

VestaTel SCADA Multi-Protocol Simulator :: INSTANCE 0 :: DNP3 CLIENT

Tools View About

Start Link Stop Link **DNP3 Master Status**

Link Status	UP
App Layer Frags	RX: 25/TX: 41/Timeouts: 0
TS Segments	RX: 50/TX: 41
DL Frames	RX: 51/TX: 42/CRC Errs: 0

Log Level: Debug

Protocol Trace
 Hex Dump
 Expert

Apply

DNP3 Master Configuration

Channel Configuration

Run As TCP Server

Transport: DNP3-TCP TCP Port: 20000

Remote IP: 192.168.0.65

COM Port: COM3 Speed: 9600

Data Bits: 8 Parity: NONE

Stop bits: 1 Hardware Flow Control:

Export Log Clear Log Log Pause **Save & Apply**

Clear **DNP3 Outstation Data Points**

Group	Index	Description	Var	Value	Quality	Time
32	1	Analog Input	7 ((32+flag+T)	59.132233	Online	2026.03.29 07:43:50.000
32	0	Analog Input	7 ((32+flag+T)	40.500000	Online	2026.03.29 07:44:05.000
1	0	Binary Input (1bit)	2 (+flag)	0	Online	
1	1	Binary Input (1bit)	2 (+flag)	1	Online	
10	0	Binary Output	2 (+flag)	0	Online,RS	
10	1	Binary Output	2 (+flag)	0	Online,RS	

DNP3 Cnds

Gro...	Description
G12v1	Binary Output Command
G41	Analog Output Command
--	Integrity Poll
--	Assign Event Class

Binary Output Command G12v1

Index: 0 Control Type: Select-Operate

Qualifier: 0x17 - 8 bit index Mode: PULSE

Control Value: ON - CLOSE / LATCH ON

On Time (Ms): 0

Off Time (Ms): 0

Count: 1

Send Command Sequence

Result:

Export Log Clear Log Log Pause **Save & Apply**

Time	Level	Text
09:48:42.680	Debug	DNP3M DL RX (88): Unconfirmed User Data
09:48:42.680	Debug	Dst:1 Src:1024 DIR:Monitor Primary FCB:0 FCV/DFC:0 FC:4
09:48:42.680	Debug	AC: FIN.FIR.CON.SEQ=15 FC: RESPONSE
09:48:42.680	Debug	DNP3M DL TX (5): Unconfirmed User Data
09:48:42.680	Debug	Dst:1024 Src:1 DIR:Control Primary FCB:0 FCV/DFC:0 FC:4
09:48:42.680	Debug	AC: FIN.FIR.SEQ=15 FC: CONFIRM
09:48:42.818	Debug	DNP3M DL TX (14): Unconfirmed User Data
09:48:42.818	Debug	Dst:1024 Src:1 DIR:Control Primary FCB:0 FCV/DFC:0 FC:4
09:48:42.818	Debug	AC: FIN.FIR.SEQ=0 FC: READ
09:48:42.821	Debug	DNP3M DL RX (5): Unconfirmed User Data
09:48:42.821	Debug	Dst:1 Src:1024 DIR:Monitor Primary FCB:0 FCV/DFC:0 FC:4
09:48:42.821	Debug	AC: FIN.FIR.SEQ=0 FC: RESPONSE

VestaTel SCADA Multi-Protocol Simulator runs on Windows and implements master / slave, client / server role of several SCADA protocols: IEC 60870-5-104, IEC 60870-5-101, IEC 61850/MMS, DNP3, MODBUS and HART.

Overview of Features:

DNP3 Protocol

- DNP3 Master / DNP3 Outstation, Dual-Endpoint (Client can accept TCP connection from Server)
- Runs over RS232 Serial and over TCP/IP
- Solicited (Polled) and Unsolicited Mode
- Initial and Periodic Time Synchronization
- Periodic and demand Integrity Poll, Event Poll
- Binary Output Command, Analog Output Command, Assign Event Classes

IEC 104 / IEC 101 Protocol

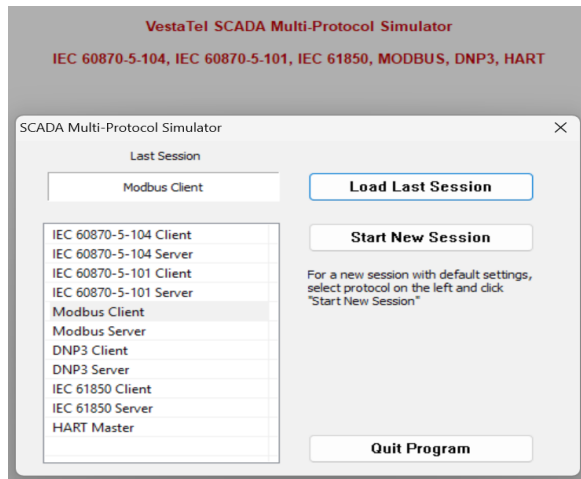
- IEC 60870-5-104 Master / IEC 60870-5-104 Slave
- IEC 60870-5-101 Master / IEC 60870-5-101 Slave
- IEC 104 Link Layer runs over TCP/IP
- IEC 101 over RS232 Serial and over TCP/IP
- IEC 101 Balanced / Unbalanced Link Mode
- Station Initialization, Clock Synchronization
- Data Acquisition, Events Acquisition
- Cyclic / Background / Spontaneous Transmission
- General Interrogation, Command Transmission
- Time Tagged and Time Untagged Commands

IEC 61850/MMS Protocol

- IEC 61850 IED Client / IEC 61850 Server
- Runs over TCP/IP
- Supports edition 2 of the IEC 61850 standard
- Data model discovery, data object polling
- Control commands: Direct Operate, Select-Operate
- Supports all major MMS data types, bool, integer, float, string, etc
- Supports parsing and displaying Timestamps, quality

MODBUS Protocol

- MODBUS Master / MODBUS Slave
- MODBUS RTU over RS232 Serial
- MODBUS TCP mode over TCP/IP
- Discreet Input Register, Coil Registers
- Holding Registers, Input Registers
- Write Single Coil, Write Multiple Coils
- Write Single Register, Write Multiple Registers



HART Protocol

HART Communication Protocol (Highway Addressable Remote Transducer) master side only is supported in the current version of software.

The simulator implements the physical layer over RS232 serial port, data link Layer and application layer.

All device dynamic variables (PV, SV, TV and QV) are polled periodically and their value is displayed in the points view.

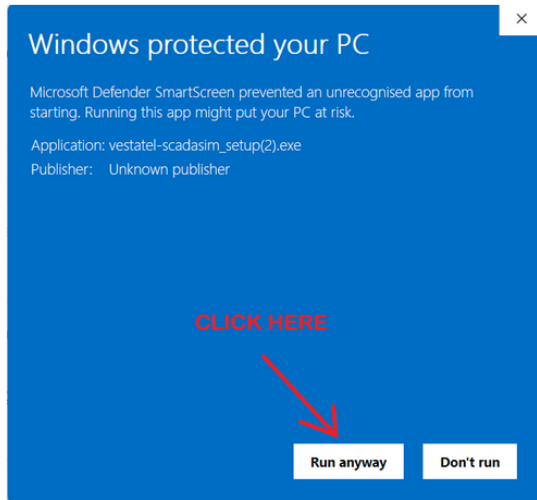
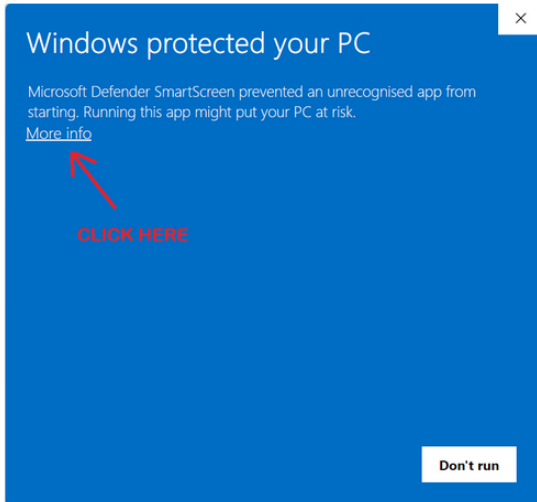
The implementation is done according to standards HCF_SPEC-127, Revision 7.1, (HART Communication Protocol, Universal Command Specification), HCF_SPEC-99, Revision 9.0 (HART Communication Protocol, Command Summary Specification)

Table of Contents

- 1 Installation Procedure 5
- 2 Licensing..... 6
- 3 Quick Start..... 7
- 4 IEC 60870-5-104 Slave (Controlled Station)..... 9
 - 4.1 Channel Configuration..... 9
 - 4.2 Link Configuration..... 9
 - 4.3 Application Layer Configuration..... 10
 - 4.4 Data Points Configuration..... 11
 - 4.5 Advanced Configuration..... 11
- 5 IEC 60870-5-104 Master (Controlling Station)..... 13
 - 5.1 Channel Configuration..... 13
 - 5.2 Link Configuration..... 14
 - 5.3 Application Layer Configuration..... 14
 - 5.4 Advanced Configuration..... 15
 - 5.5 IEC 104 Commands..... 15
- 6 IEC 60870-5-101 Slave (Controlled Station)..... 16
 - 6.1 Channel Configuration..... 16
 - 6.2 Link Configuration..... 17
 - 6.3 Application Layer Configuration..... 17
 - 6.4 Advanced Configuration..... 18
 - 6.5 Data Points Configuration..... 19
- 7 IEC 60870-5-101 Master (Controlling Station)..... 20
 - 7.1 Channel Configuration..... 20
 - 7.2 Link Configuration..... 21
 - 7.3 Application Layer Configuration..... 22
 - 7.4 Advanced Configuration..... 22
- 8 IEC 61850 Client..... 23
 - 8.1 Channel Configuration..... 23
 - 8.2 Connection Configuration..... 24
 - 8.3 Advanced Configuration..... 24
 - 8.4 IEC 61850 Commands..... 24
- 9 IEC 61850 Server..... 25
 - 9.1 General Configuration..... 25
 - 9.2 Data Points Configuration..... 26
 - 9.3 Advanced Configuration..... 26
- 10 DNP3 Master..... 27
 - 10.1 Channel Configuration..... 27
 - 10.2 Link Configuration..... 28
 - 10.3 Application Layer Configuration..... 28
 - 10.4 Advanced Configuration..... 29
 - 10.5 DNP3 Commands..... 29
- 11 DNP3 Server..... 30
 - 11.1 Channel Configuration..... 30
 - 11.2 Link Configuration..... 31
 - 11.3 Application Layer Configuration..... 31
 - 11.4 Data Points Configuration..... 31
 - 11.5 Advanced Configuration..... 32
- 12 Modbus Server..... 33
 - 12.1 Channel Configuration..... 33
 - 12.2 Link Configuration..... 34
 - 12.3 Data Points Configuration..... 34
 - 12.4 Advanced Configuration..... 34

13 Modbus Client.....	36
13.1 Channel Configuration.....	36
13.2 Link Configuration.....	37
13.3 Advanced Configuration.....	37
13.4 Modbus Commands.....	37
14 HART Master.....	38
14.1 General Configuration.....	38
14.2 Polling Configuration.....	39
15 Event Log.....	40
16 Diagnostic Counters.....	41
17 Automation Features.....	42
17.1 Running multiple instances from a script.....	42
17.2 Command line interface	
.....	44
18 VENDOR INFORMATION.....	45

1 Installation Procedure



Downloading:

To download an installation package, please visit:

<https://vestatel.eu/software.html#scadasim-download>

Fill out the form and click "Continue to DOWNLOAD"

Click on the link shown in the next page. The installation executable will be saved to your PC (typically into Downloads)

Installing:

Run the installation executable:

[vestatel-scadasim_setup.exe](#)

Due to strict security policy Windows is going to display "Windows protected your PC" dialog.

Please click "More info" as shown in the screenshot on the left.

In the next dialog, please click "Run anyway"

After this step, please run the installation program, read and accept the Software License Agreement and click Next.

