |  |  |  |
| IP-Adresse automatisch beziehen  |  |  |  |  |  |  |  |  |  |  |
| O Folgende IP-Adresse verwenden:   |  |  |  |  |  |  |  |  |  |  |
| IP-Adresse:  |  |  |  |  |  |  |  |  |  |  |
| Subnetzmaske:  |  |  |  |  |  |  |  |  |  |  |
| Standardgateway:   |  |  |  |  |  |  |  |  |  |  |
| DNS-Serveradresse automatisch beziehen   |  |  |  |  |  |  |  |  |  |  |
| O Folgende DNS-Serveradressen verwenden:   |  |  |  |  |  |  |  |  |  |  |
| Bevorzugter DNS-Server:  |  |  |  |  |  |  |  |  |  |  |
| Alternativer DNS-Server:   |  |  |  |  |  |  |  |  |  |  |
| Einstellungen beim Beenden überprüfen  |  |  |  |  |  |  |  |  |  |  |
| Erweitert  |  |  |  |  |  |  |  |  |  |  |
| OK Abbrechen   |  |  |  |  |  |  |  |  |  |  |

→ Bestätigen Sie die Änderungen und öffnen Sie in den Netzwerkverbindungen den Status der Verbindung. (→ LAN-Verbindung → Status)



 $\rightarrow$  Klicken Sie auf Details. ( $\rightarrow$  Details)

| Status von LAN-Verbindung           | ×        |
|-------------------------------------|----------|
| Allgemein                           |          |
| Verbindung                          |          |
| IPv4-Konnektivität: Kein Internetzu | ıgriff   |
| IPv6-Konnektivität: Kein Netzwerkzu | griff    |
| Medienstatus: Akti                  | viert    |
| Dauer: 02:1                         | 4:42     |
| Übertragungsrate: 1,0 G             | Bit/s    |
| Details                             |          |
| Aktivität                           |          |
| Gesendet — 🚛 — Empf                 | angen    |
| Bytes: 3.904.906 5.761              | .425     |
| Sigenschaften Diagnos Diagnos       | e        |
| Sc                                  | :hließen |

→ Stellen Sie sicher, dass das Programmiergerät eine passende IP-Adresse und ein Gateway zugewiesen bekommen hat.

| Netzwerkverbindungsdeta     | ils X                                |
|-----------------------------|--------------------------------------|
| Netzwerkverbindungsdetails: |                                      |
| Eigenschaft                 | Wert                                 |
| Verbindungsspezifisches     |                                      |
| Beschreibung                | Intel(R) PRO/1000 MT Desktop Adapter |
| Physische Adresse           | 08-00-27-9E-C9-15                    |
| DHCP-aktiviert              | Ja                                   |
| IPv4-Adresse                | 192.168.1.203                        |
| IPv4-Subnetzmaske           | 255.255.255.0                        |
| Lease erhalten              | Montag, 3. Juni 2019 19:15:39        |
| Lease läuft ab              | Montag, 3. Juni 2019 20:15:38        |
| IPv4-Standardgateway        | 192.168.1.254                        |
| IPv4-DHCP-Server            | 192.168.1.254                        |
| IPv4-DNS-Server             |                                      |
| IPv4-WINS-Server            |                                      |
| NetBIOS über TCPIP ak       | Ja                                   |
| Verbindungslokale IPv6      | fe80::e96f:1d1b:18f3:7d8f%6          |
| IPv6-Standardgateway        |                                      |
| IPv6-DNS-Server             |                                      |
| <                           | >                                    |
|                             |                                      |
|                             | Schließen                            |

## 7.5 Einrichten der Firewall

In der Werkskonfiguration lässt der SCALANCE S615 keine Verbindungen zwischen den beiden VLANs zu. Geräte an den Ports 1 bis 4 können also nicht mit Geräten am Port 5 kommunizieren und umgekehrt. Damit also Geräte z.B. aus dem Firmennetz auf den OPC UA Server der CPU zugreifen können muss diese Verbindung freigegeben werden."

 $\rightarrow$  Öffnen Sie die Firewall Einstellungen im Menü Security. ( $\rightarrow$  Security  $\rightarrow$  Firewall)

| SCALANCE S                        | 615 WEB Manageme × +   | -               | -              |                                    | ×      |
|-----------------------------------|--|-----------------|----------------|------------------------------------|--------|
| $\leftrightarrow$ $\rightarrow$ G | A Not secure https://192.168.1.254   | \$              | 9 Q            | θ                                  | *<br>* |
| SIEMENS                           | Labor/s615   | De<br>6/03/2019 | eutsch<br>20:1 | ▼ <u>Go</u><br>I:56 <sup>©</sup> ≑ | *      |
| Willkommen admin                  | Firewall Allgemein   |                 |                |                                    |        |
| Abmelden                          |  | E               | ?              | 8 *                                |        |
| ▶Wizards                          | Allgemein Vordefinierte IPv4-Regeln Benutzerspezifisch IP-Dienste ICMP-Dienste IP-Protokolle | P-Reg           | eln            |                                    | ۰,     |
| ► Information                     | <ul> <li>Firewall aktivieren</li> </ul>  |                 |                |                                    |        |
| ▶System                           | TCP Idle Timeout [s]: 86400  |                 |                |                                    |        |
| ▶Schnittstellen                   | ICMP Idle Timeout [s]: 300   |                 |                |                                    |        |
| ▶Layer 2                          | Einstellungen übernehmen Aktualisieren   |                 |                |                                    |        |
| ►Layer 3                          |  |                 |                |                                    |        |
| ✓Security                         |  |                 |                |                                    |        |
| ▶Benutzer                         |  |                 |                |                                    |        |
| ▶Passwörter                       |  |                 |                |                                    |        |
| ► AAA                             |  |                 |                |                                    |        |
| ► Firewall                        |  |                 |                |                                    |        |
| ▶IPsec VPN                        |  |                 |                |                                    |        |
| ▶ OpenVPN-<br>Client              |  |                 |                |                                    | Ŧ      |

→ Wechseln Sie auf den Reiter Vordefinierte IPv4-Regeln. (→ Vordefinierte IPv4-Regeln)

| Allgemei | n Vorde    | efinierte IPv | 4-Regeln   | Benutzersp | ezifisch   IF  | P-Dienste | ICMP-Dienste | P-Protoko | lle IP-Reg   | eln     |      |            |
|----------|------------|---------------|------------|------------|--|-----------|--------------|-----------|--|---------|------|------------|
|          |            |               |            |            |  |           |              |           |  |         |      |            |
| Gerä     | ite-Dienst | te erlauben:  |            |            |  |           |              |           |  |         |      |            |
| Schr     | ittstelle  | Alle          | HTTP       | HTTPS      | DNS  | SNMP      | Telnet       | IPsec VPN | SSH  | DHCP    | Ping | Systemzeit |
| vlan     | 1 (INT)    |               | <b></b>    | <b></b>    | Image: A start and a start | <b></b>   | <b></b>      |           | Image: A start and a start | <b></b> |      |            |
| vlan     | 2 (EXT)    |               |            |            |  |           |              | ✓         |  |         |      |            |
|          |            |               |            |            |  |           |              |           |  |         |      |            |
| Einste   | ellungen   | übernehmer    | n Aktualis | ieren      |  |           |              |           |  |         |      |            |

→ Erlauben Sie von extern den Zugriff via HTTPS und Ping auf den S615 und übernehmen Sie die Einstellungen. (→ vlan2 (EXT) →  $\checkmark$  HTTPS →  $\checkmark$  Ping)

| Allg | Ilgemein Vordefinierte IPv4-Regeln Benutzerspezifisch IP-Dienste ICMP-Dienste IP-Protokolle IP-Regeln |             |           |         |         |   |         |           |          |         |         |            |
|------|---|-------------|-----------|---------|---------|---|---------|-----------|----------|---------|---------|------------|
|      |   |             |           |         |         |   |         |           |          |         |         |            |
|      | Geräte-Dienst   | e erlauben: |           |         |         |   |         |           |          |         |         |            |
|      | Schnittstelle   | Alle        | HTTP      | HTTPS   | DNS     | SNMP  | Telnet  | IPsec VPN | SSH      | DHCP    | Ping    | Systemzeit |
|      | vlan1 (INT)   |             | <b></b>   | <b></b> | <b></b> | Image: A start and a start and a start a st | <b></b> |           | <b>e</b> | <b></b> | <b></b> |            |
|      | vlan2 (EXT)   |             |           | <b></b> |         |   |         |           |          | <b></b> | <b></b> |            |
|      |   |             |           |         |         |   |         |           |          |         |         |            |
| [    | Einstellungen i   | übernehmer  | Aktualisi | eren    |         |   |         |           |          |         |         |            |

