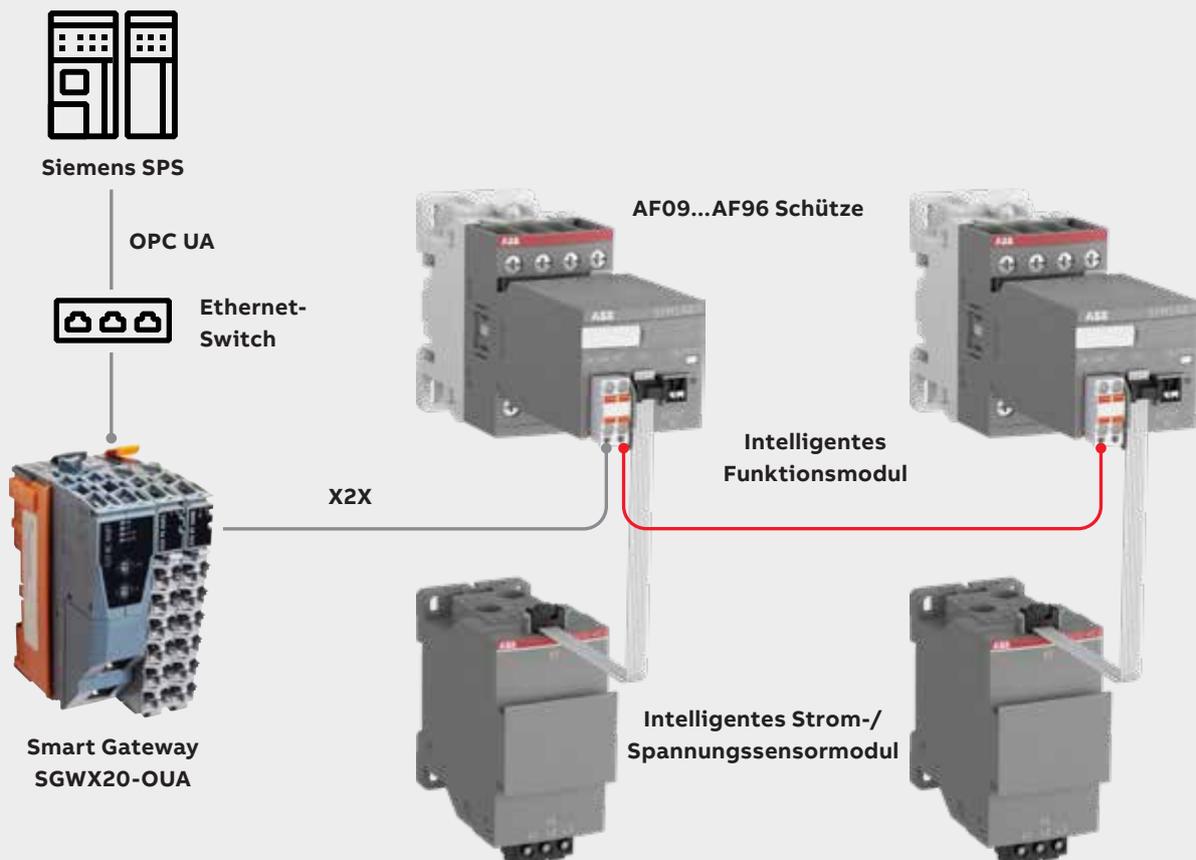


Novolink mit Siemens SPS

Smart Gateway SGWX20-OUA über TIA Portal V17 mit Siemens SPS verbinden



Inhalt

4	Zweck und grundlegende Beschreibung
4	Wichtige Haftungsausschlüsse und Empfehlungen
5	Grundkonfiguration
8	Siemens-Client
8	Vorbereitung und Zubehör
8	Eigenschaften der CPU
11	Die Client-Schnittstelle
13	Leseliste
18	Schreibliste
23	Methodenliste
27	Parameter einstellen
30	Novolink mit Smart Gateway konfigurieren
30	Fehlersuche
31	Liste zugehöriger Dokumente/Links

1. Zweck und grundlegende Beschreibung

In diesem Abschnitt werden die grundlegenden Schritte beschrieben, um ABB Novolink mit einer Siemens SPS über das Smart Gateway mittels OPC UA einzurichten.

1.1. Was ist Novolink?

Die ABB Novolink™-Geräte helfen Ihnen bei der Digitalisierung von Motorstarterlösungen und bieten Erkenntnisse über die angeschlossenen Lasten. Sie lassen sich einfach in vorhandene Verdrahtungspläne integrieren und an normale AF-Schütze anschließen. Die Installation ist dank der reduzierten Verdrahtung und weniger Komponenten schnell und einfach, sodass der technische Aufwand minimiert wird. Durch vorausschauende Wartung reduzieren die Novolink-Geräte Ausfallzeiten, verbessern die Effizienz und erhöhen die Kosteneinsparungen. Sie sind vollständig in das B&R-Automatisierungssystem integriert. Es bieten sich zudem noch viel mehr Möglichkeiten, weil der vollständige Fernzugriff auf Ihre Daten neue Wartungsservice- und Ertragschancen bietet.

2. Wichtige Haftungsausschlüsse und Empfehlungen

2.1. Haftungsausschluss Cyber-Security

Das Smart Gateway und die Novolink-Module sind für den Anschluss an Produkte von ABB und Drittanbietern vorgesehen und übertragen Daten über eine Netzwerkschnittstelle. Für die Bereitstellung und dauerhafte Gewährleistung einer gesicherten Verbindung zwischen dem Produkt und dem Netzwerk des Benutzers oder einem beliebigen anderen Netzwerk ist allein der Benutzer verantwortlich. Der Benutzer hat angemessene Verfahren einzurichten und zu pflegen (einschließlich, aber nicht beschränkt auf die Installation von Firewalls, den Einsatz von Authentifizierungsverfahren, Datenverschlüsselung, die Installation von Virenschutzprogrammen usw.), um das Produkt, das Netzwerk, sein System und die Schnittstelle gegen jede Art von Sicherheitsverletzung, unbefugtem Zugriff, Störung, Eingriff, Datenlecks und/oder Diebstahl von Daten oder Informationen zu schützen. ABB und seine verbundenen Unternehmen haften nicht für Schäden und/oder Verluste aufgrund solcher Sicherheitsverletzungen, unbefugten Zugriffs, Störungen, Eingriffen, Datenlecks und/oder Diebstahl von Daten oder Informationen. Die in diesem Handbuch enthaltenen Daten, Beispiele und Diagramme wurden ausschließlich zur Beschreibung von Konzepten oder des Produkts aufgenommen und sind nicht als Erklärung zu den garantierten Eigenschaften zu verstehen. Alle Personen, die für den Einsatz der in diesem Handbuch beschriebenen Geräte verantwortlich sind, müssen sich davon überzeugen, dass jede vorgesehene Anwendung geeignet und annehmbar ist. Dazu gehört auch, dass alle geltenden Sicherheitsanforderungen oder andere betriebliche Anforderungen erfüllt werden. Alle Risiken von Anwendungen, bei denen ein System- und/oder Produktausfall zur Gefahr von Sach- oder Personenschäden führen könnte (einschließlich, aber nicht beschränkt auf Verletzungen oder Todesfälle), liegen in der Verantwortung der Person oder des Rechtsträgers, die beziehungsweise der das Gerät einsetzt. Die Verantwortlichen werden hiermit aufgefordert, sicherzustellen, dass alle Maßnahmen ergriffen werden, derartige Risiken auszuschließen oder zu verringern. Dieses Dokument wurde von ABB mit großer Sorgfalt überprüft, aber Abweichungen können nicht vollkommen ausgeschlossen werden. Der Leser wird gebeten, den Hersteller über gefundene Fehler zu benachrichtigen. Außer wenn vertraglich ausdrücklich dazu verpflichtet, ist ABB in keinem Fall für Verluste oder Schäden verantwortlich oder haftbar, die sich aus der Nutzung dieses Handbuch oder des Geräts ergeben.

2.2. UaExpert

UaExpert ist eine von Unified Automation bereitgestellte Software. Sie sollten diese Software für die Überwachung der Daten wie in Kapitel „UaExpert“ beschrieben verwenden.

Wichtig: Diese Software ist nicht Eigentum von ABB und wir übernehmen keine Verantwortung für ihre Funktionalität.

2.3. Netzwerksicherheit erhöhen

Die folgenden Punkte werden ausdrücklich empfohlen, um die Sicherheit von Netzwerken zu erhöhen:

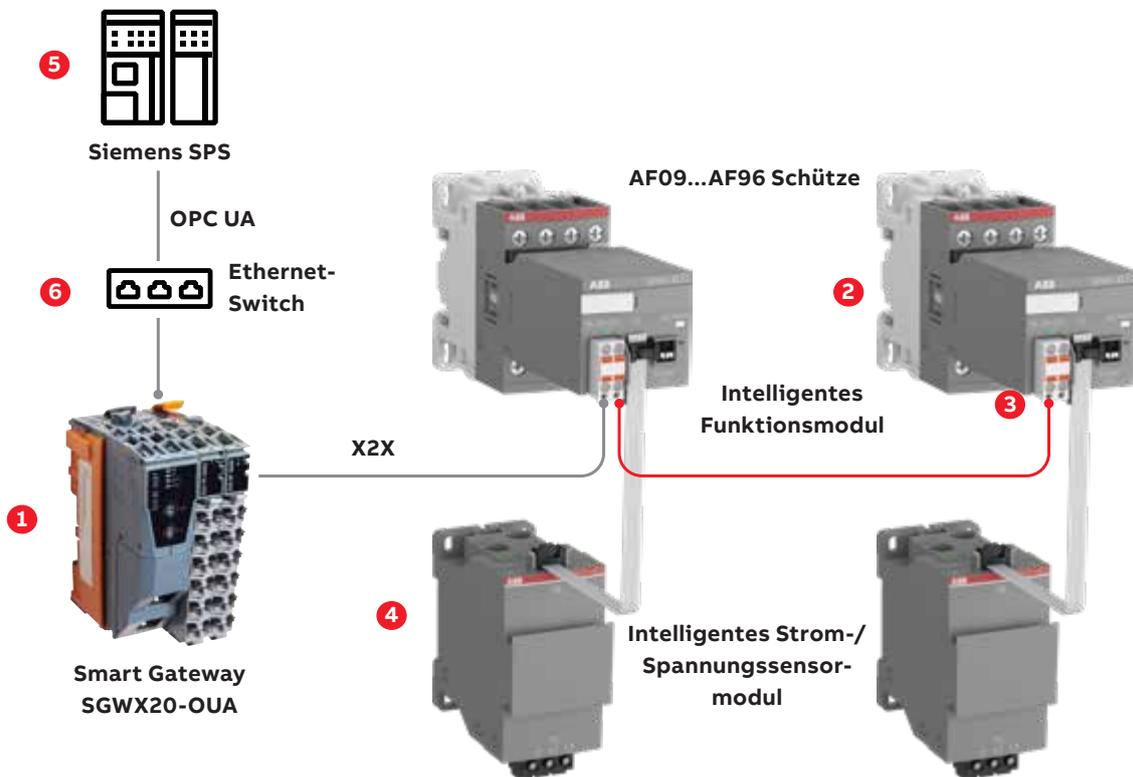
- **Netzwerk isolieren** – Trennen Sie das OT-Netzwerk (Operation Technology) vom IT-Netzwerk (Information Technology). Dies hilft zu verhindern, dass Angriffe auf das IT-Netzwerk das OT-Netzwerk erreichen.
- **Firewalls verwenden** – Implementieren Sie Firewalls, um den unbefugten Zugriff auf das OT-Netzwerk zu verhindern.

- **Zugriffskontrolle verwenden** – Implementieren Sie Zugriffskontrollen, um den Zugriff von Menschen und Geräten auf das OT-/IT-Netzwerk und Geräte einzuschränken.
- **Software auf dem neuesten Stand halten** – Stellen Sie sicher, dass die gesamte Software/Firmware der Geräte auf dem neuesten Stand ist und die aktuellen Sicherheits-Updates installiert sind.
- **Angriffsfläche von Geräten verringern** – Deaktivieren Sie nicht benötigte Gerätefunktionen, Dienste und Ports.
- **Standardpasswörter ersetzen** – Ersetzen Sie alle Standardpasswörter der Geräte, um zu verhindern, dass Angreifer mithilfe von Standardanmeldedaten Zugriff erhalten.
- **Netzwerkaktivitäten überwachen** – Überwachen Sie das OT-Netzwerk auf böswillige Aktivitäten, die Anzeichen eines Angriffs sein könnten. Ein Beispiel für ein Tool zur Netzwerküberwachung ist ein Angriffserkennungssystem (IDS).
- **Mitarbeiter schulen** – Schulen Sie Bediener und Servicepersonal zu Best Practices für IT- und OT-Sicherheit.

3. Grundkonfiguration

Dieser Abschnitt beschreibt die erforderlichen grundlegenden Schritte, um das Smart Gateway SGWX20-OUA mit intelligentem Funktionsmodul (SFM) und intelligenten Strom-/Spannungssensormodulen (SCM/SVM) einzurichten, die über OPC UA an die Siemens SPS angeschlossen sind.

Die Einrichtung kann wie in der folgenden Abbildung dargestellt vorgenommen werden:



Die Abbildung zeigt die Hauptkomponenten und wie sie für Motorstarter-Komplettlösungen kombiniert werden können:

- Smart Gateway SGWX20-OUA (1) wird über Ethernet-Switch (6) an Siemens SPS (5) angeschlossen.
- Das intelligente Funktionsmodul (SFM) (3) sollte auf AF-Schützen (2) montiert werden.
- SFMs werden über X2X-Kabel an das intelligente Strom-/Spannungssensormodul SCV (4) angeschlossen.
- Alle SFMs werden über X2X-Kabel an das Smart Gateway SGWX20-OUA (1) angeschlossen.

Hinweis: Das Smart Gateway SGWX20-OUA kann ein OPC UA-Server sein.

3.1. Verwendete Hardware

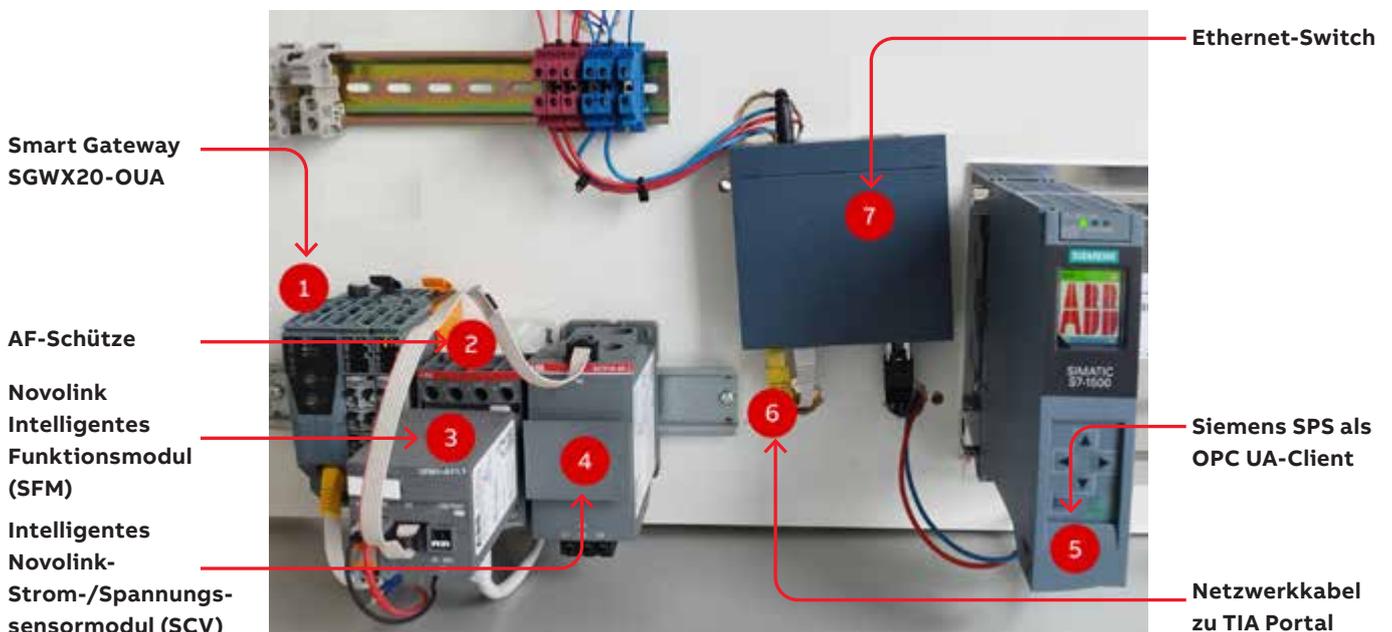
Die folgende Hardware wird verwendet.