At the end of the installation click "Finish"

By default the files are installed into "c:\VestaTel-Scadasim" folder

2 Licensing

Evaluation Mode and Full Mode:

If you have not yet purchased the software and set the license key, the software shall run in evaluation mode

Evaluation Period is limited to 7 days. In other respects the software runs fully featured.

When the program starts you will see the dialog box shown on the left. To run in evaluation mode, click "Free Trial"

After the evaluation period of 7 days runs out, at program start you will see the second dialog shown on the right. To continue, you will need to set the license key.

You can also display the "Set License Key" dialog by clicking the programs menu bar "About" → Register / Buy Online.

You receive the license key by email when you purchase the software. To purchase the software click "Buy Online" button in the same dialog window

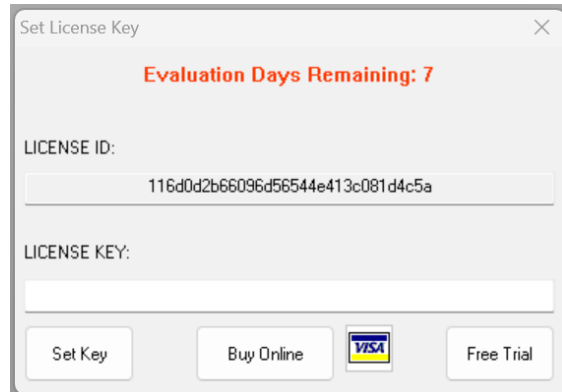
There are three license types:

- Personal
- Professional (PC locked)
- Professional (USB dongle)

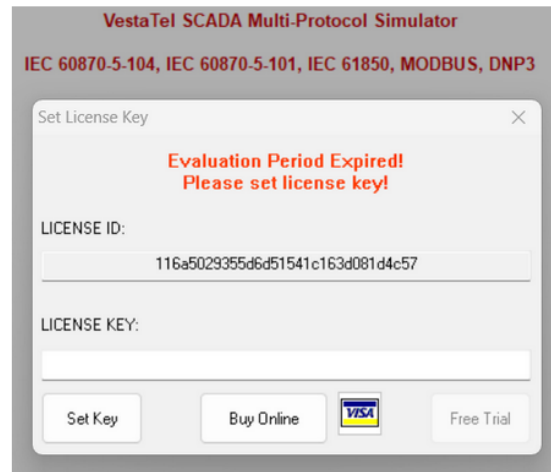
For the Personal and Professional (PC locked) the license key locks the license to the PC on which the program is installed.

Is there is a need to transfer the license to a different PC, please contact us.

For the Professional (USB Dongle) license type, we will ship the USB dongle and you will be able to run the application on any PC with the USB dongle installed. Once USB dongle is inserted, no license key is required.



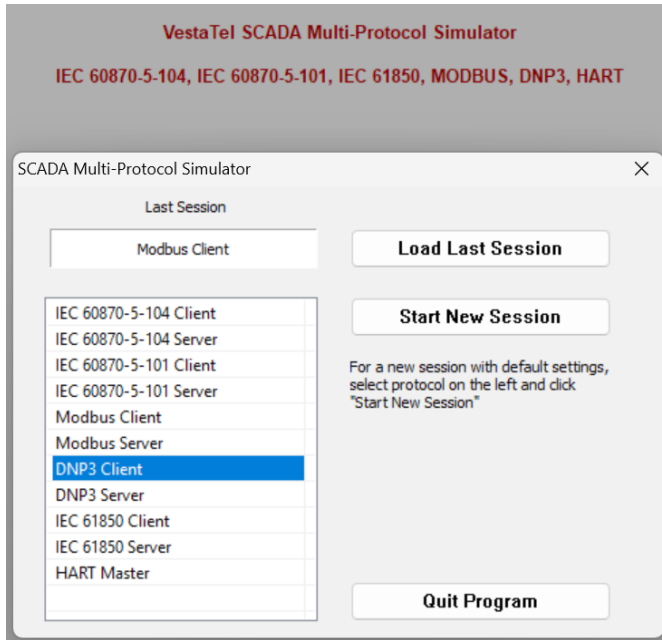
(To run in evaluation mode, click "Free Trial")



(Set the license key to continue)

3 Quick Start

SCADA Protocol Selection



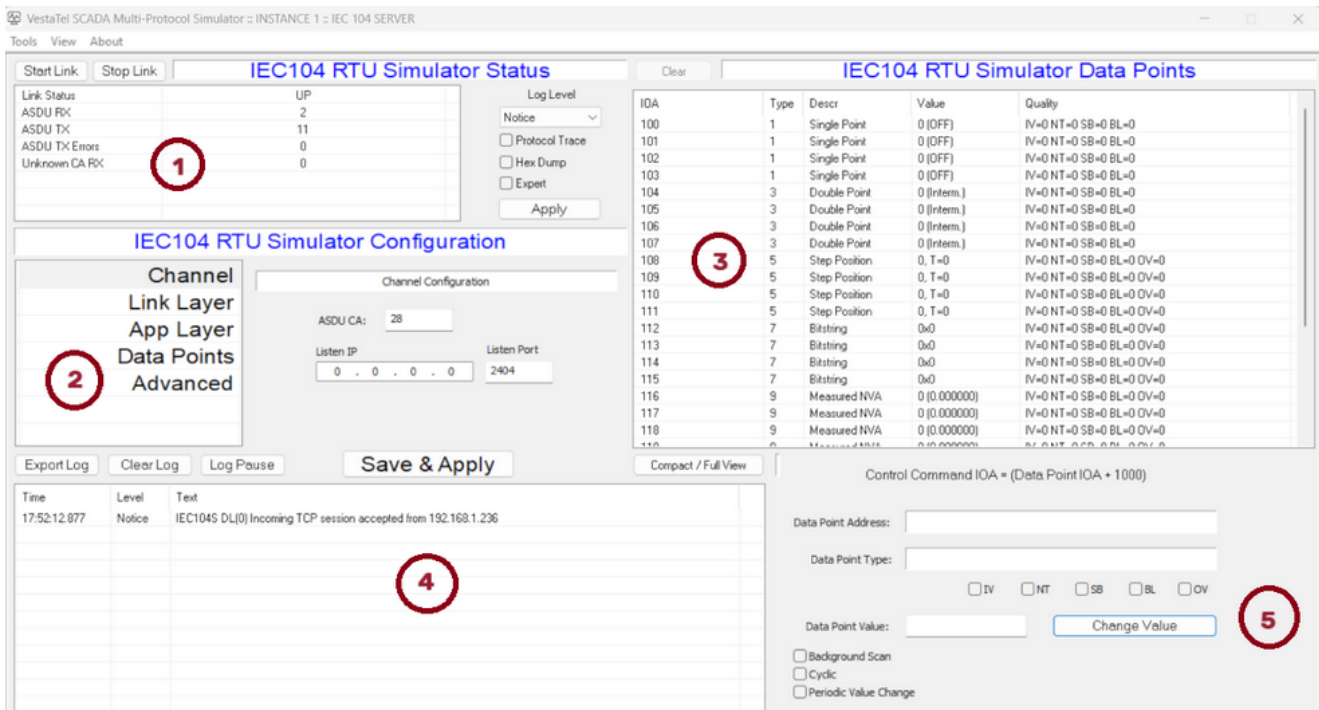
When you start the program it shows the protocol selection window

Unless the program is started for the first time, you can click "Load Last Session" to load the last used protocol configuration

Otherwise you can select and click on the required protocol and then click "Start New Session"

At run time you can bring up the same dialog window via main menu "Tools" -> "Select Protocol"

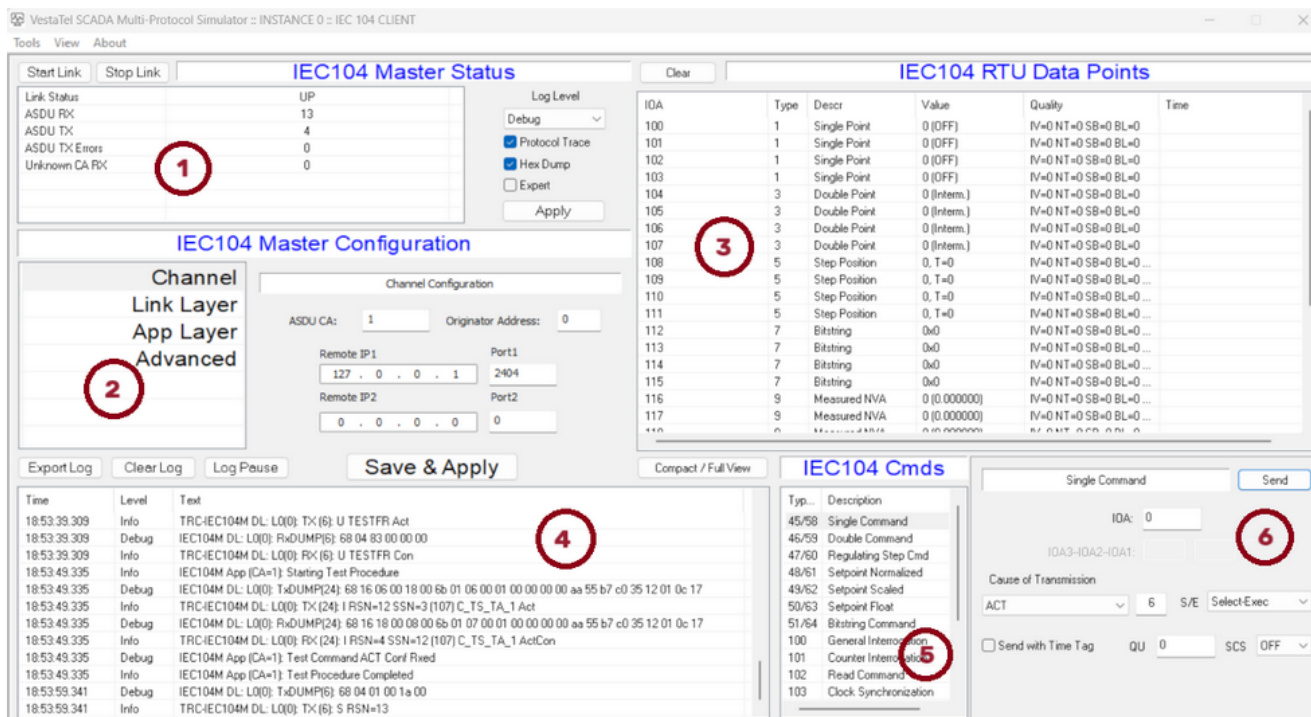
Main Program Screen



The example above shows the IEC 60 870-5-104 Slave Simulator screen

Description of main control areas (slave / server side protocols)

- (1) Link Status and Statistic counters
- (2) Protocol Configuration
- (3) Data Points Window
- (4) Log window
- (5) Selected Data Point Window



The example above shows the IEC 60 870-5-104 Master Simulator screen

Description of main control areas (master / client side protocols)

- (1) Link Status and Statistic counters
 - (2) Protocol Configuration
 - (3) Data Points Window
 - (4) Log window
 - (5) Command Window
 - (6) Selected Command details

Configure all required settings in the Protocol configuration tabs / sections on the left. Changing between tabs saves the settings. Every time you click "Save & Apply" configuration is saved and the protocol is re-started

4 IEC 60870-5-104 Slave (Controlled Station)

4.1 Channel Configuration

The screenshot shows the 'Channel Configuration' window of the IEC104 RTU Simulator. On the left is a navigation menu with options: Channel, Link Layer, App Layer, Data Points, and Advanced. The 'Channel' option is selected. The main configuration area contains the following fields:

- ASDU CA: 1
- Listen IP: 0 . 0 . 0 . 0
- Listen Port: 2404

At the bottom of the window are buttons for 'Export Log', 'Clear Log', 'Log Pause', and 'Save & Apply'.

