ProScada Siemens IO Driver

Table of Contents

1 Installation

1.1 Install the Driver

Install the Siemens Ethernet Driver by running the setup.exe provided.

The default install location is the **Program Files\ProScada\SiemensIE** Directory. The directory choice is not crucial. For iFix installations install in the iFix root directory

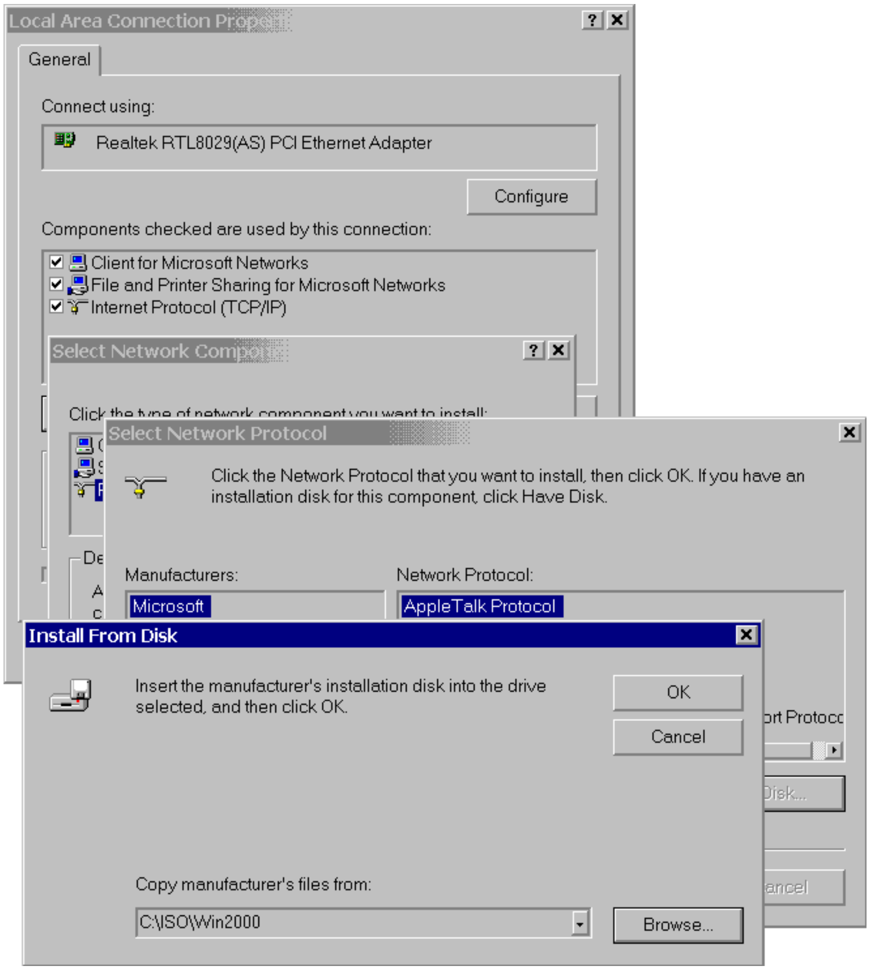
1.2 Install "Siemens H1 ISO transport" (***Not used for TCP/IP)

*This step is **optional**, depending on the protocols used to talk to the PLC's, if you are using TCP/IP you DO NOT Require the ISO transport – Please go to Setting up the driver.

Now you need to install the low level "Siemens H1 ISO transport"

This installation is only required for the Siemens Ethernet Driver.

1. Open the "Settings | Control Panel"
2. Open the "Local Area Network Properties" Settings
3. Go to the "Protocols" tab
4. Press "Add"
5. Press "Have Disk"
6. Enter or browse to the following path "<Install disk>\ISO\WIN2000 & XP\"



Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Click the type of network component you want to install:

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Manufacturers: Microsoft

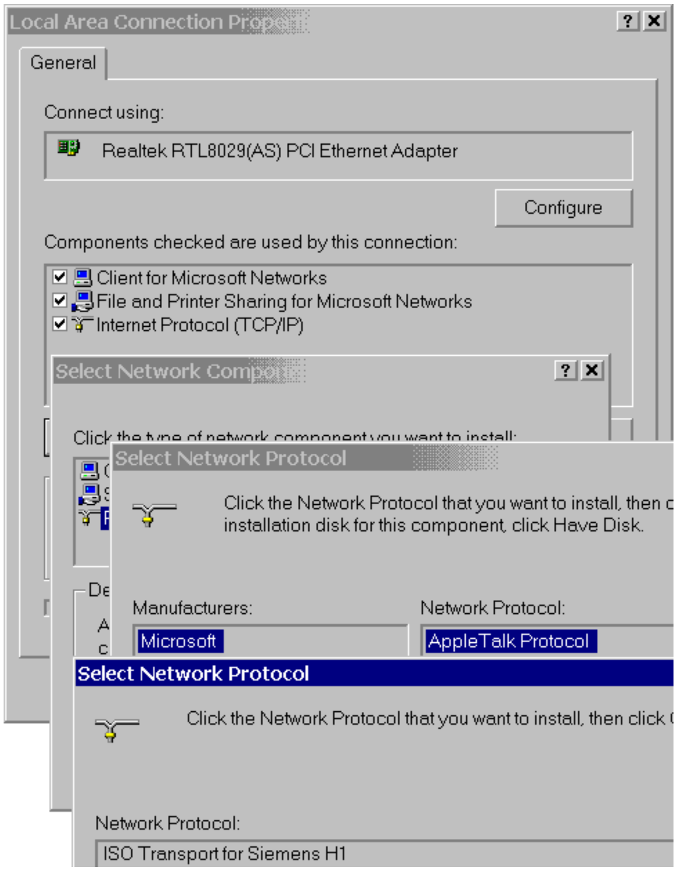
Network Protocol: AppleTalk Protocol

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from: C:\ISO\Win2000

7. Press "OK"

8. You will see a prompt “ISO transport for Siemens H1”



Local Area Connection Prope

General

Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Select Network Compo

Click the type of network component you want to install:

Select Network Protocol

Click the Network Protocol that you want to install, then c
installation disk for this component, click Have Disk.