	Gerät	Beschreibung	Artikelnummer	Anzahl
Siemens	SPS	Siemens S7 1500 mit Firmware v2.6 oder höher	1511-1PN - 6ES7 511-1AK02-0AB0 mit Firmware V2.9	1
Novolink	SFM-CAB-RJTB.1-500	Anschlussleitung RJ45 - X20 Reihenklemme von X20BT9400	1SVM823000R0500	2
Novolink	SFM-CAB-S.1-50	Anschlussleitung SFM zu Sensor 0,5 m	1SVM811000R0050	2
Novolink	SCV10-40.1	Intelligenter Strom-/Spannungssensor	1SVM320010R0000	1
Novolink	SFM1-A11.1	Erweitertes Funktionsmodul mit X2X	1SVM120012R0000	2
Schütz	AF09	Schütze	1SBL137001R1101 AF09-30-01-11	2
X2X OPC UA-Gateway	X2X OPC UA-Gateway	B&R-Controller	X20BT08T	1
X2X OPC UA-Gateway	Spannungsversorgung für den Sammelschienenverbinder	B&R-Controller	X20PS9400	1
X2X OPC UA-Gateway	Spannungsversorgung und Schnittstelle des X2X-Bus	B&R-Controller	X20BT9400	1
X2X OPC UA-Gateway	Backplane-Modul	B&R-Controller	X20BB80X	1

3.2. Verwendete Architektur

Dieser Abschnitt beschreibt die erforderlichen grundlegenden Schritte für die Einrichtung des Smart Gateways und der Novolink-Module mit der Siemens SPS.

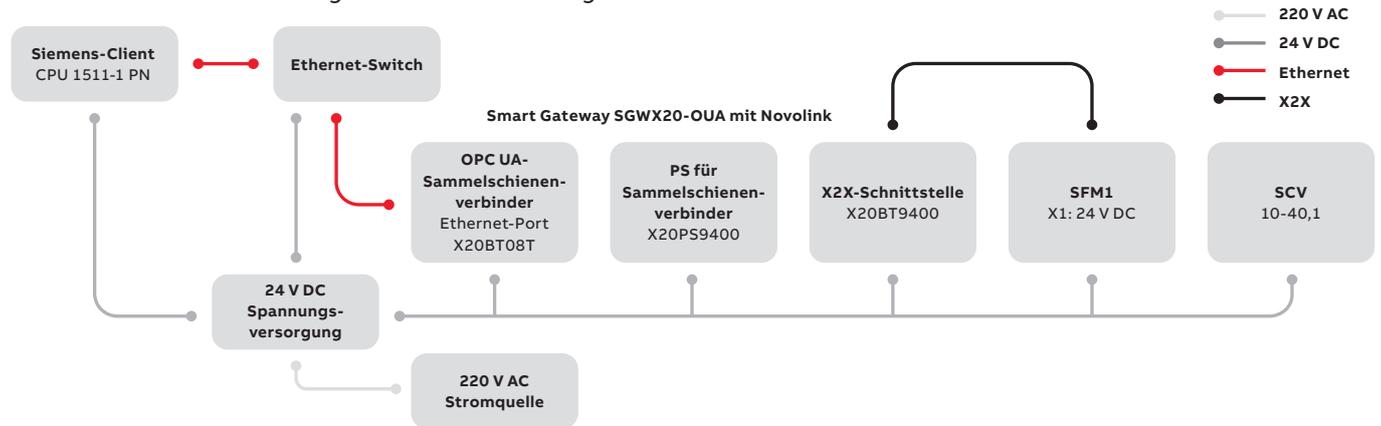
Die Einrichtung kann wie in der folgenden Abbildung dargestellt vorgenommen werden:



Nummer	Beschreibung
1	Smart Gateway SGWX20-OUA
2	AF-Schütze
3	Intelligentes Novolink-Funktionsmodul (SFM)
4	Intelligentes Novolink-Strom-/Spannungssensormodul (SCV)
5	Siemens SPS als OPC UA-Client
6	Netzwerkkabel zu TIA Portal (auf einem PC installieren)
7	Ethernet-Switch

3.2.1. Verdrahtung und Einschalten

Stellen Sie anhand der verwendeten Architektur sicher, dass die gesamte Verdrahtung vorgenommen wurde und Geräte mithilfe des unten dargestellten Schemas eingeschaltet wurden.



24 V DC	24 V DC wird an Smart Gateway, Novolink-Module und SPS angeschlossen.
220 V AC	220 V AC ist für die Spannungsversorgung erforderlich. 220 V AC kann auch zum Einschalten von Schützen verwendet werden.
OPC UA	Für OPC UA: Smart Gateway und Siemens SPS an den Ethernet-Switch anschließen
X2X	Smart Gateway mit Kabel „SFM-CAB-RJTB.1-500“ an SFM anschließen SFM mit Kabel „SFM-CAB-S.1-50“ an Sensoren anschließen

3.2.2. Softwarekonfiguration

Konfiguration von Siemens SPS	Für die Siemens SPS-Konfiguration wird die folgende Software verwendet: <ul style="list-style-type: none"> Siemens TIA Portal V17 oder höher Siemens OPC-UA-Lizenz
Konfiguration von B&R-Gateway	UaExpert
Lesen/Schreiben von Daten von Novolink über B&R-Controller	UaExpert

4. Siemens-Client

4.1. Vorbereitung und Zubehör

In diesem Abschnitt wird beschrieben, was Sie für die Konfiguration in TIA V17 benötigen.

- Novolink-Einrichtung:
siehe [Handbuch „SGWX20-OUA Smart Gateway X20 zu OPC UA Novolink™-Geräte mit OPC UA-Clients verbinden“](#).
- Siemens S7 1500 mit Firmware v2.6 oder höher (Beispiel: 1511-1PN - 6ES7 511-1AK02-0AB0 mit Firmware V2.9)
- Siemens TIA Portal V17 oder höher
- Siemens OPC-UA-Lizenz
- Die Module sind miteinander verdrahtet.
- IP-Adresse des Servers (Beispiel: 192.168.2.11)

In diesem Beispiel wird die CPU 1511 mit Firmware V2.9 verwendet.

4.2. Eigenschaften der CPU

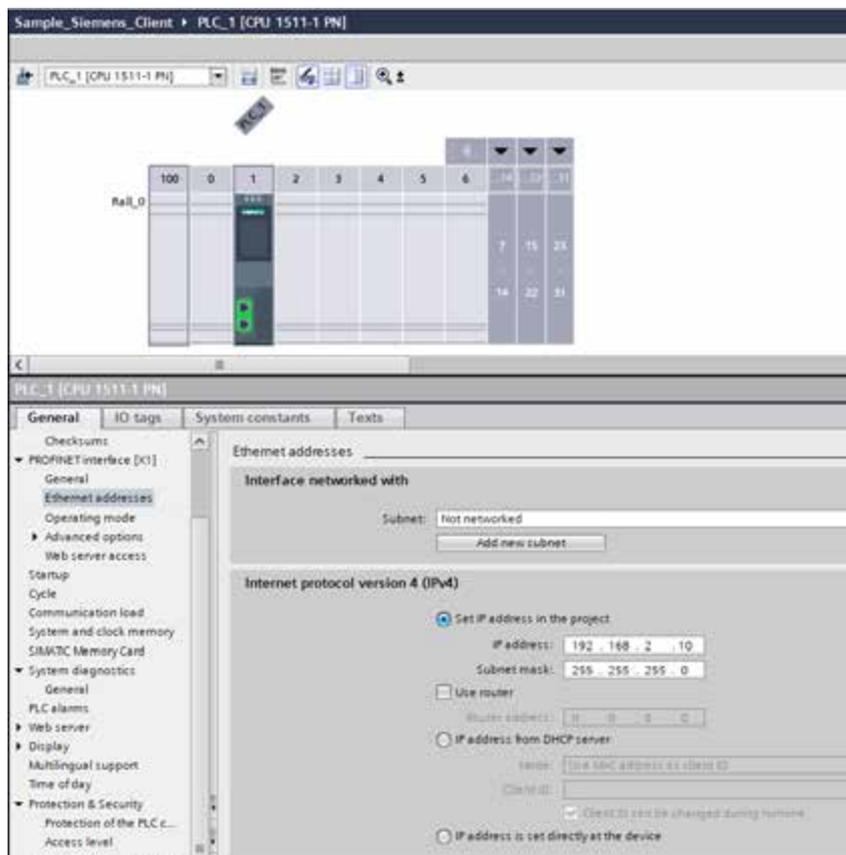


Abbildung 1: CPU_IP Address

- Stellen Sie sicher, dass sich die IP-Adressen von Server und Client im selben Netzwerk befinden.

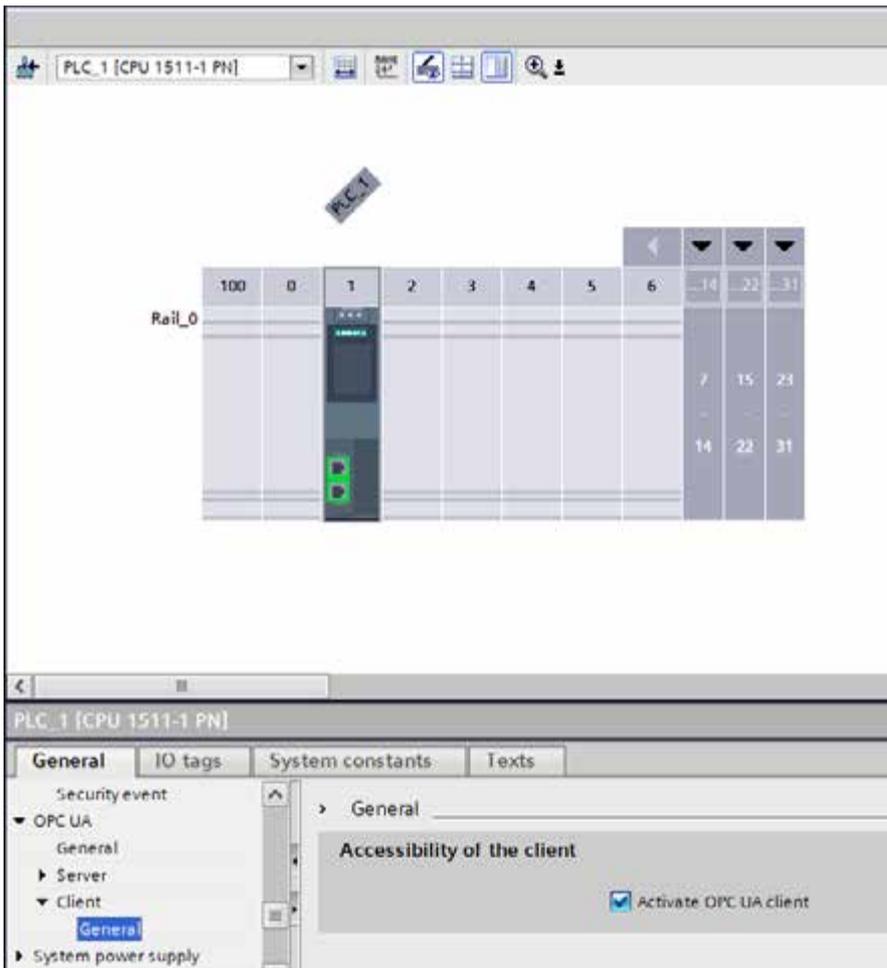


Abbildung 2: CPU_OPCUA_Client

- Aktivieren Sie das Kontrollkästchen „Activate OPC UA Client“.

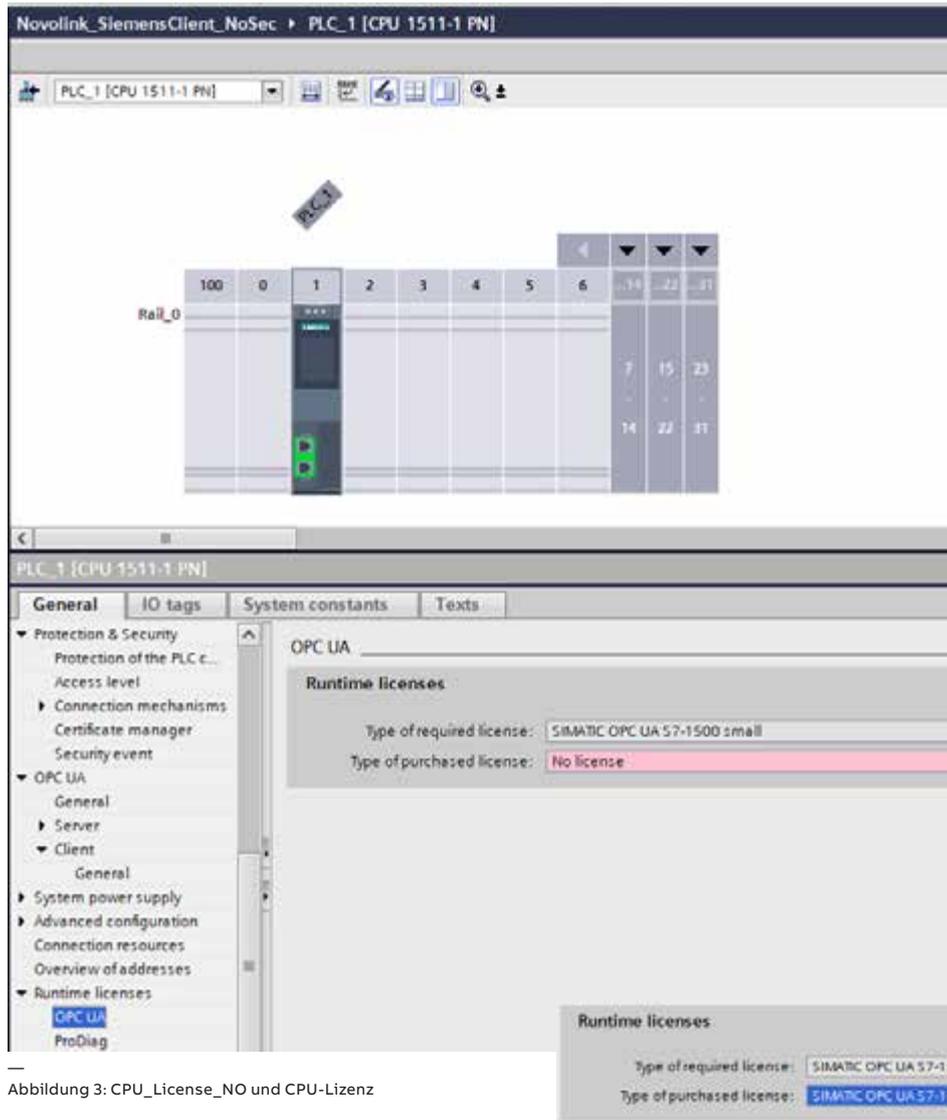


Abbildung 3: CPU_License_NO und CPU-Lizenz

- Wählen Sie die Lizenz aus. Informationen zur benötigten Lizenz erhalten Sie von Siemens.

Der Lizenztyp wird durch die verwendete SPS bestimmt.

Licensing

An OPC UA Server or OPC UA Client is available on the target systems (CPUs) and is activated using runtime licenses. Runtime licenses are offered in three levels for different target systems:

Target system	OPC UA S7-1200 Basic	OPC UA S7-1500 Small	OPC UA S7-1500 Medium	OPC UA S7-1500 Large
S7-1200 CPUs	Yes	No	No	No
ET 200SP CPU 1510SP/1512SP/1515SP (Open Controller) S7-1500 CPU 1511/1513 CPU 1504D Drive Controller	No	Yes	Yes	Yes
ET 200pro CPU 1516pro S7-1500 CPU 1515/1516 PLC 1507S software	No	No	Yes	Yes
S7-1500 CPU 1517/1518/1508S CPU 1507D Drive Controller	No	No	No	Yes

The runtime license includes the certificate for OPC UA (Server and Client) and can be run on the respective target systems including F, C and T/TF as from firmware V2.0 (Client V2.6).