ASDU CA - Sets ASDU Common Address as specified in the IEC 60870-5-101. Acceptable values are from 1 to 65534. The same value must be configured in the IEC 104 master for successful communication

Listen IP - Local IP address on which the IEC104 slave shall accept incoming TCP connections from IEC104 Master

Listen Port - Local TCP port number on which the IEC104 slave shall accept incoming TCP connections from IEC104 Master. The same number must be configured in the corresponding IEC104 client parameter, default is 2404

4.2 Link Configuration

The screenshot shows the 'Link Layer Configuration' window of the IEC104 RTU Simulator. The navigation menu on the left has 'Link Layer' selected. The main configuration area contains the following fields:

- T1 (sec) Response Timeout: 15
- T2 (sec) ACK during inactivity: 10
- T3 (sec) Send test frames: 20
- K - Max unacked I-frames: 12
- W - Latest ACK after rx W I frames: 8

At the bottom of the window are buttons for 'Export Log', 'Clear Log', 'Log Pause', and 'Save & Apply'.

T1 - Time-out of send or test APDUs

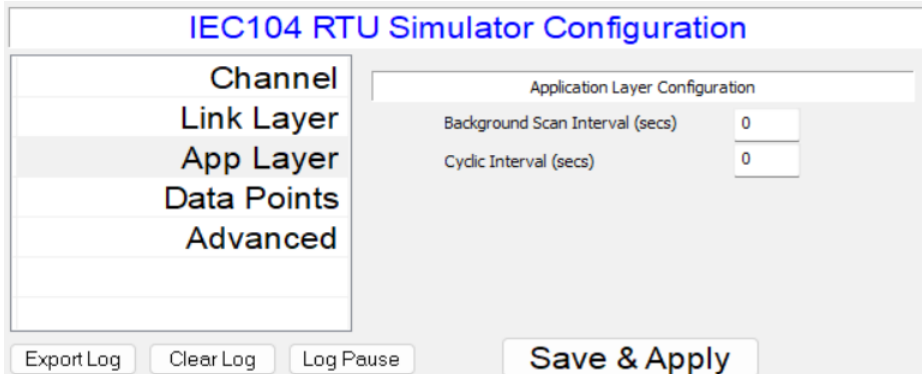
T2 - Time-out for acknowledges in case of no data messages $t2 < t1$

T3 - Time-out for sending test frames in case of a long idle state

K - Maximum difference receive sequence number to send state variable

W - Latest acknowledge after receiving w l format APDUs

4.3 Application Layer Configuration



Background Scan Interval - sets the frequency in seconds of sending data point messages with cause of transmission 2 (Background Scan). When set to 0, background scan sending is disabled for all points. Only data points that are configured for sending Background Scan are sending these messages. To select a data point for background scan, first choose the required point in the Data Points window in the top right part of the main screen, then click on that point and check tickbox "Background Scan" in the data point window in the bottom right part of main screen

Cyclic Interval - sets the frequency in seconds for sending data point messages with cause of transmission 1 (Cyclic). When set to 0, cyclic transmission is disabled. Measured value data points can be sent periodically using this procedure. To select a data point for cyclic transmission, first choose the required point in the Data Points window in the top right part of the main screen, then click on that point and check tickbox "Cyclic" in the data point window in the bottom right part of main screen

Clear IEC104 RTU Simulator Data Points

IOA	Type	Descr	Value	Quality
100	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
101	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
102	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
103	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
104	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
105	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
106	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
107	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
108	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
109	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
110	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
111	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
112	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
113	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
114	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
115	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
116	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
117	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
118	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
119	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0

Compact / Full View Control Command IOA = (Data Point IOA + 1000)

Data Point Address:

Data Point Type:

IV NT SB BL OV

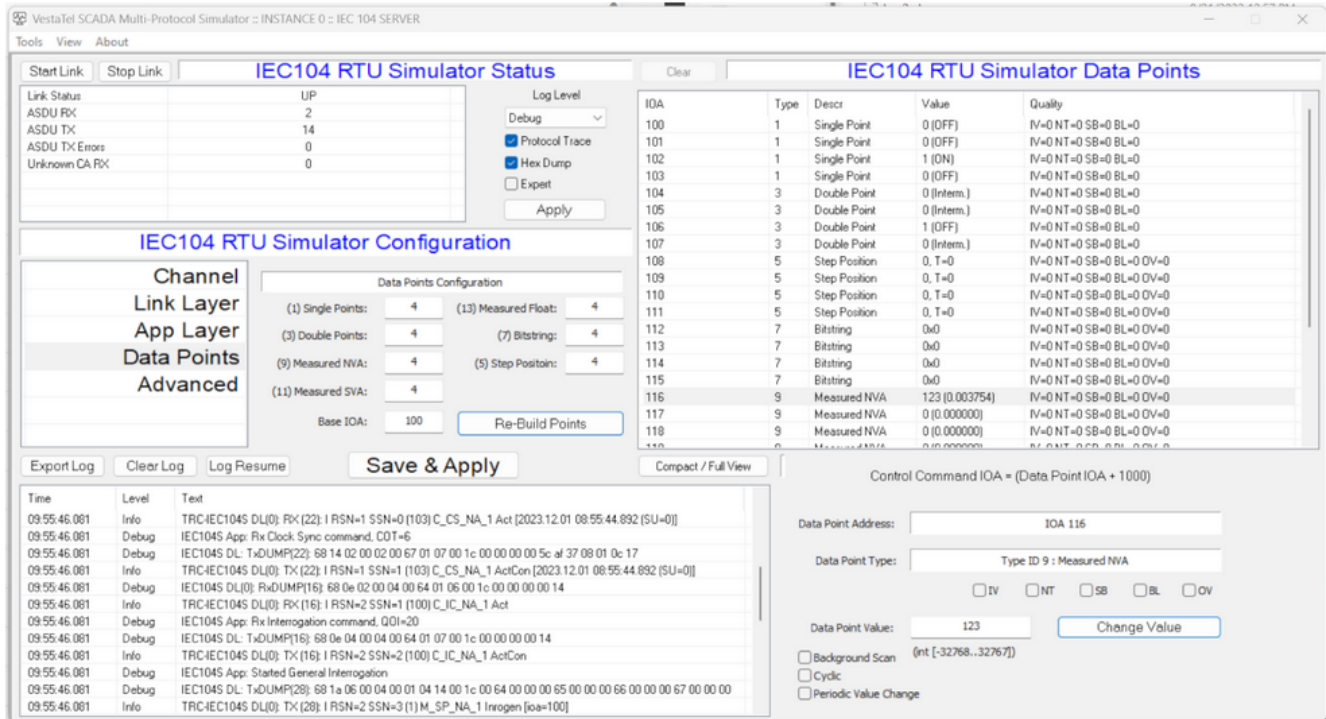
Data Point Value:

Background Scan (int [-32768..32767])

Cyclic

Periodic Value Change

4.4 Data Points Configuration

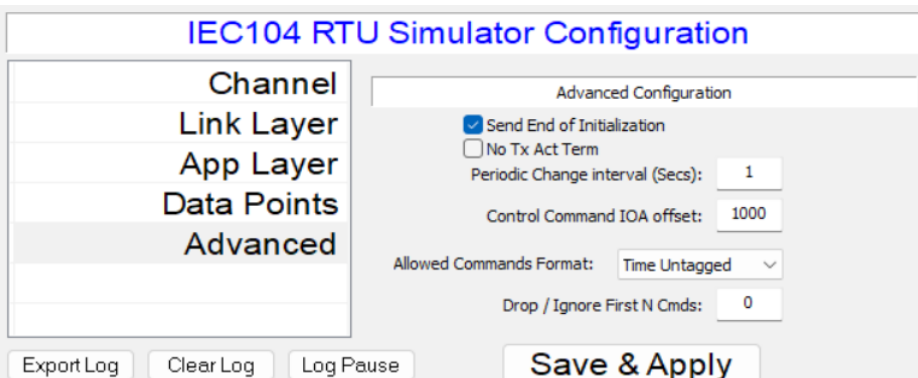


This tab contains configuration of the number of data points of specific type IDs that shall be emulated and that shall appear in the data points window on the right top of the screen.

Base IOA field defines the starting IOA (Information object address) for the first data point. Please note that the maximum total number of points currently supported is 1024

When the desired number of points of each type is set, click "Re-Build Points" to apply new configuration

4.5 Advanced Configuration



Send End of Initialization - Controls whether or not the slave simulator sends message type ID 70 (M_EI_NA_1) - End of Initialization after data link connection is established

Periodic Change Interval - sets the frequency at which the data point values change (increment) if selected for Periodic Value Change. When set to 0, no data points are changed periodically. To select a data point for periodic change, select it in the data point list in the top right, then tick checkbox "Periodic Value Change" in the selected data point window in the right bottom of the main screen. When a point is changed periodically its value is incremented, written into configuration and an event message with cause of transmission Spontaneous is sent to the connected Master

Control Command IOA offset - defines IOA (information object address) to which the connected Master can send a command to change the addressed data point value. For example to change a Single Point Information point at IOA 100, the Master should send the Single Command to IOA 1100 if the control offset is configured at 1000

Allowed Command Format - Sets the format of control commands accepted by the slave simulation to Time Tagged or Time untagged

No Tx Act Term - skip sending Activation Termination during General Interrogation Procedure

Drop / Ignore First N Cmds - makes the simulator drop first specified number of received application layer PDUs

5 IEC 60870-5-104 Master (Controlling Station)

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for an IEC 104 Client. It is divided into several functional areas:

- IEC104 Master Status:** Shows link status (UP), ASDU RX (234), ASDU TX (217), ASDU TX Errors (0), and Unknown CA RX (0). It includes a Log Level dropdown set to Debug and checkboxes for Protocol Trace, Hex Dump, and Expert.
- IEC104 Master Configuration:** Features a sidebar with 'Channel', 'Link Layer', 'App Layer', and 'Advanced' options. The 'Link Layer Configuration' section includes:
 - T0 (sec) Connection Establishment: 30
 - T1 (sec) Response Timeout: 15
 - T2 (sec) ACK during inactivity: 10
 - T3 (sec) Send test frames: 20
 - K - Max unacked I-frames: 12
 - W - Latest ACK after rx W I frames: 8
- IEC104 RTU Data Points:** A table listing data points with columns for IOA, Type, Descr, Value, Quality, and Time. The table contains 17 rows of data points, including Single Points and Double Points.
- IEC104 Cmds:** A list of command types and descriptions, such as Single Command, Double Command, Regulating Step Cmd, Setpoint Normalized, Setpoint Scaled, Setpoint Float, Bitstring Command, General Interrogation, Counter Interrogation, Read Command, and Clock Synchronization.
- Log Window:** Displays a real-time log of events with columns for Time, Level, and Text. Recent entries include test frame transmissions and acknowledgments.
- Single Command Panel:** Allows for sending a single command with fields for IOA (0), Cause of Transmission (ACT), and S/E (Select-Exec).

5.1 Channel Configuration

The 'IEC104 Master Configuration - Channel Configuration' dialog box is shown. It includes a sidebar with 'Channel', 'Link Layer', 'App Layer', and 'Advanced' options. The main configuration area contains the following fields:

- ASDU CA:** 1
- Originator Address:** 0
- Remote IP1:** 0 . 0 . 0 . 0
- Port1:** 2404
- Remote IP2:** 0 . 0 . 0 . 0
- Port2:** 0

Buttons for 'Export Log', 'Clear Log', 'Log Pause', and 'Save & Apply' are located at the bottom of the dialog.