Manufacturers: Microsoft

Network Protocol: AppleTalk Protocol

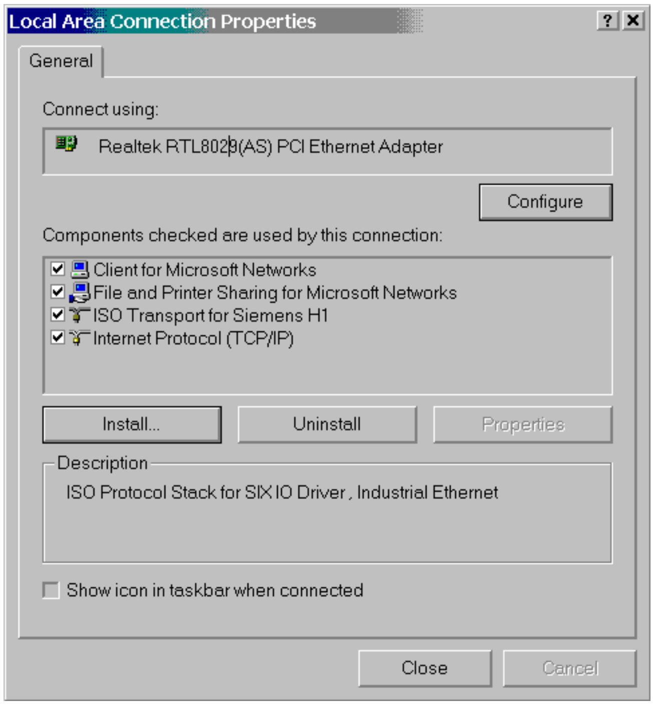
Select Network Protocol

Click the Network Protocol that you want to install, then click

Network Protocol:

ISO Transport for Siemens H1

9. Press “OK”



Local Area Connection Properties

General

Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ ISO Transport for Siemens H1
☑ Internet Protocol (TCP/IP)

Description

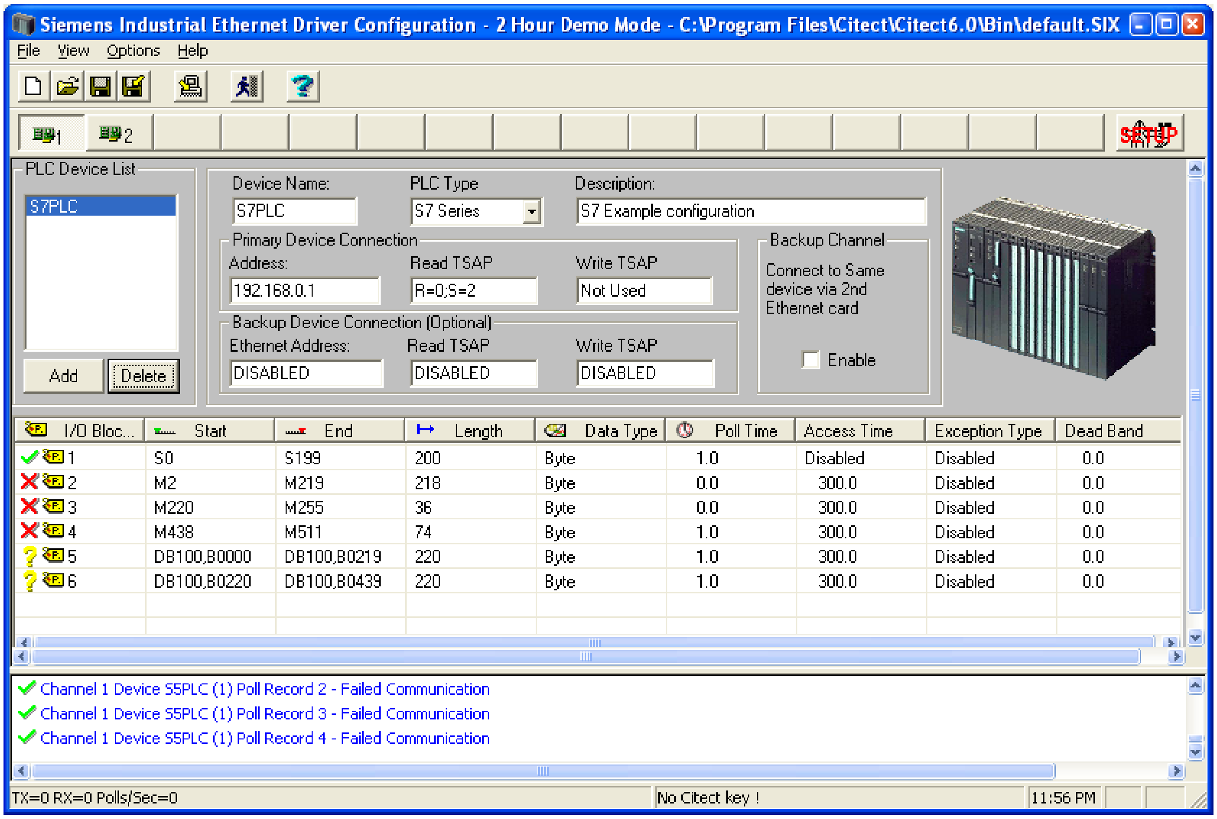
ISO Protocol Stack for SIX IO Driver , Industrial Ethernet

□ Show icon in taskbar when connected

10. Close and restart the computer

2 Setting Up the driver

Run the “Siemens Industrial Ethernet Driver Configurator”



Siemens Industrial Ethernet Driver Configuration - 2 Hour Demo Mode - C:\Program Files\Citect\Citect6.0\Bin\default.SIX

PLC Device List: S7PLC

Device Name: S7PLC

PLC Type: S7 Series

Description: S7 Example configuration

Primary Device Connection

Address: 192.168.0.1

Read TSAP: R=0;S=2

Write TSAP: Not Used

Backup Device Connection (Optional)

Ethernet Address: DISABLED

Read TSAP: DISABLED

Write TSAP: DISABLED

Backup Channel

Connect to Same device via 2nd Ethernet card

□ Enable

I/O Bloc...	Start	End	Length	Data Type	Poll Time	Access Time	Exception Type	Dead Band
✓ 1	S0	S199	200	Byte	1.0	Disabled	Disabled	0.0
✗ 2	M2	M219	218	Byte	0.0	300.0	Disabled	0.0
✗ 3	M220	M255	36	Byte	0.0	300.0	Disabled	0.0
✗ 4	M438	M511	74	Byte	1.0	300.0	Disabled	0.0
? 5	DB100,B0000	DB100,B0219	220	Byte	1.0	300.0	Disabled	0.0
? 6	DB100,B0220	DB100,B0439	220	Byte	1.0	300.0	Disabled	0.0

```
✓ Channel 1 Device S5PLC (1) Poll Record 2 - Failed Communication
✓ Channel 1 Device S5PLC (1) Poll Record 3 - Failed Communication
✓ Channel 1 Device S5PLC (1) Poll Record 4 - Failed Communication
```

TX=0 RX=0 Polls/Sec=0 | No Citect key ! | 11:56 PM

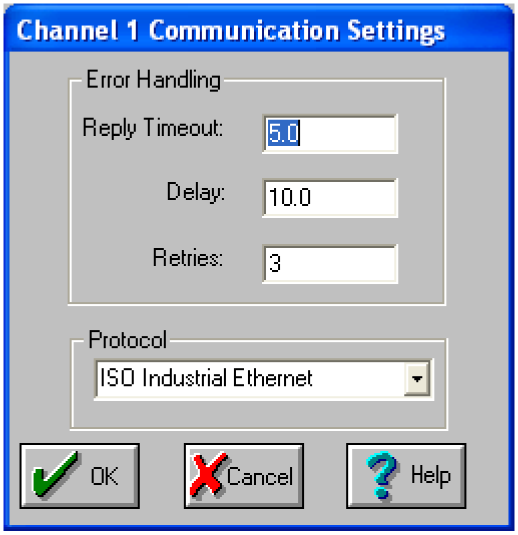
The Default configuration file will open, this includes 3 PLC’s an S5, S7 & TI.