#### Hinweis:

- Der Haken bei HTTPS erlaubt von außen den Zugriff auf die Konfigurationsoberfläche und sollte nicht unüberlegt eingeschaltet werden. Wir benötigen diesen Zugriff jedoch später für die Authentifizierung am S615. Da das außen angeschlossene Firmennetz kein öffentliches Netzwerk ist, ist das Risiko hier relativ gering. Ein am Internet angeschlossener SCALANCE S615 sollte von extern nur IPsec VPN, Ping und je nach Konfiguration DHCP erlauben.
- $\rightarrow$  Wechseln Sie in den Reiter IP-Dienste. ( $\rightarrow$  IP-Dienste)

| Allgemein | Vordefinie   | rte IPv4-Regeln | Benutzerspezifisch IF | Dienste ICMP-Dien | ste IP-Protokolle I  | P-Regeln            |
|-----------|--------------|-----------------|-----------------------|-------------------|----------------------|---------------------|
|           |              |                 |                       |                   |                      |                     |
| Name d    | les Diensts: |                 |                       |                   |                      |                     |
|           |              | Selektieren     | Name des Diensts      | Transport         | Quell-Port (Bereich) | Ziel-Port (Bereich) |
|           |              | 0 Einträge.     |                       |                   |                      |                     |
| Erstelle  | n Löschen    | Aktualisieren   |                       |                   |                      |                     |
|           |              |                 |                       |                   |                      |                     |

→ Erstellen Sie einen neuen Dienst für den Webserver der CPU. (→ Name des Diensts: https → Erstellen)

Allgemein Vordefinierte IPv4-Regeln Benutzerspezifisch IP-Dienste ICMP-Dienste IP-Protokolle IP-Regeln

| Name des Diensts: |                    |                     |           |                      |                     |
|-------------------|--------------------|---------------------|-----------|----------------------|---------------------|
|                   | Selektieren        | Name des Diensts    | Transport | Quell-Port (Bereich) | Ziel-Port (Bereich) |
|                   |                    | https               | TCP 🔻     | *                    | *                   |
|                   | 1 Eintrag.         |                     |           |                      |                     |
| Erstellen Löschen | Einstellungen über | nehmen Aktualisiere | en        |                      |                     |

→ Geben Sie den HTTPS Port als Ziel-Port an und übernehmen Sie die Einstellungen. ( $\rightarrow$  Ziel-Port: 443  $\rightarrow$  Einstellungen übernehmen)

| Allgemein Vordefinie | rte IPv4-Regeln Be | nutzerspezifisch IP | -Dienste ICMP-Die | nste IP-Protokolle IF | P-Regeln            |
|----------------------|--------------------|---------------------|-------------------|-----------------------|---------------------|
| Name des Diensts:    |                    |                     |                   |                       |                     |
|                      | Selektieren        | Name des Diensts    | Transport         | Quell-Port (Bereich)  | Ziel-Port (Bereich) |
|                      |                    | https               | TCP 🔻             | *                     | 443                 |
|                      | 1 Eintrag.         |                     |                   |                       |                     |
| Erstellen Löschen    | Einstellungen über | nehmen Aktualisiere | en                |                       |                     |

 $\rightarrow$  Wechseln Sie auf den Reiter IP-Regeln. ( $\rightarrow$  IP-Regeln)

| Allgemein | Vordefinierte IP | v4-Regeln   | Benutzerspezifisch | IP-Dienste | ICMP-Dienste | IP-Protokolle | IP-Regeln   |               |
|-----------|------------------|-------------|--------------------|------------|--------------|---------------|-------------|---------------|
|           |                  |             |                    |            |              |               |             |               |
| IP-Versi  | on: IPv4 v       |             |                    |            |              |               |             |               |
| Regelsa   | atz: _           | •           |                    |            |              |               |             |               |
|           | 🕑 Alle anzei     | gen         |                    |            |              |               |             |               |
|           | Selektieren      | Protokoll   | Aktion             | Von        | Nach         | Quell         | e (Bereich) | Ziel (Bereich |
|           | •                |             |                    |            |              |               |             | ۱. E          |
|           | 0 Einträge.      |             |                    |            |              |               |             |               |
| Erstelle  | n Löschen Ak     | tualisieren |                    |            |              |               |             |               |

 $\rightarrow$  Erstellen Sie eine neue Regel. ( $\rightarrow$  Erstellen)

| Allgemein | Vordefinierte IP | v4-Regeln     | Benutzerspezifisch | IP-Dienste  | ICMP-Dienste                  | IP-Protokolle | IP-Regeln     |    |
|-----------|------------------|---------------|--------------------|-------------|-------------------------------|---------------|---------------|----|
|           |                  |               |                    |             |                               |               |               |    |
| IP-Versi  | on: IPv4 🔻       |               |                    |             |                               |               |               |    |
| Regelsa   | atz: -           | •             |                    |             |                               |               |               |    |
|           | 🕑 Alle anzeig    | gen           |                    |             |                               |               |               |    |
|           | Selektieren      | Protokoll     | Aktion             | Von         | Nach                          | Que           | lle (Bereich) |    |
|           |                  | IPv4          | Drop 🔻             | vlan1 (INT) | <ul> <li>vlan1 (IN</li> </ul> | T) ▼ 0.0.     | 0.0/0         |    |
|           |                  |               |                    |             |                               |               |               | ۱. |
|           | 1 Eintrag.       |               |                    |             |                               |               |               |    |
|           |                  |               |                    |             |                               |               |               |    |
| Erstelle  | n Löschen Ein    | istellungen ü | bernehmen Aktuali  | sieren      |                               |               |               |    |

- $\rightarrow$  Stellen Sie die Aktion auf Accept. ( $\rightarrow$  Aktion: Accept)
- $\rightarrow$  Wählen Sie als Quell-Interface vlan2 aus. ( $\rightarrow$  Von: vlan2 (EXT))
- $\rightarrow$  Wählen Sie als Ziel-Interface vlan1 aus. ( $\rightarrow$  Nach: vlan1 (INT))
- $\rightarrow$  Geben Sie als Quellnetz das Firmensubnetz 10.0.0.0/24 an. ( $\rightarrow$  Quelle: 10.0.0.0/24)
- $\rightarrow$  Geben Sie Ziel die X2 IP der S7-1500 an. ( $\rightarrow$  Ziel: 192.168.1.1/32)
- → Wählen Sie als Dienst den soeben erstellten HTTPS Dienst aus. (→ Dienst: https)
- → Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)

| Selektieren   | Protokoll | Aktion | Von                             | Nach                           |         |
|---------------|-----------|--------|---------------------------------|--------------------------------|---------|
|               | IPv4      | Accept | <ul> <li>vlan2 (EXT)</li> </ul> | <ul> <li>vlan1 (INT</li> </ul> | ) 🔻     |
|               |           |        |                                 |                                |         |
| Quelle (Berei | ch)       | Z      | iel (Bereich)                   | [                              | Dienst  |
| 10.0.0/24     |           | 1      | 92.168.1.1/32                   |                                | https 🔻 |

| Allgemein | Vordefinierte IP | v4-Regeln     | Benutzerspezifisch | h IP-Dienste | ICMP-Dienste                   | IP-Protokoll | e IP-Regeln    |   |
|-----------|------------------|---------------|--------------------|--------------|--------------------------------|--------------|----------------|---|
|           |                  |               |                    |              |                                |              |                |   |
| IP-Versi  | on: IPv4 🔻       |               |                    |              |                                |              |                |   |
| Regelsa   | atz: _           | T             |                    |              |                                |              |                |   |
|           | 🗌 Alle anzei     | gen           |                    |              |                                |              |                |   |
|           | Selektieren      | Protokoll     | Aktion             | Von          | Nach                           | Qu           | elle (Bereich) |   |
|           |                  | IPv4          | Accept 🔻           | vlan2 (EXT)  | <ul> <li>vlan1 (IN)</li> </ul> | T) 🔻 10.     | 0.0.0/24       |   |
|           | •                |               |                    |              |                                |              |                | + |
|           | 1 Eintrag.       |               |                    |              |                                |              |                |   |
| Erstelle  | n Löschen Eir    | istellungen ú | ibernehmen Aktual  | isieren      |                                |              |                |   |

## 7.6 Einrichten des Service Benutzers

Nachdem der Zugriff auf den Webserver von außen eingerichtet worden ist, werden im nächsten Schritt spezifische Regeln angelegt, welche durch die Anmeldung am System mittels eines Benutzers, freigeschaltet werden.