ASDU CA - Sets ASDU Common Address as specified in the IEC 60870-5-101. Acceptable values are from 1 to 65534. The same value must be configured in the IEC 104 server for successful communication

Originator Address - Sets the OA (originator address) field that is the second byte of the cause of transmission part in the IEC104 ADSU packets

Remote IP1 - Remote IP address to which the IEC104 master shall connect, Remote IP2 can be used for redundancy

Port1 - Remote TCP port number to which the IEC104 master shall connect. The same number must be configured in the corresponding IEC104 server parameter, default is 2404. Port2 can be used for redundancy

5.2 Link Configuration

T0 - Connection Establishment Timeout

T1 - Time-out of send or test APDUs

T2 - Time-out for acknowledges in case of no data messages $t2 < t1$

T3 - Time-out for sending test frames in case of a long idle state

K - Maximum difference receive sequence number to send state variable

W - Latest acknowledge after receiving w I format APDUs

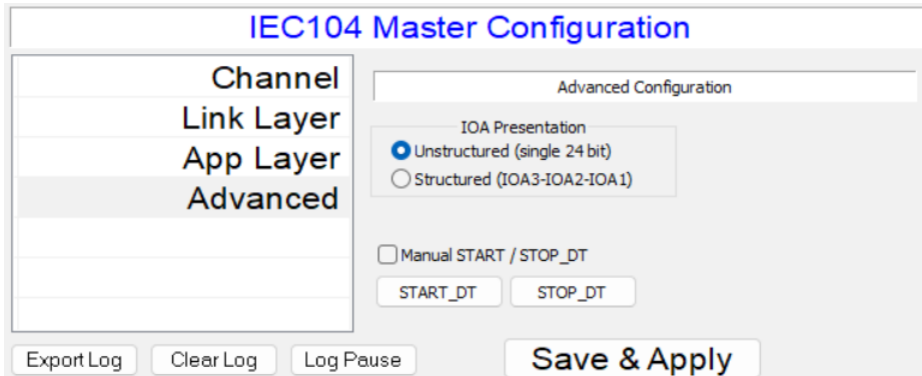
5.3 Application Layer Configuration

Clock synchronization period - sends the frequency in seconds of performing periodic clock synchronization procedure

General interrogation period - sets the frequency in seconds of performing periodic general interrogation procedure

Test procedure period - sets the frequency in seconds of performing test procedure

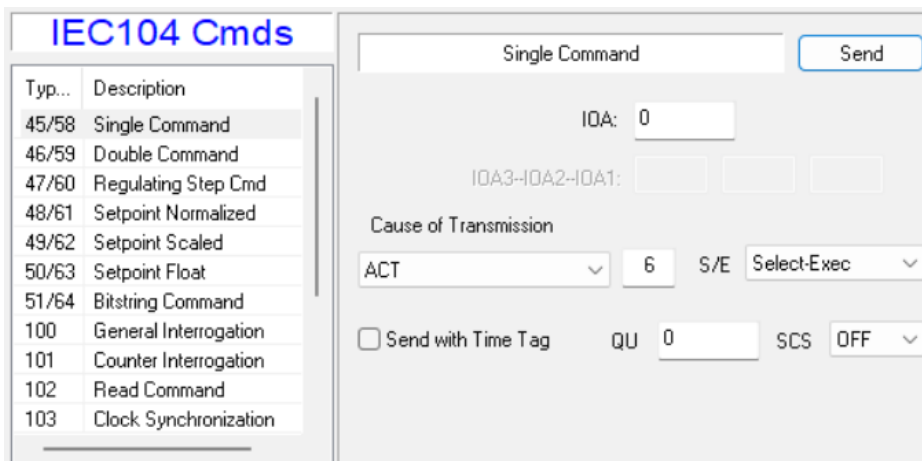
5.4 Advanced Configuration



IOA Presentation - sets the view (structured as 3 bytes or unstructured as 24 bit integer) of IOA (information object addresses) in the IOA column in the data points list and in the commands

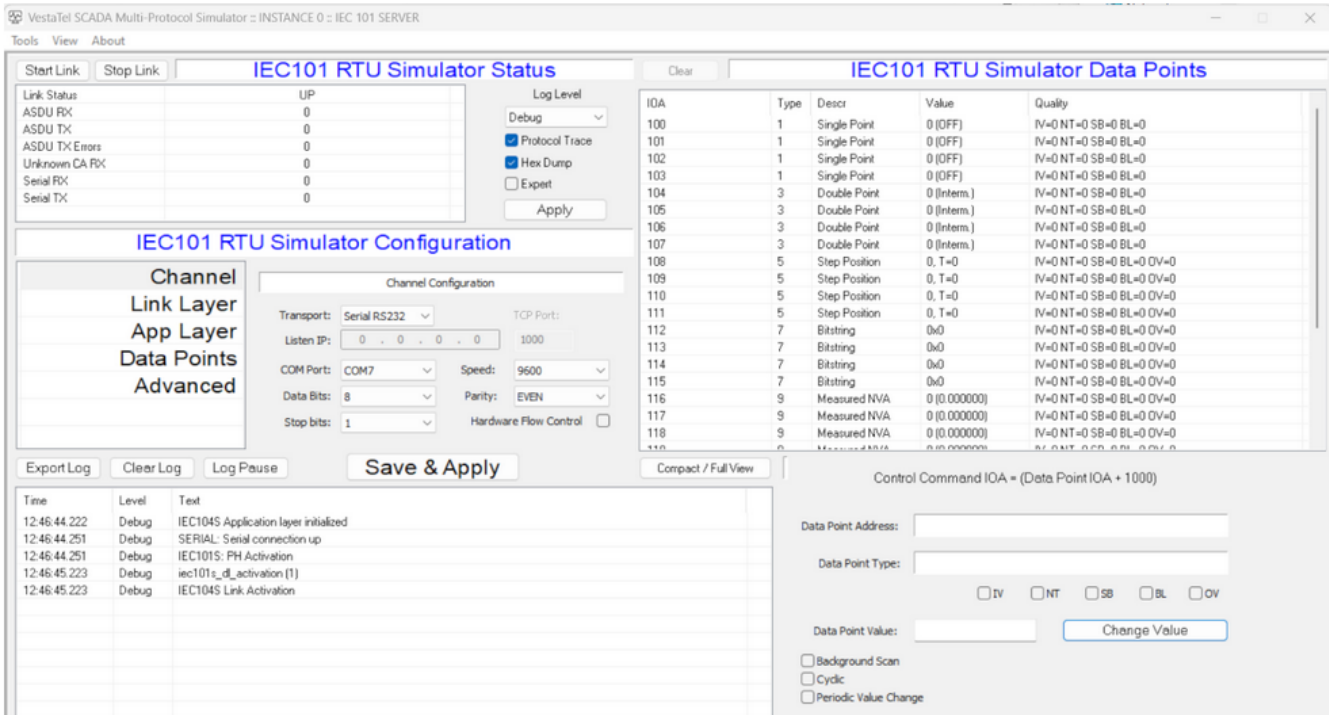
Start DT - Stop DT - Allows manual sending of START DT and STOP DT packets to the slave station

5.5 IEC 104 Commands



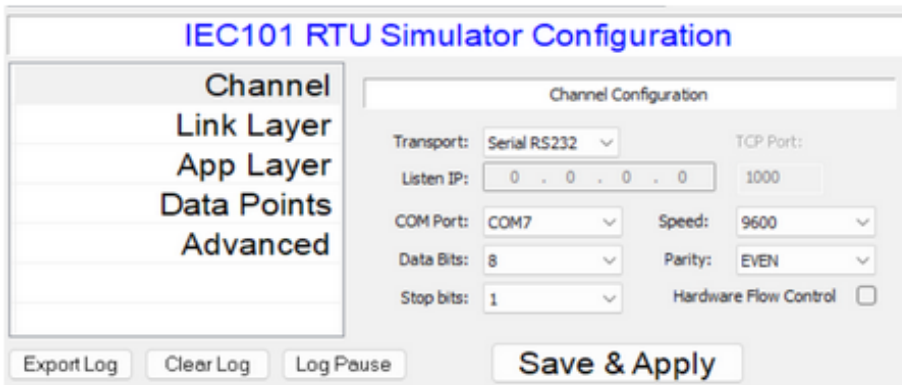
To send the required command, select one from the IEC104 Cmds list in the bottom right of the screen, then setup the IOA and value fields and click Send button

6 IEC 60870-5-101 Slave (Controlled Station)



6.1 Channel Configuration

VestaTel SCADA Multi-Protocol Simulator in IEC101 slave mode can operate over RS232 serial interface or over TCP/IP. To select / switch between serial and TCP/IP choose Transport selector as required. Note that when COMx ports are present they are shown in the COM Port selector. If no serial interfaces are detected that list is empty



Transport: Selects Serial RS232 or TCP/IP transport for IEC 60870-5-101 protocol

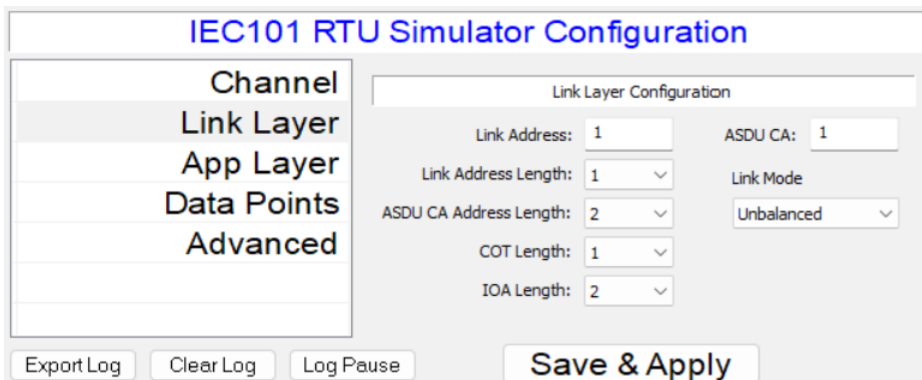
Listen IP: When TCP/IP transport is selected, sets the listening IP address

TCP Port: When TCP/IP transport is selected, sets the listening TCP port

COM Port: Sets the COM port number for operation over RS232

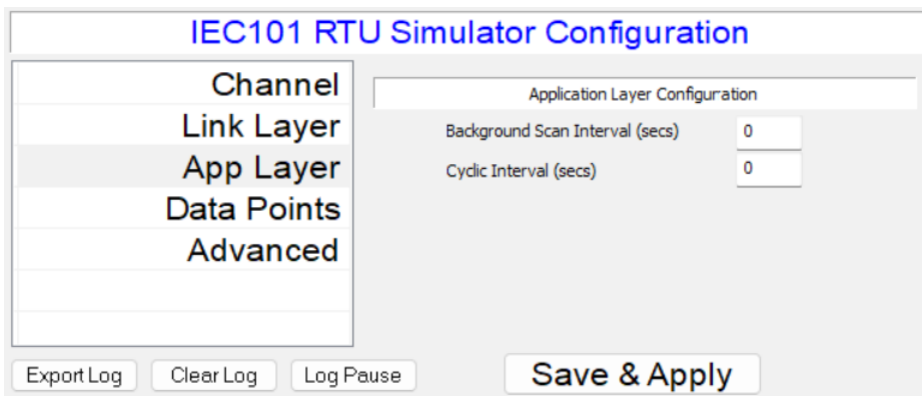
Data Bits: Sets number of serial data bits
 Stop Bits: Sets number of serial stop bits
 Speed: Sets serial interface speed
 Parity: Sets serial interface parity
 Hardware Flow Control: Enables RTS/CTS flow control

6.2 Link Configuration



Link Address: Sets IEC 60870-5-101 Link address value
 ASDU CA: Sets IEC 60870-5-101 ASDU Common Address value
 Link Address Length: Sets IEC101 link address length
 ASDU CA Length: Sets IEC101 ASDU Common Address length
 COT length: Sets cause of transmission length
 IOA Length: Sets information object address length
 Link Mode: Sets IEC101 link mode (currently only Unbalanced is supported)

6.3 Application Layer Configuration



Background Scan Interval - sets the frequency in seconds of sending data point messages with cause of transmission 2 (Background Scan). When set to 0, background scan sending is disabled for all points. Only data points that are configured for sending Background Scan are sending these messages. To select a data point for background scan, first choose the required point in the Data Points window in the top right part of the main screen, then click on that point and check tickbox "Background Scan" in the data point window in the bottom right part of main screen

Cyclic Interval - sets the frequency in seconds for sending data point messages with cause of transmission 1 (Cyclic). When set to 0, cyclic transmission is disabled. Measured value data points can be sent periodically using this procedure. To select a data point for cyclic transmission, first choose the required point in the Data Points window in the top right part of the main screen, then click on that point and check tickbox "Cyclic" in the data point window in the bottom right part of main screen

Clear
IEC101 RTU Simulator Data Points

IOA	Type	Descr	Value	Quality
100	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
101	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
102	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
103	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
104	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
105	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
106	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
107	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
108	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
109	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
110	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
111	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
112	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
113	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
114	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
115	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
116	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
117	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
118	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
119	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0

Compact / Full View

Control Command IOA = (Data Point IOA + 1000)