You can find more information on the Software Update Service, license types, Online Software Delivery and handling your SW licenses with the Automation License Manager under [this link](#).

<https://mall.industry.siemens.com/mall/de/WW/Catalog/Products/10315991>

4.3. Die Client-Schnittstelle

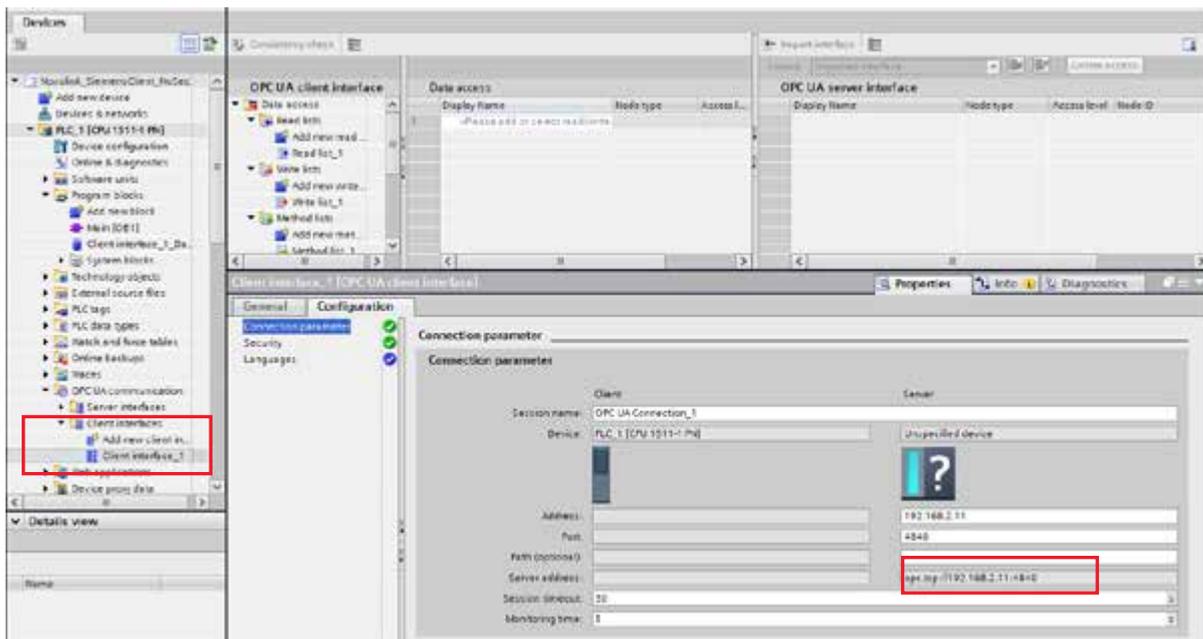


Abbildung 4: ClientInterface_ConnectParameter

- Fügen Sie eine neue Client-Schnittstelle hinzu.
- Geben Sie die IP-Adresse des Servers ein.

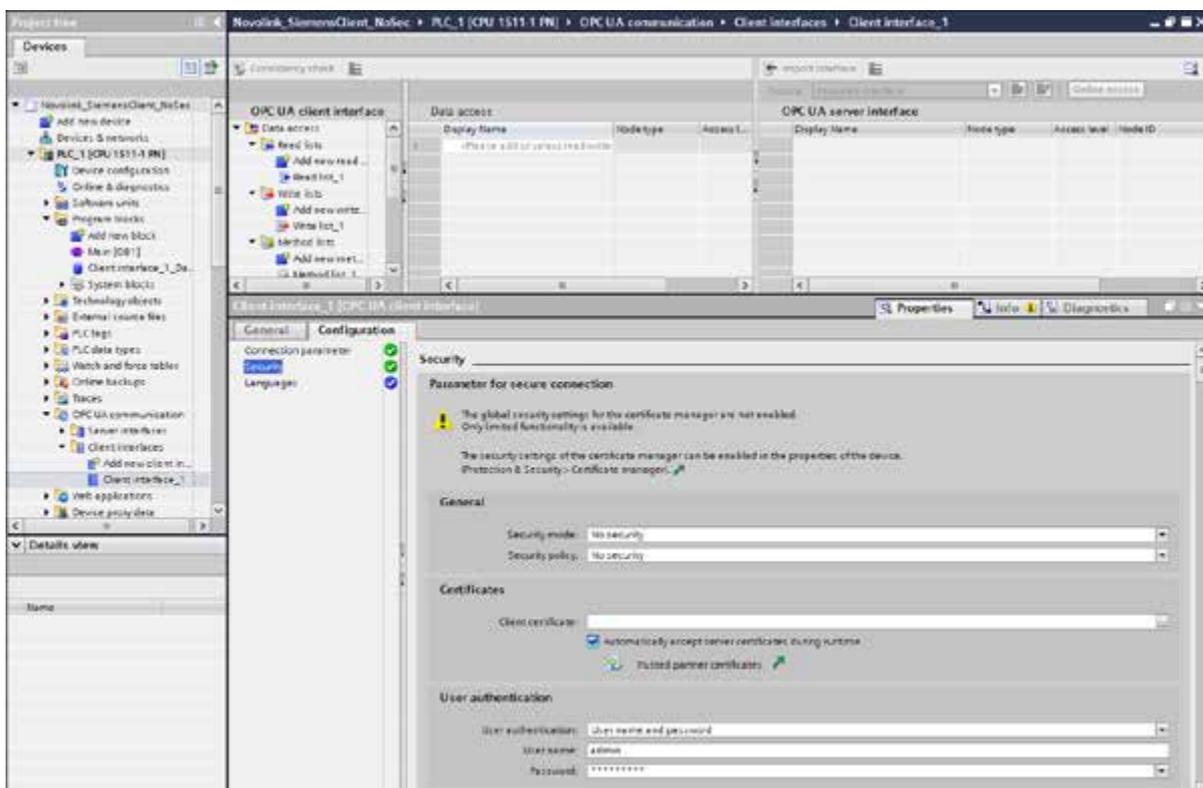


Abbildung 5: ClientInterface_Security

- Stellen Sie sicher, dass „No security“ ausgewählt und „Automatically accept server certificates during runtime“ aktiviert ist.
- Geben Sie den Benutzernamen und das Passwort für den Server ein.

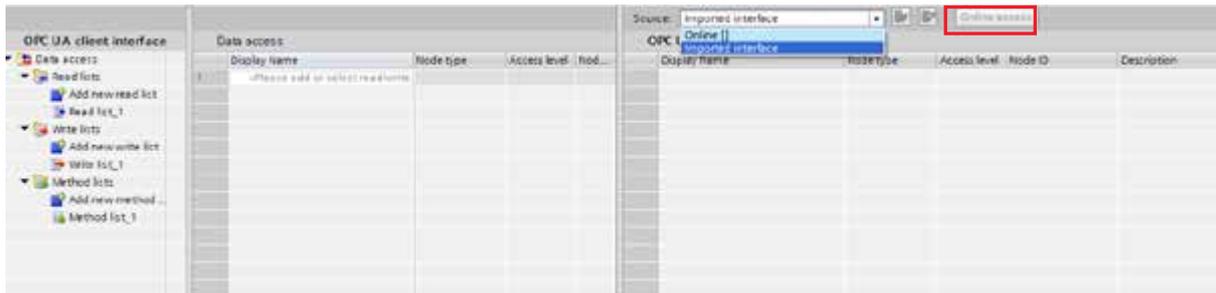


Abbildung 6: ClientInterface_OnlineAcces

Führen Sie im oberen Teil des Bildschirms für die Client-Schnittstelle folgende Schritte aus:

- Wählen Sie für „Source“ die Option „Online []“ aus.
- Klicken Sie auf die Schaltfläche „Online Access“.

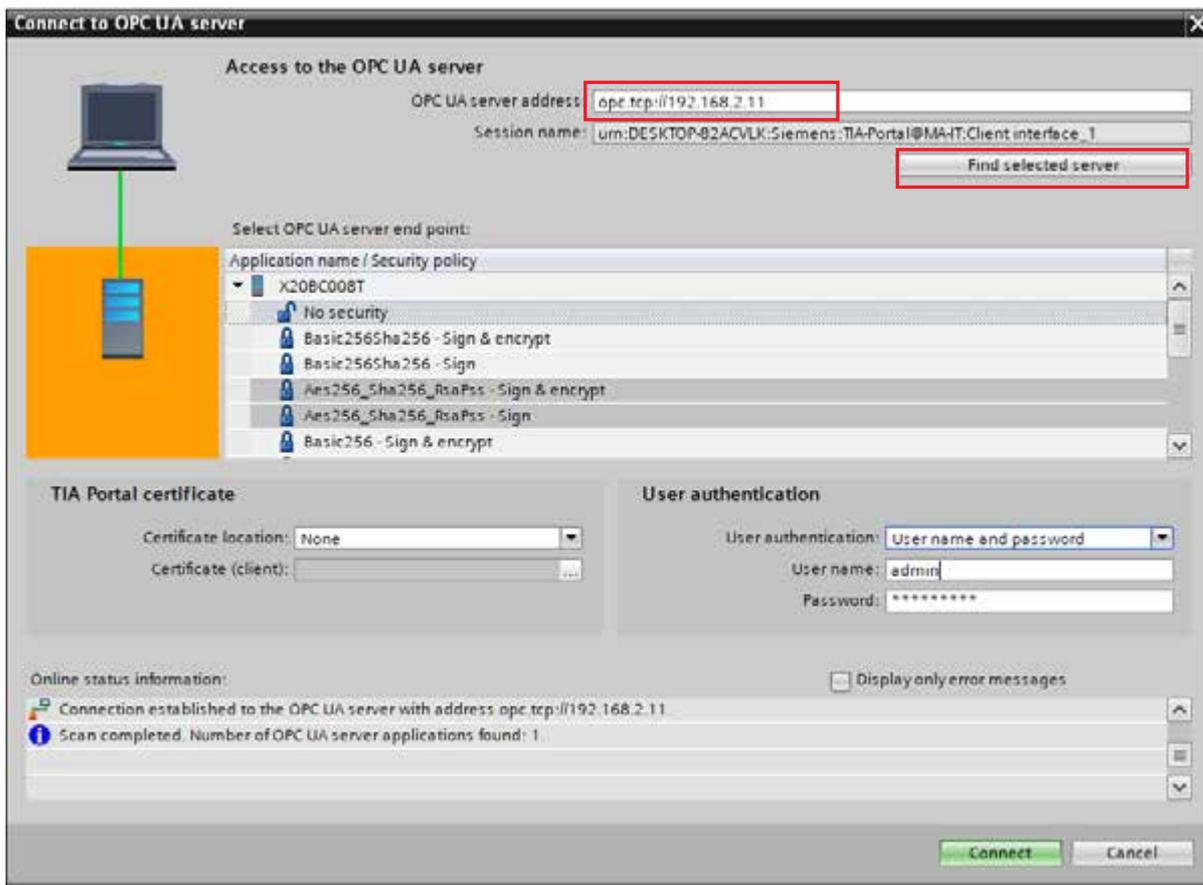


Abbildung 7: Popup-Dialogfeld für Online-Zugriff

Das Popup-Dialogfeld für den Zugriff wird angezeigt.

- Geben Sie die IP-Adresse des Servers ein.
- Klicken Sie auf die Schaltfläche „Find Selected Server“.

Der Server mit den Sicherheitsprotokollen wird angezeigt.

- Wählen Sie „No Security“ aus.
- Wählen Sie für „User authentication“ die Option „User name and password“ aus.
- Geben Sie den Benutzernamen für den Server ein.
- Geben Sie das Passwort für den Server ein.
- Klicken Sie auf die Schaltfläche „Connect“.



Abbildung 8: ClientInterface_ServerTrust

Wenn Sie gefragt werden, ob Sie dem Serverzertifikat vertrauen, und Sie ihm vertrauen:

- Klicken Sie auf „Yes“.

Auf der rechten Seite des Bildschirms erhalten Sie die verfügbaren Objekte des Servers.

4.4. Leseliste

4.4.1. Programmleseliste

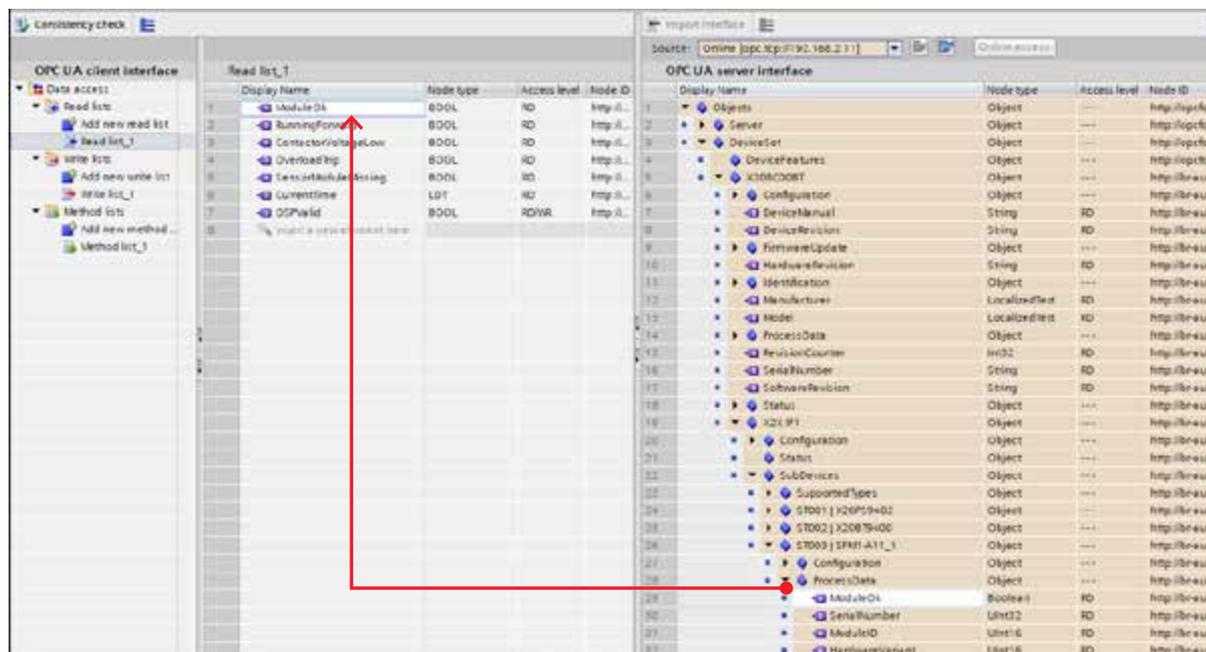


Abbildung 9: Read_list

- Fügen Sie eine neue Leseliste hinzu.
- Wählen Sie die Variablen aus, die gelesen werden sollten, ziehen Sie die gewünschten Variablen nach links und legen Sie sie in der Leseliste ab.
- Kompilieren Sie die Software.

Hinweis:

Sie können mehrere Leselisten hinzufügen. Für jede Leseliste können Sie andere Leseintervalle verwenden.

