

RTU3011C DNP3 Setup Guide

Overview

This guide walks through setting up a Siemens RTU3011C to send analogue input data via DNP3, first testing with KEPServerEX, then transitioning to custom C++ code.

Hardware Setup

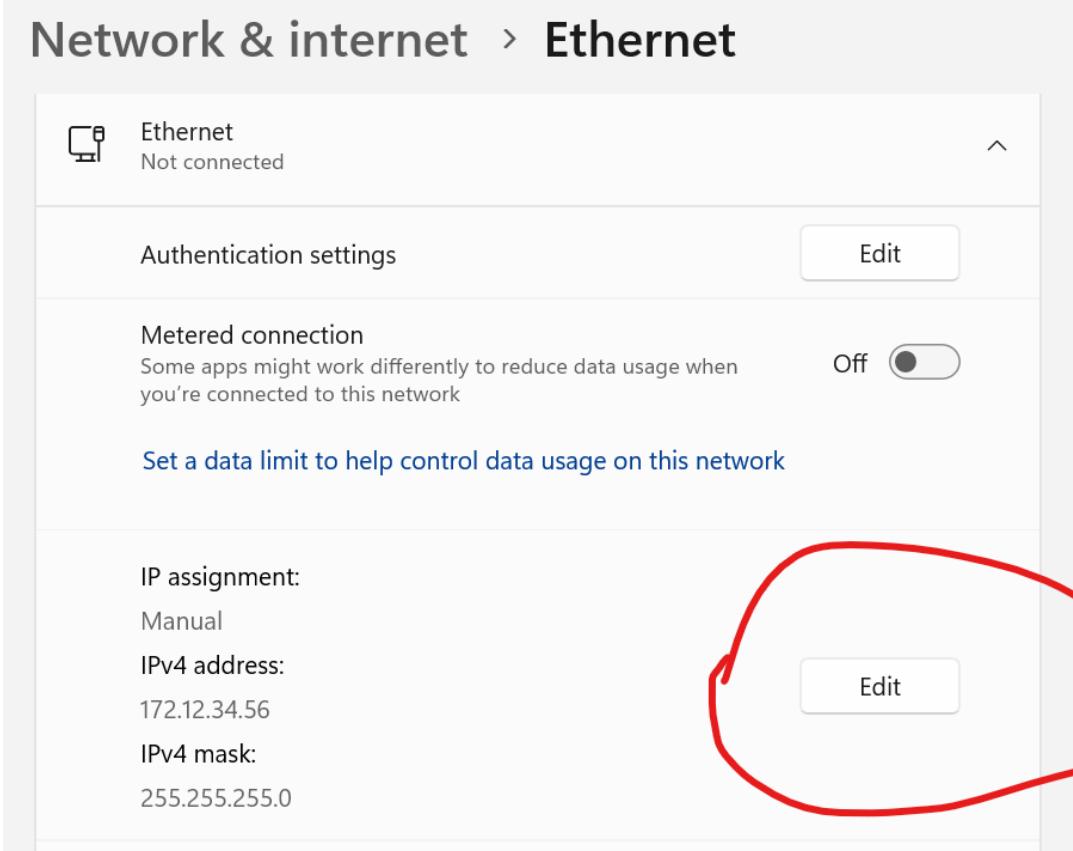
Physical Connections

- Connect computer directly to RTU with an ethernet cable, if this doesn't work try connecting via a network switch.

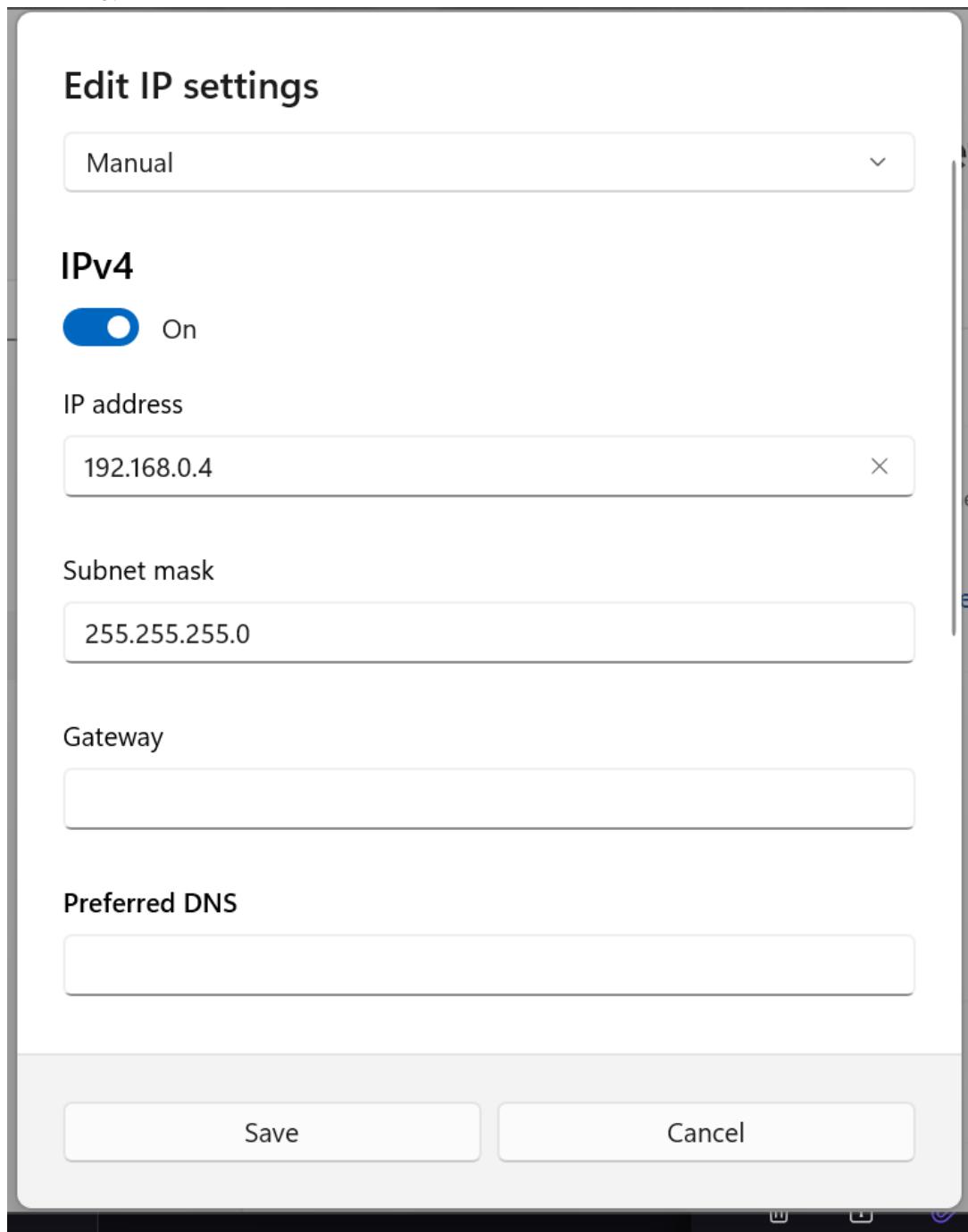
RTU Configuration for DNP3

Access RTU Web Interface

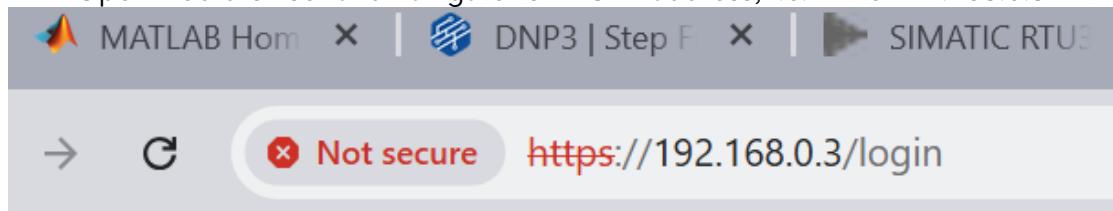
- Out of the box the RTU has IP address 192.168.0.3, to access it you will need to put your computer on the same subnet.
- To do this (using Windows) navigate to System Settings > Network & Internet > Ethernet then find the Ethernet port that you wish to use to connect to the RTU. Click Edit:



- Change your IP address so that it is on the same subnet as the RTU, 192.168.0.4 should work fine:



- Open web browser and navigate to RTU IP address; i.e. write 192.168.0.3 in the URL bar:



- Your browser will most likely give a warning that the connection isn't private. Click 'Advanced':

A screenshot of a web browser window. The address bar shows the URL <https://192.168.0.3/login>. Above the address bar, there are several tabs open, including "DNP3 | Step Function I/C", "Privacy error", "Sent | gphaworth@proto", and "MathWorks Certification". Below the address bar, there are browser control icons like star, refresh, and download. A large red warning icon (an exclamation mark in a triangle) is displayed prominently.



Your connection is not private

Attackers might be trying to steal your information from **192.168.0.3** (for example, passwords, messages or credit cards). [Learn more about this warning](#)

NET::ERR_CERT_AUTHORITY_INVALID



[Turn on enhanced protection](#) to get Chrome's highest level of security

Advanced

Back to safety

- Then click 'Proceed to 192.168.0.3 (unsafe)':

A screenshot of a web browser window, identical to the one above, showing the same 'Your connection is not private' warning for the URL <https://192.168.0.3/login>. A red circle highlights the 'Advanced' button at the bottom left of the warning area.

Your connection is not private

Attackers might be trying to steal your information from **192.168.0.3** (for example, passwords, messages or credit cards). [Learn more about this warning](#)

NET::ERR_CERT_AUTHORITY_INVALID



[Turn on enhanced protection](#) to get Chrome's highest level of security

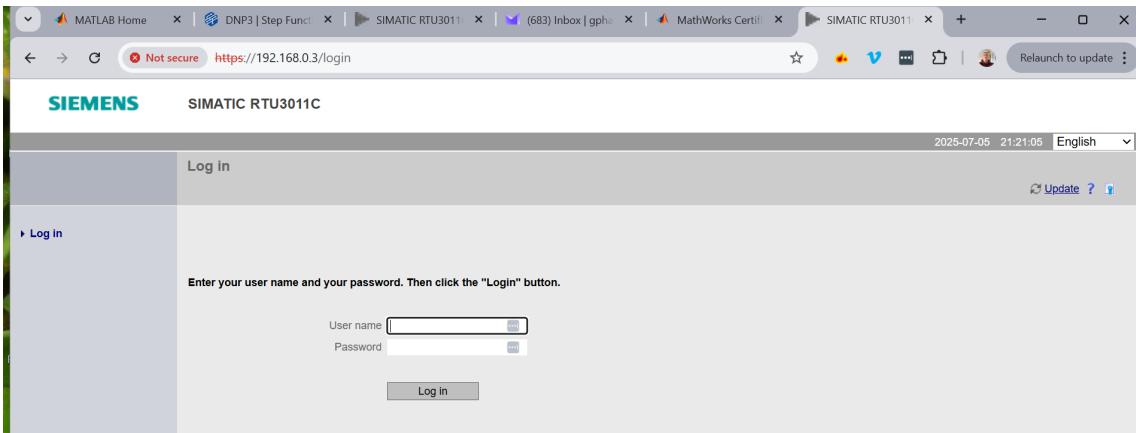
Hide advanced

Back to safety

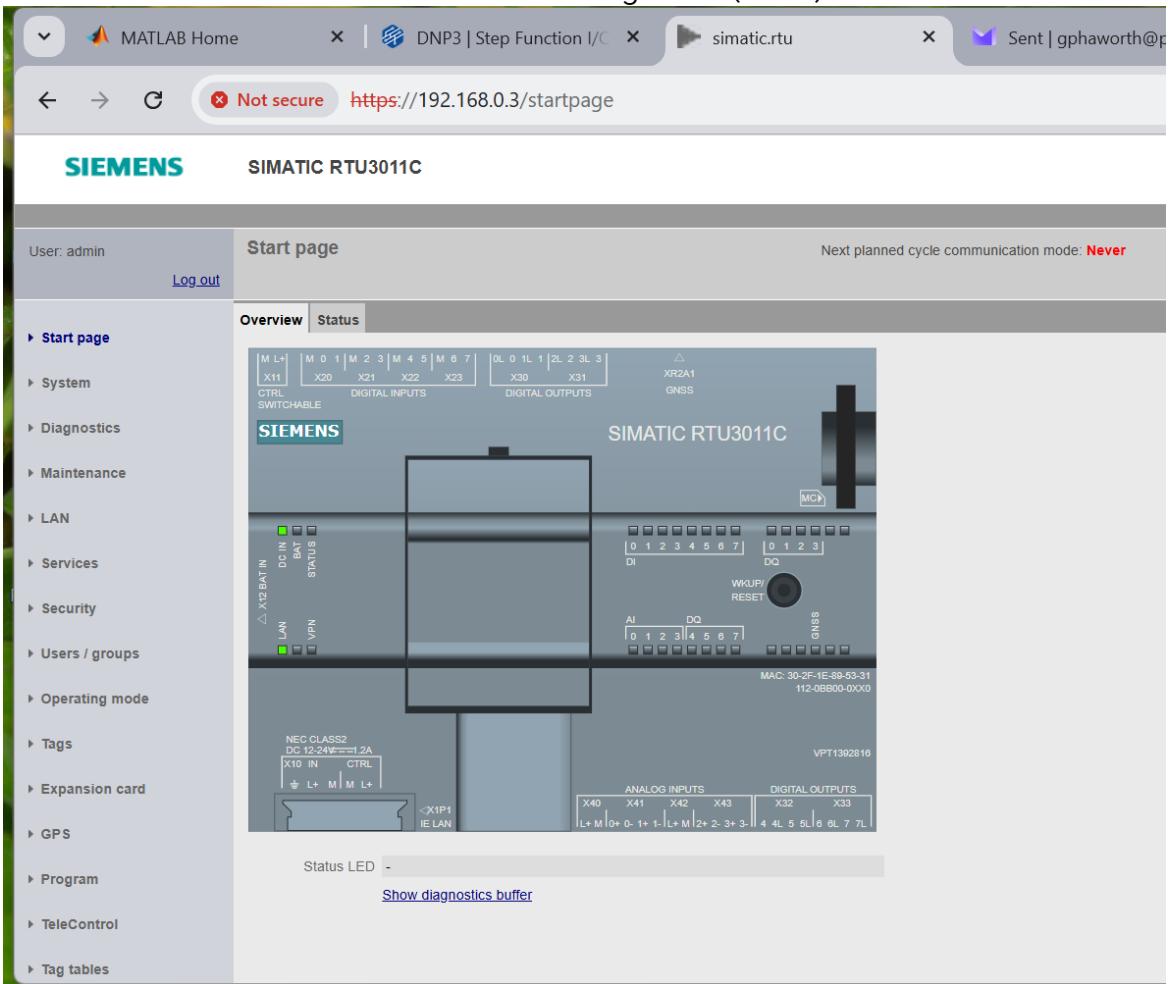
This server could not prove that it is **192.168.0.3**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.0.3 \(unsafe\)](#)