Data Point Address:

Data Point Type:

IV
 NT
 SB
 BL
 OV

Data Point Value: Change Value

Background Scan
 Cyclic
 Periodic Value Change

6.4 Advanced Configuration

IEC101 RTU Simulator Configuration

Channel

Link Layer

App Layer

Data Points

Advanced

Advanced Configuration

Send End of Initialization

Periodic Change interval (Secs):

Control Command IOA offset:

Allowed Commands Format:

Show IEC101 Slave DL Stats

Export Log
Clear Log
Log Pause
Save & Apply

Send End of Initialization - Controls whether or not the slave simulator sends message type ID 70 (M_EI_NA_1) - End of Initialization after data link connection is established

Periodic Change Interval - sets the frequency at which the data point values change (increment) if selected for Periodic Value Change. When set to 0, no data points are changed periodically. To select a data point for periodic change, select it the data point list in the top right, then tick checkbox "Periodic Value Change" in the selected data point window in the right bottom of the main screen. When a point is changed periodically its value is incremented, written into configuration and an event message with cause of transmission Spontaneous is sent to the connected Master

Control Command IOA offset - defines IOA (information object address) to which the connected Master can send a command to change the addressed data point value. For example to change a Single Point Information point at IOA 100, the Master should send the Single Command to IOA 1100 if the control offset is configured at 1000

Allowed Command Format - Sets the format of control commands accepted by the slave simulation to Time Tagged or Time untagged

Show IEC101 DL Stats - displays IEC 101 data link statistic counters in the event log

6.5 Data Points Configuration

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for an IEC 101 SERVER. It is divided into several functional areas:

- IEC101 RTU Simulator Status:** Shows link status (DOWN) and various error counters (ASDU RX, TX, Errors, CA RX, FX, TX).
- IEC101 RTU Simulator Configuration:** Contains a 'Data Points Configuration' section with input fields for:
 - (1) Single Points: 4
 - (3) Double Points: 4
 - (9) Measured NVA: 4
 - (11) Measured SVA: 4
 - (13) Measured Float: 4
 - (7) Bitstring: 4
 - (5) Step Position: 4
 - Base IOA: 100
 A 'Re-Build Points' button is available to apply these settings.
- IEC101 RTU Simulator Data Points:** A table listing configured data points with columns for IOA, Type, Descr, Value, and Quality.

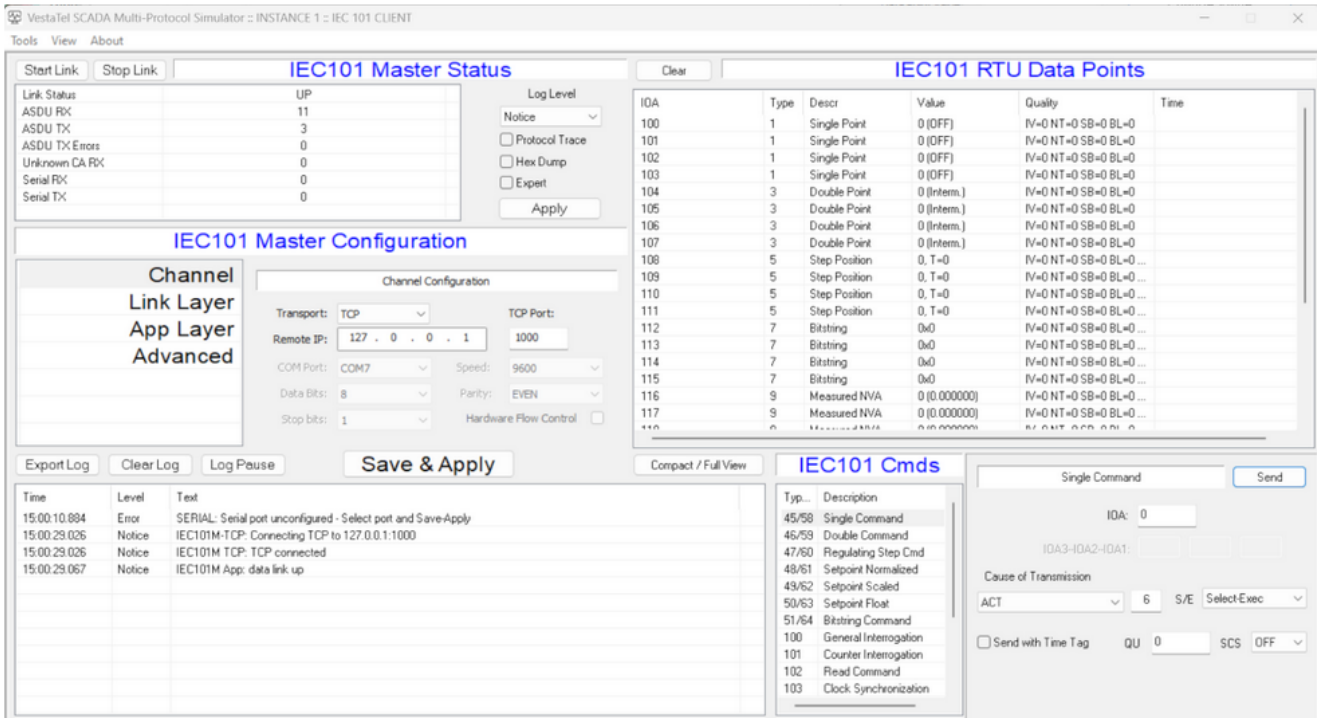
IOA	Type	Descr	Value	Quality
100	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
101	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
102	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
103	1	Single Point	0 (OFF)	IV=0 NT=0 SB=0 BL=0
104	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
105	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
106	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
107	3	Double Point	0 (Interm.)	IV=0 NT=0 SB=0 BL=0
108	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
109	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
110	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
111	5	Step Position	0, T=0	IV=0 NT=0 SB=0 BL=0 OV=0
112	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
113	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
114	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
115	7	Bitstring	0x0	IV=0 NT=0 SB=0 BL=0 OV=0
116	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
117	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
118	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
119	9	Measured NVA	0 (0.000000)	IV=0 NT=0 SB=0 BL=0 OV=0
- Control Command IOA = (Data Point IOA + 1000):** A section for configuring the master's command address, including fields for Data Point Address, Data Point Type (IV, NT, SB, BL, OV), and Data Point Value.
- Log Level:** A dropdown menu set to 'Notice' with checkboxes for Protocol Trace, Hex Dump, and Expert.
- Event Log:** A table at the bottom left showing time, level, and text of events, such as 'SERIAL: Serial port unconfigured - Select port and Save-Apply'.

This tab contains configuration of the number of data points of specific type IDs that shall be emulated and that shall appear in the data points window on the right top of the screen.

Base IOA field defines the starting IOA (Information object address) for the first data point. Please note that the maximum total number of points currently supported is 1024

When the desired number of points of each type is set, click "Re-Build Points" to apply new configuration

7 IEC 60870-5-101 Master (Controlling Station)



7.1 Channel Configuration

VestaTel SCADA Multi-Protocol Simulator in IEC101 master mode can operate over RS232 serial interface or over TCP/IP. To select / switch between serial and TCP/IP choose Transport selector as required. Note that when COMx ports are present they are shown in the COM Port selector. If no serial interfaces are detected that list is empty



Transport: Selects Serial RS232 or TCP/IP transport for IEC 60870-5-101 protocol

Remote IP: When TCP/IP transport is selected, sets the remote IP address

TCP Port: When TCP/IP transport is selected, sets the remote TCP port

COM Port: Sets the COM port number for operation over RS232

Data Bits: Sets number of serial data bits

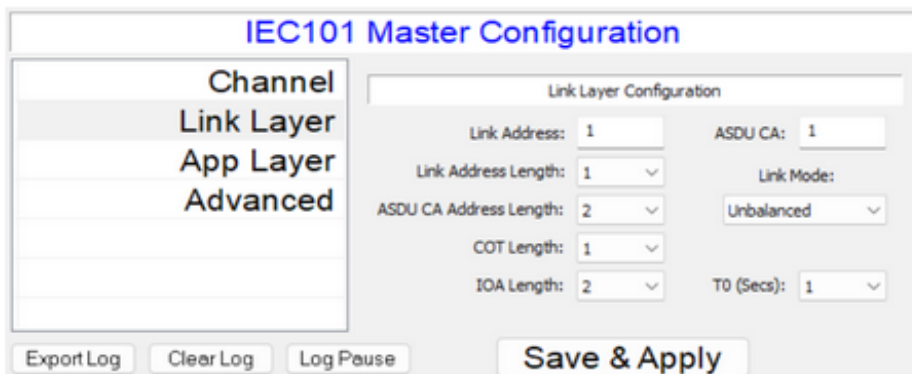
Stop Bits: Sets number of serial stop bits

Speed: Sets serial interface speed

Parity: Sets serial interface parity

Hardware Flow Control: Enables RTS/CTS flow control

7.2 Link Configuration



The screenshot shows the 'IEC101 Master Configuration' dialog box. On the left is a navigation pane with 'Channel', 'Link Layer', 'App Layer', and 'Advanced' options. The 'Link Layer' option is selected. The main area is titled 'Link Layer Configuration' and contains several input fields and dropdown menus: 'Link Address' (text box with '1'), 'ASDU CA' (text box with '1'), 'Link Address Length' (dropdown with '1'), 'ASDU CA Address Length' (dropdown with '2'), 'COT Length' (dropdown with '1'), 'IOA Length' (dropdown with '2'), 'Link Mode' (dropdown with 'Unbalanced'), and 'T0 (Secs)' (dropdown with '1'). At the bottom, there are buttons for 'Export Log', 'Clear Log', 'Log Pause', and a large 'Save & Apply' button.

Link Address: Sets IEC 60870-5-101 Link address value

ASDU CA: Sets IEC 60870-5-101 ASDU Common Address value

Link Address Length: Sets IEC101 link address length

ASDU CA Length: Sets IEC101 ASDU Common Address length

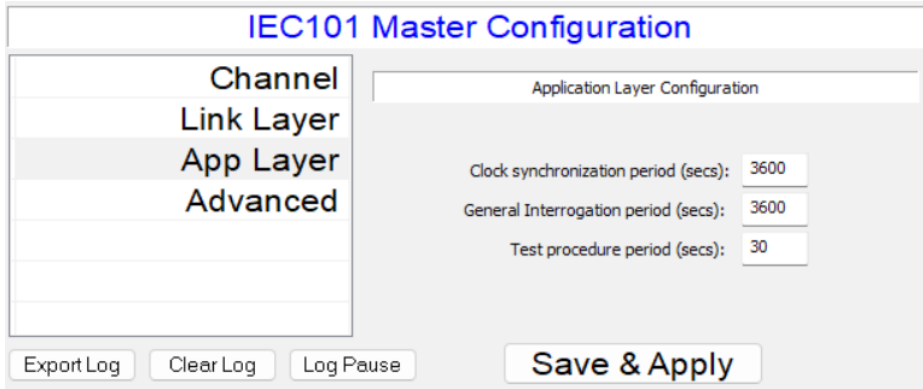
COT length: Sets cause of transmission length

IOA Length: Sets information object address length

Link Mode: Sets IEC101 link mode to Balanced or Unbalanced

T0 Secs: Sets IEC101 link layer timer T0 value

7.3 Application Layer Configuration

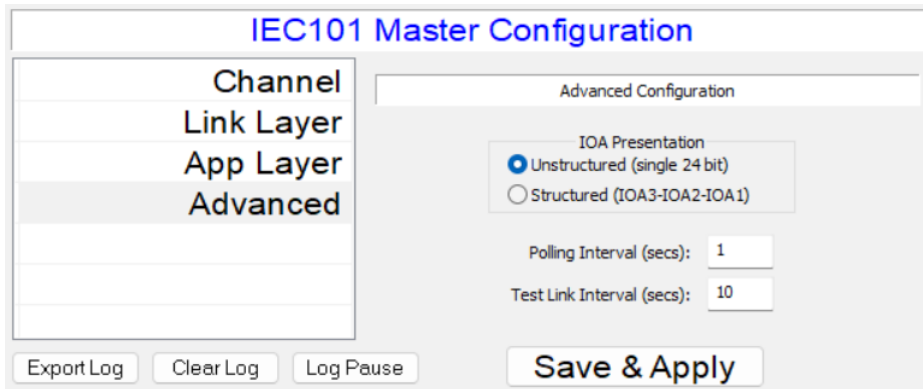


Clock synchronization period - sends the frequency in seconds of performing periodic clock synchronization procedure

General interrogation period - sets the frequency in seconds of performing periodic general interrogation procedure

Test procedure period - sets the frequency in seconds of performing test procedure

7.4 Advanced Configuration



IOA Presentation - sets the view (structured as 3 bytes or unstructured as 24 bit integer) of IOA (information object addresses) in the IOA column in the data points list and in the commands

Polling Interval: Interval at which the master station polls the slave station for CLASS data

Test Link Interval: Interval at which the master station sends out link test frames during inactivity

8 IEC 61850 Client

8.1 Channel Configuration

Remote IP: sets the remote IP address to connect to

Port: sets the remote TCP port to connect to

8.2 Connection Configuration

The screenshot shows the 'IEC61850 Client Configuration' window with the 'Connection Parameters' tab selected. On the left, there is a 'Channel Connection Advanced' table with several empty rows. The main area contains the following fields:

- Destination TSAP: 0
- Source TSAP: 0
- Remote AP ID: 1.1.1.999.1
- Local AP ID: 1.1.1.999
- Remote AE Qualifier: 12
- Local AE Qualifier: 12
- Remote P Selector: 1
- Local P Selector: 1
- Remote S Selector: 1
- Local S Selector: 1

At the bottom, there are buttons for 'Export Log', 'Clear Log', 'Log Pause', and a large 'Save & Apply' button.