In diesem Beispiel werden die folgenden Variablen verwendet:

- ProcessData >> ModuleOk
- ProcessData >> RunningForward
- ProcessData >> ContactorVoltageLow
- ProcessData >> OverloadTrip
- ProcessData >> SensorModuleMissing
- ProcessData >> OSPValid

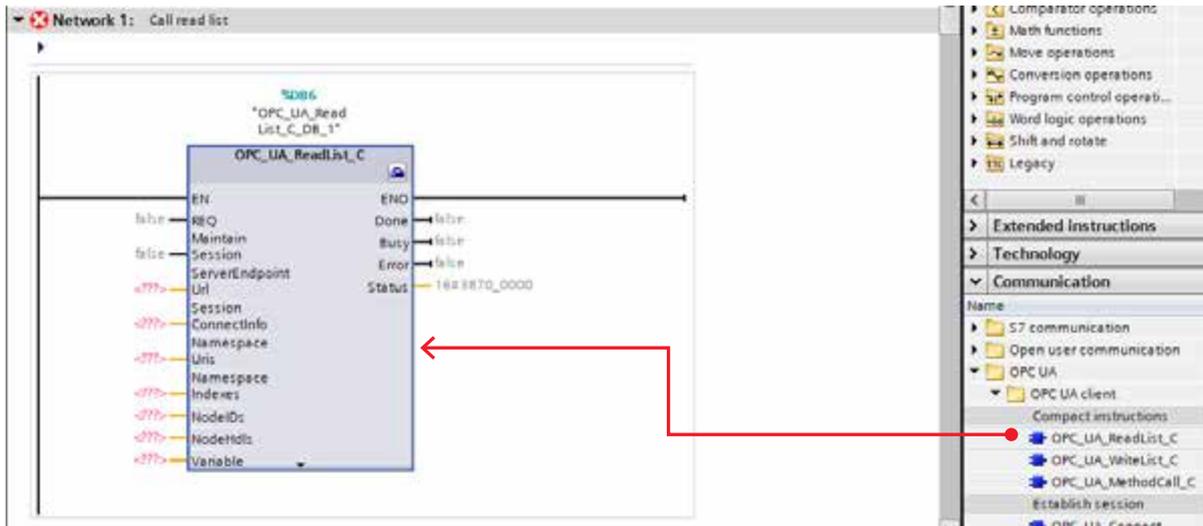


Abbildung 10: OB1_Readlist

- Ziehen Sie die Leseliste OPC_UA_ReadList_C und legen Sie sie in OB1 ab.

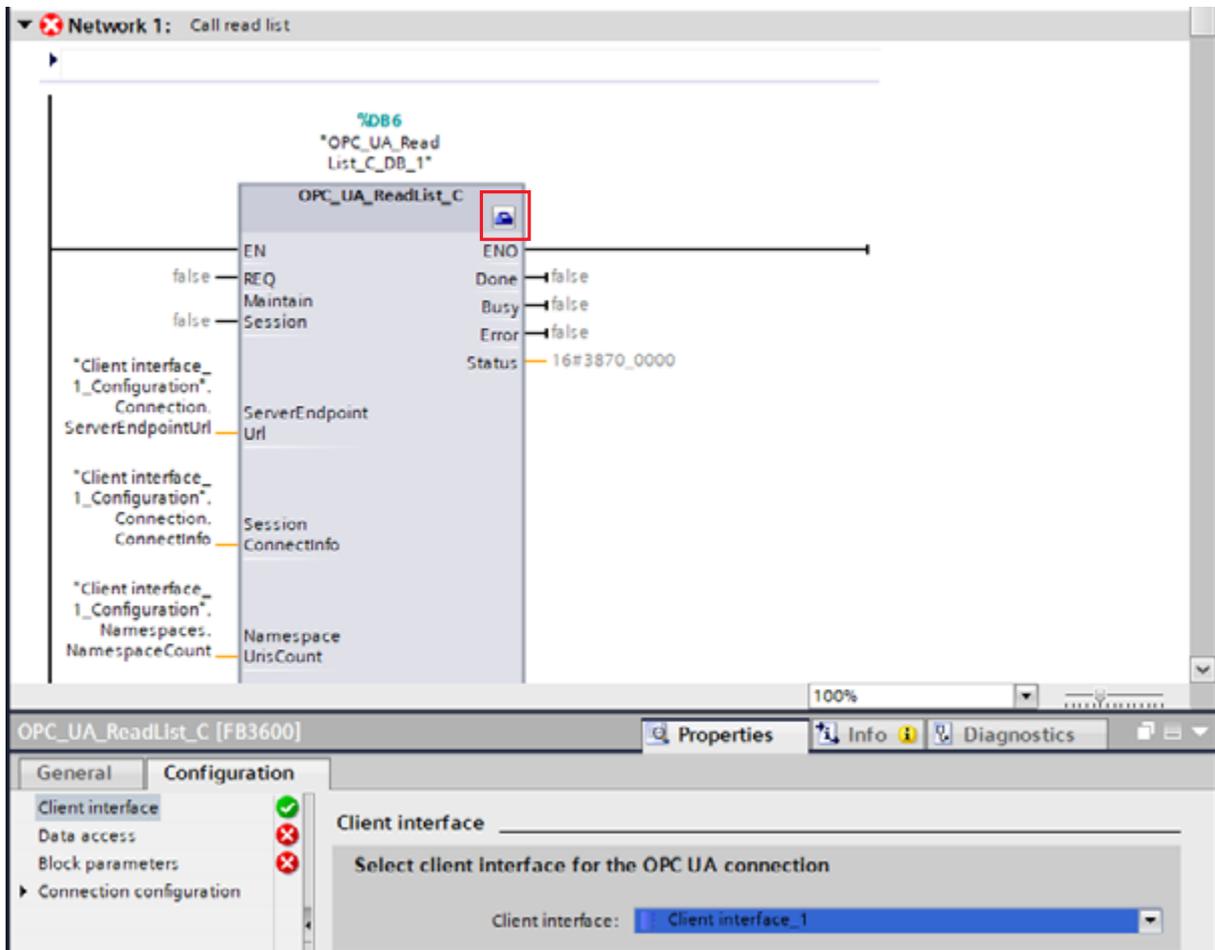


Abbildung 11: OB1_Readlist_ClientInterface

- Klicken Sie auf das Toolbox-Symbol in der rechten oberen Ecke des OPC_UA_ReadList_C-Blocks.

Die Konfiguration des OPC-UA_ReadList_C-Blocks wird unten angezeigt.

- Wählen Sie die zuvor erstellte Client-Schnittstelle aus.

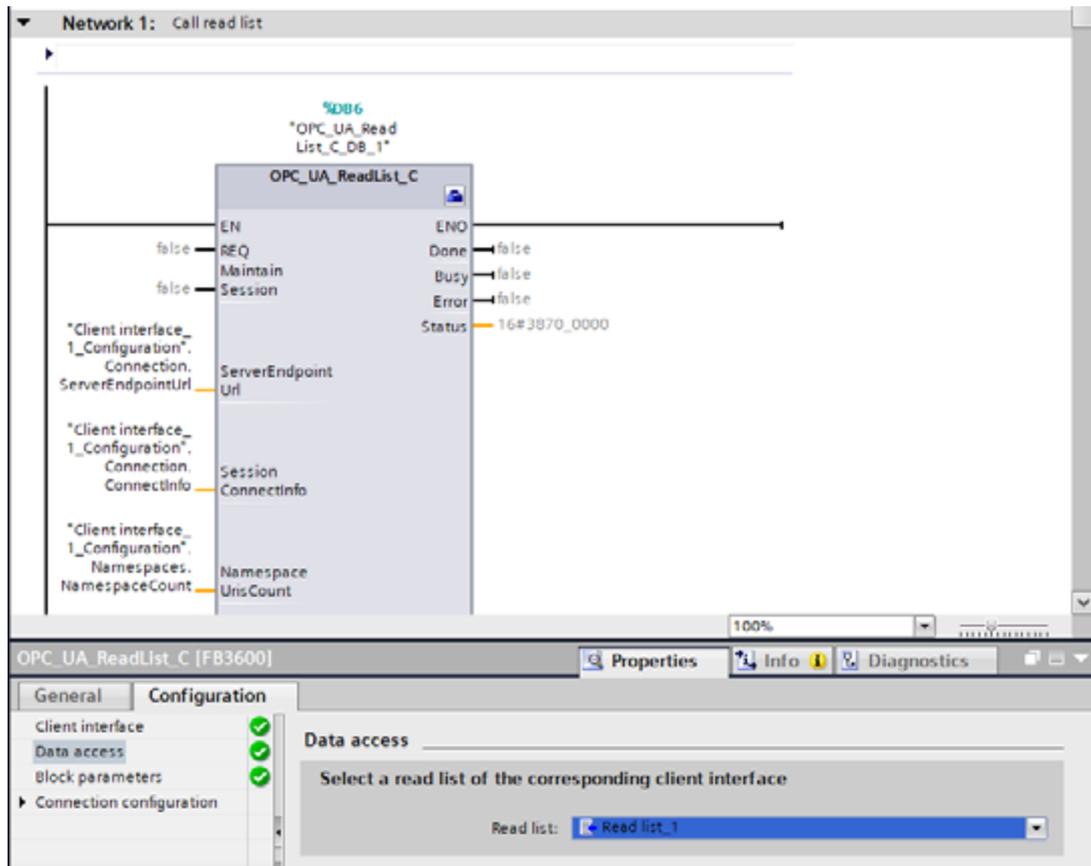


Abbildung 12: OB1_Readlist_DataAcces

- Wählen Sie die zuvor erstellte Leseliste aus.
- Die restlichen Parameter werden automatisch von Siemens eingestellt.

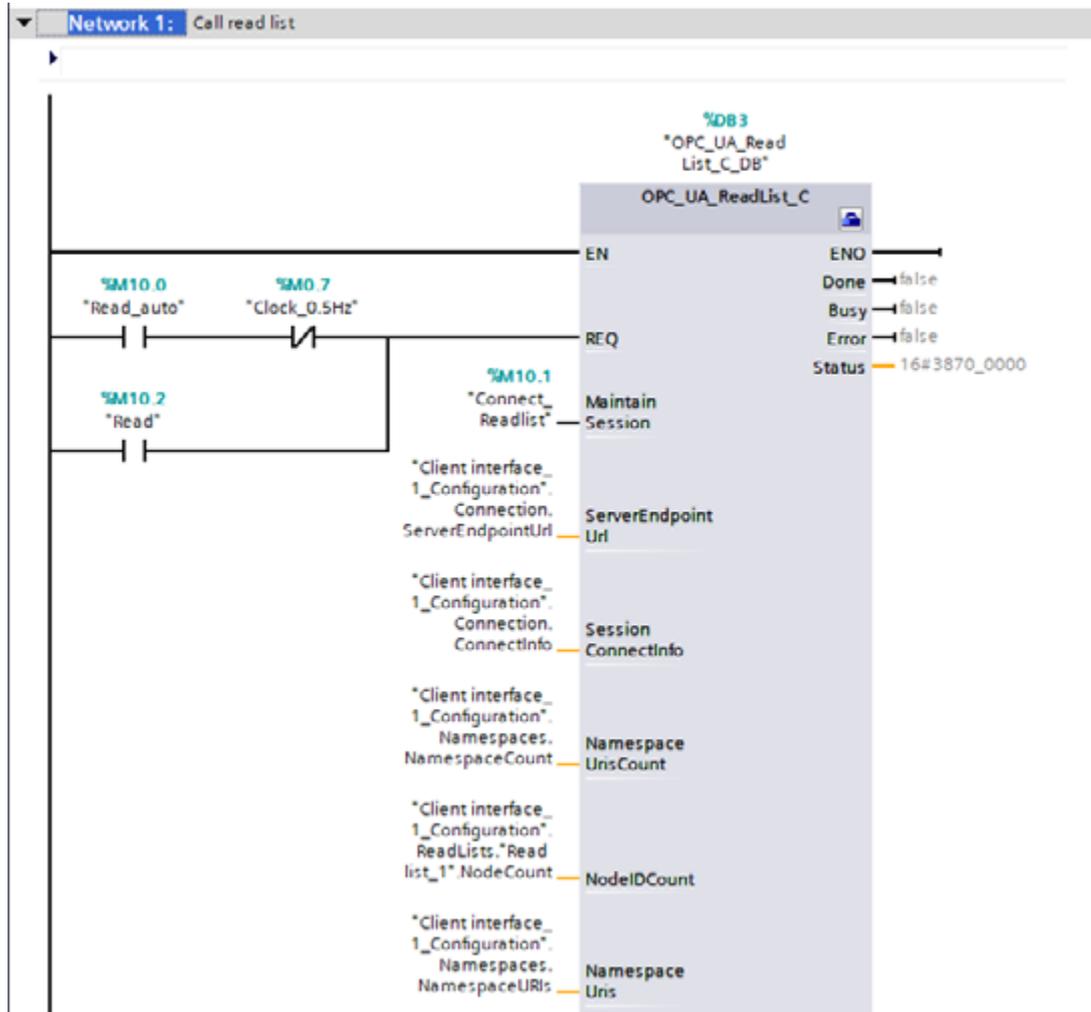


Abbildung 13: OB1_Readlist_Merker

- Fügen Sie ein Tag zum Request-Eingang (REQ) hinzu. Bei jeder positiven Flanke wird eine Verbindung mit dem Server hergestellt und die Variablen werden vom Server gelesen.
- Fügen Sie ein Tag zu „Maintain Session“ hinzu.
- Kompilieren Sie das Projekt mit einem „Rebuild all“ für Hardware und Software.
- Laden Sie „hardware configuration“ herunter.
- Laden Sie „Software all“ herunter.

Hinweis:

Mit „Maintain Session“ wird die Verbindung zwischen Server und Client beibehalten. Das Festlegen auf „True“ ist hier nicht notwendig, aber bei jeder positiven Flanke von REQ kann die Verbindung schneller wiederhergestellt werden.

Wenn ein Fehler auftritt, muss der Benutzer Maintain deaktivieren und wieder aktivieren, um die Verbindung zum Server wiederherzustellen.

4.4.2. Leseliste prüfen

Zum Lesen der Daten vom Server:

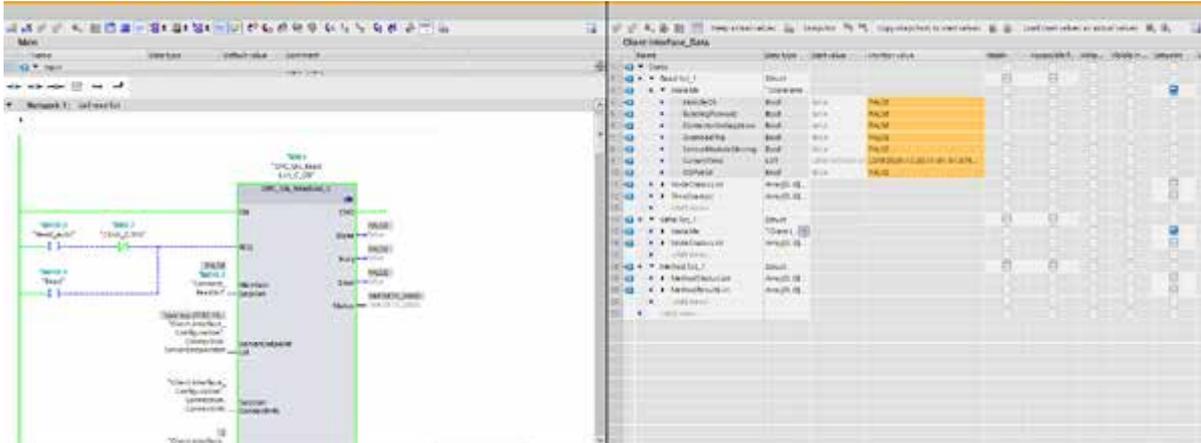


Abbildung 14: Online_setup_Reading

- Öffnen Sie „OB1“ und „Client_Interface_Data“ und ordnen Sie die Bildschirme nebeneinander an.
- Öffnen Sie das Menü „Readlist_1 >> Variable“.
- Überwachen Sie beide Bildschirme.