- The login screen for the RTU looks like this. Straight out of the box the username and password are both 'admin'. You will be asked to change the password when you first log in:



- You should now see the Web Based Management (WBM) interface:



Install DNP3 Firmware

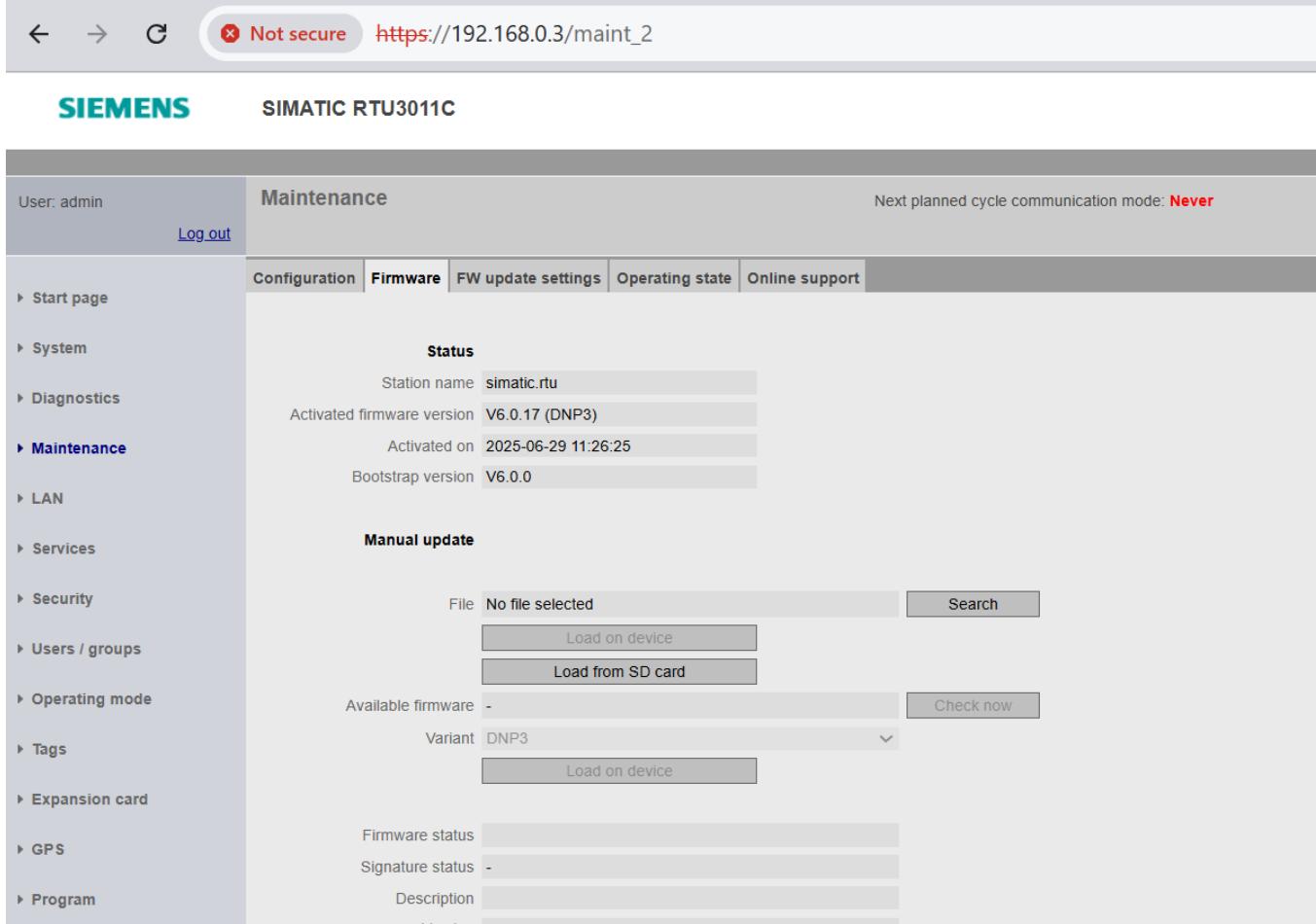
- You will now need to install the DNP3 firmware. This can be downloaded from the Siemens website here: [SIOS](#)

Download FW V6.0.17 for DNP3

RTU3051C and RTU3011C:

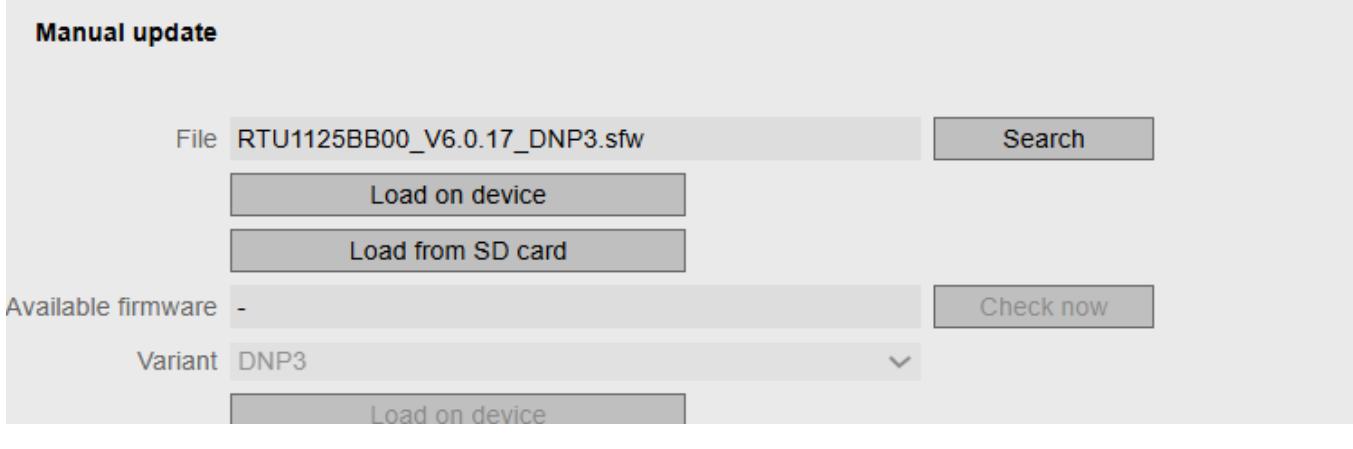
 [RTU1125BB00_V6.0.17_DNP3_OSS.zip \(1.8 MB\) \(SHA-256\)](#)

- When downloaded, extract the contents of the zip folder, there should be an SWF file.
- Navigate to the ‘Maintenance’ page and the ‘Firmware’ tab, click the ‘Search’ button:



The screenshot shows the SIMATIC RTU3011C maintenance interface. On the left is a sidebar with various navigation links. The main area is titled 'Maintenance' and has tabs for Configuration, Firmware, FW update settings, Operating state, and Online support. The 'Firmware' tab is currently selected. Under the 'Status' section, it shows the station name as 'simatic.rtu', activated firmware version as 'V6.0.17 (DNP3)', activation date as '2025-06-29 11:26:25', and bootstrap version as 'V6.0.0'. Below this is a 'Manual update' section. It includes fields for 'File' (containing 'RTU1125BB00_V6.0.17_DNP3.sfw'), 'Search' button, 'Load on device' and 'Load from SD card' buttons, an 'Available firmware' dropdown set to '-', a 'Variant' dropdown set to 'DNP3' with a 'Check now' button, and sections for 'Firmware status', 'Signature status', and 'Description'.