Since you will probably be using an S7 select the S5 PLC & press delete, do the same for the TI PLC

The S7 example configuration is setup to poll M0-M99; this address exists in all S7 PLC’s so it should poll correctly without setting up a Step 7 program on the PLC.

Before setting addresses etc. please set the protocol type in the channel settings

- Open the channel settings to set the protocol – press the Setup button



Channel 1 Communication Settings

Error Handling

Reply Timeout: 5.0

Delay: 10.0

Retries: 3

Protocol: ISO Industrial Ethernet

You have a choice between TCP/IP and ISO. If ISO is chosen then the ISO transport must be installed (supplied with the driver).

- Set the PLC's address, for ISO this is a 12 digit Hexadecimal MAC address, for TCP/IP this is of the form 0.0.0.0
- Now press ok to go back to the main device settings

The read TSAP setting defaults to "R=0;S=2" which means read the CPU in Rack 0 Slot 2. This is Correct for an S7-300. On a S7-400 with 2 slot power supply, meaning the CPU is in Slot 3, this should be R=0;S=3. **Note the Slot is the slot number of the CPU, NOT the CP 443 card!

***For the S7-200 PLC Set the read TSAP to "CP243" because the S7-200 does not comply with the rack & slot system.

Now "Reload" the configuration by pressing the 🖫 button. This is IMPORTANT; always reload any configuration change changes. The configurator works on the configuration file on disk, the reload command loads that into memory, briefly interrupting the polling as it does so

Now check that you have communications. The transmit and receive counters at the bottom of the window should increment

The Status of the M0 block should change to a ✓

3 Quick Start

3.1 Configuration in a nutshell

3.1.1 Channel settings

- The driver will install with a default configuration file that must be changed to suit your configuration.
- The default channel settings should be acceptable in most situations read more

3.1.2 Device Settings

- Change the "Device name" to something descriptive for your PLC *note for the rest of this text, our example will be "PLC1".
- Set the Ethernet Address of the PLC
- In the Read TSAP set the S7 Rack Number & Slot number **Note the slot number is the slot number of the CPU, example : an S7 400 has a 2 slot power supply so the CPU is in Slot 3. Example "R=0;S=2" means the CPU is in Rack Zero Slot 2
- The S7-200 requires that the READ TSAP be set to "CP243"
- The driver has provision for several redundancy modes, you can leave the backup addresses disabled by typing "DIS"

3.1.3 Poll Block List Settings

- Add poll blocks to the configuration, mostly you will poll Datablocks and Merker Words. In this example since all PLC's have Merker memory, we configure m0-m100.
- NOTE at the pollblock configuration the only data type available is "byte" you select variable data types later in the database or OPC level.
- Maximum length of poll block is 220 bytes
- Example 400 byte Datablock 15 will require 2 poll blocks (make sure that no variable crosses the B219 boundary)

DB15,B0 -> DB15,B219	len=220
DB15,B220 -> DB15,B399	len=180

Important !! After Saving the configuration, Reload it into memory with the File|Reload Menu or the reload Toolbar Button

3.2 Connecting to The Fix SCADA Database (S7 example)

- Set the IO device to “SIX”
- Set the IO address field as below

3.2.1 IO address field

For Analog addresses in Data blocks, use the following format:

```
<device>:DB<block num>,<format><byte addr>
```

For Digital addresses in Data blocks, use the following format:

```
<device>:DB<block num>,X<byte addr>.<bit>
```

For Analog addresses in other memory areas, use the following format:

```
<device>:<memory area><format><byte addr>
```

For Digital addresses in other memory areas, use the following format:

```
<device>:<memory area><byte addr>.<bit>
```

Block I/O Address fields accepts a maximum of 128 characters. For examples of valid I/O addresses, refer to Supported Mnemonics table below. The following are descriptions of the parts of the I/O Address:

Device — indicates the name you assigned in the Device Name field of the Device Definition in the I/O Driver Configuration program. It is an alphanumeric tag that the Database Builder uses to differentiate poll records collected from different field devices.

memory area — specifies the block type in the PLC e.g. DB,M,I,Q

byte addr — specifies the address of the I/O point within the section. It has the same style as the Start Address and Length fields on the Poll Record Edit dialog box of the I/O Driver Configuration program, that is AREA:ADDRESS.

Format --- specifies the data length of the variable eg
X or none for digital
B for byte (8 bit integer)
W for word (16 bit integer)
S for swapped word (16 bit integer, bytes swapped)
D for Double word (32 bit integer or float)

bit — specifies a particular digital point in a data word. The bit entry is used for Digital blocks and ranges from 0 - 15.

3.3 Connecting Via OPC

3.3.1 *Installing the OPC Server*

- Install the Siemens IE OPC Server
- Install your desired OPC client on this or another computer
- If no other OPC software is installed on the machine then you may need to install the OPC foundation common components from here Download

3.3.2 *From Your OPC Client Software*

- First Configure the required data in the configurator & reload it into memory
- Browse to the OPC Server “ProScada.SiemensIE” (Also known as the Server Classname or CLSID)
- Browse down to a PLC Device
- The Browser (client dependant) then lists all the poll blocks configured on that device
- Add a OPC Group (some clients hide this from the user)
- then add an Item browsed above

3.3.3 *OPC Item ID Format (IO Address format)*

<IO Address>[[|$]<Signal Conditioning>[,<Lo Egu>,<Hi Egu>,<HW opt>,<units>]]

where :
IO Address

For Analog addresses in Data blocks, use the following format:

```
<device>:DB<block num>,<format><byte addr>
```

For Digital addresses in Data blocks, use the following format:

```
<device>:DB<block num>,X<byte addr>.<bit>
```

For Analog addresses in other memory areas, use the following format:

```
<device>:<memory area><format><byte addr>
```

For Digital addresses in other memory areas, use the following format:

```
<device>:<memory area><byte addr>.<bit>
```

For String addresses in Data blocks, use the following format:

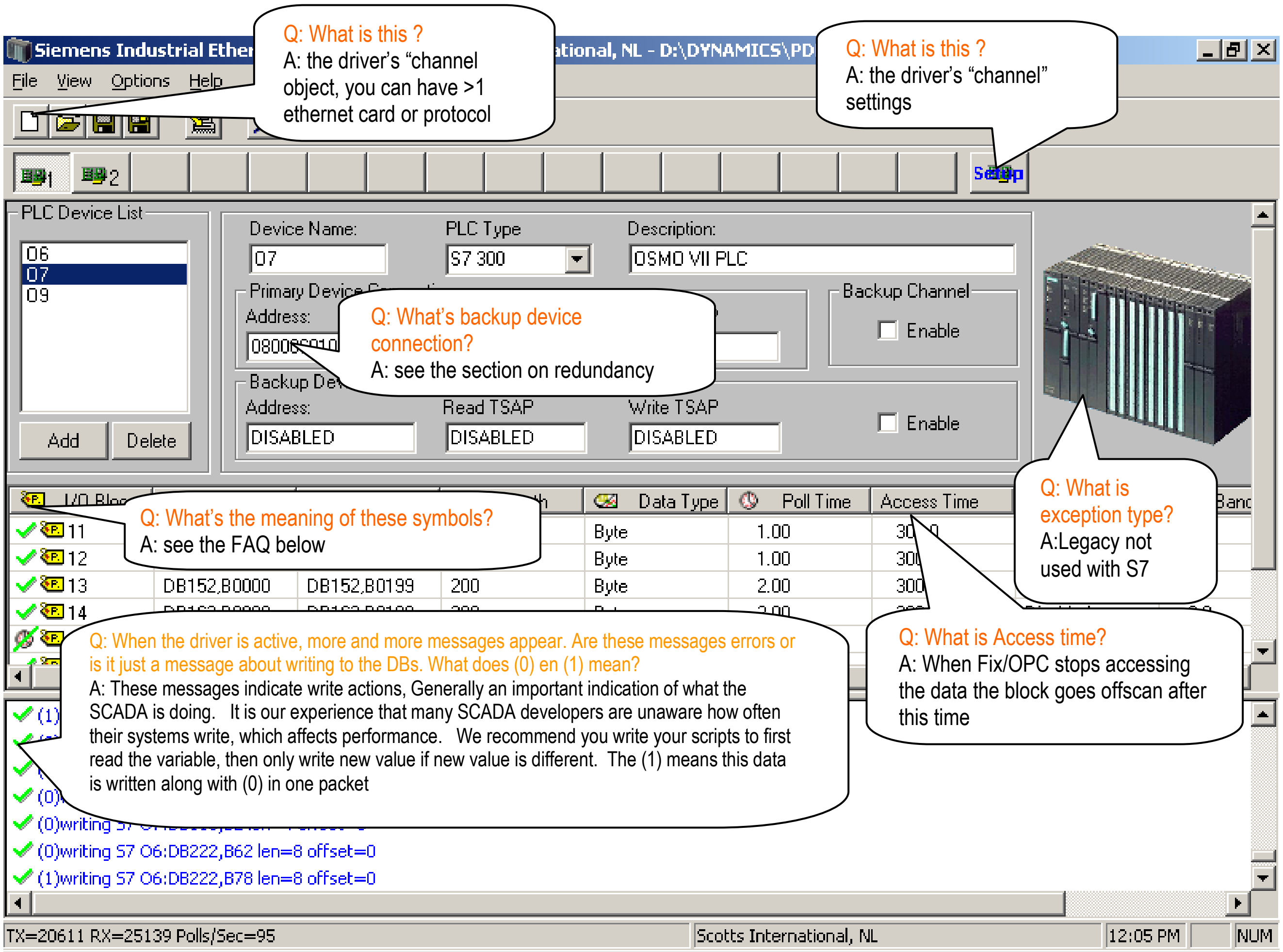
```
<device>:DB<block num>,B<byte addr>$<max string len>
```

Signal Conditioning is discussed here: Signal Conditioning
Lo & Hi Egu - Low & High Engineering units range
HW opt - Hardware Options is discussed here Hardware Options
Units - are optional, not used at present

Examples

Digital inputs	“PLC1:I2.0”
Digital outputs	“PLC1:Q2.0”
Digital setpoints	“PLC1:M2.0”
S7 Real numbers	“PLC1:MD80|FLT” “PLC1:DB15,D80|FLT”
S7 Analog inputs	“PLC1:IW2|S7A1,0,100.0,,%”
S5 Timer Setpoint	“PLC1:MW2|TIMR” (value is read / write in seconds)
Array of characters	“PLC1:M2$20” “PLC1:DB15,B80$20”
S7 String structure	“PLC1:M2$,,,S7STRING”
Analog Input with user instrument range eg. 12 bit value with 4ma offset	“PLC1:MW2|PROP,0,100.0,819:4095,%”

Frequently asked questions & troubleshooting



Q: What is this ?
A: the driver's "channel object, you can have >1 ethernet card or protocol

Q: What is this ?
A: the driver's "channel" settings

PLC Device List: 06, 07, 09

Device Name: 07

PLC Type: S7 300

Description: OSMO VII PLC

Primary Device … Address: 08006C010…

Backup Channel: □ Enable

Backup Dev… Address: DISABLED Read TSAP: DISABLED Write TSAP: DISABLED □ Enable

Q: What's backup device connection?
A: see the section on redundancy

Q: What's the meaning of these symbols?
A: see the FAQ below

```
✓ 11                                  Byte   1.00   30…
✓ 12                                  Byte   1.00   300
✓ 13  DB152,B0000  DB152,B0199  200   Byte   2.00   300
✓ 14  DB162,B0000  DB162,B0199  200   Byte   2.00   300
```

Q: What is exception type?
A:Legacy not used with S7

Q: When the driver is active, more and more messages appear. Are these messages errors or is it just a message about writing to the DBs. What does (0) en (1) mean?
A: These messages indicate write actions, Generally an important indication of what the SCADA is doing. It is our experience that many SCADA developers are unaware how often their systems write, which affects performance. We recommend you write your scripts to first read the variable, then only write new value if new value is different. The (1) means this data is written along with (0) in one packet

Q: What is Access time?
A: When Fix/OPC stops accessing the data the block goes offscan after this time

```
✓ (1)…
✓ (0)…
✓ (0)writing S7 …
✓ (0)writing S7 06:DB222,B62 len=8 offset=0
✓ (1)writing S7 06:DB222,B78 len=8 offset=0
```

TX=20611 RX=25139 Polls/Sec=95 | Scotts International, NL | 12:05 PM | NUM

Q: The latest version 7.9.52 has PLC options for S7-300 & S7-400, what has changed since I note that my old configurations still work & have defaulted to S7-300

A: The protocol is indentical, the S7-400 can handle larger block sizes than the S7-300 and is therefore faster – so it is a performance optimisation.

Q: What do the Icons in the configurator mean ?

A:

✓ The block is healthy & contains current data

✗ Communications failure

⊘ The block is currently not in use, it is off poll, all the blocks on a standby server should be in this state

? This block is newly configured & is not currently being polled. You need to reload the configuration

Q: The driver configurator us using all my PC's CPU time and the whole machine is slow, what is wrong ?