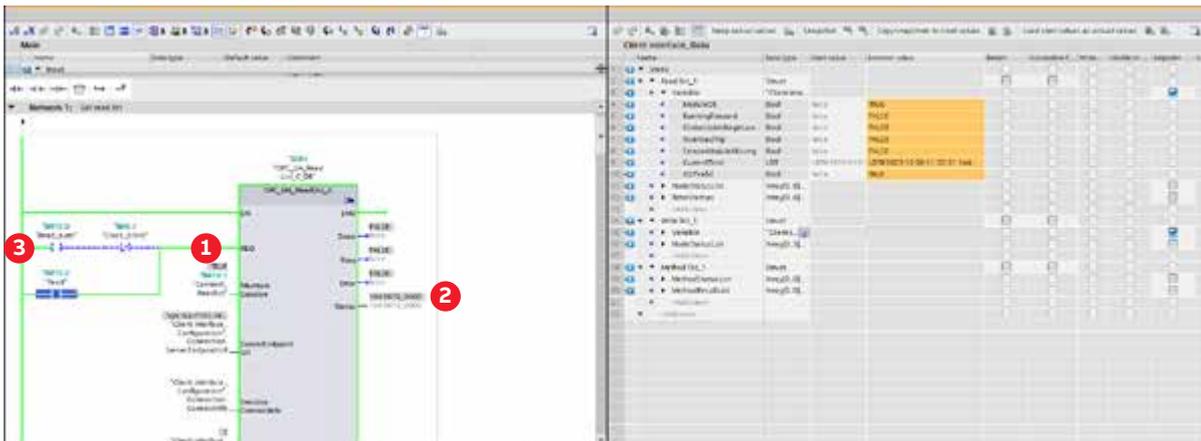


Abbildung 15: Online_Connect_Reading

- Stellen Sie eine Verbindung zum Server her und setzen Sie dazu das Tag „Connect_Readlist (Maintain Session)“ auf TRUE. **1**
- Überprüfen Sie die Statusvariable in OB1. Der Status sollte 16#3870_0400 zurückgeben. **2**
- Lesen Sie die Werte und setzen Sie dazu das Tag „Read“ oder „Read_auto“ auf TRUE. Bei jeder positiven Flanke des REQ-Signals werden die Daten vom Server gelesen. **3**
- Die Variablen auf dem Bildschirm „Client_Interface_Data“ wurden nun vom Server gelesen.

4.5. Schreibliste

4.5.1. Programmschreibliste

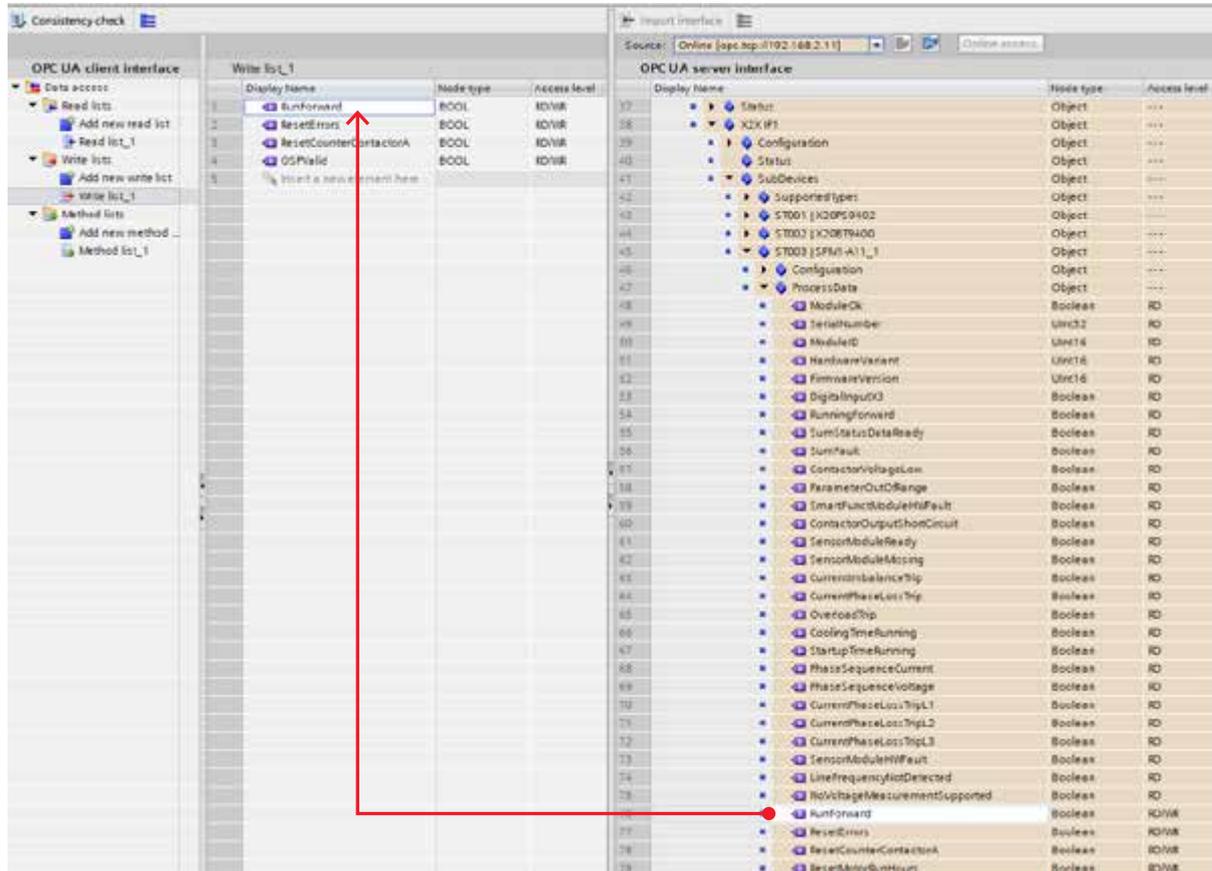


Abbildung 16: Write_list

- Fügen Sie eine neue Schreibliste hinzu.
- Wählen Sie die Variablen aus, die geschrieben werden sollten, ziehen Sie die gewünschten Variablen nach links und legen Sie sie in der Schreibliste ab.
- Kompilieren Sie die Software.

Hinweis: Sie können mehrere Schreiblisten hinzufügen.

In diesem Beispiel werden die folgenden Variablen verwendet:

- ProcessData >> RunForward
- ProcessData >> ResetErrors
- ProcessData >> ResetCounterContactorA
- ProcessData >> OSPValid

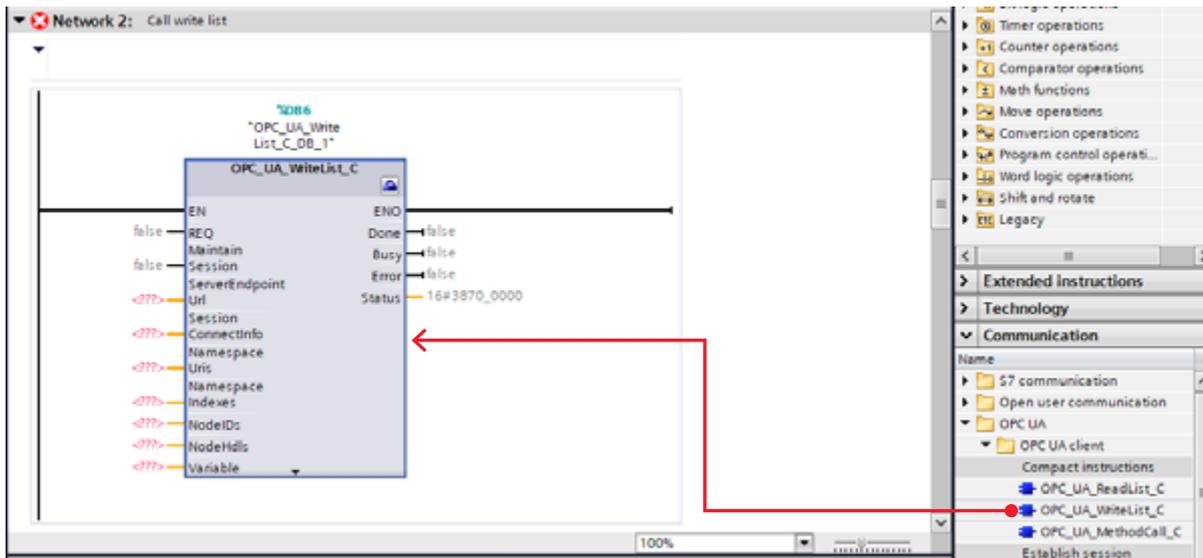


Abbildung 17: OB1_writelist

- Ziehen Sie die Schreibliste OPC_UA_WriteList_C und legen Sie sie in OB1 ab.

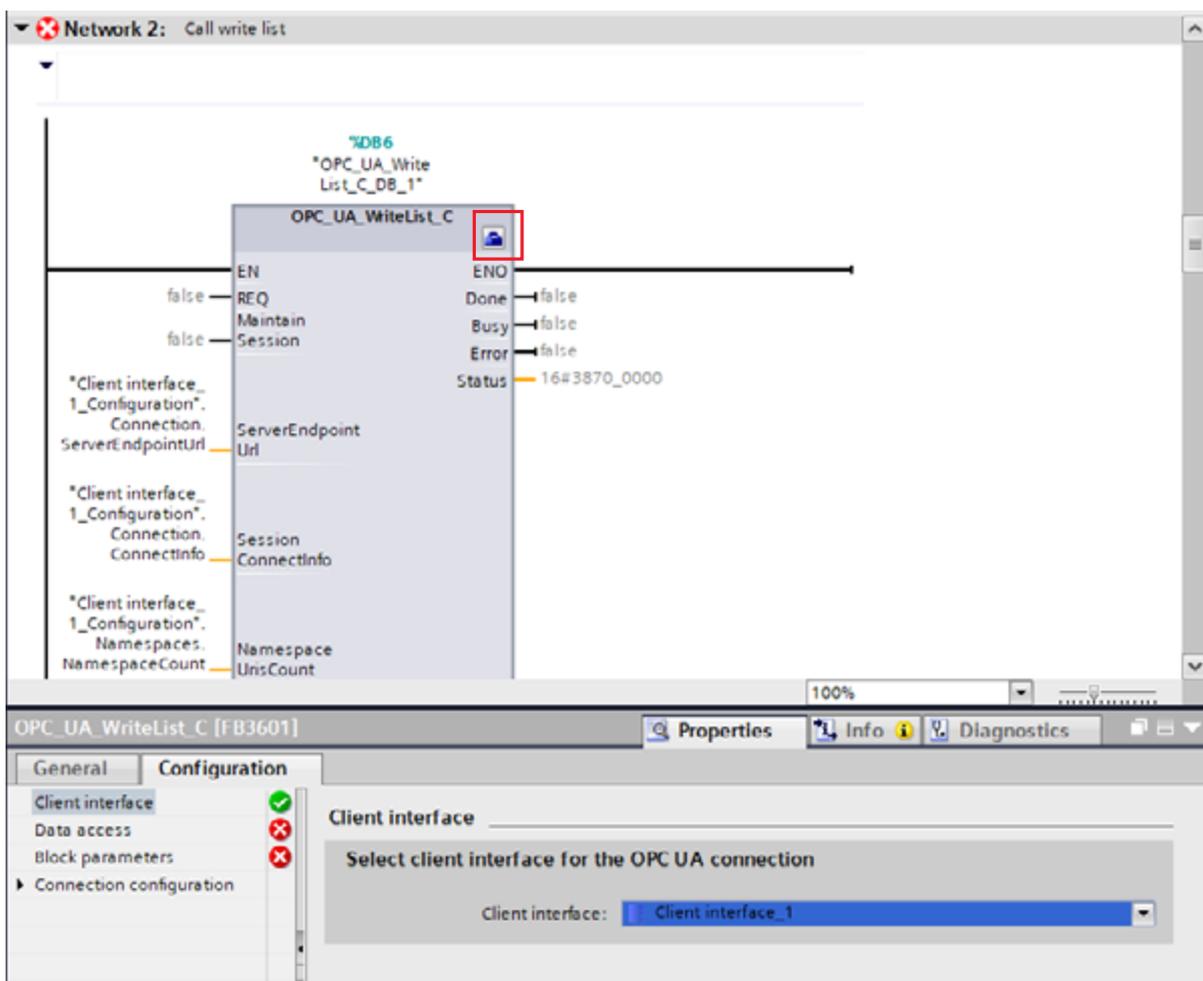


Abbildung 18: OB1_writelist_ClientInterface

- Klicken Sie auf das Toolbox-Symbol in der rechten oberen Ecke des OPC_UA_WriteList_C-Blocks.

Die Konfiguration des OPC_UA_WriteList_C-Blocks wird unten angezeigt.

- Wählen Sie die zuvor erstellte Client-Schnittstelle aus.

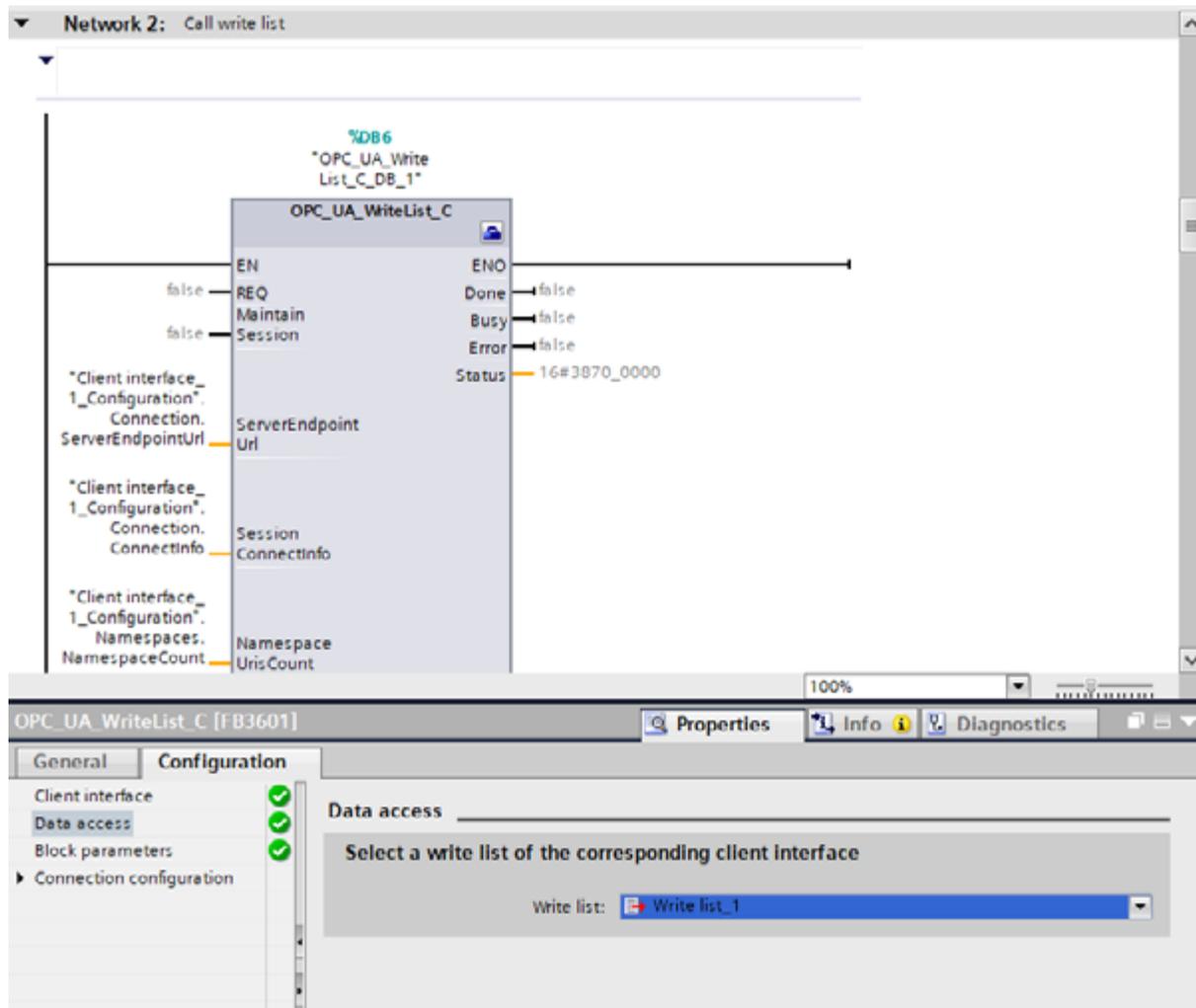


Abbildung 19: OB1_Writelst_DataAcces

- Wählen Sie die zuvor erstellte Schreibliste aus.
- Die restlichen Parameter werden automatisch von Siemens eingestellt.