- Navigate to the SWF file and click ‘Load on device’:



This is a zoomed-in view of the 'Manual update' section from the previous screenshot. It shows the 'File' field containing 'RTU1125BB00_V6.0.17_DNP3.sfw', the 'Search' button, and two large buttons: 'Load on device' and 'Load from SD card'. Below these are fields for 'Available firmware' (set to '-'), 'Variant' (set to 'DNP3'), and another 'Load on device' button.

Activate Analogue Inputs

- Navigate to the ‘Tags’ page and the ‘Analog inputs’ tab:

Active	Name	Type	Process value, range	Unit	Format	Update cycle	Measure	Logging (actual value / mean value)
0	No	Voltage / 0 ... 5 V	0.00 ... 5.00	[V]	10 Seconds	0 ms / 40 ms / S...	OFF / OFF	
1	No	Voltage / 0 ... 5 V	0.00 ... 5.00		10 Seconds	0 ms / 40 ms / S...	OFF / OFF	
2	No	Voltage / 0 ... 5 V	0.00 ... 5.00		10 Seconds	0 ms / 40 ms / S...	OFF / OFF	
3	No	Voltage / 0 ... 5 V	0.00 ... 5.00		10 Seconds	0 ms / 40 ms / S...	OFF / OFF	

- Apply the appropriate configurations for the sensors being used, here I will be testing with a Fluke 789 Processmeter so I have selected a 4...20mA 2-wire connector. Give the input a name. In this case I changed the Process value range to be from 0.0 to 100.0, by changing ‘Process value (interpolation point 1)’ and ‘Process value (interpolation point 2)’; these will be the values that actually get sent via DNP3 corresponding to the 4 to 20mA signal (i.e. 4mA = 0.0, 20mA =100.0). Check the ‘Active’ box and click ‘Apply’:

Active

Name AI_0

Measure

Measured variable / measurement type Current (2-wire connector) ▾

Output signal / measuring range 4 ... 20 mA ▾

Power supply ON ▾

Settling time of the sensor (ms) 0

Integration time of the sensor (ms) 40 ms ▾

Smoothing None ▾

Current sensor value 0.000000

Current process value 0.000000

Specification of the measuring range

Sensor value (interpolation point 1) 4.00

Process value (interpolation point 1) 0.00

Sensor value (interpolation point 2) 20.00

Process value (interpolation point 2) 100.00

Process value, range 0.00 ... 100.00

Additional value

Mean value generation None ▾

Logging

Current value OFF ▾

Mean value OFF ▾

Diagnostics message

Wire break

Outside the measuring range

Apply

- If you now go to the ‘Overview’ tab in the ‘Tags’ page, the input that you just activated should show green:

User: admin [Log out](#)

Tags

Next planned cycle communication mode: **Never**

[Overview](#) [Digital inputs](#) [Digital outputs](#) [Digital memory bits](#) [Analog inputs](#) [Analog memory bits](#) [Temperature \(internal\)](#) [Power supply \(external\)](#) [Battery](#)

Start page

System

Diagnostics

Maintenance

LAN

Services

Security

Users / groups

Operating mode

Tags

Expansion card

GPS

Program

TeleControl

Tag tables

	0	1	2	3	4	5	6	7
Digital inputs								
Digital outputs								
Digital memory bits								
Analog inputs	0 / - 10s							
Analog memory bits								

Update cycle

Basic cycle 10 seconds

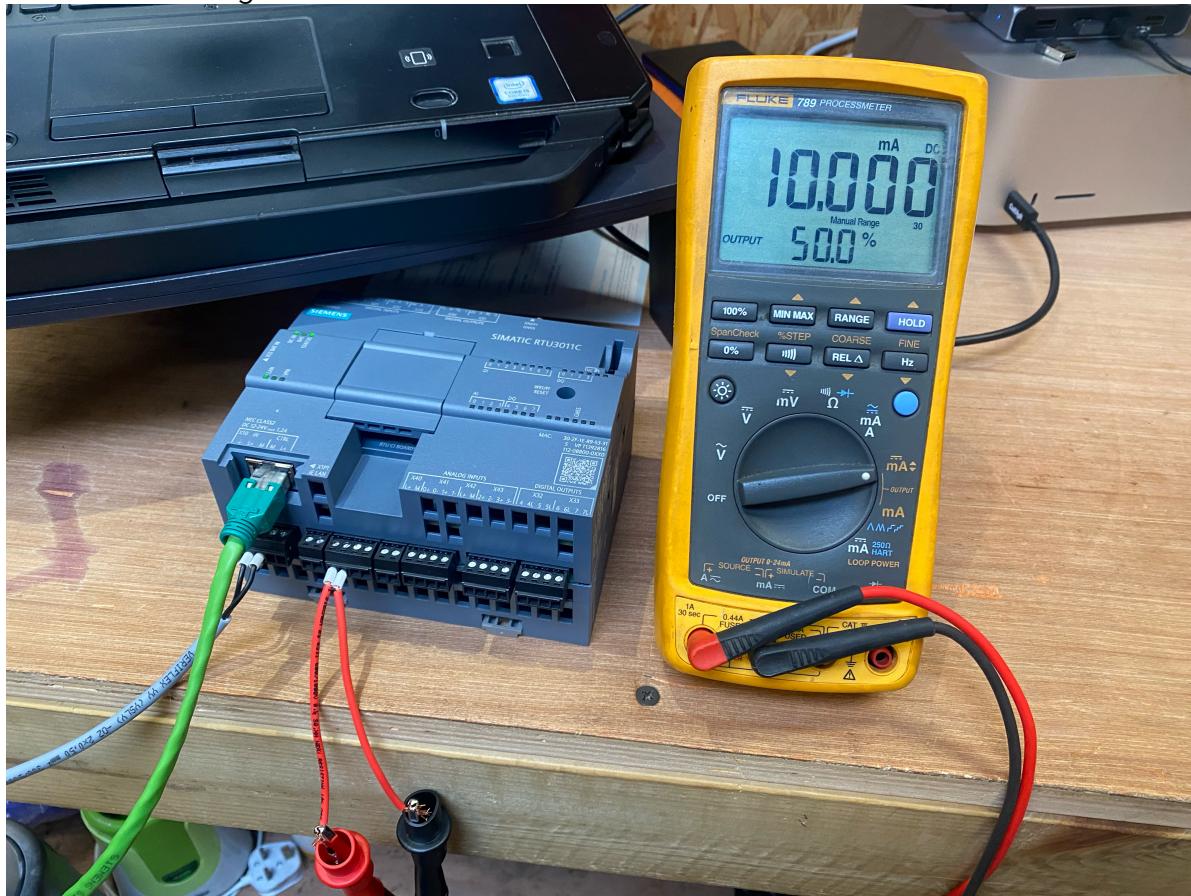
Additional cycle 10 seconds

Copy of the process image

[Save](#)

- It is possible (and advisable) at this stage to test that the analogue input with an actual input.