 $\rightarrow$  Öffnen Sie die Lokale Benutzerverwaltung. ( $\rightarrow$  Security  $\rightarrow$  Benutzer  $\rightarrow$  Lokale Benutzer)

|                  |                                  |                       |                           |       |                           | Deutsch 🔻 💁                  |
|------------------|----------------------------------|-----------------------|---------------------------|-------|---------------------------|------------------------------|
| SIEWIENS         | Labor/s615                       |                       |                           |       |                           | 06/04/2019 11:41:16 <b>%</b> |
| Willkommen admin | Lokale Benutzer                  |                       |                           |       |                           |                              |
| Abmelden         |                                  |                       |                           |       |                           | <b>□ ?</b> ≞ ★               |
| ▶Wizards         | Lokale Benutzer Rollen           | Gruppen               |                           |       |                           |                              |
| ► Information    | Benutzerkonto:                   |                       |                           |       |                           |                              |
| ▶System          | Passwortrichtlinie:<br>Passwort: | Hoch                  |                           |       |                           |                              |
| ▶Schnittstellen  | Passwort bestätigen:             |                       |                           |       |                           |                              |
| ▶Layer 2         | ruie.                            | user •<br>Belektieren | Benutzerkonto             | Rolle | Beschreibung              | Remote-Zi                    |
| ▶Layer 3         |                                  | 4                     | admin                     | admin | System defined local user | Keine                        |
| ✓Security        | 1                                | Eintrag.              |                           |       |                           |                              |
| ▶Benutzer        | Erstellen Löschen F              | instellunge           | n übernehmen Aktualisiere | 1     |                           |                              |
| ▶Passwörter      | Elotononi Edocrioni              | Instantigo            | Automotion Automotion of  | -     |                           |                              |
| ►AAA             |                                  |                       |                           |       |                           |                              |
| ► Eirowall       |                                  |                       |                           |       |                           |                              |
| HPsec VPN        |                                  |                       |                           |       |                           |                              |
| ► OpenVPN-       |                                  |                       |                           |       |                           |                              |
| Cildin           |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           |                              |
|                  |                                  |                       |                           |       |                           | -                            |

- $\rightarrow$  Geben Sie einen neuen Benutzernamen an. ( $\rightarrow$  Benutzerkonto: Support)
- → Geben Sie ein Passwort an. (→ Passwort: \*\*\* → Passwort bestätigen: \*\*\*)
- $\rightarrow$  Wählen Sie als Rolle "user" aus. ( $\rightarrow$  Rolle: user)

| Benutzerkonto:       | support |
|----------------------|---------|
| Passwortrichtlinie:  | Hoch    |
| Passwort:            |         |
| Passwort bestätigen: | ••••••  |
| Rolle:               | user 🔻  |

 $\rightarrow$  Klicken Sie auf Erstellen. ( $\rightarrow$  Erstellen)

| Lokale Benutzer | Rollen     | Gruppen       |                          |       |                           |
|-----------------|------------|---------------|--------------------------|-------|---------------------------|
|                 |            |               |                          |       |                           |
| Denviren        |            |               |                          |       |                           |
| Benutzer        | KONIO:     |               |                          |       |                           |
| Passwortrick    | htlinie: H | Hoch          |                          |       |                           |
| Pas             | swort:     |               |                          |       |                           |
| Passwort besta  | ätigen:    |               |                          |       |                           |
|                 | Rolle:     | user 🔻        |                          |       |                           |
|                 | 5          | Selektieren   | Benutzerkonto            | Rolle | Beschreibung              |
|                 |            |               | admin                    | admin | System defined local user |
|                 |            |               | support                  | user  |                           |
|                 |            | 4             |                          |       | •                         |
|                 | 2          | Einträge.     |                          |       |                           |
|                 |            |               |                          |       |                           |
| Erstellen Lös   | chen       | Einstellungen | übernehmen Aktualisieren |       |                           |

- $\rightarrow$  Wählen Sie als Remote-Zugriff "nur" aus. ( $\rightarrow$  support  $\rightarrow$  Remote-Zugriff: nur)
- $\rightarrow$  Übernehmen Sie die Einstellungen. ( $\rightarrow$  Einstellungen übernehmen)

| Lokale Benutzer Rolle | n Gruppen     |                          |       |                           |                |
|-----------------------|---------------|--------------------------|-------|---------------------------|----------------|
|                       |               |                          |       |                           |                |
| Benutzerkonto:        |               |                          |       |                           |                |
| Passwortrichtlinie:   | Hoch          |                          |       |                           |                |
| Passwort:             |               |                          |       |                           |                |
| Passwort bestätigen:  |               |                          |       |                           |                |
| Rolle:                | user 🔻        |                          |       |                           |                |
|                       | Selektieren   | Benutzerkonto            | Rolle | Beschreibung              | Remote-Zugriff |
|                       |               | admin                    | admin | System defined local user | Keine 🔻        |
|                       |               | support                  | user  |                           | Nur 🔻          |
|                       | 2 Einträge.   |                          |       |                           |                |
|                       |               |                          |       |                           |                |
| Erstellen Löschen     | Einstellungen | übernehmen Aktualisieren |       |                           |                |

- $\rightarrow$  Wechseln Sie unter Firewall in den Reiter Benutzerspezifisch.
  - $(\rightarrow \text{Security} \rightarrow \text{Firewall} \rightarrow \text{Benutzerspezifisch})$

| JILIVIENS                               | Labo      | or/s61      | 5          |                |                       |                   |   |
|---|-----------|-------------|------------|----------------|-----------------------|-------------------|---|
| Willkommen admin                        | Benut     | zerspezifi  | sch        |                |                       |                   |   |
| Abmelden                                |           |             |            |                |                       |                   |   |
| ►Wizards                                | Allgemein | Vordefinie  | rte IPv4-R | egeln Benutz   | erspezifisch IP-Diens | te ICMP-Dienste I | P-Protokolle IP-Regeln  |
| ► Information                           |           | Regelsatz   |            |                |                       |                   |   |
| ▶System                                 | Name:     | Calaldiaraa | Mr         | Nama           | Kommontor             |                   | Time out [min]  |
| Schnittstellen                          |           | 0 Einträge. | INL.       | Name           | Kommentar             |                   | rimeour (mini)  |
| NL aver 2                               |           |             |            |                |                       |                   |   |
| N aver 3                                |           | Zuordnung F | Regelsatz  |                |                       |                   |   |
| -Security                               | Тур:      | User Accou  | nt 🔻       |                |                       |                   |   |
| Benutzer                                |           | Benutzerkor | nto F      | tolle          | Regelsatz             | Verbleibende Zeit | Deaktivieren erzwingen  |
| ▶Passwörter                             |           |             |            |                |                       |                   | o o ana construction o a |
| ►AAA<br>►Zertifikate                    | Erstell   | en Löschen  | Einstellu  | ingen übernehi | Men Aktualisieren     |                   |   |
| Firewall                                |           |             |            |                |                       |                   |   |
| ▶IPsec VPN                              |           |             |            |                |                       |                   |   |
| <ul> <li>OpenVPN-<br/>Client</li> </ul> |           |             |            |                |                       |                   |   |
|   |           |             |            |                |                       |                   |   |