A: You have many error messages flooding the bottom window of the configurator, this is caused by all the scrolling. This happens if the database or OPC client contains references to not in the poll configuration

- Pull the horizontal splitter down to close the bottom window, this reduces CPU time
- Use “Menu>Options>Learn addresses” to solve the NIO-*Address… errors, then driver reload

Q: Why do I see messages like “Nio-*Address Error DB15,W248” in the bottom window of the configurator ?

A: This means that Fix or the OPC client is reading that address however this address is not configured for polling in the backend.

- **It is Crucial to resolve this issue**, before doing any other testing
- You only see these errors when the client tries to access the data, so seldom used addresses may not be noticed.
- There is a Semi automatic method of solving this
  - By selecting Menu>Options>Learn addreses, the configurator uses those error messages to stretch existing blocks or add new ones.
  - Reload the iFix Database, it will cause the errors, the configurator will use these to stretch & add blocks
  - Reload the Driver config & Reload the iFix database again

***Note this only changes the edited file in disk you need to “reload” 🖫 to make it active in the Background polling program. Then you should see fewer address errors, you then need to Learn addresses again. Read more

Q: I am unable to get communication, what are the most common problems?

A: If using ISO protocol Check that the siemens ISO transport is installed, if you see the message in the bottom window “failed to open ISO channel 1” then the ISO transport is not correctly installed OR there may be a problem in the registry and the driver is not using the correct Ethernet card.

The read TSAP setting defaults to “R=0;S=2” which means read the CPU in Rack 0 Slot 2. This is Correct for an S7-300. On a S7-400 with 2 slot power supply, meaning the CPU is in Slot 3, this should be R=0;S=3. **Note the Slot is the slot number of the CPU, NOT the CP 443 card!

If you have 2 SCADA’s communicating to a S7-300 the third SCADA connection will fail. By default the S7-300 has 8 communication channels – 2 for step 7, 2 for SCADA, 4 for PLC-PLC, This configuration can be changed in later model CPU’s

Q: How do I update the configuration after making changes ? Or Why do newly added blocks show a ? status

A: Remember the configurator is not actually polling the PLC’s The background polling program sixspoll.exe is doing that. Save the file then Select “File|Reload” off the menu, or press 🖫. This saves the configuration and tells the background polling program to stop & reload it's configuration into memory. During this process you may see ????? in FIX or OPC quality bad.

Q: I have problems reading Direct S7 IO (I,Q,PI etc.) what do I do ?

A: You need to make sure that the poll blocks exactly match the configuration in the PLC. The PLC WILL NOT allow you to poll across an address for which no IO cards exist. You need to break this up into smaller blocks. **Note we Do not recommend writing directly to outputs for safety reasons.

Q: My communications are Slow, WHY ?

A: Please Note the following, typical performance achievable

- This driver polls as fast as the PLC allows, the PLC is the bottleneck(slow side), the figures below are per PLC, the driver performance scales linearly per PLC.
- S7-315 CPU typically achieves 15-20 polls per second (We believe it is crippled)
- S7-416 CPU typically achieves upto 150 polls per second (10 x faster). This is with 2 IO Devices talking to the same PLC.
- A Vipa PLC typically achieves upto 40 polls per second with default settings, if communications resources are increased this can reach 100+
- The driver has a Built in Limit of 100 polls per second per IO Device, so in some cases you can get better performance by splitting your data into 2 IO Devices. However we do not recommend this as, the spare PLC resources should be reserved for Writing data & PLC-PLC communications & other SCADA servers.
- From version 7.9.52 performance has been increased substantially over the above the difference is more noticeable for configurations of lots of small blocks

Q: The communications are Slow, how do I make it faster ?

A: read the section about optimisation of the driver & try some of the following modifications at the PLC side.

- Try to increase the PLC scan cycle by moving code to the Idle processing OB's OR process half the code each scan & thereby doubling the scan cycle.
- Try Increasing the PLC process time dedicated to communications this is in the CPU Properties seen below

Q: How do I configure communications to an S5 PLC ?

A: This is far more complicated than an S7 PLC. Please read the Driver help file (SIXHLP.DOC) section "Setting up the hardware" for Full instructions. In addition there are example S5 PLC programs & CP card setup files in the backend distribution in the "PLC" directory.

Q Does the driver support the S7-400H hotstandby PLC ?

A: Yes simply configure the second IP addresses & rack & slot in the Backup fields, read more in Configuring for Redundancy

Q: How do I debug the operation of the low level backend redundancy

A: read the section on Using the Special Debug addresses

4 Communication Optimisation

4.1 *note on performance in new version 7.9.52

This version can reads multiple block simultaneously, and when upgrading you should notice an improvement in the backend driver poll rate. This new version requires no additional changes, it will open existing configuration files. To take full advantage of this the only change to the configuration required is to set the PLC type to "S7-400" in the PLC type. The greatest performance improvement will be seen with configurations with large numbers of small poll blocks.

4.2 How to Measure Driver Performance

- Create a minimal backend configuration with 1 poll block, 1 variable and a poll time of 0.0 seconds
- Note how many polls per sec you get in the configurator status at the bottom
- After measuring the speed, you can calculate the update time of your full configuration. e.g. If you get 10 pps (Pollblocks per second), you can have
  - 1 pollblock updating 10 times a second or
  - 10 pollblocks updating at 1.0 seconds
  - 5 pollblocks updating at 1.0 seconds + 10 pollblocks updating at 2 seconds

If you configure more pollblocks, no errors will occur but you are not actually achieving your configuration update time. In this case the driver just processes each block in turn. This is not a problem most of the time but as you add more blocks your system will slow down & if you need faster update on a specific block, changing its polltime will achieve little.

4.3 Optimisation Techniques

To make a limited bandwidth system appear faster, you have to **slow down** the updating of less critical data to give more bandwidth to the critical data. (Increasing the pollrate of a block when the system is already at full stretch will have no effect) The basic principle is - poll only the data that the operator needs for a given picture & at the minimum rate he is prepared to accept. It is usually better to set slow polltimes at the start of a project which leaves plenty of room to expand, this sets a lower expectation and if you need more speed later you have spare bandwidth resources.