Here I am sourcing 10mA with a Fluke 789 Processmeter:



- If you click the ‘Read’ button on the ‘Analog inputs’ tab, it will update the actual reading at that input:

The screenshot shows the configuration interface for an analog input (AI_0). The 'Active' checkbox is checked. The 'Name' is set to 'AI_0'. Under the 'Measure' section, the 'Measured variable / measurement type' is 'Current (2-wire connector)'. The 'Output signal / measuring range' is '4 ... 20 mA'. The 'Power supply' is 'ON'. The 'Settling time of the sensor (ms)' is '0'. The 'Integration time of the sensor (ms)' is '40 ms'. The 'Smoothing' option is 'None'. The 'Current sensor value' is '9.997305' and the 'Current process value' is '37.483154'. A 'Read' button is visible next to the current sensor value. Below this, under 'Specification of the measuring range', there are four pairs of fields: 'Sensor value (interpolation point 1)' and 'Process value (interpolation point 1)', and 'Sensor value (interpolation point 2)' and 'Process value (interpolation point 2)'. The first pair has values '4.00' and '0.00' respectively. The second pair has values '20.00' and '100.00'. The 'Process value, range' field shows '0.00 ... 100.00'. Under the 'Additional value' section, 'Mean value generation' is set to 'None'. In the 'Logging' section, both 'Current value' and 'Mean value' are set to 'OFF'. The 'Diagnostics message' section contains two checkboxes: 'Wire break' and 'Outside the measuring range', neither of which is checked.

DNP3 Station Settings

- Navigate to the ‘Telecontrol’ page and the ‘DNP3’ tab:

User: admin [Log out](#)

TeleControl

[Overview](#) **DNP3** [DNP3 SA](#) [Data points](#)

Start page

System

Diagnostics

Maintenance

LAN

Services

Security

Users / groups

Operating mode

Tags

Expansion card

GPS

Program

TeleControl

Tag tables

Active

IP address master station 192.168.0.4

IP address master station (alternative) 0.0.0.0

Port number 20000

Station address 7

Master station address 3

Interface LAN

IP protocol TCP/UDP

Partner monitoring time (s) 600

Reconnection cycle of the partner (s) 10

Save values acc. to event classes

Class 1 All values chronologically

Class 2 All values chronologically

Class 3 All values chronologically

Send buffer

Class 1 1

Class 2 1

Class 3 1

Delay time for events (s)

Class 1 1

Class 2 1

Class 3 1

DNP3 level Extended

Max. time between Select and Operate 5

- Set 'IP address master station' to the IP address of your computer.
- Set 'Port number' to 20000.
- Set 'Station address' and 'Master station address' to a unique address (example: 7 and 3).
- Check the 'Active' box.

DNP3 Data Points Setup

- In order to send the analogue reading via DNP3, the data point needs to be configured.
Navigate to the 'Telecontrol' page and the 'Data points' tab:

User: admin Log out SIMATIC RTU3011C

Next planned cycle communication mode: Never Number of active sessions: 1

► Stop ⚏ Update ? ⓘ

Start page System Diagnostics Maintenance LAN Services Security Users / groups

Overview | DNP3 | DNP3 SA | **Data points**

Name	Data point type	Type of transfer	Index	Trigger	Threshold (%)	Threshold (abs.)
Digital inputs	-	-	-	-	-	-
Analog inputs	-	-	-	-	-	-
AI_0 (A10)	Single-prec flt-pt with flag (30.5) / With time (32.7)	Class 2	0	Cyclic	0.00	0.00
Counter inputs	-	-	-	-	-	-
Digital outputs	-	-	-	-	-	-
Analog outputs	-	-	-	-	-	-

Apply

- The analogue input that was just activated should appear here, by default ‘Type of transfer’ is set to ‘Only internal use’. This means that the point is not available via DNP3. This needs to be set to either Class 1, 2 or 3:

Class 1: High priority events (critical alarms, important changes)

Class 2: Medium priority events (normal operational data)

Class 3: Low priority events (non-critical data, historical logs)

- Set the ‘Index’ appropriately; this is the DNP3 reference number that the DNP3 client shall refer to. This can be any integer value but here I will simply use 0 for AI0.
- If ‘Trigger’ is set to ‘Change’ this will update the value sent to a DNP3 client whenever the analogue reading changes more than the deadband specified.
- If ‘Trigger’ is set to ‘Cyclic’ this will update the value sent to a DNP3 client at the time interval specified in the ‘Update cycle of this input’ setting for the analogue input (found in the ‘Analog inputs’ tab in the ‘Tags’ page).
- ‘Trigger’ can also be set to ‘Both’.

RTU Time Synch

- The system time for the RTU cannot be synchronised with an NTP server.
- When you activate telecontrol communication, the time-of-day synch is activated automatically and set by the telecontrol master station.
- If time-of-day synchronization is already activated, the currently active method is maintained.
- When you deactivate telecontrol communication and the time-of-day synchronization is activated by the telecontrol master station, the time-of-day synchronization is automatically deactivated.
- The ‘System time’ tab of the System page in the RTU web interface should look like this:

System Next planned cycle communication mode: **Never**

General Device info SD card System time System tags

Local time zone
 (UTC) London
 00 h 00 min
 Automatic daylight saving time switch
 Beginning of daylight saving time Last Sunday March 01 h 00 min
 End of daylight saving time Last Sunday October 02 h 00 min

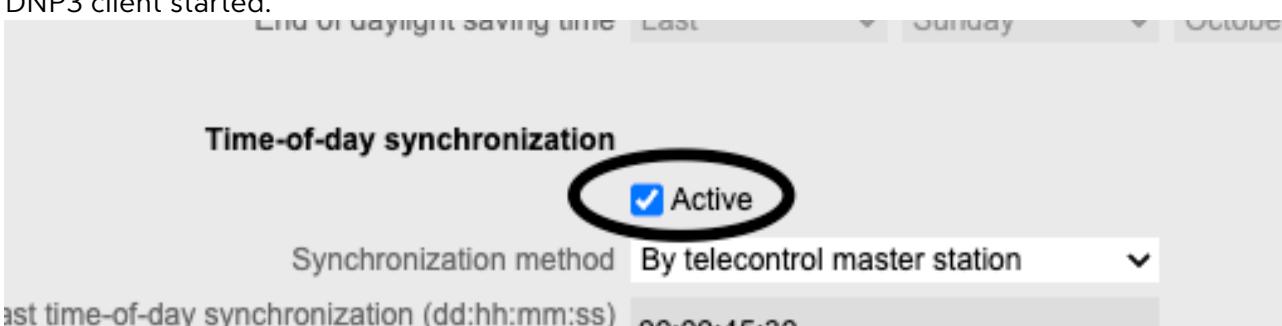
Time-of-day synchronization
 Active
 Synchronization method By telecontrol master station
 Last time-of-day synchronization (dd:hh:mm:ss) ago 00:00:45:30

NTP settings
 Interface VPN 1
 Accept time-of-day from non-synchronized NTP servers
 IP address or DNS name of the NTP server

Diagnostics message
 Check time-of-day synchronization
 Reduction factor for communication cycle 1
 Communication cycle: 10 Minutes.
 Test cycle: 10 Minutes.