→ Fügen Sie einen neuen Regelsatz "support\_regeln" hinzu. (→ Regelsatz → Name: support\_regeln → Erstellen)

| Name:  | Regelsatz<br>support_rege | In           |                 |                           |  |
|--------|---------------------------|--------------|-----------------|---------------------------|--|
|        | Selektieren               | Nr.          | Name            | Kommentar                 | Timeout [min]                          |
|        | 0 Einträge.               |              |                 |                           |  |
| Allgem | ein Vordefin              | ierte IPv4-F | Regeln Benutzer | rspezifisch IP-Dienste IC | MP-Dienste IP-Protokolle IP-Regeln     |
|        |                           |              |                 |                           |  |
|        | Regelsatz                 |              |                 |                           |  |
| Nan    | ne:                       |              |                 |                           |  |
|        | Selektiere                | n Nr.        | Name            | Kommentar                 | Timeout [min]                          |
|        |                           | 1            | support_rege    | ln                        | 30                                     |
|        | 1 Eintrag.                |              |                 |                           |  |
|        |                           |              |                 |                           |  |
|        |                           |              |                 |                           |  |
|        | Zuordnung                 | g Regelsatz  |                 |                           |  |
| Т      | yp: User Acc              | ount 🔻       |                 |                           |  |
|        | Poputzork                 | onto         | Pollo           | Pogoloatz Vor             | rbleibende Zeit Deaktivieren erzwingen |
|        | support                   | Unito        | user            | rtegeisaiz vei            | Deaktivieren erzwingen                 |
|        | Support                   |              | user            |                           | Deakuvieren eizwingen                  |
| Erst   | tellen Lösche             | en Einstell  | ungen übernehme | Aktualisieren             |  |

- → Ordnen Sie dem Benutzer "support" den Regelsatz "support\_regeln" zu. (→ Zuordnung Regelsatz → support → Regelsatz: support\_regeln)
- $\rightarrow$  Übernehmen Sie die neuen Einstellungen. ( $\rightarrow$  Einstellungen übernehmen)

| Тур:    | Zuordnung Regelsat | 2                  |                  |                   |                        |
|---------|--------------------|--------------------|------------------|-------------------|------------------------|
|         | Benutzerkonto      | Rolle              | Regelsatz        | Verbleibende Zeit | Deaktivieren erzwingen |
|         | support            | user               | support_regeln 🔻 | -                 | Deaktivieren erzwingen |
| Erstell | en Löschen Einste  | llungen übernehmen | Aktualisieren    |                   |                        |

### Hinweis:

 Hierdurch wird auf dem Computer des Benutzers "support", nach erfolgreicher Anmeldung am System, das zusätzliche Regelwerk "support\_regeln" angewendet.  $\rightarrow$  Wechseln Sie in den Reiter IP-Regeln. ( $\rightarrow$  Security  $\rightarrow$  Firewall  $\rightarrow$  IP-Regeln)

| SIEMENS              |  | Deutsch 🔻 Go                 |
|----------------------|--|------------------------------|
|                      | Labor/s615   | 06/03/2019 18:50:52 <b>%</b> |
| Willkommen admin     | Internet Protocol (IP) Regeln  |                              |
|                      |  | <b>□?</b> ► ★                |
| Abmelden             | Allgemein Vordefinierte IPv4.Regeln Reputzerspezifisch IP.Dienste ICMP.Dienste IP.Protokolle IP.Regeln                             |                              |
| ▶Wizards             |  |                              |
| ►Information         | IP-Version: IPv4 v   |                              |
| ▶ Svstom             | Regelsatz: -   |                              |
| Poystein             | Alle anzeigen  |                              |
| Schnittstellen       | Selektieren Protokoll Aktion Von Nach Quelle (Bereich) Ziel (Bereich)  | Dienst Log                   |
| ▶Layer 2             | IPv4         Accept         V         vian2 (EXT)         V         vian1 (INT)         v         10.0.0/24         192.168.1.1/32 | https 🔻 none 🔻               |
| N avor 2             | 1 Fintrag  | ,                            |
| PLayer 5             |  |                              |
| -Security            | Erstellen Löschen Einstellungen übernehmen Aktualisieren   |                              |
| ▶Benutzer            |  |                              |
| Passwörter           |  |                              |
| ►AAA                 |  |                              |
| ►Zertifikate         |  |                              |
| Firewall             |  |                              |
| ▶IPsec VPN           |  |                              |
| ► OpenVPN-<br>Client |  |                              |

- $\rightarrow$  Erstellen Sie eine neue Regel. ( $\rightarrow$  Erstellen)
- $\rightarrow$  Stellen Sie die Aktion auf Accept. ( $\rightarrow$  Aktion: Accept)
- $\rightarrow$  Wählen Sie als Quell-Interface vlan2 aus. ( $\rightarrow$  Von: vlan2 (EXT))
- $\rightarrow$  Wählen Sie als Ziel-Interface vlan1 aus. ( $\rightarrow$  Nach: vlan1 (INT))
- $\rightarrow$  Geben Sie als Quellnetz "DYNAMIC" an. ( $\rightarrow$  Quelle: DYNAMIC)
- $\rightarrow$  Geben Sie als Ziel die X2 IP der S7-1500 an. ( $\rightarrow$  Ziel: 192.168.1.1/32)
- $\rightarrow$  Wählen Sie als Dienst "all" aus. ( $\rightarrow$  Dienst: all)
- → Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)

|         | IPv4 | Accept | <ul> <li>vlan2 (EXT)</li> </ul> | <ul> <li>vlan1 (I)</li> </ul> | T) T | · |
|---------|------|--------|---------------------------------|-------------------------------|------|---|
|         |      |        |                                 |                               |      |   |
| DYNAMIC |      | 19     | 92.168.1.1/32                   |                               | all  | • |

| Allgemein | Vordefinierte IF      | v4-Regeln    | Benutzerspezif | isch   | IP-Dienste  | ICMI | P-Dienste  | IP-Pro | tokoll                  | IP-Regeln     |                |         |      |   |
|-----------|-----------------------|--------------|----------------|--------|-------------|------|------------|--------|-------------------------|---------------|----------------|---------|------|---|
|           |                       |              |                |        |             |      |            |        |                         |               |                |         |      |   |
| IP-Versi  | on: IPv4 v            |              |                |        |             |      |            |        |                         |               |                |         |      |   |
| Regelsa   | atz: 🕒                | ¥            |                |        |             |      |            |        |                         |               |                |         |      |   |
|           | Alle anzei            | gen          |                |        |             |      |            |        |                         |               |                |         |      |   |
|           | Selektieren           | Protokoll    | Aktion         | V      | /on         |      | Nach       |        | Que                     | lle (Bereich) | Ziel (Bereich) | Dienst  | Log  |   |
|           |                       | IPv4         | Accept         | •      | vlan2 (EXT) | •    | vlan1 (INT | r) '   | <ul> <li>10.</li> </ul> | .0.0/24       | 192.168.1.1/32 | https 🔻 | none | • |
|           |                       | IPv4         | Accept         | •      | vlan2 (EXT) | ۲    | vlan1 (IN1 | r) '   | <ul> <li>DY</li> </ul>  | IAMIC         | 192.168.1.1/32 | all 🔻   | none | ۲ |
|           | •                     |              |                |        |             |      |            |        |                         |               |                |         |      | • |
|           | 2 Einträge.           |              |                |        |             |      |            |        |                         |               |                |         |      |   |
| Erctollo  | n Löschon <b>Fi</b> r | stellungen ( | bornohmon Ak   | tualia | tioron      |      |            |        |                         |               |                |         |      |   |

→ Wählen Sie als Nächstes unter Regelsatz "support\_regeln" aus. (→ Regelsatz: support\_regeln →  $\checkmark$  Alle anzeigen)

| Allgemein Vordefinierte IPv4-Regeln E                                | Benutzerspezifisch | IP-Dienste | ICMP-Dienste | IP-Protokolle | IP-Regeln |  |
|--|--------------------|------------|--------------|---------------|-----------|--|
| IP-Version: IPv4 ▼<br>Regelsatz: support_regelr ▼<br>✔ Alle anzeigen |                    |            |              |               |           |  |

 $\rightarrow$  Markieren Sie bei der soeben angelegten Regel die Option Zuordnen. ( $\rightarrow$  Zuordnen)

| 1 | Nach          | Quelle (Bereich) | Ziel (Bereich) | Dienst  | Log    | Reihenfolge | Zuordnen | Zugeordnet |
|---|---------------|------------------|----------------|---------|--------|-------------|----------|------------|
| l | vlan1 (INT)   | 10.0.0/24        | 192.168.1.1/32 | https 🔻 | none 🔻 | 0           |          | -          |
| l | vlan1 (INT) 🔻 | DYNAMIC          | 192.168.1.1/32 | all 🔻   | none 🔻 | 1           | <b></b>  | all        |
|   | 4             |                  |                |         |        |             |          |            |