Destination TSAP: Destination transport access point number
 Source TSAP: Source transport access point number
 Remote AP ID, Local AP ID: Local and remote Access Point ID
 Remote AE Qualifier, Local AE Qualifier:
 Remote P Selector, Local P Selector, Remote S Selector, Local S Selector: IEC 61850 / MMS connection parameters.

8.3 Advanced Configuration

The screenshot shows the 'IEC61850 Client Configuration' window with the 'Advanced Configuration' tab selected. On the left, there is a 'Channel Connection Advanced' table with several empty rows. The main area contains the following fields:

- Polling Interval (Secs): 3 (dropdown menu)
- Log list of device MMS variables:

At the bottom, there are buttons for 'Export Log', 'Clear Log', 'Log Pause', and a large 'Save & Apply' button.

Polling Interval – MMS / IEC 61850 data objects polling interval
 Log list of device MMS variables – dumps the list of variables to event log

8.4 IEC 61850 Commands

The screenshot shows the 'IEC61850 Cmds' window. On the left is a table with columns for 'Description', 'Control Command', and 'Write Data'. The main area is titled 'Control Command' and contains the following fields:

- Click to Select a Control Object in the List Above Or type in ObjRef directly:
- Device/LN.DO.attr
- Control Operation: Direct Operate (dropdown menu)
- Control Value: 0
- Send Command(s) button
- Result: (text field)

Currently Control Command and Write Data commands are supported, Select the required command in the list on the left, configure command parameters, e.g. (Object reference, Control Operation, control value, and click "Send Commands". The result of operation shall be displayed in the "Result" field

9 IEC 61850 Server

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for the IEC 61850 Server. It is divided into several sections:

- IEC61850 Server Simulator Status:** Shows link status (UP), IED Name (VestaTel), and Logical Device Name (GenericIO). It includes checkboxes for Protocol Trace, Hex Dump, and Expert, along with an Apply button.
- IEC61850 Server Simulator Configuration:** Contains a General Configuration section with fields for Local IP (0.0.0.0), Port (102), IED Name (VestaTel), and Logical Device Name (GenericIO). It also features buttons for Export Log, Clear Log, Log Pause, and Save & Apply.
- IEC61850 Server Simulator Data Points:** A table listing various data points with their values and validity.

Object Ref	Value	Validity
GenericIO/GGIO1.SPS000	0 (false)	0x0000 Good
GenericIO/GGIO1.SPS001	0 (false)	0x0000 Good
GenericIO/GGIO1.SPS002	0 (false)	0x0000 Good
GenericIO/GGIO1.SPS003	0 (false)	0x0000 Good
GenericIO/GGIO1.DPS000	0 (Intermediate)	0x0000 Good
GenericIO/GGIO1.DPS001	0 (Intermediate)	0x0000 Good
GenericIO/GGIO1.DPS002	0 (Intermediate)	0x0000 Good
GenericIO/GGIO1.DPS003	0 (Intermediate)	0x0000 Good
GenericIO/GGIO1.INS000	0	0x0000 Good
GenericIO/GGIO1.INS001	0	0x0000 Good
GenericIO/GGIO1.INS002	0	0x0000 Good
GenericIO/GGIO1.INS003	0	0x0000 Good
GenericIO/GGIO1.MV000	0	0x0000 Good
GenericIO/GGIO1.MV001	0	0x0000 Good
GenericIO/GGIO1.MV002	0	0x0000 Good
GenericIO/GGIO1.MV003	0	0x0000 Good
GenericIO/GGIO1.SPC000	0 (false)	0x0000 Good
GenericIO/GGIO1.SPC001	0 (false)	0x0000 Good
GenericIO/GGIO1.SPC002	0 (false)	0x0000 Good
GenericIO/GGIO1.SPC003	0 (false)	0x0000 Good
- Log:** A table showing system events:

Time	Level	Text
10:39:41.380	Notice	IEC61850: Server Started OK.
10:39:41.380	Notice	IEC61850S: Init OK.
10:40:17.509	Notice	IEC61850 Srv. connection established. 127.0.0.1:54887
- Data Point Control:** Fields for Data Point Address (GenericIO/GGIO1.SPS000), Data Point Type (Boolean), Data Point Value (0), and a Change Value button. It also includes a checkbox for Periodic Value Change and a Validity dropdown (0x0000 - Valid).

9.1 General Configuration

The screenshot shows the IEC61850 Server Simulator Configuration dialog box. It features a General Configuration section with the following fields:

- Local IP:** 0 . 0 . 0 . 0
- Port:** 102
- IED Name:** VestaTel
- Logical Device Name:** GenericIO

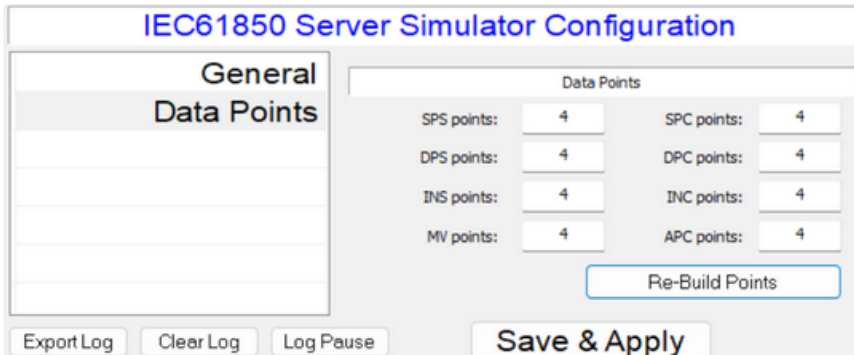
At the bottom, there are buttons for Export Log, Clear Log, Log Pause, and Save & Apply.

Local IP: sets the local IP address on which IEC 61850 server listens for incoming connections

Port: sets the local TCP port on which IEC 61850 server listens for incoming connections

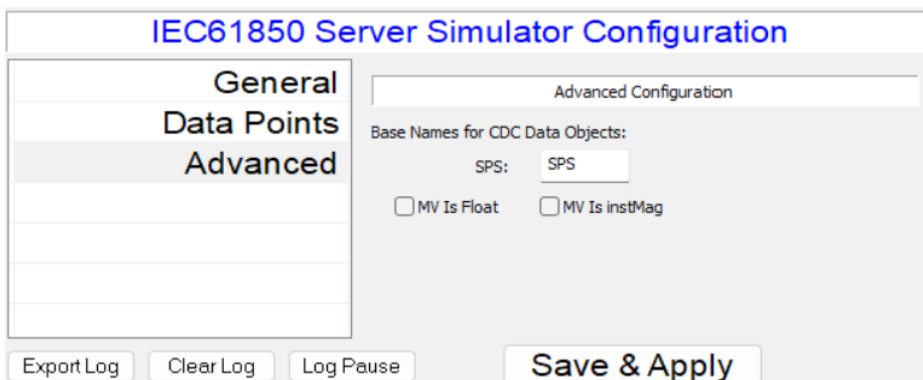
IED Name and Logical Device name are self-explanatory

9.2 Data Points Configuration



- SPS points: Sets number of Single Point Status data points
- DPS points: Sets number of Double bit Point Status data points
- INS points: Sets number of Integer Status data points
- MV points: Sets number of Measured Value data points
- SPC points: Sets number of Single Point Controllable Status data points
- DPC points: Sets number of Double bit Controllable Status data points
- INS points: Sets number of Controllable Integer Status data points
- APC points: Sets number of Controllable Analog Points

9.3 Advanced Configuration



SPS: configures the base name for SPS data objects

MV Is Float: 1=Measured values are Floats, 0=Measured values are integers

MV is instMag: Report instMag component of the measured values

10 DNP3 Master

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for the DNP3 CLIENT. It is divided into several sections:

- DNP3 Master Status:** Shows link status (UP), app layer fragments, TS segments, and DL frames. It includes a log level dropdown (Debug) and checkboxes for Protocol Trace, Hex Dump, and Expert.
- DNP3 Outstation Data Points:** A table listing data points with columns for Group, Index, Description, Var, Value, Quality, and Time.

Group	Index	Description	Var	Value	Quality	Time
32	0	Analog Input	7 (#32+flag+T)	41.093750	Online	2026.03.30 07:17:10.000
32	1	Analog Input	7 (#32+flag+T)	59.710747	Online	2026.03.30 07:17:00.000
1	0	Binary Input (1bit)	2 (+flag)	0	Online	
1	1	Binary Input (1bit)	2 (+flag)	1	Online	
10	0	Binary Output	2 (+flag)	0	Online_RS	
10	1	Binary Output	2 (+flag)	0	Online_RS	
- DNP3 Master Configuration:** A detailed configuration panel with a sidebar for Channel, Link Layer, App Layer, and Advanced. The main area includes:
 - Run As TCP Server
 - Transport: DNP3-TCP
 - Remote IP: 192 . 168 . 0 . 65
 - TCP Port: 20000
 - COM Port: COM3
 - Speed: 9600
 - Data Bits: 8
 - Parity: NONE
 - Stop bits: 1
 - Hardware Flow Control:
- Export Log:** A log window showing a series of debug messages with timestamps, levels, and text.
- DNP3 Cmds:** A list of commands including G12v1 Binary Output Command, G41 Analog Output Command, Integrity Poll, and Assign Event Class.
- Binary Output Command G12v1:** A control panel for the G12v1 command, including fields for Index (0), Control Type (Select-Operate), Qualifier (0x17 - 8 bit index), Model (PULSE), Control Value (ON - CLOSE / LATCH ON), On Time (0), Off Time (0), and Count (1).

10.1 Channel Configuration

This is a close-up view of the DNP3 Master Configuration window. It features a sidebar on the left with the following options: Channel, Link Layer, App Layer, and Advanced. The main configuration area includes:

- Run As TCP Server
- Transport: DNP3-TCP
- Remote IP: 192 . 168 . 0 . 65
- TCP Port: 20000
- COM Port: COM3
- Speed: 9600
- Data Bits: 8
- Parity: NONE
- Stop bits: 1
- Hardware Flow Control:

Buttons at the bottom include Export Log, Clear Log, Log Pause, and Save & Apply.