Apply

Set system time manually
 New system time Year-month-day hour:minute:second
 Apply new time of day
 Adopt PC time

- When the DNP3 client is run for the very first time it may be necessary for 'Time-of-day synchronization' to be deactivated and reactivated in the RTU if it was already running when the DNP3 client started.
- 
- The screenshot shows the 'Time-of-day synchronization' configuration. The 'Active' checkbox is highlighted with a black oval. Below it, the 'Synchronization method' is set to 'By telecontrol master station'. A note at the bottom indicates the last time-of-day synchronization was at 00:00:45:30.
- In order to check if time-of-day synch is working, deactivate it, then set the system time manually

Set system time manually

New system time

Apply new time of day

Adopt PC time

- Then reactivate ‘Time-of-day synchronization’ with the DNP3 client already running.
- Keep an eye on whether the time in the top right hand corner changes:



Testing with KEPServerEX

- Download and install KEPServerEX Demo: [Download the KEPServerEX demo](#)

KEPServerEX Channel Setup

- Open KEPServerEX and right click on ‘Connectivity’, then click ‘New Channel’:

[Connected to Runtime] - KEPServerEX 6 Configuration

File Edit View Tools Runtime Help

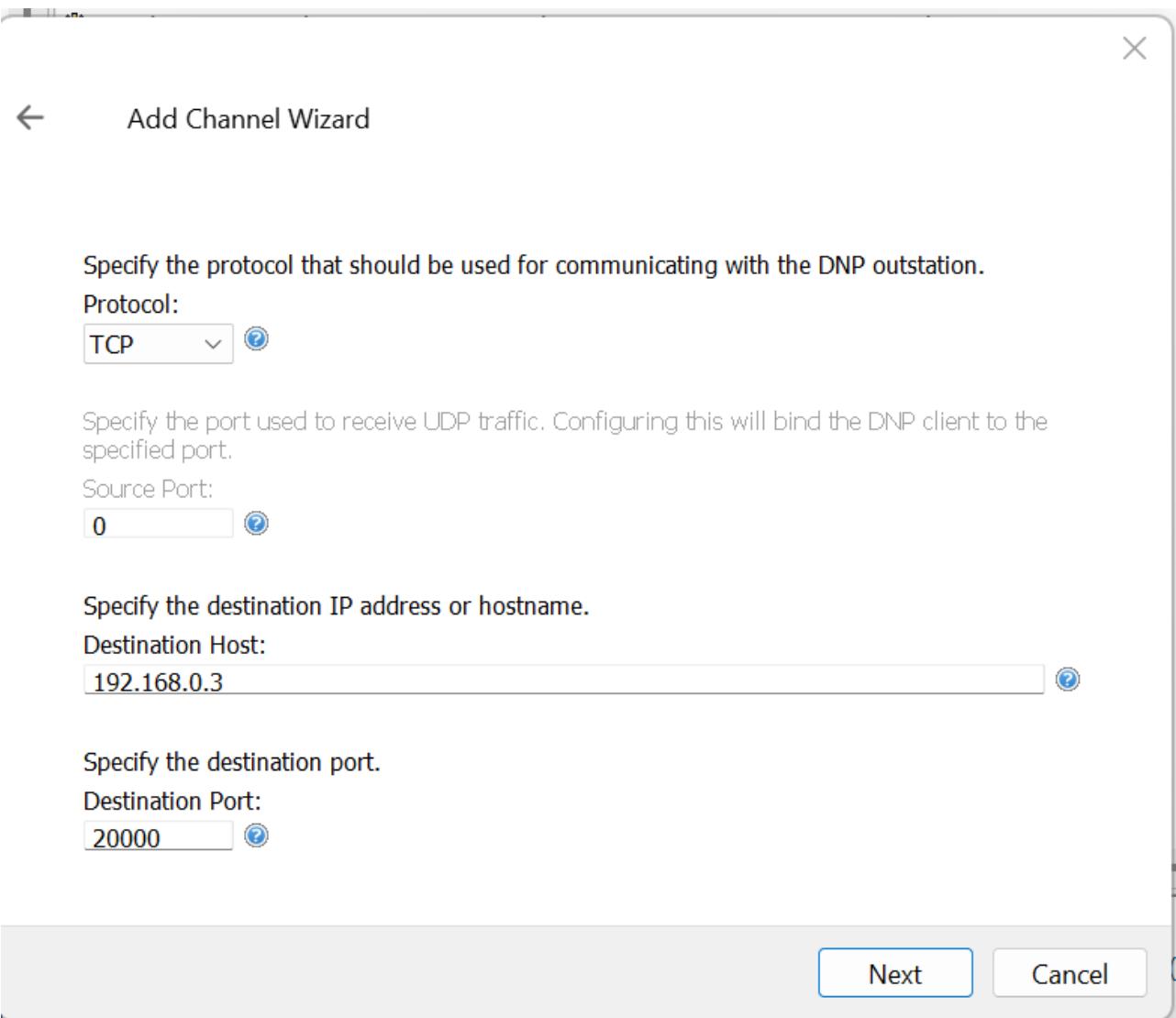


Project

- Connectivity
 - Channel1
 - Data Type Examples
 - Simulation Examples
- Aliases
- Advanced Tags
- Alarms & Events
 - Add Area...
- Data Logger
 - Add Log Group...
- EFM Exporter
 - Add Poll Group...
- IDF for Splunk
 - Add Splunk Connection...
- IoT Gateway
 - Add Agent...
- Local Historian
 - Add Datastore...
- Profile Library

Channel Name
Channel1
Data Type Examples
Simulation Examples

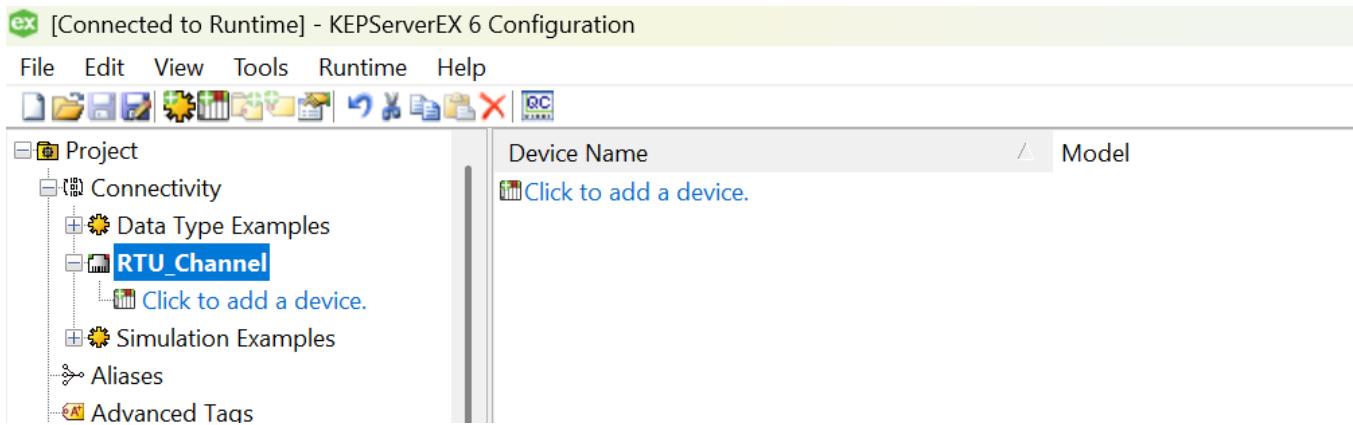
- Select channel type as ‘DNP Client Ethernet’ and give it a name such as ‘RTU_Channel’.
- Leave ‘Virtual Network’ set as ‘None’ and ‘Transactions per Cycle’ set to 1.
- Set the appropriate network adapter for the port on your computer the RTU is connected to.
- Leave ‘Optimization Method’ and ‘Duty Cycle’ as default.
- Set floating-point values to be sent ‘Unmodified’.
- Leave the communication protocol set as TCP.
- Ensure that the destination IP address and port match those set in the RTU (192.168.0.3 and 20000):



- Leave ‘Connection Timeout’, ‘Response Timeout’ and ‘Max Link Layer Retries’ as default.
- Click ‘Finish’.