→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)

| Allgemein | Vordefinierte IP | v4-Regeln    | Benutzerspezif | isch   | IP-Dienste  | ICM | P-Dienste | IP-Pro | tok | olle IP-Regeln  |                |         |      |   |
|-----------|------------------|--------------|----------------|--------|-------------|-----|-----------|--------|-----|-----------------|----------------|---------|------|---|
|           |                  |              |                |        |             |     |           |        |     |                 |                |         |      |   |
| IP-Versi  | on: IPv4 v       |              |                |        |             |     |           |        |     |                 |                |         |      |   |
| Regelsa   | atz: support_reg | elr 🔻        |                |        |             |     |           |        |     |                 |                |         |      |   |
|           | 🕑 Alle anzeig    | gen          |                |        |             |     |           |        |     |                 |                |         |      |   |
|           | Selektieren      | Protokoll    | Aktion         | ١      | /on         |     | Nach      |        | (   | uelle (Bereich) | Ziel (Bereich) | Dienst  | Log  |   |
|           |                  | IPv4         | Accept         | •      | vlan2 (EXT) | ۲   | vlan1 (IN | T) '   | •   | 0.0.0/24        | 192.168.1.1/32 | https 🔻 | none | ۲ |
|           |                  | IPv4         | Accept         | •      | vlan2 (EXT) | •   | vlan1 (IN | T) 1   | •   | YNAMIC          | 192.168.1.1/32 | all 🔻   | none | • |
|           | 4                |              |                |        |             |     |           |        |     |                 |                |         |      | • |
|           | 2 Einträge.      |              |                |        |             |     |           |        |     |                 |                |         |      |   |
| Erstelle  | n Löschen Ein    | stellungen ü | ibernehmen Ak  | tualis | sieren      |     |           |        |     |                 |                |         |      |   |

#### Hinweis:

 Der Platzhalter DYNAMIC wird bei der Anmeldung mit der IP des angemeldeten Benutzers ersetzt. Durch die Zuordnung der Regel an das Regelwerk "support\_regeln" ist diese erst aktiv, nachdem der entsprechende Benutzer sich angemeldet hat.

## 7.7 Konfiguration der CPU 1516F

Daraufhin muss in der CPU 1516F die Netzwerkkonfiguration angepasst und übertragen werden.

- → Verbinden Sie die Schnittstelle X2 der CPU 1516F-3 PN/DP mit dem Port 1 des SCALANCE S615.
- → Öffnen Sie im TIA Portal die Eigenschaften der X2-Schnittstelle der CPU\_1516F. ( $\rightarrow$  CPU\_1516F  $\rightarrow$  X2  $\rightarrow$  Eigenschaften)
- → Wechseln Sie in die IP-Konfiguration. (→ Ethernet-Adressen → IP-Protokoll)

| Eigenschaften                    |                   |                          |            |             |                       |                 |            |   |
|----------------------------------|-------------------|--------------------------|------------|-------------|-----------------------|-----------------|------------|---|
| PROFINET-Schr                    | nittstelle_2 [X2] |                          |            |             | 🔍 Eigenschaften       | 🛄 Info          | 🛿 Diagnose |   |
| Allgemein                        | IO-Variablen      | Systemkonstanten         | Texte      |             |                       |                 |            |   |
| Allgemein<br>F-Parameter         |                   | Ethernet-Adressen        |            |             |                       |                 |            | * |
| Ethernet-Adres<br>Uhrzeitsynchro | sen<br>nisation   | Schnittstelle vernetzt n | nit        |             |                       |                 |            |   |
| Betriebsart                      |                   | Sul                      | bnetz: nic | ht vernetzt | t                     |                 | -          |   |
| Erweiterte Opti                  | ionen             |                          | N          | eues Subn   | etz hinzufügen        |                 |            |   |
| Zugriffaufden                    | Webserver         |                          |            |             |                       |                 |            |   |
|                                  | •                 | IP-Protokoll             |            |             |                       |                 |            |   |
|                                  | •                 |                          | ا 📀        | P-Adresse   | im Projekt einstellen |                 |            |   |
|                                  |                   |                          |            | IP-Ac       | dresse: 192.168       | 3.1.1           |            |   |
|                                  |                   |                          |            | Subnetzr    | maske: 255 . 255      | 5.255.0         |            |   |
|                                  |                   |                          |            | Router verv | venden                |                 |            |   |
|                                  |                   |                          |            | Router-Ad   | dresse: 0.0           | .0.0            |            |   |
|                                  |                   |                          | 0,         | Anpassen    | der IP-Adresse direkt | am Gerät erlaub | en         |   |
|                                  |                   |                          |            |             |                       |                 |            | ¥ |

→ Stellen Sie die IP-Adresse des S615 als Router ein. (→  $\blacksquare$ Router verwenden → Router-Adresse: 192.168.1.254)

| IP-Protokoll |                      |                                |
|--------------|----------------------|--------------------------------|
|              | IP-Adresse im Projel | kt einstellen                  |
|              | IP-Adresse:          | 192.168.1.1                    |
|              | Subnetzmaske:        | 255 . 255 . 255 . 0            |
|              | 🛃 Router verwenden   |                                |
|              | Router-Adresse:      | 192 . 168 . 1 . 254            |
|              | 🔵 Anpassen der IP-Ad | resse direkt am Gerät erlauben |

→ Öffnen Sie die Eigenschaften des Webservers der CPU 1516F-3 PN/DP. ( $\rightarrow$  CPU\_1516F  $\rightarrow$  Eigenschaften  $\rightarrow$  Webserver)

| CPU 1516F [CF    | U 1516F-3 PN/DF  |     |                  |                |              | Q Fig                | enschaften      | 1 Info | P. Diagnose | e   |
|------------------|------------------|-----|------------------|----------------|--------------|----------------------|-----------------|--------|-------------|-----|
| Allgemein        | IO-Variablen     | Sys | stemkonstanten   | Texte          | 1            |                      | ,               |        |             |     |
| DP-Schnittstelle | [X3]             |     | ]                |                |              |                      |                 |        |             |     |
| Anlauf           | 1001             |     | Webserver        |                |              |                      |                 |        |             | - 1 |
| Zvklus           |                  |     |                  |                |              |                      |                 |        |             |     |
| Kommunikation    | nslast           |     | Algemein         |                |              |                      |                 |        |             | -   |
| System- und Ta   | ktmerker         |     |                  |                |              |                      |                 |        |             |     |
| SIMATIC Memor    | y Card           |     |                  |                | Webserve     | er auf dieser Baugn  | uppe aktivieren |        |             |     |
| Systemdiagnos    | e                |     |                  |                | - Zugriff nu | ur über HTTPS zulass |                 |        |             |     |
| PLC-Meldungen    |                  |     |                  |                | Zuginini     | n aber min 5 zalas.  |                 |        |             |     |
| Webserver        |                  |     |                  |                |              |                      |                 |        |             |     |
| Allgemein        |                  |     | Automatische Akt | ualisierung    |              |                      |                 |        |             |     |
| Automatisch      | e Aktualisierung |     |                  |                |              |                      |                 |        |             |     |
| Benutzerven      | waltung          |     |                  |                | 🗹 Automat    | ische Aktualisierun  | g aktivieren    |        |             |     |
| Security         |                  |     | Aktualisi        | ierungsinterva |              |                      | <               |        |             |     |
| Beobachtun       | gstabellen       | -   |                  | ierangsmeerre  |              |                      | -               |        |             |     |
| Anwenderse       | iten             |     | Poputangonualtu  |                |              |                      |                 |        |             |     |
| Einstiegssei     | te               |     | benuizerverwaltu | ing            |              |                      |                 |        |             | =1  |
| Übersicht de     | r Schnittstellen |     |                  |                |              |                      |                 |        |             |     |
| DNS-Konfigurat   | ion              |     | Passwortverse    | chlüsselung a  | ktualisieren |                      |                 |        |             |     |
| Display          |                  |     | Name             | 7              | ugriffsstufe | Passwort             |                 |        |             |     |
| Mehrsprachigke   | eit              |     | leder            |                | /inimal      |                      |                 |        |             |     |
| Uhrzeit          |                  |     | Neuen            | Benutzer       |              |                      |                 |        |             |     |
| Schutz & Securi  | ty               |     |                  |                |              |                      |                 |        |             |     |
| OPC UA           |                  |     |                  |                |              |                      |                 |        |             |     |
| Systemstromye    | rsorauna         | ~   |                  |                |              |                      |                 |        |             |     |

aktivieren)  $\rightarrow$  Schränken Sie den Zugriff auf HTTPS ein. ( $\rightarrow$  Allgemein  $\rightarrow$   $\checkmark$  Zugriff nur über HTTPS

zulassen)