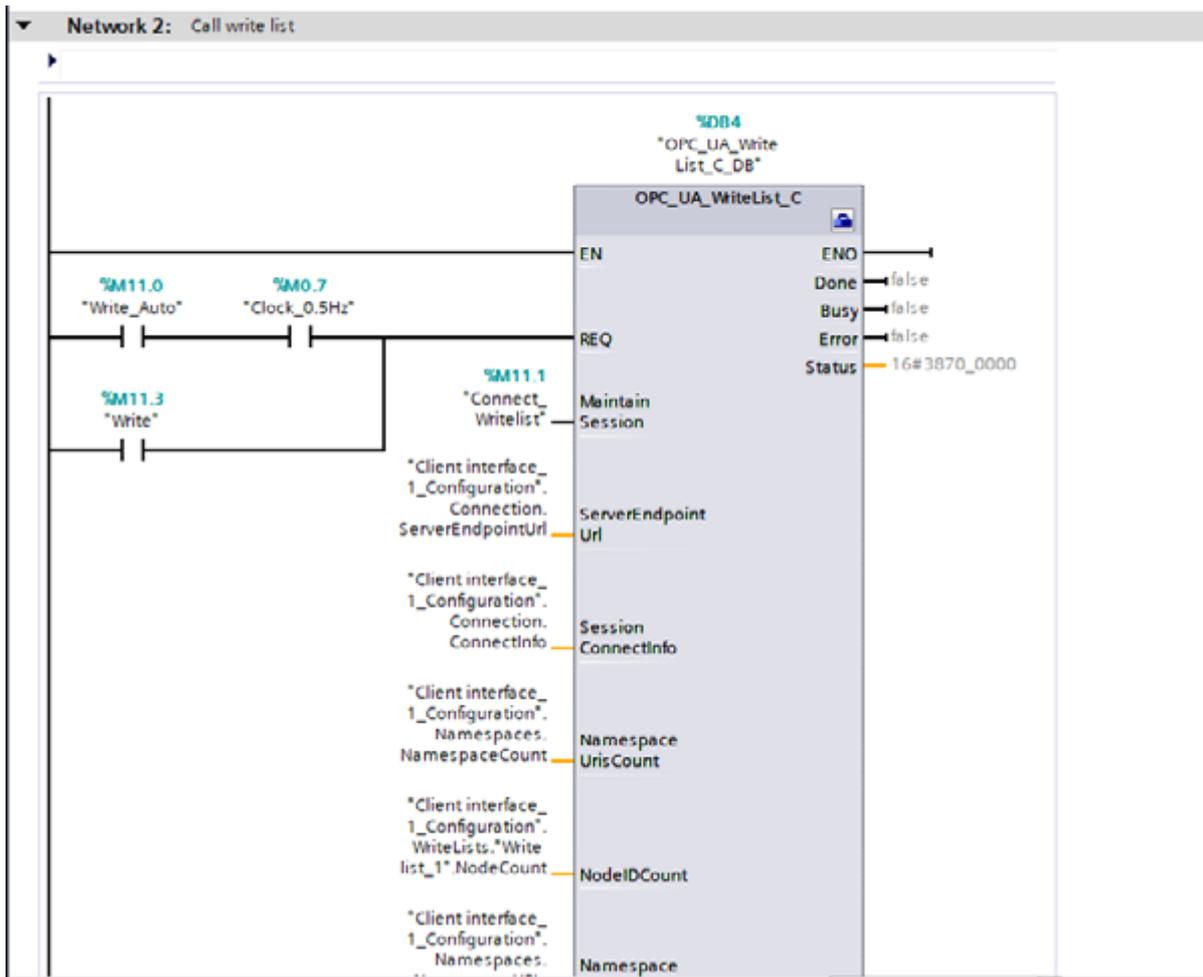


Abbildung 20: OB1_writelst_Merker

- Fügen Sie ein Tag zum Request-Eingang (REQ) hinzu. Bei jeder positiven Flanke wird eine Verbindung mit dem Server hergestellt und die Variablen werden auf den Server geschrieben.

Fügen Sie ein Tag zu „Maintain Session“ hinzu.

- Kompilieren Sie das Projekt mit einem „Rebuild all“ für Hardware und Software.
- Laden Sie „hardware configuration“ herunter.
- Laden Sie „Software all“ herunter.

Hinweis:

Mit „Maintain Session“ wird die Verbindung zwischen Server und Client beibehalten. Das Festlegen auf „True“ ist hier nicht notwendig, aber bei jeder positiven Flanke von REQ kann die Verbindung schneller wiederhergestellt werden.

Wenn ein Fehler auftritt, muss der Benutzer Maintain deaktivieren und wieder aktivieren, um die Verbindung zum Server wiederherzustellen.

4.5.2. Schreibliste prüfen

Zum Schreiben der Daten auf den Server:

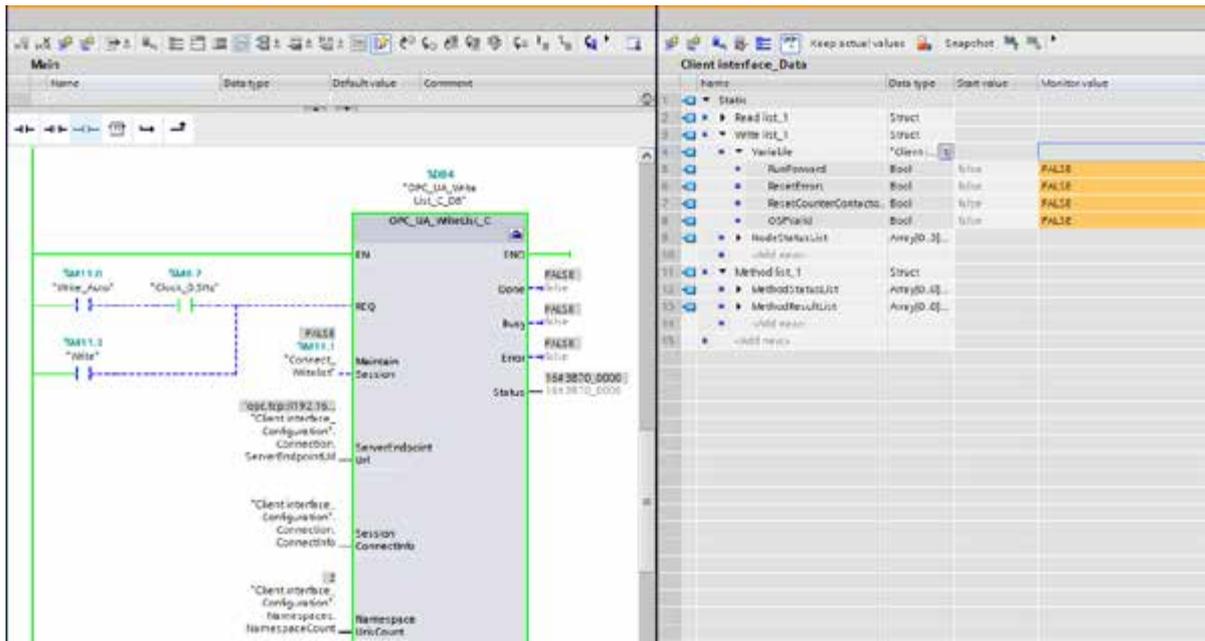


Abbildung 21: Online_setup_Writing

- Öffnen Sie „OB1“ und „Client_Interface_Data“ und ordnen Sie die Bildschirme nebeneinander an.
- Öffnen Sie das Menü „Writelist_1 >> Variable“.
- Überwachen Sie beide Bildschirme.

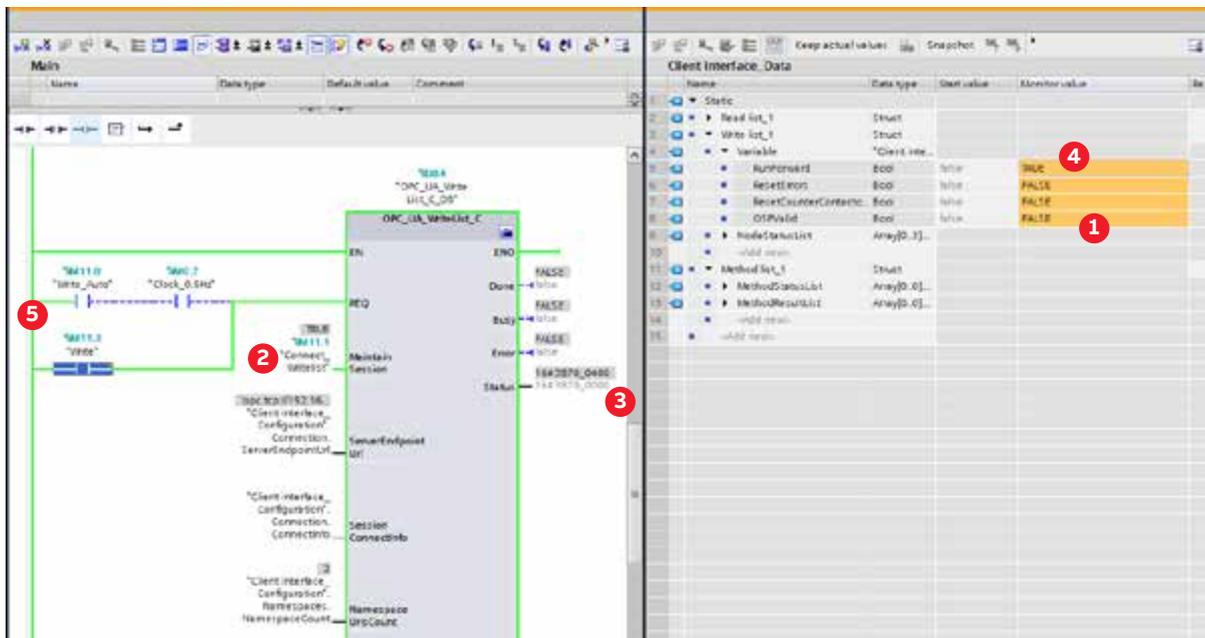


Abbildung 22: Online_Connect_Writing

- Prüfen Sie, ob „OSPValid“ in der Lesevariable „True“ ist. Setzen Sie anderenfalls die Variable „OSPValid“ in der Schreibliste auf TRUE. ①
- Stellen Sie eine Verbindung zum Server her und setzen Sie dazu das Tag „Connect_Writelist (Maintain Session)“ auf TRUE. ②
- Überprüfen Sie die Statusvariable in OB1. Der Status sollte 16#3870_0400 zurückgeben. ③
- Ändern Sie einen Wert auf dem Bildschirm „Client_Interface_Data“. Setzen Sie zum Beispiel „RunForward“ auf TRUE. ④
- Schreiben Sie die Werte und setzen Sie dazu das Tag „Write“ oder „Write_auto“ auf TRUE. Bei jeder positiven Flanke des REQ-Signals werden die Daten auf den Server geschrieben. ⑤
- Prüfen Sie, ob vom Schütz ein Klickgeräusch kommt.

4.6. Methodenliste

4.6.1. Programmmethodenliste

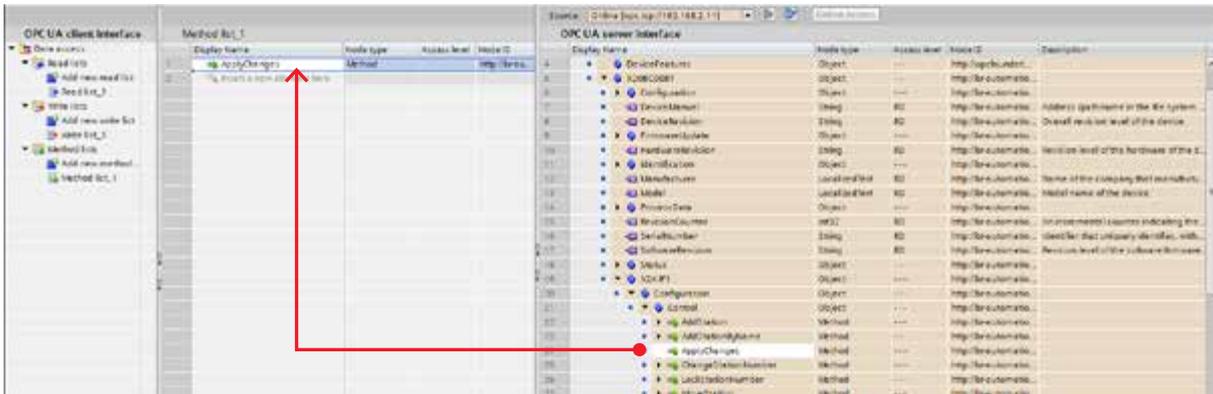


Abbildung 23: Method_list

- Fügen Sie eine neue Methodenliste hinzu.
- Wählen Sie „ApplyChanges“, ziehen Sie die Variable nach links und legen Sie sie in der Methodenliste ab.
- Kompilieren Sie die Software.

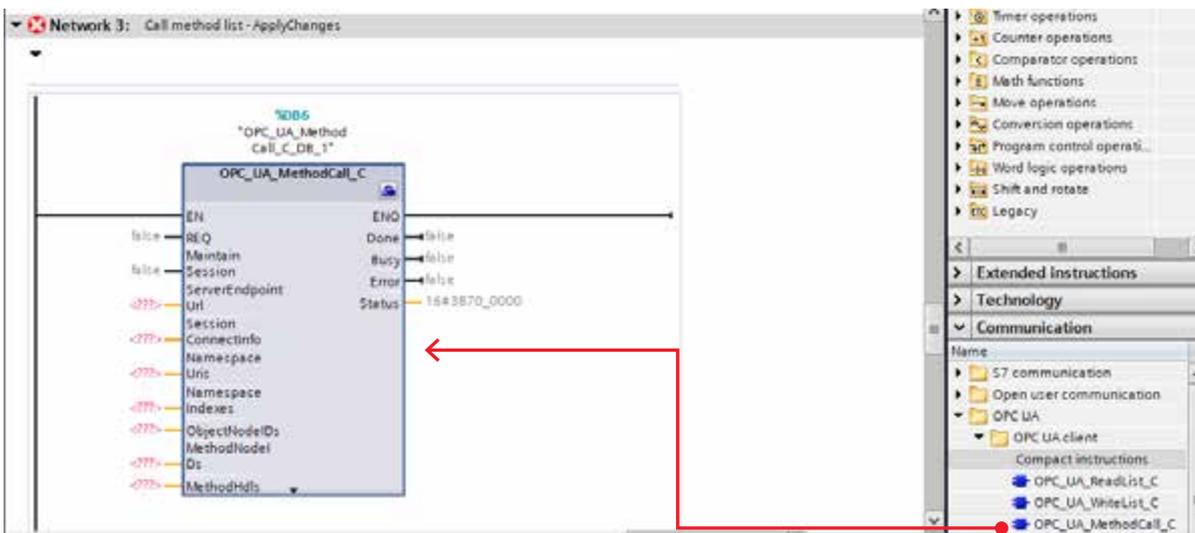


Abbildung 24: OB1_Methodlist

- Ziehen Sie OPC-UA-MethodCall_C und legen Sie ihn in OB1 ab.