Device Configuration

- The RTU_Channel you just created will now appear and have an option to add a device, click on this:



- Give it a name e.g. Siemens_RTU.
- Leave ‘Scan Mode’ and ‘Initial Updates from Cache’ as default.
- Leave ‘Demote on Failure’ as ‘Disable’.
- Leave all the next page settings as default.
- Make sure that the DNP Client (your computer) and Server (the RTU) match the settings we set in the RTU. In this case 3 and 7:

Specify the 16-bit address for the DNP client (this device).

DNP Client Address:



Specify the 16-bit address for the DNP server (remote device).

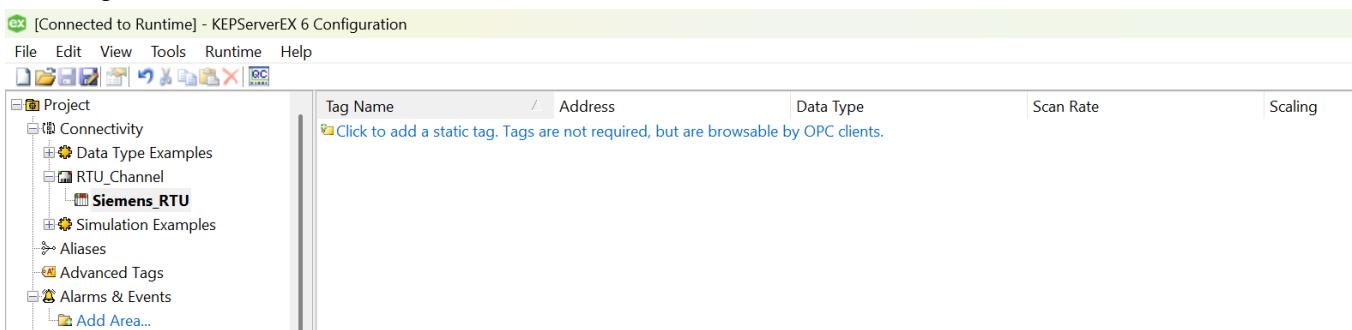
DNP Server Address:



- Set ‘Request Timeout’ to 5000ms. Leave all other settings on this page and the next as default.
- Enable unsolicited messaging for all data classes.
- Leave all other settings as default.
- Click ‘Finish’.

Tag Creation

- The RTU_Channel will now have a device associated with it, and this will have an option to add a tag. Click on this:



The screenshot shows the KEPServerEX 6 Configuration interface. The top menu bar includes File, Edit, View, Tools, Runtime, Help, and a toolbar with various icons. The left sidebar displays a project structure under 'Project' with nodes like Connectivity, Data Type Examples, RTU_Channel, Siemens_RTU, Simulation Examples, Aliases, Advanced Tags, and Alarms & Events. A button 'Add Area...' is also present. The main area features a table with columns: Tag Name, Address, Data Type, Scan Rate, and Scaling. A tooltip at the top of the table says: 'Click to add a static tag. Tags are not required, but are browsable by OPC clients.' There is one row in the table with the tag name 'Siemens_RTU'.

Tag Name	Address	Data Type	Scan Rate	Scaling
Siemens_RTU				

- Populate the settings for the tag like this:

Property Groups	Identification	
	Name	AI_Channel_0
General		Description
Scaling	Analogue Input 0	
Data Properties		
Address	30.0.0.Value	
Data Type	Double	
Client Access	Read Only	
Scan Rate (ms)	100	

- Address *30.0.0.Value* corresponds to analogue input 0, *30.0.1.Value* for input 1 etc.

Testing Procedure

1. Start KEPServerEX Runtime
2. Open OPC Quick Client
3. Browse to tags: KEPServerEX > RTU_Channel > Siemens_RTU > AI_Channel_0

Item ID	Data Type	Value	Timestamp	Quality	Update Cou...
[RTU_Channel.Siemens_RTU.AI_Channel_0]	Double	Unknown	09:40:14.003	Bad	1
[RTU_Channel.Siemens_RTU.TimeSyncStyle]	Byte	1	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU.SourcePort]	Word	0	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU.SlaveAddress]	DWord	7	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU.Protocol]	Byte	0	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU.MasterAddress]	DWord	3	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._IntegrityPollInterval]	DWord	3600	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._EventClass3PollInterval]	DWord	5	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._EventClass2PollInterval]	DWord	5	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._EventClass1PollInterval]	DWord	5	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._DNPServerAddress]	DWord	7	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU.DNPClientAddress]	DWord	3	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._DeviceRequestTimeout]	DWord	5000	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._DeviceRequestQueue...]	DWord	0	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._DestinationPort]	Word	20000	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._DestinationHost]	String	192.168.0.3	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._ChannelResponseTim...]	DWord	10000	09:40:06.974	Good	1
[RTU_Channel.Siemens_RTU._AuthCurrentUserNum...]	Word	1	09:40:06.974	Good	1

4. Testing with Fluke 789:

4mA

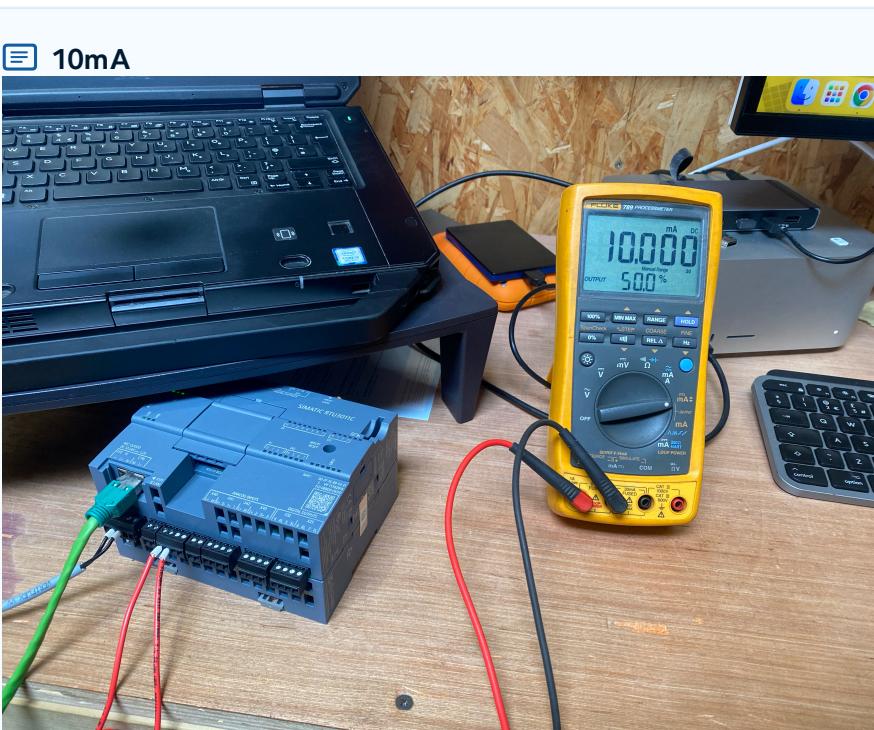


OPC Quick Client - Untitled *

File Edit View Tools Help

KEPware.KEPServerEX.V6

Item ID	Data Type	Value	Timestamp	Quality	Update Cou...
RTU_Channel.Siemens_RTU.AI_Channel_0	Double	0.0317723	10:26:40.000	Good	26
RTU_Channel.Siemens_RTU_TimeSyncStyle	Byte	1	09:40:06.974	Good	1
RTU_Channel.Siemens_RTU_SourcePort	Word	0	09:40:06.974	Good	1