Allgemein \_\_\_\_\_

| Webserver auf dieser Baugruppe aktivieren |
|---|
|   |

 $\rightarrow$  Legen Sie einen neuen Benutzer an. ( $\rightarrow$  Benutzerverwaltung  $\rightarrow$  Name: admin  $\rightarrow$  Passwort: \*\*\*)

| Benut | zerverwaltung   |                |          |  |
|-------|---|----------------|----------|--|
|       | a success and the solution                                    | alitualisiasan |          |  |
|       | asswortverschlusselung  | aktualisieren  |          |  |
|       | Name  | Zugriffsstufe  | Passwort |  |
|       | Jeder   | Minimal        |          |  |
|       | admin   | Minimal 💌      | *****    |  |
|       | <neuen benutzer<="" td=""><td></td><td></td><td></td></neuen> |                |          |  |
|       |   |                |          |  |

→ Setzen Sie hier die Zugriffsstufe des neuen Benutzers auf Administrativ. (→ Benutzerverwaltung → admin → Zugriffsstufe → Administrativ)

| Administrativ 💌 *********                  |
|--|
| Der Benutzer ist autorisiert               |
| 🗹die Diagnose abzufragen                   |
| 🗹Variablen zu lesen                        |
| 🗹Variablen zu schreiben                    |
| 🗹den Variablenstatus zu lesen              |
| 🗹den Variablenstatus zu schreiben          |
| 🗹Meldungen zu quittieren                   |
| 🗹anwenderdefinierte Seiten aufzurufen      |
| 🗹in anwenderdefinierte Seiten zu schreiben |
| 🗹Dateien zu lesen                          |
| 🗹Dateien zu schreiben/löschen              |
| 🛃den Betriebszustand zu ändern             |
| 🛃die LED blinken zu lassen                 |
| 🛃ein Firmware-Update durchzuführen         |
| Systemparameter zu ändern                  |
| Anwendungsparameter zu ändern              |
| 🛃eine Sicherung der PLC zu erstellen       |
| eine Sicherung auf die PLC zu laden        |
| 🗹Änderungen als F-Admin durchzuführen 📃    |
|  |

→ Aktivieren Sie nun den Webserver auf der Schnittstelle X2. (→ Übersicht der Schnittstellen → PROFINET-Schnittstelle\_2)

Übersicht der Schnittstellen

| Gerät     | Schnittstelle            | Zugriff auf den W |
|-----------|--------------------------|-------------------|
| CPU_1516F | PROFINET-Schnittstelle_1 |                   |
| CPU_1516F | PROFINET-Schnittstelle_2 |                   |

→ Laden Sie die Konfiguration in die CPU. (→ CPU\_1516F →  $\boxed{1}$  →  $\boxed{1}$ )

| K Siemens - C:\00_TIA_Portal\140-200_Indust | ial_Security_mit_S6151140-200_Industrial_Security_mit_S615   | _ ¤ ×                        |
|---|--|------------------------------|
| Projekt Bearbeiten Ansicht Einfügen Onlin   | e Extras Werkzeuge Fenster Hilfe To  | otally Integrated Automation |
| 📑 🎦 🔚 Projekt speichern 📇 🐰 🗐 🗐 🗙           | S ± (* ± 🖥 🛄 🗊 🖳 🖉 Online verbinden 🖉 Online-Verbindung trennen 🐰 🖪 🖉 📩 📜 '  | PORTAL                       |
| Projektnavigation 🔲 📢                       | 140-200_Industrian_security_init_S615 ► Geräte & Netze   | Hardware-Katalog 📑 🗉 🕨       |
| Geräte                                      | 🔐 Topologiesicht 🛛 🔒 Netzsicht 🔄 👔 Gerätesicht   | Optionen 💷                   |
| 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1       | 💦 Vernetzen 🔢 Verbindungen 🖃 HM-Verbindung 🔍 🕅 🗮 🖽 🛄 🍳 🛨 📑   | Har                          |
| 0   |  | × Katalog                    |
| 🗧 💌 📋 140-200_Industrial_Security_mit_S615  |  | Suchers                      |
| a Neues Gerät hinzufügen                    |  |                              |
| e 💼 Geräte & Netze                          | CPU_1516F  | Filter <alie></alie>         |
| CPU_1516F [CPU 1516F-3 PN/DP]               |  |                              |
| Nicht gruppierte Gerate                     |  | PC-Systeme                   |
| Gemeinsame Daten                            |  | Antriebe & Starter           |
| Dokumentationseinstellungen                 | PN/E_1   | ▼ In Netzkomponenten         |
| Sprachen & Ressourcen                       |  | ا 🛱 IE Switches 🖗            |
| Online-Zugänge                              | - The second sec | 🕨 🛅 IWLAN                    |
| Card Reader/USB-Speicher                    |  | 👻 🗽 Industrial Security 🛛 🗖  |
|   |  | Security-Gerät               |
|   |  | SCALANCE M                   |
|   |  | CI SCALANCE S                |
|   |  | 66K5 632-26                  |
|   |  | 6GK5 636-2G                  |
|   | · · · · · · · · · · · · · · · · · · ·  | 6GK5 642-2G                  |
|   | < III > 100%   | 🚺 6GK5 646-2G 🛄              |
|   | 🔍 Eigenschaften 🔣 Info 🖳 Diagnose 💷 🖃  | [ 6GK5 602-0BA1 ₩            |
|   | Alleemein Quenenanise Übersetzen   | GGK5 612-0BA1                |
|   |  | 6GK5 623-0BA1                |
| ✓ Detailansicht                             | Alle Meldungen anzeigen  | 6GK5 627-2BA1                |
| Module                                      | Ubersetzen beendet (Fehler: 0; Warnungen: 4)   | Pouter                       |
|   | Prad     Beschreibung     Gehe zu ?     Fe   | Diagnose-Repeater            |
| Name  | Des Display der 57-1500 CPU enthalt keinen Passwort-schutz.  | ▶ 📑 Erfassen & Überwachen    |
| Gerätekonfiguration                         | Kein Baustein wurde übersetzt. Alle Bausteine sind aktuell.  | 🕨 🧊 Dezentrale Peripherie    |
| Soline & Diagnose                           | Übersetzen beendet (Fehler: 0; Warnungen: 4)   | 🕨 🛅 Stromversorgung und -v 💙 |
| g Programmbausteine                         |  |                              |
|   |  | Information                  |
| Portalansicht 🔀 Übersicht                   | 🚠 Geräte & Net 🗄 🗹 Die Parameter wu  | ırden erfolgreich über 🏼 🎾   |