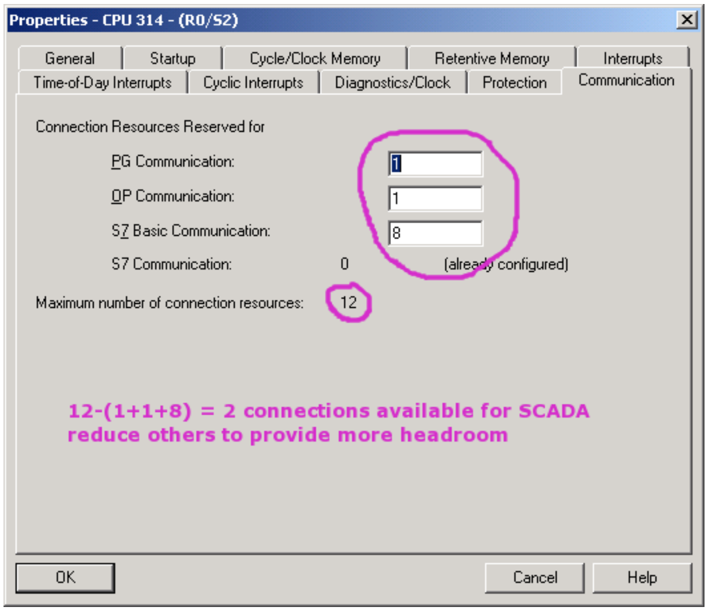
- Setpoints, Outputs, controls or any value that never changes in the PLC (only changes when modified from the SCADA) can be setup so that they hardly use any channel bandwidth at all. Set the polltime to a large value like 60 seconds. If a value is written the driver automatically forces the block to update so the user does not notice the slow poll times.
- Configure iFix to stop reading data not in use, to do this change all AI/DI blocks that are NOT alarmed to AR/DR blocks.
- Prioritize your data; find out how fast the data changes in the PLC. Do not poll faster than necessary especially while you are constructing your system. You can always speed up certain blocks later once your system is fully configured. Generally analog values can be polled slower e.g. 5 sec but Digital Inputs may need 1 sec.

4.4 PLC Optimisation

Try to increase the PLC scan cycle by moving code to the Idle processing OB's OR process half the code each scan & thereby doubling the scan cycle.

4.4.1 Number of Network connection resources(CPU properties)

Resources available for the driver on the S7-300 is Two(2) by default, which can be changed this means 2 IO servers can connect but the third will fail, unless you change this configuration in Step 7. The S7-400 allows 4-8 connections by default.



Properties - CPU 314 - (R0/S2)

Connection Resources Reserved for

PG Communication: 1

OP Communication: 1

S7 Basic Communication: 8

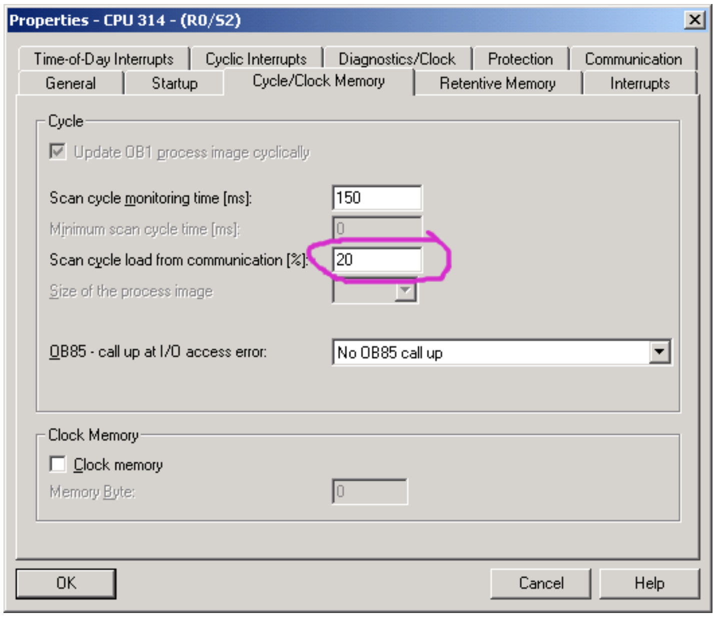
S7 Communication: 0 (already configured)

Maximum number of connection resources: 12

12-(1+1+8) = 2 connections available for SCADA
reduce others to provide more headroom

4.4.2 CPU communication load priority (CPU properties)

You can try increasing communication priority



Properties - CPU 314 - (R0/S2)

Cycle

☑ Update OB1 process image cyclically

Scan cycle monitoring time [ms]: 150

Minimum scan cycle time [ms]: 0

Scan cycle load from communication [%]: 20

Size of the process image:

OB85 - call up at I/O access error: No OB85 call up

Clock Memory

□ Clock memory

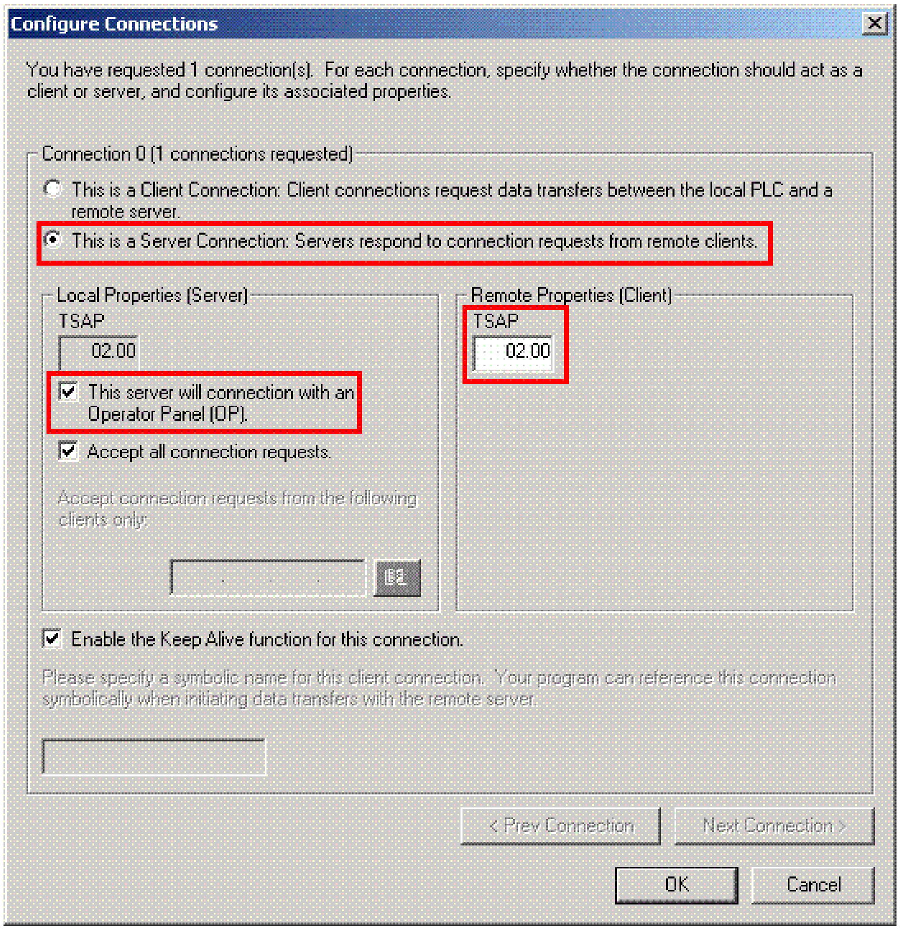
Memory Byte: 0

4.4.3 Block size (CP card properties)

Some CP cards (not all) have an option in the options tab for large PDU block size – set this.