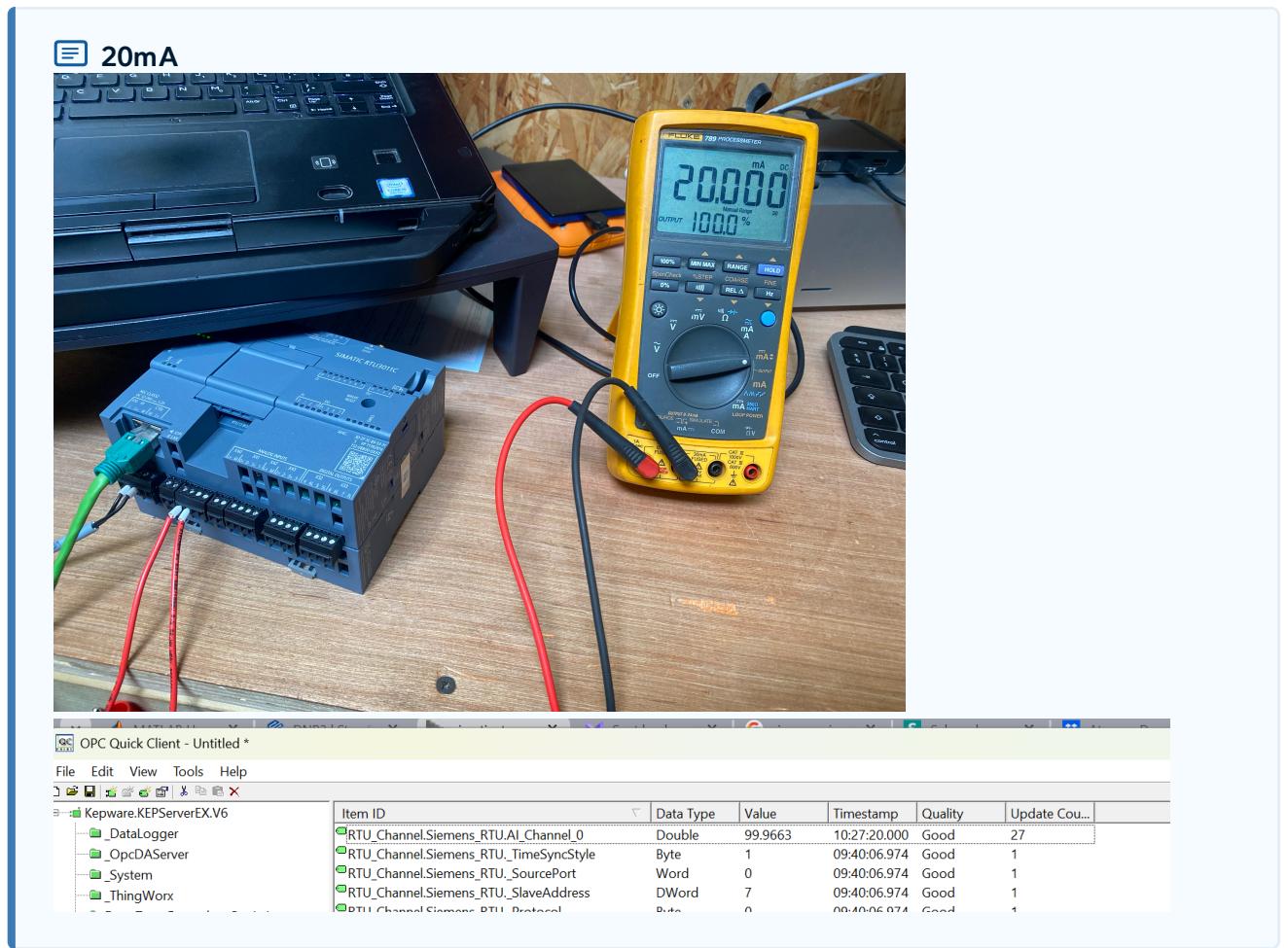


OPC Quick Client - Untitled *

File Edit View Tools Help

KEPware.KEPServerEX.V6

Item ID	Data Type	Value	Timestamp	Quality	Update Cou...
RTU_Channel.Siemens_RTU.AI_Channel_0	Double	37.5152	10:26:00.000	Good	25
RTU_Channel.Siemens_RTU_TimeSyncStyle	Byte	1	09:40:06.974	Good	1
RTU_Channel.Siemens_RTU_SourcePort	Word	0	09:40:06.974	Good	1
RTU_Channel.Siemens_RTU_SlaveAddress	DWord	7	09:40:06.974	Good	1
RTU_Channel.Siemens_RTU_Protocol	Byte	0	09:40:06.974	Good	1



Transition to C++ Implementation

I have created a C++ client for reading analog inputs from Siemens RTU via DNP3 protocol here:

<https://github.com/ghaworth/dnp3-rtu-reader>

Step Function I/O DNP3 Library

- **Download:** <https://github.com/stepfunc/dnp3>
- **Language:** Use C++ bindings for integration
- **Installation:** Follow library documentation for C++ setup

C++ DNP3 Master Configuration

Use the same proven settings from KEPServerEX:

```
// Connection parameters (same as KEPServerEX)
std::string rtu_ip = "192.168.0.3";
uint16_t port = 20000;
uint16_t station_address = 7;
```

```
// Analogue input addressing (same as KEPServerEX tags)
// Group 30 = Analogue Inputs
// Index 0, 1, 2 = Your configured channels
```

Data Integration

Replace existing TCP/serial parsing in data logger with DNP3 calls:

- **Connect** to RTU using proven parameters
 - **Request** Group 30 analogue inputs (Class 2)
 - **Handle** both polled data and unsolicited events
 - **Convert** DNP3 analogue values to proprietary format
-

Performance Characteristics

Communication Modes

- **Polling:** 1-10 Hz typical for DNP3 (avoid 60Hz polling)
- **Unsolicited Events:** 10-50ms response time to changes
- **Hybrid Approach:** Combine slow polling (integrity) with fast events (responsiveness)

Event Configuration

- **Small deadbands** for sensitive change detection
 - **Class 2** for normal operational data
 - **Change trigger** for immediate event reporting
-

Troubleshooting

Common Issues

1. **No Connection:** Check IP addresses, port numbers, firewall settings
2. **No Data:** Verify DNP3 is enabled, check station addresses match
3. **Incorrect Values:** Check analogue input scaling and engineering units
4. **Slow Updates:** Verify unsolicited messaging is enabled, check deadband settings

Verification Steps

1. **Network:** Ping RTU IP address
2. **DNP3:** Use KEPServerEX diagnostics or DNP3 protocol analyser

- 3. Values:** Cross-check with Fluke 789 output current
 - 4. Events:** Monitor for unsolicited DNP3 events when changing input
-

Summary

The KEPServerEX testing phase validates all configuration before moving to custom code, ensuring a smooth transition to the final implementation.