→ Achten Sie beim Ladevorgang darauf, dass Sie nun mit der Schnittstelle X2 verbunden sind.
 (→ Verbindung mit Schnittstelle/Subnetz: Direkt an Steckplatz ,1 X2')

| Erweitertes | Laden |   |                       |          |                                    |                      | ×         |  |
|-------------|-------|---|-----------------------|----------|------------------------------------|----------------------|-----------|--|
|             |       | Konfigurierte Zugriffskno   | oten von "CPU_1516    | F"       |                                    |                      |           |  |
|             |       | Gerät   | Gerätetyp             | Steckpl  | Schnittstellen.                    | . Adresse            | Subnetz   |  |
|             |       | CPU_1516F   | CPU 1516F-3 PN/       | 1 X3     | PROFIBUS                           | 2                    |           |  |
|             |       |   | CPU 1516F-3 PN/       | 1 X1     | PN/IE                              | 192.168.0.1          | PN/IE_1   |  |
|             |       |   | CPU 1516F-3 PN/       | 1 X2     | PN/IE                              | 192.168.1.1          |           |  |
|             |       |   |                       |          |                                    |                      |           |  |
|             |       |   |                       |          |                                    |                      |           |  |
|             |       | Ту  | /p der PG/PC-Schnitts | telle:   | PN/IE                              |                      | •         |  |
|             |       |   | PG/PC-Schnitts        | telle:   | Intel(R) PRO/1                     | 000 MT Desktop Adapt | er 💌 💎 🔯  |  |
|             |       | Verbindung mit Schnittstelle/Subnetz: Direkt an Steckplatz '1 X1' |                       |          |                                    |                      |           |  |
|             |       |   | 1. Gate               | eway:    | Bitte auswähler<br>Direkt an Steck | 1<br>platz '1 X1'    | ۲         |  |
|             |       |   |                       |          | Direkt an Steck<br>PN/IE 1         | platz '1 X2'         |           |  |
|             |       | Zielgerät auswählen: Versuche alle Schnittstellen en              |                       |          |                                    |                      |           |  |
|             |       | Gerät   | Gerätetyp             | Schnitts | tellentyp Ad                       | resse                | Zielgerät |  |
|             |       | -   |                       | PN/IE    | Zu                                 | griffsadresse        |           |  |
|             |       |   |                       |          |                                    |                      |           |  |

# 7.8 Testen des Regelwerkes

- $\rightarrow$  Verbinden Sie den Computer mit dem Port 5 auf dem SCALANCE S615.
- → Stellen Sie sicher, dass der Computer eine neue Adresse im Subnetz 10.0.0.0/24 vom SCALANCE S615 bekommen hat. (→ LAN-Verbindung → Status)

| Netzwerkverbindungsdeta    | ils X                                |
|----------------------------|--------------------------------------|
| Netzwerkverbindungsdetails |                                      |
| Eigenschaft                | Wert                                 |
| Verbindungsspezifisches    |                                      |
| Beschreibung               | Intel(R) PRO/1000 MT Desktop Adapter |
| Physische Adresse          | 08-00-27-9E-C9-15                    |
| DHCP-aktiviert             | Ja                                   |
| IPv4-Adresse               | 10.0.0.1                             |
| IPv4-Subnetzmaske          | 255.255.255.0                        |
| Lease erhalten             | Dienstag, 4. Juni 2019 12:29:50      |
| Lease läuft ab             | Dienstag, 4. Juni 2019 13:29:49      |
| IPv4-Standardgateway       | 10.0.254                             |
| IPv4-DHCP-Server           | 10.0.254                             |
| IPv4-DNS-Server            |                                      |
| IPv4-WINS-Server           |                                      |
| NetBIOS über TCPIP ak      | Ja                                   |
| Verbindungslokale IPv6     | fe80::e96f:1d1b:18f3:7d8f%6          |
| IPv6-Standardgateway       |                                      |
| IPv6-DNS-Server            |                                      |
| <                          | >                                    |
|                            |                                      |
|                            | Schließen                            |

→ Öffnen Sie mit dem Browser den Webserver der CPU 1516F-3 PN/DP. ( $\rightarrow$  <u>https://192.168.1.1</u>)

| ← → C ▲ Not set             | cure https://192.168.1.1/Portal/Portal.m  | wsl?intro_enter_button=ENTER&PriNav=Start&coming_from_intro=tr   | ue&no_intro=false 🔄 🖸 🗄          |
|-----------------------------|---|--|----------------------------------|
| SIEMENS                     | S71500/ET200MP-Station_1/CP   | J_1516F  |                                  |
|                             |   |  | 11:32:28 am 06/04/2019 English 🔻 |
| User name                   | CPU_1516F   |  | ट प्रा 🛎                         |
| Start page     Introduction | SIEMENS SIMATIC<br>S7-1600<br>CPU 1516F-3 PN/DP<br>CPU 1516F-3 PN/DP<br>CEST 516-3FN0D-0ABD | General:<br>TIA Portal: V15.1<br>Step 7 Safety: V15.0<br>Station name: \$71500/ET200/IP-Station_1<br>Module hype: CPU 1516F-3 PN/DP<br>Status:<br>Operating Mode: RUN<br>Status: ✓ OK<br>Mode selector: RUN<br>Fail-safe:<br>Safety mode:<br>Collective F-signature: |                                  |
|                             |   | Last fail-safe modification:   |                                  |
|                             |   |  |                                  |

→ Versuchen Sie mit dem TIA Portal eine Online-Verbindung zur CPU 1516F-3 PN/DP aufzubauen. (→ TIA Portal → CPU\_1516F →  $\bigcirc$  Online verbinden)

| Info   |         |         |            |          |            |   |
|--|---------|---------|------------|----------|------------|---|
|  | S E     | igensch | aften      | i Info   | 🗓 Diagnose |   |
| Allgemein Querverweise Übersetzen  |         |         |            |          |            |   |
| 😢 🛕 🚺 Alle Meldungen anzeigen 🔽  |         |         |            |          |            |   |
|  |         |         |            |          |            |   |
| ! Meldung  | Gehe zu | ?       | Datum      | Zeit     |            |   |
| Verbunden mit CPU_1516F, über Adresse IP = 192.168.1.1.                              |         |         | 04.06.2019 | 12:38:58 |            |   |
| Verbindung mit CPU_1516F getrennt.   |         |         | 04.06.2019 | 12:39:01 |            |   |
| Verbindung mit CPU_1516F, über Adresse IP = 192.168.1.1, fehlgeschlagen.             |         |         | 04.06.2019 | 12:40:00 |            |   |
| Online: Es konnte keine Verbindung hergestellt werden. Der Verbindungspartner meldet |         | ?       | 04.06.2019 | 12:40:00 |            |   |
|  |         |         |            |          |            |   |
|  |         |         |            |          |            |   |
|  |         |         |            |          |            |   |
|  |         |         |            |          |            |   |
| <  |         |         |            |          |            | > |

#### Hinweis:

- Ein Verbindungsaufbau mit der CPU\_1516F sollte zu diesem Zeitpunkt nicht möglich sein, da nur Port 443 und 4840 freigeschaltet sind.
- → Öffnen Sie im Browser die Weboberfläche des SCALANCE S615, da Sie sich diesmal auf der externen Seite des Gerätes befinden, nutzen Sie bitte die externe IP-Adresse des Gerätes. (→ <u>https://10.0.0.254</u>)



→ Wechseln Sie zur Firewall-Anmeldung. (→ Wechsel zur Firewall-Anmeldung)

| SCALANCE S615 WEB Manageme × +   | _      |               | × |
|--|--------|---------------|---|
| ← → C ▲ Not secure   https://10.0.0.254  | Å      | •             | : |
| SIEMENS  | Deutso | h 🔻 <u>Go</u> | * |
| Name Passwort Anmeiden   |        | ? 🔒           |   |
| Firewall warne: Passwort Anmelden Wechsel zur Anmeldung Wechsel zu unsicherer HTTP-Verbindung Informationen zur Kompatibilität des Browsers finden Sie in der Dokumentation. |        |               |   |
|  |        |               | - |

 $\rightarrow$  Melden Sie sich mit dem Benutzer "support" an. ( $\rightarrow$  Name: support  $\rightarrow$  Passwort: \*\*\*)

| SCALANCE S615 WEB Manageme × +          |          |   | - C        | ב  | × |
|---|----------|---|------------|----|---|
| ← → C ▲ Not secure   https://10.0.0.254 |          | ☆ | 6 <u>6</u> | θ  | : |
| SIEMENS                                 |          | D | eutsch ▼   | Go | * |
| Name Passwort Anmelden                  |          |   | ?          | -  |   |
| Informationer                           | Figewall |   |            |    | · |

 $\rightarrow$  Klicken Sie auf Anmelden. ( $\rightarrow$  Anmelden)

 $\rightarrow$  Der Firewall-Regelsatz "support\_regeln" sollte daraufhin für 30 Minuten aktiviert worden sein.