5 S7 200 Setup

1/ Run the Micro Win Ethernet Wizard
2/ We recommend that the CP243 be installed in position 0
3/ Set the CP243's Ethernet address
4/ Configure a New connection & set it as follows



Configure Connections

You have requested 1 connection(s). For each connection, specify whether the connection should act as a client or server, and configure its associated properties.

Connection 0 (1 connections requested)

○ This is a Client Connection: Client connections request data transfers between the local PLC and a remote server.

● This is a Server Connection: Servers respond to connection requests from remote clients.

Local Properties (Server)

TSAP 02.00

☑ This server will connection with an Operator Panel (OP).

☑ Accept all connection requests.

Accept connection requests from the following clients only:

Remote Properties (Client)

TSAP 02.00

☑ Enable the Keep Alive function for this connection.

Please specify a symbolic name for this client connection. Your program can reference this connection symbolically when initiating data transfers with the remote server.

In the backend configuration set the Read TSAP field to "CP243"

You can poll the following

M0-M32 (S7-200 has very small M area)
DB1,0->x is equivalent to the "V" mem area e.g. VW8 == analog address DB1,8
I0 len 2
Q1 len 1

6 Configuring for Redundancy

6.1 Standard Fix redundancy

- Normally this is simply twin SCADA servers with the same database & driver config

6.2 Using driver redundancy with S7-400H systems OR >1 CP card in the PLC

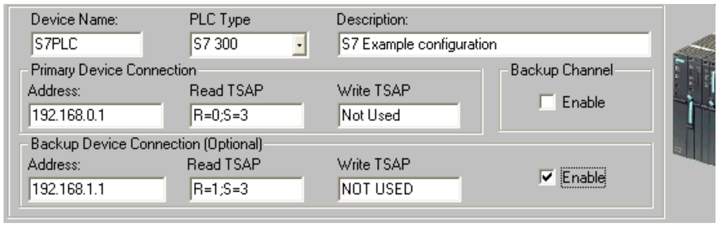
The driver level has a backup address per IO Device, typically on a S7-400H system you setup as follows:

Primary address:

IP 192.168.0.1 Read TSAP = "R=0;S=3"

Backup address:

IP 192.168.1.1 Read TSAP = "R=1;S=3" (check enable backup address)



Device Name: S7PLC

PLC Type: S7 300

Description: S7 Example configuration

Primary Device Connection

Address: 192.168.0.1

Read TSAP: R=0;S=3

Write TSAP: Not Used

Backup Channel

□ Enable

Backup Device Connection (Optional)

Address: 192.168.1.1

Read TSAP: R=1;S=3

Write TSAP: NOT USED

☑ Enable

*Note** the Rack number of the backup CPU is "1", note I specifically gave the IP addresses different subnets (Ethernet cards in the IO server) you probably have twin Ethernet networks.*

6.2.1 Notes

- A potential issue is that the device takes 2x longer to show communication. The timers that affect this are the settings in the channel setup (backend) We recommend settings (do not set any lower)
    - timeout time = 3 sec
    - Delay = 30 sec
    - Retries = 1
- You can monitor which connection the driver is using via the debug addresses
- Unfortunately you cannot at present force the backend to switch over manually
- Read more about monitoring the status in Using the Special Debug addresses

7 Using the Special Debug addresses

This driver is a cached Front End / Back End driver, so the standard CitectSCADA driver statistics are not very useful. This section describes the Special Tag addresses available for debugging purposes. All datatypes are INT

<PLC NAME>:SW0	Connection	current connection number an Internal value, this is normally static, is only meaning full when backup addresses are used. Connection number of connection inuse, stays the same if backup feature not used.
<PLC NAME>:SW2	State	means trying to connect to PLC, =2 means Connected. Use this address to alarm communication failure
<PLC NAME>:SW24	Reconnections	Increments every time the driver attempts to reconnect after the connection failure. If this is going up, you have a bad network
<PLC NAME>:SW26	Poll blocks per sec	Poll rate for this PLC - useful for checking optimisation. The rate shown at the bottom block of the configurator should be the sum of these per channel.
<PLC NAME>:SW28	Disconnect Req's	Increments when PLC sends Disconnect Request. This Means that your Network is OK but the PLC is refusing connection requests.
<PLC name>:SW32	PDU size	PLC request block size, 240 or 480 bytes
<PLC name>:SW40	Primary connection	Connection number
<PLC name>:SW42	Primary connection state	=2 means connected
<PLC name>:SW80	Backup connection	Connection number of backup connection

When using the Backup IP address, the following logic may be used to indicate which connection is active.

<PLC name>:SW0= =<PLC name>:SW40 means that the Primary IP address is being polled

<PLC name>:SW0= =<PLC name>:SW80 means that the Backup IP address is being polled

8 Using the S7 Simulator application

8.1 What is it ?

The small console application “S7simulator.exe” may be downloaded from a link on

http://www.proscada.com/Siemens_Ethernet.htm

8.2 Introduction - why a PLC simulator ?

We originally wrote this as a simple application to regression test the driver particularly to test hard to find PLC’s like old S5 models. We soon realised that others would also find it useful for quick test & setup without having to have to setup a *real* PLC. As such it lowers the barriers to using the PSDIRECT Driver. We would not want to pretend that it is a “Full” emulation in particular it has not been tested against Siemens software like the OPC server or WinCC. It certainly does not emulate the protocol fully but is sufficient for the ProScada Siemens Driver. It is a low priority project for us, with minimal support.

8.3 Capabilities

- Emmulates Both S5 & S7 PLC’s (TI sort of…)
- Only Supports TCP/IP
- Automatically emulates any datablock you poll with the DB’s initialised to []0, any data written is stored, like a PLC with no program running. Emulates 4kb DB’s upto DB 1999. M,I,Q memory areas are emulated as DB0
- Supports 2 incoming connections so you can setup a redundant pair of SCADA IO Servers.
- Only Supports Rack 0 Slot 2 (deliberate for training purposes)
- DB 1 & DB15 contain some forced values

8.4 Installation

run from the command line or explorer there are no parameters.

The program simply listens for Incoming connections. Being a TCP/IP server you need to unblock any firewall systems. *Note it is receiving connections on TCP port 102.