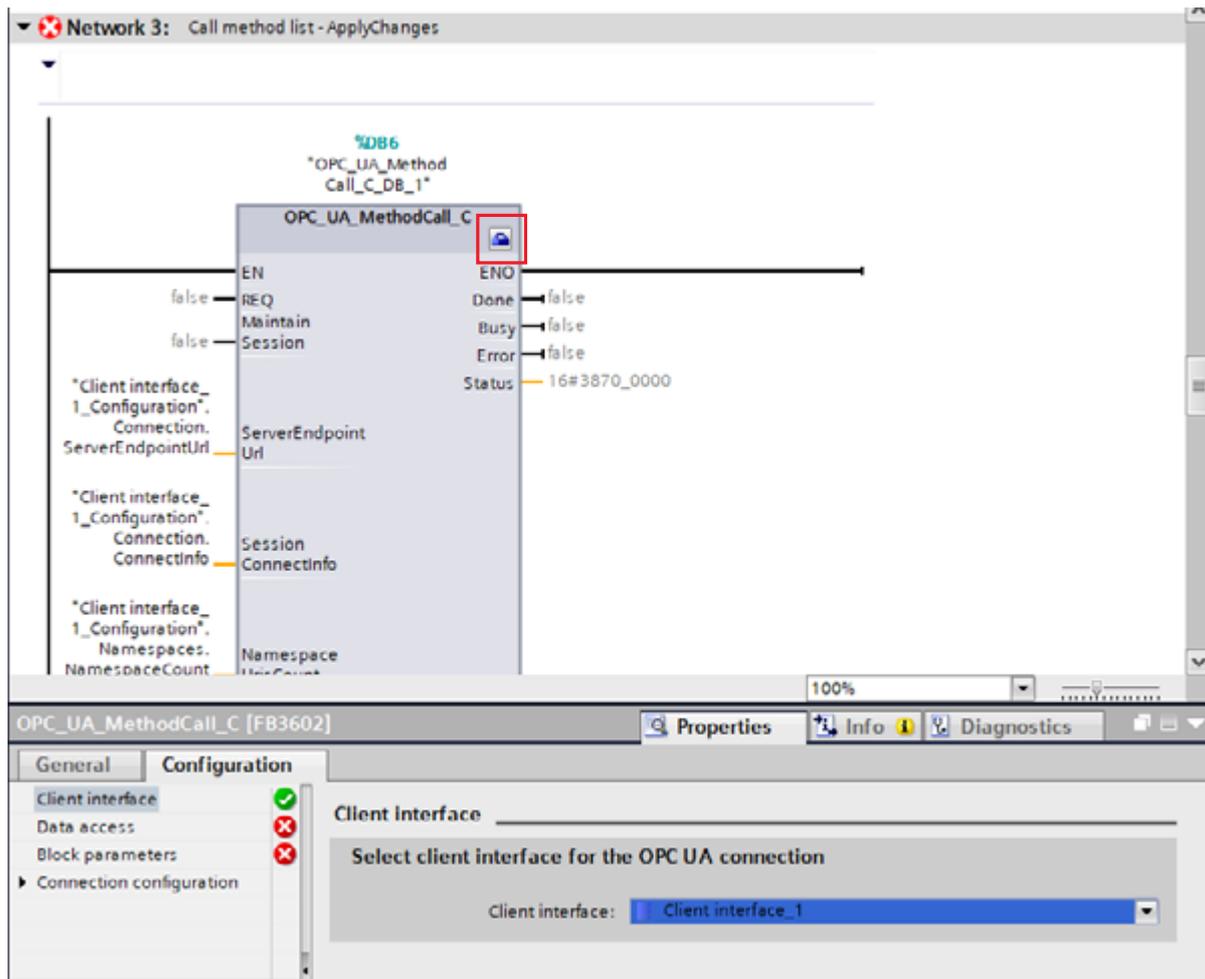


Abbildung 25: OB1_Methodlist_ClientInterface

- Klicken Sie auf das Toolbox-Symbol in der rechten oberen Ecke des OPC-UA-MethodCall_C-Blocks.

Die Konfiguration des OPC-UA-MethodCall_C-Blocks wird unten angezeigt.

- Wählen Sie die zuvor erstellte Client-Schnittstelle aus.

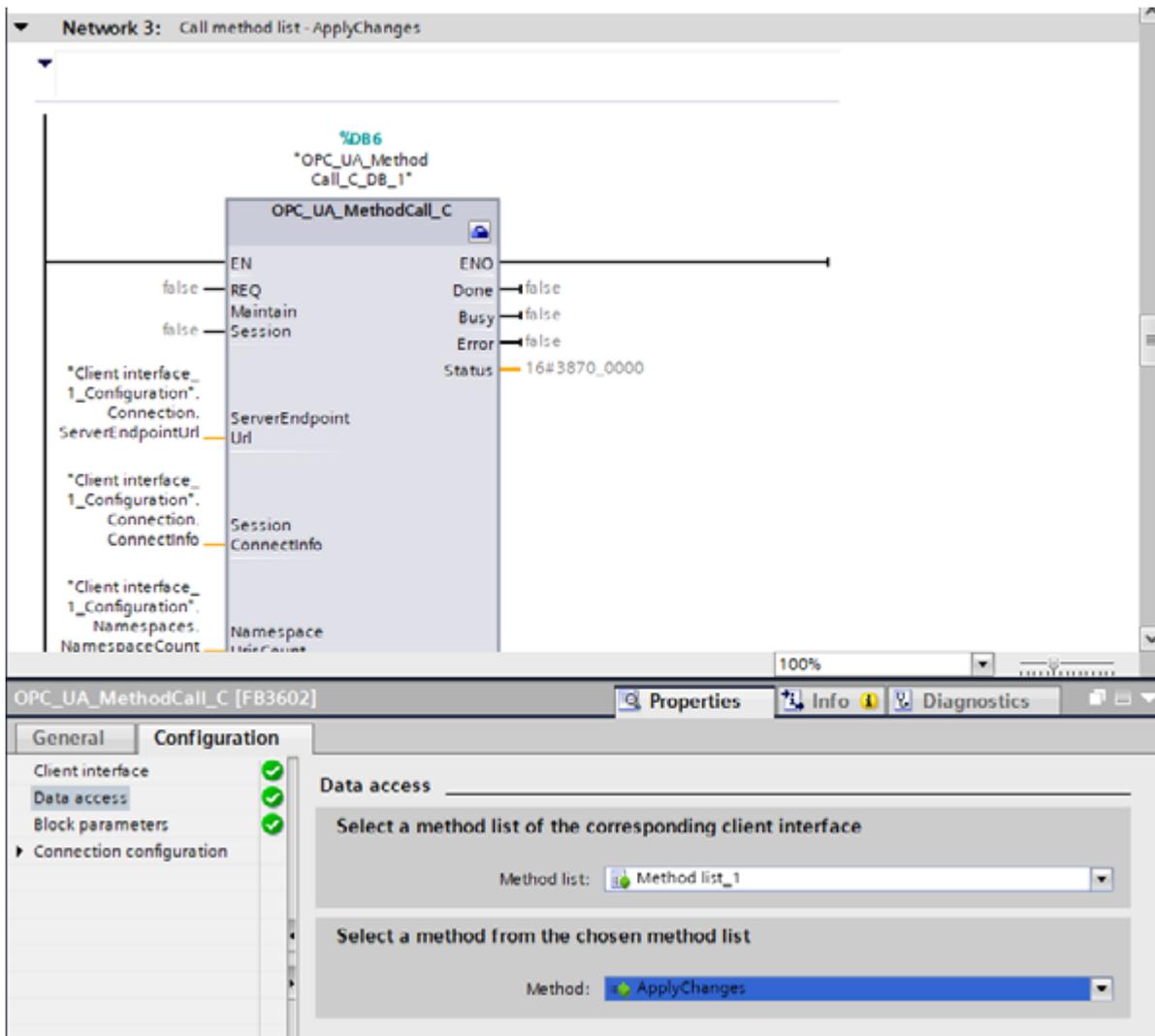


Abbildung 26: OB1_Methodelist_DataAcces_AC

- Wählen Sie die zuvor erstellte Methodenliste aus.
- Wählen Sie die Methode „ApplyChanges“ aus.
- Die restlichen Parameter werden automatisch von Siemens eingestellt.

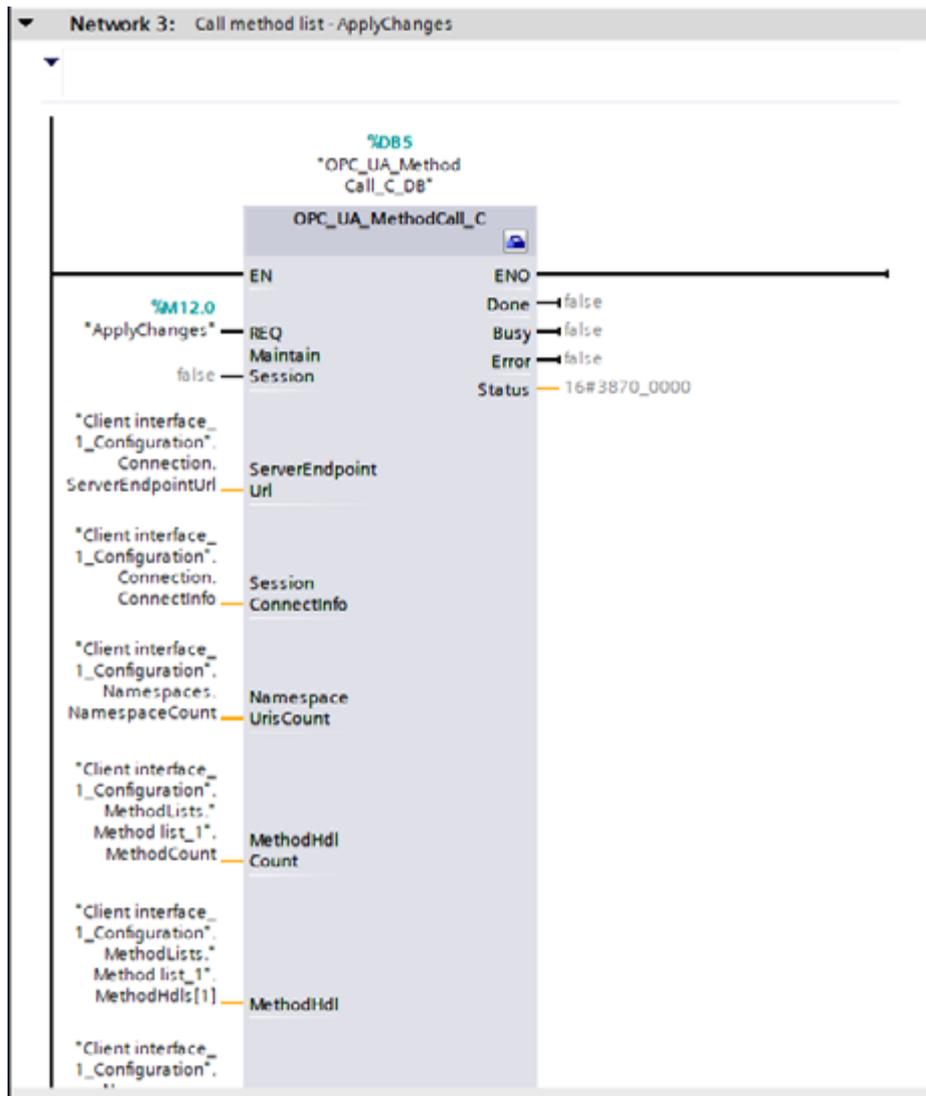


Abbildung 27: OB1_Methodlist_Merker_AC

- Fügen Sie ein Tag zum Request-Eingang (REQ) hinzu. Bei jeder positiven Flanke wird eine Verbindung mit dem Server hergestellt und die Änderungen werden auf den Server angewendet.
- Kompilieren Sie das Projekt mit einem „Rebuild all“ für Hardware und Software.
- Laden Sie „hardware configuration“ herunter.
- Laden Sie „Software all“ herunter.

4.7. Parameter einstellen

Zum Einstellen des Parameterwerts müssen Sie die Methodenliste verwenden.

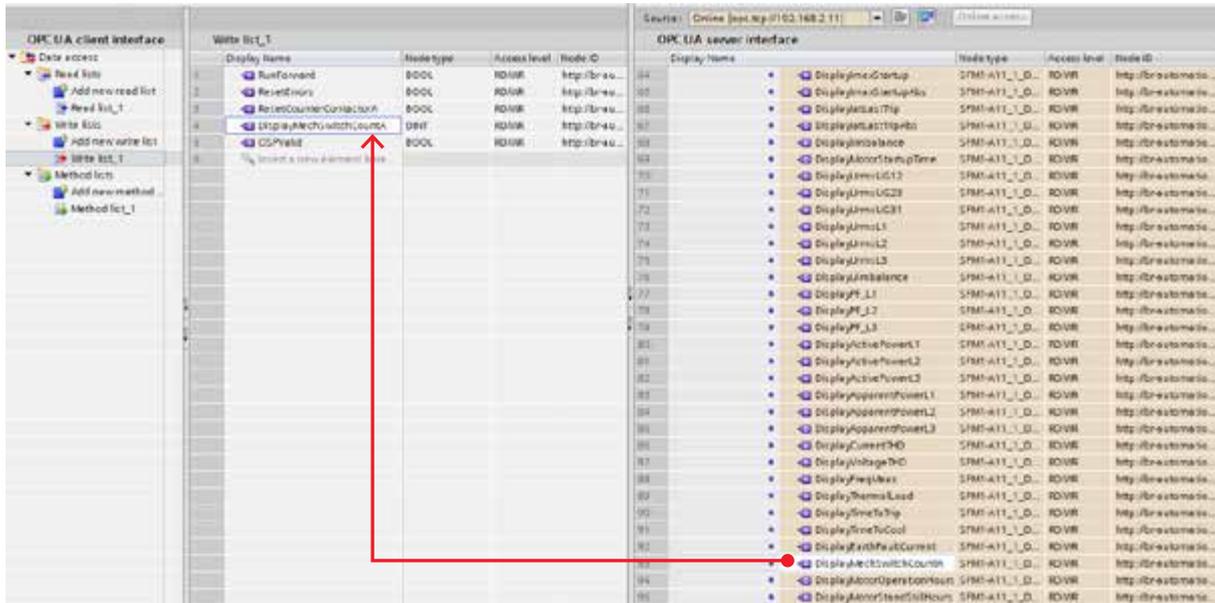


Abbildung 28: Online_Set_Parameter_Writeliste

- Ziehen Sie den Parameter und legen Sie ihn in der Schreibliste ab.
- Kompilieren Sie die Software.

In diesem Beispiel soll ermittelt werden, wie oft das Schütz geschaltet wurde.

Dazu müssen die folgenden Schritte ausgeführt werden:

- Legen Sie den Parameter "DisplayMechSwitchCountA" auf TRUE fest.
- Schreiben Sie den Parameter auf den Server.
- Verwenden Sie die Methode „Apply Changes“.
- Lesen Sie die Variable in der Leseliste.
- ParameterSet >> DisplayMechSwitchCountA

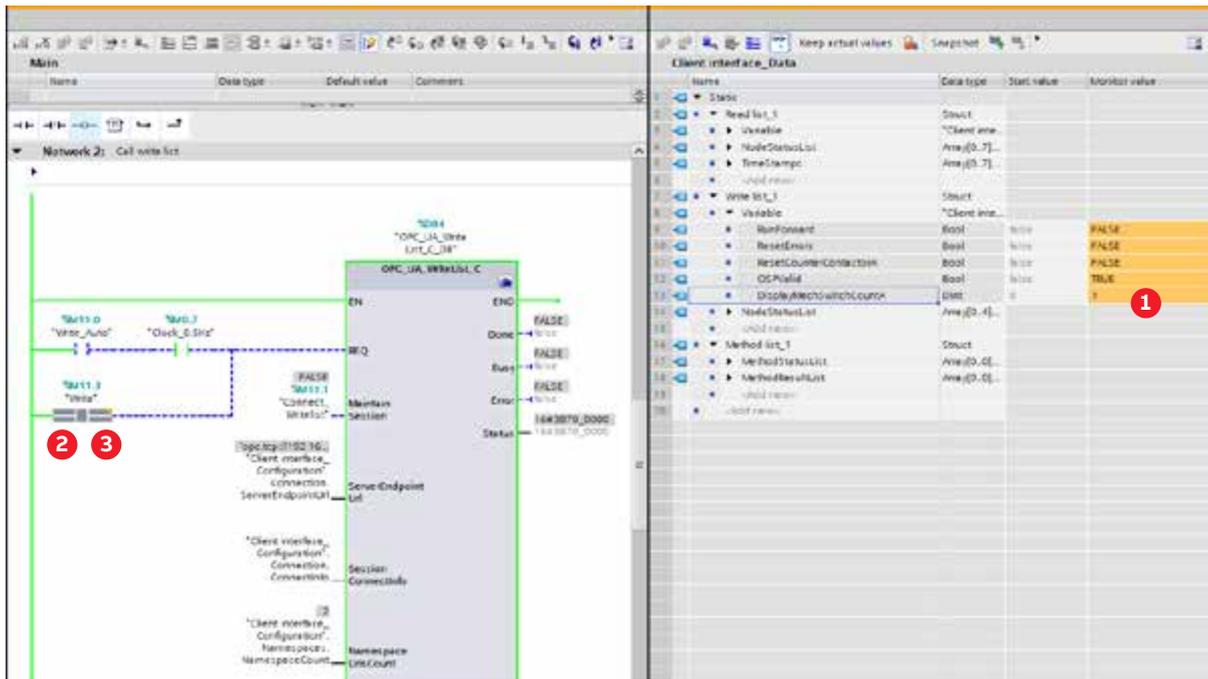


Abbildung 29: Online_Set_Parameter_Set

- Öffnen Sie „OB1“ und „Client_Interface_Data“ und ordnen Sie die Bildschirme nebeneinander an.
- Öffnen Sie das Menü „Writelist_1 >> Variable“.
- Überwachen Sie beide Bildschirme.
- Legen Sie „DisplayMechSwitchCountA“ auf 1 fest. 1
- Aktivieren Sie das Tag zum Schreiben. 2
- Deaktivieren Sie das Tag zum Schreiben. 3