- Run as TCP Server: the DNP3 client accepts connections from DNP3 master – for testing of “Dual Endpoint” mode
- Transport: Selects Serial RS232 or TCP/IP transport for DNP3 protocol
- Remote IP: When TCP/IP transport is selected, sets the remote IP address
- TCP Port: When TCP/IP transport is selected, sets the remote TCP port
- COM Port: Sets the COM port number for operation over RS232
- Data Bits: Sets number of serial data bits
- Stop Bits: Sets number of serial stop bits
- Speed: Sets serial interface speed
- Parity: Sets serial interface parity

- Hardware Flow Control: Enables RTS/CTS flow control

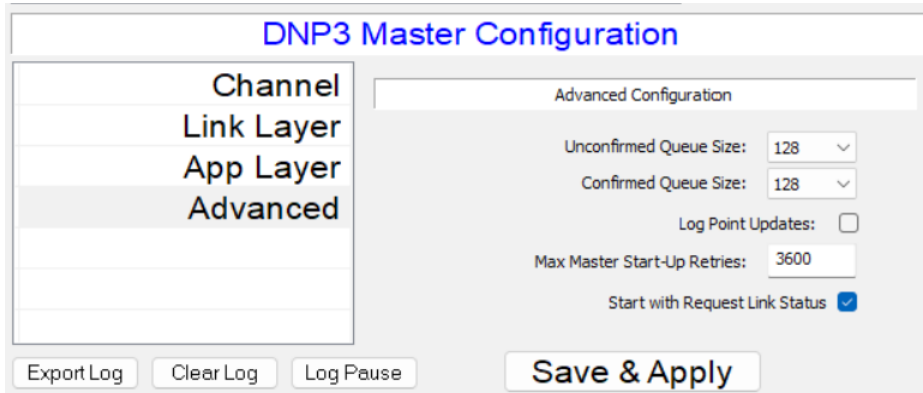
10.2 Link Configuration

- SRC ADDRESS: DNP3 link source address
- DST ADDRESS: DNP3 link destination address
- Keep Alive Interval: DNP3 link keep alive timeout
- Frame Reply Timeout: DNP3 link frame reply timeout
- Max Frame Retries: Maximum number of DNP3 link frame re-transmits
- Request Link Layer Confirmations: Enables or Disables link layer confirmations

10.3 Application Layer Configuration

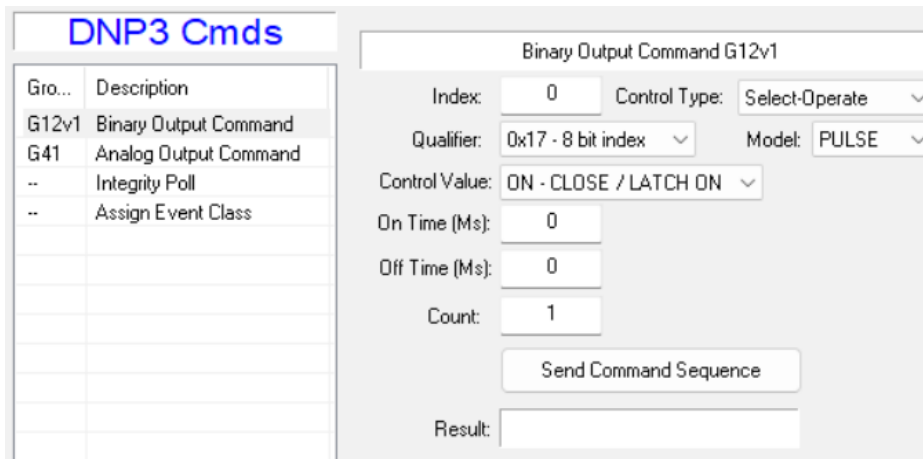
- Enable Unsol Mode: Enables or disables unsolicited response mode in the DNP3 slave
- Integrity Poll Interval: Sets interval in seconds for sending integrity poll to DNP3 slave
- Event Poll Interval: Sets interval in seconds for sending periodic event polls to DNP3 slave
- Fragment Response Timeout: Sets response timeout in seconds for receiving response fragments from DNP3 slave
- Enable Time Synchronization: Enables or disables time synchronization procedure
- Periodic Time Synchronization Interval: Sets periodic time synchronization interval in seconds, 0=periodic time synchronization off.

10.4 Advanced Configuration



- Unconfirmed Queue Size: Sets the frame queue size for unconfirmed transmit fragments
- Confirmed Queue Size: Sets the frame queue size for confirmed transmit fragments
- Log Point Updates: Enables or disables logging data point updates
- Start with Request Status of Link: when enabled Request Status of Link is the first messages sent to server
- Master startup retries: Sets the maximum number of times to re-try failed Master startup procedure

10.5 DNP3 Commands



This view contains a list of supported commands. To run a desired command, select in the the list on the left, configure the necessary fields and click “Send Command”

11 DNP3 Server

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for the DNP3 Server. It is divided into several sections:

- DNP3 Outstation Simulator Status:** Shows link status (DOWN), application fragments, transport segments, data link frames, and data link errors. It also includes a log level selector (Notice) and checkboxes for Protocol Trace, Hex Dump, and Expert.
- DNP3 Outstation Simulator Configuration:** Contains a sidebar with navigation options (Channel, Link Layer, App Layer, Data Points, Advanced) and a main configuration area. The configuration includes:
 - Transport: DNP3-TCP
 - Local IP: 0 . 0 . 0 . 0
 - TCP Port: 20000
 - COM Port: COM7
 - Speed: 9600
 - Data Bits: 8
 - Parity: NONE
 - Stop bits: 1
 - Hardware Flow Control: Disabled
- DNP3 Outstation Simulator Data Points:** A table listing various data points with their Group, Index, Description, Value, and Quality.

Group	Index	Description	Value	Quality
1	0	Binary Input (1bit)	0	OL
1	1	Binary Input (1bit)	0	OL
1	2	Binary Input (1bit)	0	OL
1	3	Binary Input (1bit)	0	OL
3	0	Binary Input (2bit)	0 (Intermediate)	OL
3	1	Binary Input (2bit)	0 (Intermediate)	OL
3	2	Binary Input (2bit)	0 (Intermediate)	OL
3	3	Binary Input (2bit)	0 (Intermediate)	OL
20	0	Counter	0	OL
20	1	Counter	0	OL
20	2	Counter	0	OL
20	3	Counter	0	OL
30	0	Analog Input	0	OL
30	1	Analog Input	0	OL
30	2	Analog Input	0	OL
30	3	Analog Input	0	OL
10	0	Binary Output	0	OL
10	1	Binary Output	0	OL
10	2	Binary Output	0	OL
10	3	Binary Output	0	OL
- Log View:** Shows a log entry at 15:16:50.896 with level Notice and text "DNP3-S App layer init OK".
- Data Point Configuration:** A panel for configuring a specific data point, showing address (Group: 1, Index: 0), type (Binary Input (1bit)), and value (0).

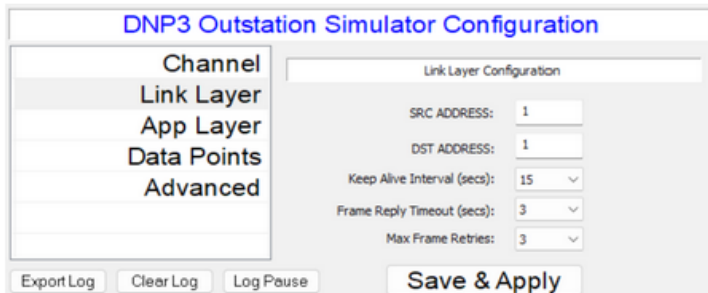
11.1 Channel Configuration

This close-up view of the Channel Configuration section shows the following settings:

- Transport: DNP3-TCP
- Local IP: 0 . 0 . 0 . 0
- TCP Port: 20000
- COM Port: COM7
- Speed: 9600
- Data Bits: 8
- Parity: NONE
- Stop bits: 1
- Hardware Flow Control: Disabled

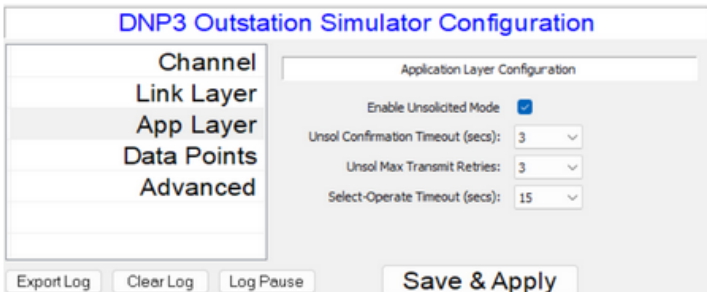
- Transport: Selects Serial RS232 or TCP/IP transport for DNP3 protocol
- Local IP: When TCP/IP transport is selected, sets the local IP address
- TCP Port: When TCP/IP transport is selected, sets the local TCP port
- COM Port: Sets the COM port number for operation over RS232
- Data Bits: Sets number of serial data bits
- Stop Bits: Sets number of serial stop bits
- Speed: Sets serial interface speed
- Parity: Sets serial interface parity
- Hardware Flow Control: Enables RTS/CTS flow control

11.2 Link Configuration



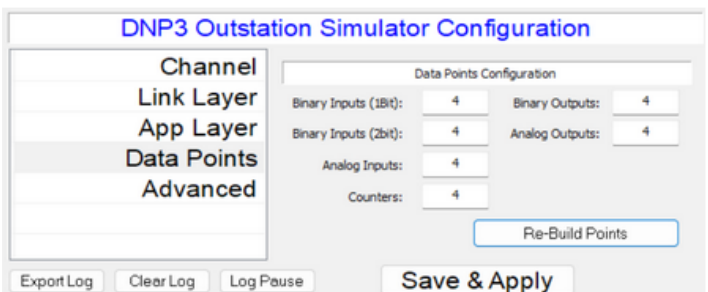
- SRC ADDRESS: DNP3 link source address
- DST ADDRESS: DNP3 link destination address
- Keep Alive Interval: DNP3 link keep alive timeout
- Frame Reply Timeout: DNP3 link frame reply timeout
- Max Frame Retries: Maximum number of DNP3 link frame re-transmits

11.3 Application Layer Configuration



- Enable Unsolicited Mode: Enables or disables Unsolicited Response Mode
- Unsol Confirmation Timeout: Timeout value for waiting for unsolicited confirmations
- Unsol Max transmit retries: Maximum number of re-transmit attempts for unsolicited mode
- Select Operate Timeout: Sets maximum time allowed between Select and Operate commands

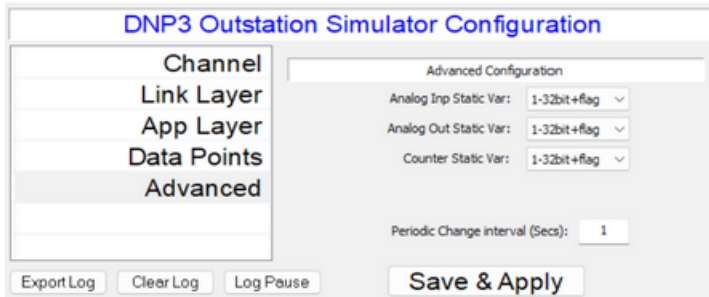
11.4 Data Points Configuration



This tab contains configuration for the number of DNP3 Slave simulator data points of different types: Binary Inputs (single and double bit), Analog Inputs, Binary Outputs and Analog Outputs.

To change the default data point setup, change the number of points as needed and click "Re-Build Points". Note that the total maximum number of data points supported is 1024.