When run on the same PC as the IO Server you can use the IP address 127.0.0.1(local loop back) in the driver

8.5 Forced variables

DB15 is in S5 format
DB15:0 increments up infinitely every 10msec
DB15:1 increments to pi * 1000
DB15:2 is sin(DB15:1)

DB1 is in S7 format
DB1,2 increments upto 100 every 10msec
DB1,0 increments everytime DB1,2 gets to 100 aprox every second

STRING SDB1,128[32] contains "Hello there"

Pseudo code for S7

```
IF DB1,4.0=1 THEN
    DB1,5.6 =1
ELSE
    DB1,5.6 =0
END

IF DB1,4.1 AND DB1,4.2 THEN
    DB1,5.7 =1
ELSE
    DB1,5.7 =0
END

DB1,4.3 blink every 1 sec.
```

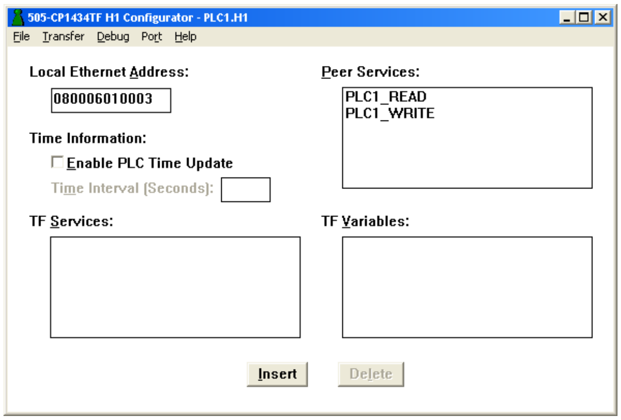
Pseudo Code for S5

```
IF DB15,4.0=1 THEN
    DB15,4.14 =1
ELSE
    DB15,4.14 =0
END

IF DB15,4.1 AND DB1,4.2 THEN
    DB15,4.15 =1
ELSE
    DB15,4.15 =0
END

DB15,4.3 blink every 1 sec.
```

9 Setting up the Simatic TI

The steps to migrating an existing system are as follows:

9.1.1 *Step 1: Adding peer-peer jobs to the PLC CP card setup. You can leave the old TF Jobs in place simply add these new ones.*



505-CP1434TF H1 Configurator - PLC1.H1

Local Ethernet Address: 080006010003

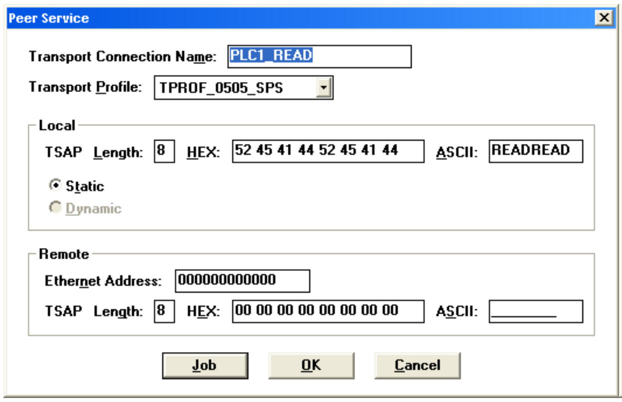
Peer Services:
PLC1_READ
PLC1_WRITE

Time Information:
□ Enable PLC Time Update
Time Interval (Seconds):

TF Services:

TF Variables:

They look like this

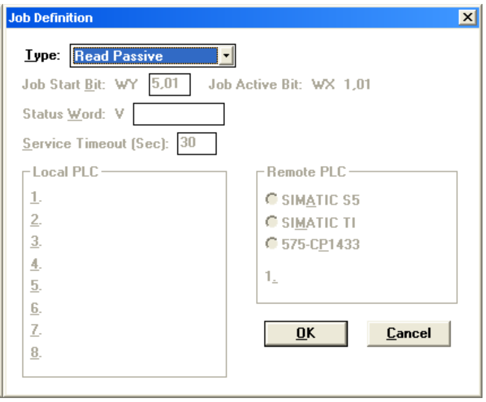


Peer Service

Transport Connection Name: PLC1_READ
Transport Profile: TPROF_0505_SPS

Local
TSAP Length: 8 HEX: 52 45 41 44 52 45 41 44 ASCII: READREAD
● Static
○ Dynamic

Remote
Ethernet Address: 000000000000
TSAP Length: 8 HEX: 00 00 00 00 00 00 00 00 ASCII: ________



Job Definition

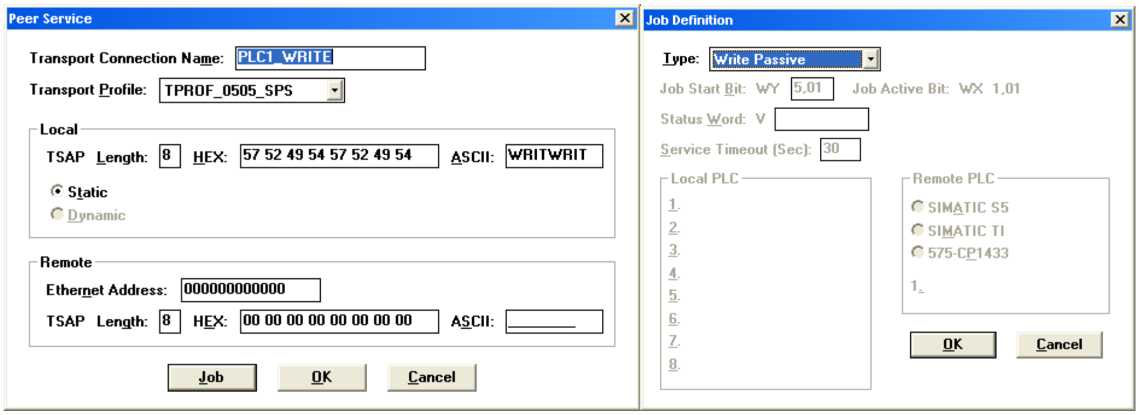
Type: Read Passive
Job Start Bit: WY 5,01 Job Active Bit: WX 1,01
Status Word: V
Service Timeout (Sec): 30

Local PLC
1.
2.
3.
4.
5.
6.
7.
8.

Remote PLC
○ SIMATIC S5
○ SIMATIC TI
○ 575-CP1433
1.

- Local TSAP must be 8 chars
- Remote Ethernet address should be “0000” – accepts any incoming
- This should be a read Passive job

- The Write job should be a Write passive



Peer Service

Transport Connection Name: PLC1_WRITE

Transport Profile: TPROF_0505_SPS

Local

TSAP Length: 8 HEX: 57 52 49 54 57 52 49 54 ASCII: WRITWRIT

● Static

○ Dynamic

Remote

Ethernet Address: 000000000000

TSAP Length: 8 HEX: 00 00 00 00 00 00 00 00 ASCII:

Job Definition

Type: Write Passive

Job Start Bit: WY 5,01 Job Active Bit: WX 1,01

Status Word: V

Service Timeout (Sec): 30

Local PLC

1.
2.
3.
4.
5.
6.
7.
8.

Remote PLC

○ SIMATIC S5

○ SIMATIC TI

○ 575-CP1433

1.

9.1.2 Step 2: Configure the poll configuration

- Setup the Siemens ISO transport in the newtwork settings, this is the same as for the S7 & S5 PLC's described earlier in this document

- Check that you have communications, you should do this before setting up the database. Simply setup 1 block of "V" registers. You should see green ticks & blocks per second at the bottom of the configurator window indicating successful communication

9.1.3 Step 3: Configure the backend blocks

- Open the database file in excel, sort on IO Address. Then manually add equivalent blocks in the backend

- At present there are no Learn address & variable import features for TI.