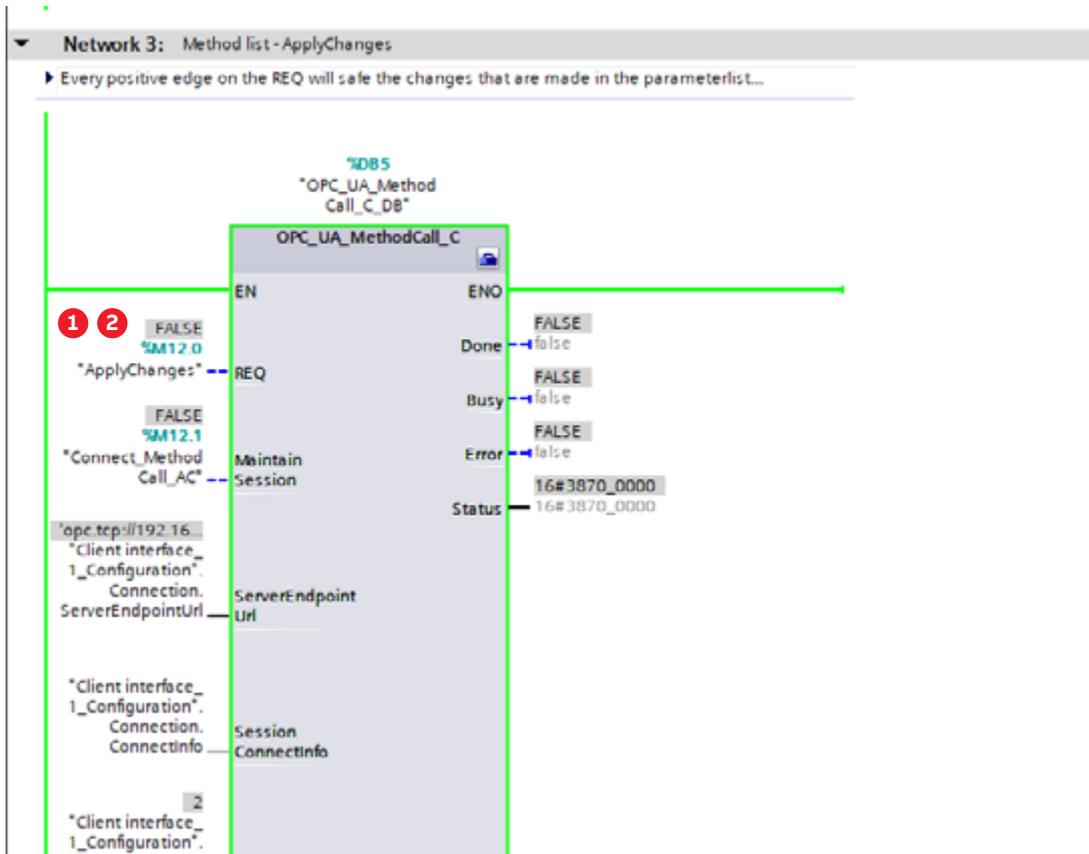


Abbildung 30: Online_Set_Parameter_ApplyChanges

- Aktivieren Sie „ApplyChanges“ (REQ). 1
- Deaktivieren Sie „ApplyChanges“ (REQ). 2

Nachdem der Server getrennt und wieder verbunden wurde, sollte die Variable in den processData der Client-Schnittstelle verfügbar sein.

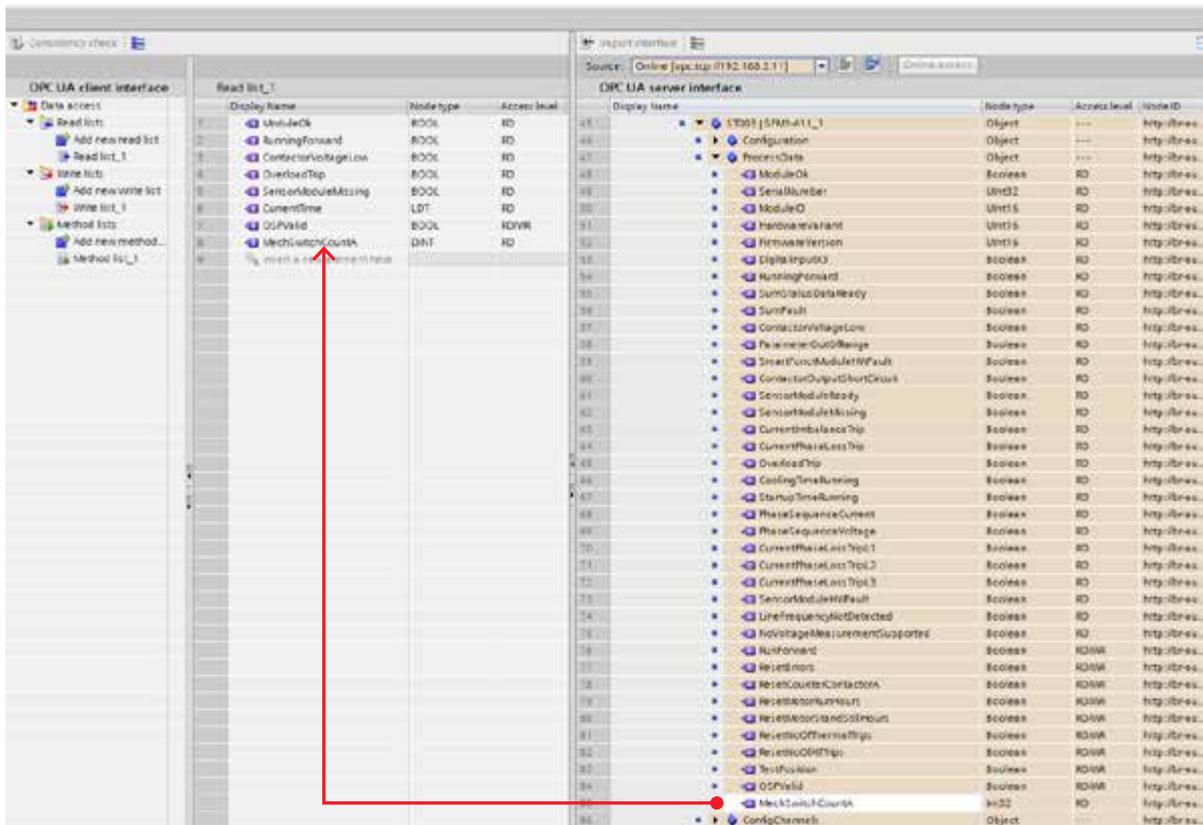


Abbildung 31: Online_Set_Parameter_Result

Beispiel:

- ProcessData >> MechSwitchCountA

5. Novolink mit Smart Gateway konfigurieren

Verwenden Sie die folgenden Dokumente, um Novolink mit Smart Gateway zu konfigurieren:

Dokumenttyp	Dokumentnummer	Link
Handbuch Novolink™ – Intelligente Funktions- und Sensor-Module für AF-Schütze	2CDC100017M0101	Link
Benutzerhandbuch für Novolink	9AKK108468A3939	Link

6. Fehlersuche

6.1. Keine OPC UA-Server-Anwendung gefunden

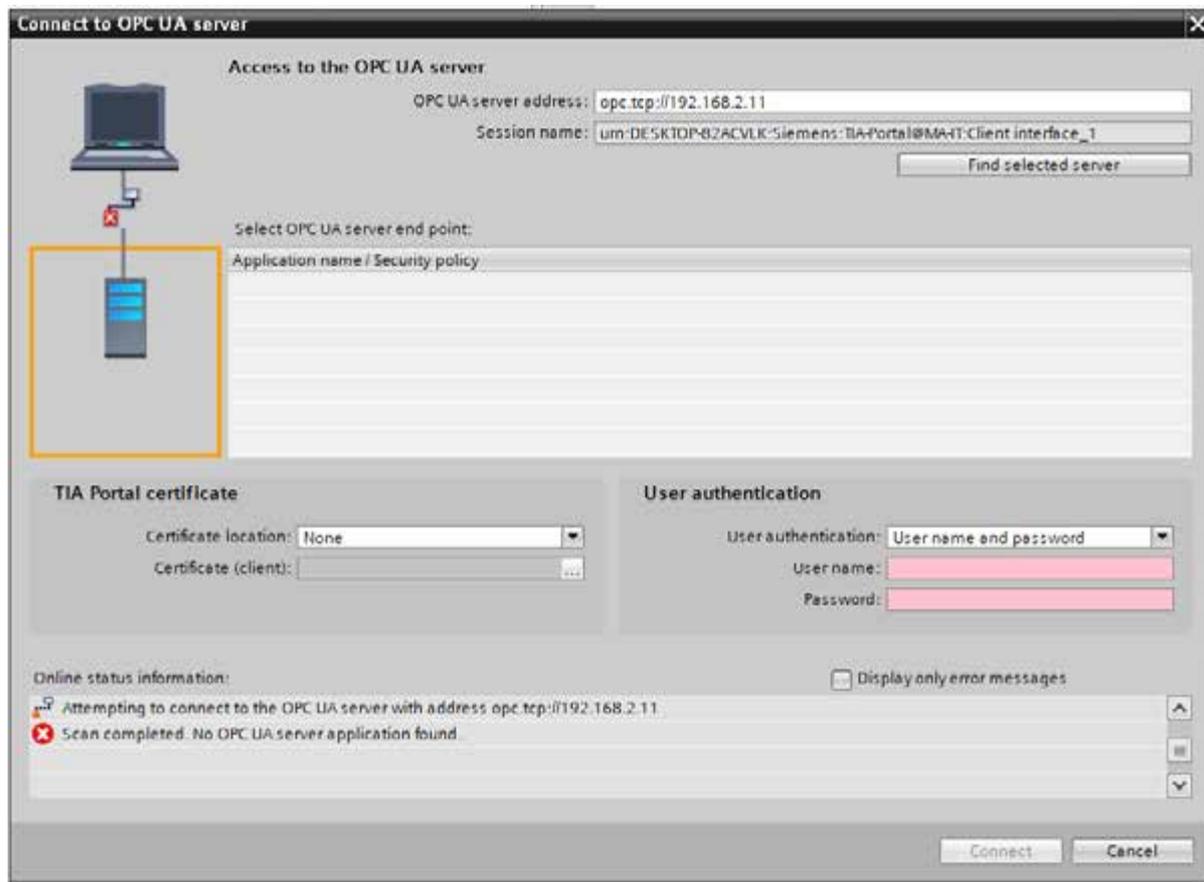


Abbildung 32: Pop-up-Dialogfeld für fehlenden Onlinezugriff

- Überprüfen Sie, ob TIA Portal das Smart Gateway erreichen kann.
- Überprüfen Sie die IP-Adresse des Servers.
- Überprüfen Sie die IP-Adresse Ihres Clients (TIA Portal).
- Überprüfen Sie, ob Sie den Server mit Ping erreichen können.
- Starten Sie den Server neu.

6.2. Status 16#3870_0600

Initiieren Sie die Verbindung und prüfen Sie im Fall des Fehlerstatus 3870_0600 die folgende Konfiguration:

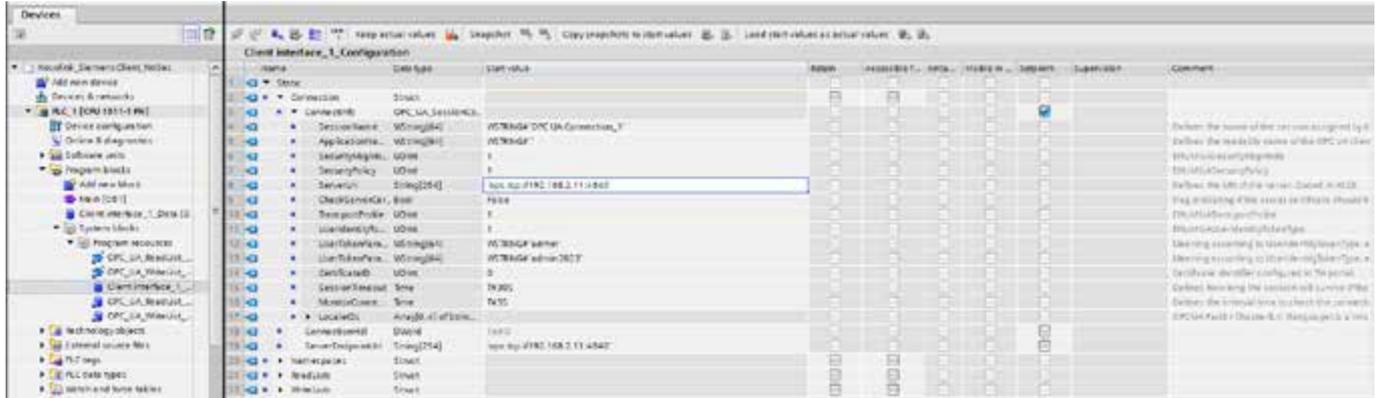


Abbildung 33: ClientInterface_Configuration

- Öffnen Sie den Block mit den Konfigurationsdaten der Client-Schnittstelle.
- Überprüfen Sie, ob „ServerEndpointUrl“ und „ServerUri“ den gleichen Startwert aufweisen.
 - Wenn dies nicht der Fall ist?
 - Kopieren Sie „ServerEndpointUrl“ in „ServerUri“.
- Kompilieren Sie das Projekt mit einem „Rebuild all“ für Hardware und Software.
- Laden Sie „hardware configuration“ herunter.
- Laden Sie „Software all“ herunter.

7. Liste zugehöriger Dokumente/Links

Dokumenttyp	Dokumentnummer	Link
Handbuch Novolink™ – Intelligente Funktions- und Sensor-Module für AF-Schütze	2CDC100017M0101	Link
Benutzerhandbuch für Novolink	9AKK108468A3939	Link
Siemens-Lizenzen		Link
Siemens SPS		Link



Großhandels- und Handwerkskunden:

Busch-Jaeger Elektro GmbH

Freisenbergstraße 2
58513 Lüdenscheid, Deutschland

Kundenservice:

Tel.: +49 (0) 2351 956-1600

info.bje@de.abb.com

Industriekunden:

ABB STOTZ-KONTAKT GmbH

Eppelheimer Straße 82
69123 Heidelberg, Deutschland

Kundenservice:

Tel.: +49 (0) 6221 701-777

info.stotz@de.abb.com

abb.de/niederspannung

Technische Änderungen der Produkte sowie Änderungen im Inhalt dieses Dokuments behalten wir uns jederzeit ohne Vorankündigung vor. Bei Bestellungen sind die jeweils vereinbarten Spezifikationen maßgebend. ABB übernimmt keinerlei Verantwortung für eventuelle Fehler oder Unvollständigkeiten in diesem Dokument.

Wir behalten uns alle Rechte an diesem Dokument und den darin enthaltenen Gegenständen und Abbildungen vor. Jede Vervielfältigung, Offenlegung gegenüber Dritten oder Verwendung der Inhalte – sowohl in ihrer Gesamtheit als auch teilweise – ist ohne die vorherige schriftliche Zustimmung von ABB untersagt.
Copyright© 2024 ABB
Alle Rechte vorbehalten