#### Hinweis:

 Mit der Schaltfläche "Timeout zurücksetzen" können Sie die Gültigkeit der Regelsätze wieder auf 30 Minuten zurücksetzen. Mit einem Klick auf Abmelden, werden alle Regelsätze wieder beendet. → Versuchen Sie erneut eine Online-Verbindung mit der CPU 1516F-3 PN/DP im TIA Portal herzustellen. (→ TIA Portal → CPU\_1516F →  $\bigcirc$  Online verbinden)

|                                 |          | 🔊 ± (# ± 🖥 🗓 📓 🙀 💋 Online verbinden 🖉 Online-Verbindung trennen 🏭 🖪 🖪 🛪 🖃 🛄 🕈                | PORTAL                     |
|---------------------------------|----------|--|----------------------------|
|                                 | □ ◀      | 140-200_Industrial_Security_mit_S615 	▶ Geräte & Netze 🖬 🖬                                   | 🗙 Hardware-Katalog 🛛 🗊 🕨 🕨 |
| Geräte                          |          | 🛃 Topologiesicht 🛛 📩 Netzsicht 🔄 👔 Gerätesicht   | Optionen                   |
| 音                               | 🔟 🛃      | 💦 Vernetzen 🔢 Verbindungen 🛛 HM-Verbindung 🔍 🕎 👯 🖽 🛄 🍳 🛨 🔤                                   |                            |
|                                 | _        |  | ✓ Katalog                  |
| 🕶 🛅 140-200_Industrial_Security | M 🔵 🔼    |  | Suchen>                    |
| 🍟 Neues Gerät hinzufügen        |          |  |                            |
| 📩 Geräte & Netze                | _        | CPU_1516F  | Filter Alle>               |
| CPU_1516F [CPU 1516F            |          |  |                            |
| Geratekonfiguration             | =        |  | PC-Systeme                 |
| Programmbausteine               |          |  | Antriebe & Starter         |
| Technologieobiekte              | -        | PN/E_1   | ▼ 🕞 Netzkomponenten        |
| Externe Quellen                 |          |  | E Switches                 |
| 🕨 🌄 PLC-Variablen               |          |  | 🗧 🕨 🛅 IWLAN                |
| E PLC-Datentypen                |          |  | Industrial Security        |
| Beobachtungs- und For           |          |  | Security-Gerät             |
| Online-Sicherungen              |          |  | SCALANCE M                 |
| Traces                          |          |  | SCALANCE S                 |
| Geräte-Proxy-Daten              |          |  | 6GK5 615-0/40 =            |
| Programminformationen           |          |  | 6GK5 636-2G                |
| El RIC Maldatastistan           |          | V  | 6GK5 642-2G                |
| Online-Kartendaten              |          | < III > 100% 💌 📵   | 6GK5 646-2G                |
| Lokale Module                   | <b>V</b> | G Figenschaften  | - 6GK5 602-0BA1            |
| Nicht grunpierte Geräte         | ~        |  | GGK5 612-0BA1              |
| ¢ j …                           | >        | Aligemein Querverweise Übersetzen  | GGK5 623-0BA1              |
| ✓ Detailansicht                 |          | 😧 🛕 🚺 🛛 Alle Meldungen anzeigen 🔹  | 6GK5 627-2BA1              |
| Module                          |          |  | Netzübergänge              |
|                                 |          | 1 Meldung Gehe zu ? Datum  | Router                     |
| Name                            |          | Online: Es konnte keine Verbindung hergestellt werden. Der Verbindungspartner meldet 7 04.06 | Bigridsenkepeater          |
| Gerätekonfiguration             | ^        | Verbunden mit CPU_1516F, über Adresse IP =192.168.1.1. 04.06                                 | Dezentrale Peripherie      |
| 🖞 Online & Diagnose             | =        | Verbindung mit CPU 1516F abgebrochen. 04.06 04.06  | Stromversorgung und -v V   |
| Programmbausteine               |          | Verbunden mit Cr0_1516F, über Adresse if =192.168.1.1. 04.06                                 | < III >                    |
|                                 |          |  |                            |

#### Hinweis:

 Diesmal sollte der Verbindungsaufbau durch das zusätzliche Regelwerk einwandfrei funktionieren.

# 7.9 Checkliste – Schritt-für-Schritt-Anleitung

Die nachfolgende Checkliste hilft den Auszubildenden/Studierenden selbstständig zu überprüfen, ob alle Arbeitsschritte der Schritt-für-Schritt-Anleitung sorgfältig abgearbeitet wurden und ermöglicht eigenständig das Modul erfolgreich abzuschließen.

| Nr. | Beschreibung  | geprüft |
|-----|---|---------|
| 1   | Projekt erfolgreich dearchiviert                            |         |
| 2   | Programmiergerät auf den Port 4 des S615 gesteckt           |         |
| 3   | IP-Adresse erfolgreich gesetzt                              |         |
| 4   | Webmanagement angemeldet und Passwort geändert              |         |
| 5   | System mit dem Assistenten korrekt konfiguriert             |         |
| 6   | DHCP-Pool für vlan1 erstellt                                |         |
| 7   | DHCP-Pool für vlan2 erstellt                                |         |
| 8   | DHCP-Optionen für beide Pools korrekt konfiguriert          |         |
| 9   | DHCP-Server und beide Pools aktiviert                       |         |
| 10  | Programmiergerät bezieht IP automatisch                     |         |
| 11  | Globale Regel für HTTPS zur CPU hinzugefügt                 |         |
| 12  | Support-Benutzer angelegt                                   |         |
| 13  | Support-Regelwerk angelegt                                  |         |
| 14  | Webserver auf der CPU_1516F aktiviert                       |         |
| 15  | Programmiergerät auf den Port 5 des S615 gesteckt           |         |
| 16  | Programmiergerät bezieht auch hier IP automatisch           |         |
| 17  | Webserver der CPU 1516F erfolgreich aufgerufen              |         |
| 18  | Keine Online-Verbindung zur CPU_1516F mit TIA möglich       |         |
| 19  | Erfolgreich als Support-Benutzer an der Firewall angemeldet |         |
| 21  | Online-Verbindung zur CPU_1516F mit TIA nun möglich         |         |

# 8 Übung

# 8.1 Aufgabenstellung – Übung

Durch die Digitalisierung der Fertigungsanlage wird in diesem Schritt auch ein globaler Zugriff auf den OPC UA Server der Steuerung benötigt. Erstellen Sie eine neue Regel, die den Zugriff auf den OPC UA Server der Steuerung aus dem Firmennetz heraus ermöglicht.

Informieren Sie sich vor der Konfiguration welchen Port die OPC UA Verbindung zur CPU benötigt.

## 8.2 Planung

Planen Sie nun selbstständig die Umsetzung der Aufgabenstellung.

# 8.3 Checkliste – Übung

Die nachfolgende Checkliste hilft den Auszubildenden/Studierenden selbständig zu überprüfen, ob alle Arbeitsschritte der Übung sorgfältig abgearbeitet wurden und ermöglicht eigenständig das Modul erfolgreich abzuschließen.

| Nr. | Beschreibung   | geprüft |
|-----|--|---------|
| 1   | Neue Regel angelegt  |         |
| 2   | OPC UA Verbindung aus dem Firmennetz erfolgreich aufgebaut       |         |
| 3   | Weiterhin keine Online-Verbindung zur CPU ohne Anmeldung möglich |         |

# 9 Weiterführende Information

Zur Einarbeitung bzw. Vertiefung finden Sie als Orientierungshilfe weiterführende Informationen, wie z. B.: Getting Started, Videos, Tutorials, Apps, Handbücher, Programmierleitfaden und Trial Software/Firmware, unter nachfolgendem Link:

siemens.de/sce/s7-1500

Voransicht "Weiterführende Informationen" - In Vorbereitung

## Weitere Informationen

Siemens Automation Cooperates with Education siemens.de/sce

SCE Lern/Lehrunterlagen siemens.de/sce/module

SCE Trainer Pakete siemens.de/sce/tp

SCE Kontakt Partner siemens.de/sce/contact

Digital Enterprise siemens.de/digital-enterprise

Industrie 4.0 siemens.de/zukunft-der-industrie

Totally Integrated Automation (TIA) siemens.de/tia

TIA Portal siemens.de/tia-portal

SIMATIC Controller siemens.de/controller

SIMATIC Technische Dokumentation siemens.de/simatic-doku

Industry Online Support support.industry.siemens.com

Katalog- und Bestellsystem Industry Mall mall.industry.siemens.com

Siemens Digital Industries, FA Postfach 4848 90026 Nürnberg Deutschland

Änderungen und Irrtümer vorbehalten © Siemens 2019

siemens.de/sce