11.5 Advanced Configuration



- Analog Inp Static Var: Sets the variation number used for static DNP3 Inputs
- Analog Out Static Var: Sets the variation number used for static DNP3 Outputs
- Counter Static Var: Sets the variation number used for static Counters
- Periodic Change Interval: Sets the interval in seconds for generating periodic change (incrementation) in the selected data points

12 Modbus Server

VestaTel SCADA Multi-Protocol Simulator :: INSTANCE 1 :: MODBUS SERVER

Tools View About

Modbus Slave Status

Link Status	DOWN
PDU RX	0
PDU TX	0
CRC Errors	0
Addr Mismatch	0
Interchar Timeout	0

Log Level: Notice

Protocol Trace

Hex Dump

Expert

Apply

Modbus Slave Data Points

Register Type	Index	Words	Register Dump	Register Value	Data Format
Discreet Input	1000	1	0x0	0	--
Discreet Input	1001	1	0x0	0	--
Discreet Input	1002	1	0x0	0	--
Discreet Input	1003	1	0x0	0	--
Holding Register	2000	1	0x0000	0	16bit Unsigned
Holding Register	2001	1	0x0000	0	16bit Unsigned
Holding Register	2002	1	0x0000	0	16bit Unsigned
Holding Register	2003	1	0x0000	0	16bit Unsigned
Holding Register	2004	2	0x0000 0000	0	32bit Unsigned BE
Holding Register	2006	2	0x0000 0000	0	32bit Unsigned BE
Holding Register	2008	4	0x0000 0000 0000 0000	0	64bit Unsigned BE
Holding Register	2012	4	0x0000 0000 0000 0000	0	64bit Unsigned BE
Input Register	3000	1	0x0000	0	16bit Unsigned
Input Register	3001	1	0x0000	0	16bit Unsigned
Input Register	3002	2	0x0000 0000	0	32bit Unsigned BE
Coil	4000	1	0x0	0	--
Coil	4001	1	0x0	0	--
Coil	4002	1	0x0	0	--

Modbus Slave Configuration

Channel

Link Layer

Data Points

Advanced

Channel Configuration

Transport: Modbus-TCP TCP Port: 502

Local IP: 0 . 0 . 0 . 0

COM Port: COM3 Speed: 9600

Data Bits: 8 Parity: NONE

Stop bits: 1 Hardware Flow Control

Export Log Clear Log Log Pause Save & Apply Compact / Full View

Time	Level	Text
09:56:43.716	Notice	MODBUS-S App layer init OK

Data Point Address: 1000

Data Point Type: Discreet Input

Data Point Value: 0 Change Value

Binary (0..1)

Disable

Periodic Value Change Data Format: --

12.1 Channel Configuration

Modbus Slave Configuration

Channel

Link Layer

Data Points

Advanced

Channel Configuration

Transport: Modbus-TCP TCP Port: 502

Local IP: 0 . 0 . 0 . 0

COM Port: COM3 Speed: 9600

Data Bits: 8 Parity: NONE

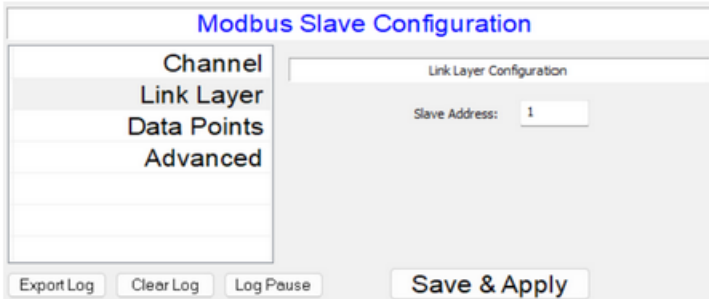
Stop bits: 1 Hardware Flow Control

Export Log Clear Log Log Pause Save & Apply

- Transport: Selects Seral RS232 or TCP/IP transport for Protocol protocol
- Local IP: When TCP/IP transport is selected, sets the local IP address
- TCP Port: When TCP/IP transport is selected, sets the local TCP port
- COM Port: Sets the COM port number for operation over RS232
- Data Bits: Sets number of serial data bits
- Stop Bits: Sets number of serial stop bits
- Speed: Sets serial interface speed

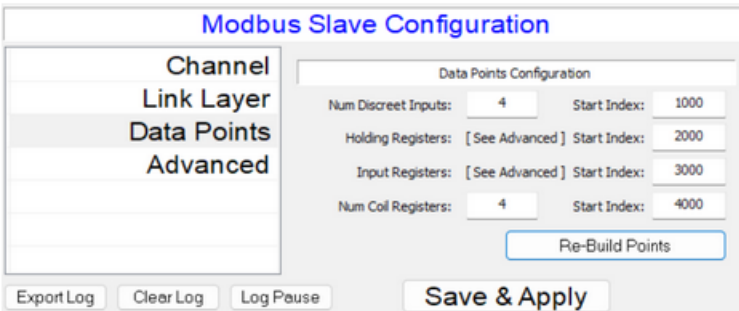
- Parity: Sets serial interface parity
- Hardware Flow Control: Enables RTS/CTS flow control

12.2 Link Configuration



Slave Address: Sets the Modbus slave address

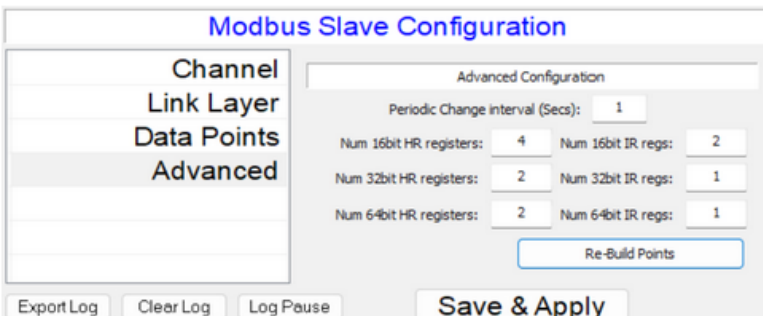
12.3 Data Points Configuration



This configuration tab contains the configuration fields that define the number of Modbus data points emulated in Modbus slave simulator mode by the application

Set the required number of registers of each type and their start index and click Re-Build Points when done. The total number of points supported is 1024

12.4 Advanced Configuration

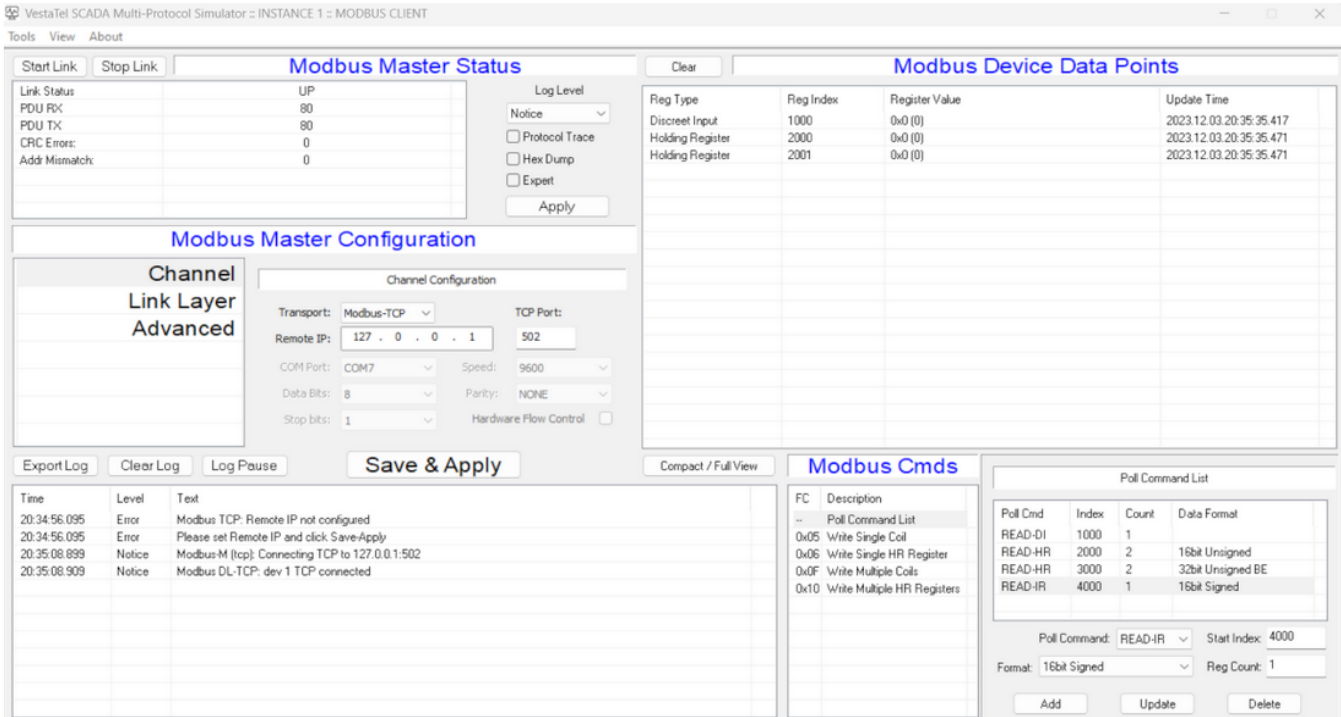


This configuration tab contains the configuration fields that define the number of Modbus data points and specific data formats of HR and IR registers emulated in Modbus slave simulator mode by the application

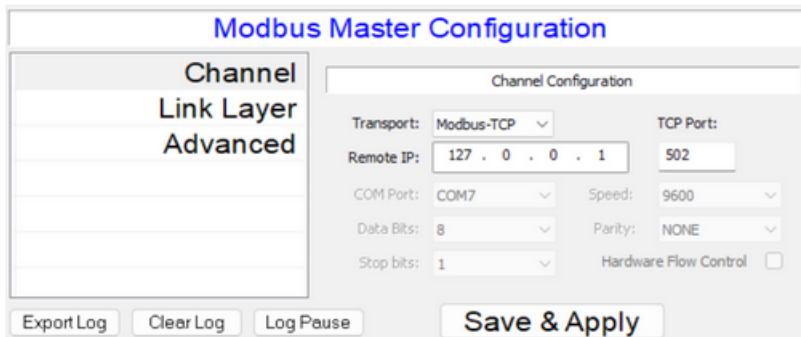
16, 32 and 64 bit sized registers can be defined here. Once defined the format can be further changed for each register in the data points list as signed, unsigned, little Endian, big Endian, integer or float, etc.

Set the required number of registers of each type and their start index and click Re-Build Points when done. The total number of points supported is 1024

13 Modbus Client

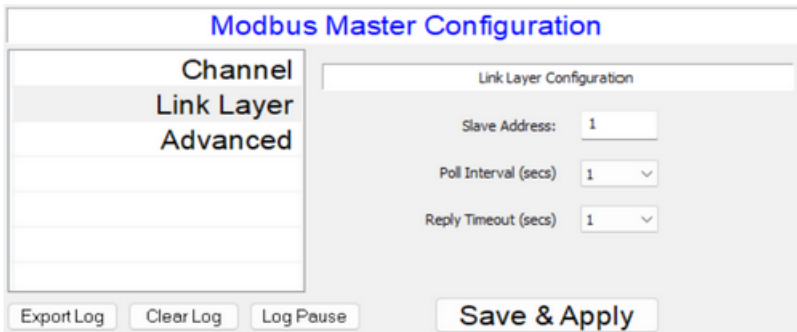


13.1 Channel Configuration



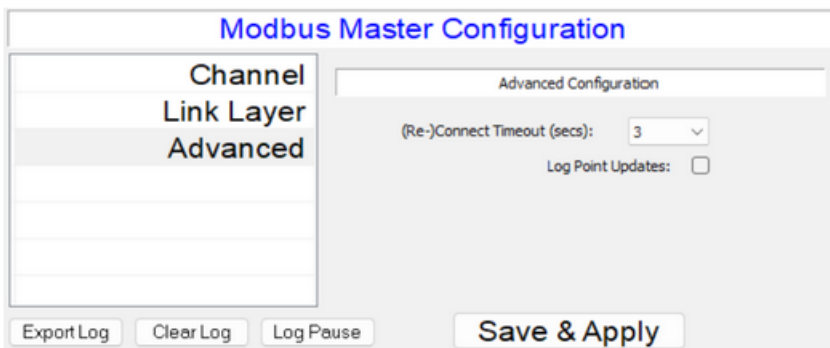
- **Transport:** Selects Serial RS232 or TCP/IP transport for Modbus protocol
- **Remote IP:** When TCP/IP transport is selected, sets the remote IP address
- **TCP Port:** When TCP/IP transport is selected, sets the remote TCP port
- **COM Port:** Sets the COM port number for operation over RS232
- **Data Bits:** Sets number of serial data bits
- **Stop Bits:** Sets number of serial stop bits
- **Speed:** Sets serial interface speed
- **Parity:** Sets serial interface parity
- **Hardware Flow Control:** Enables RTS/CTS flow control

13.2 Link Configuration



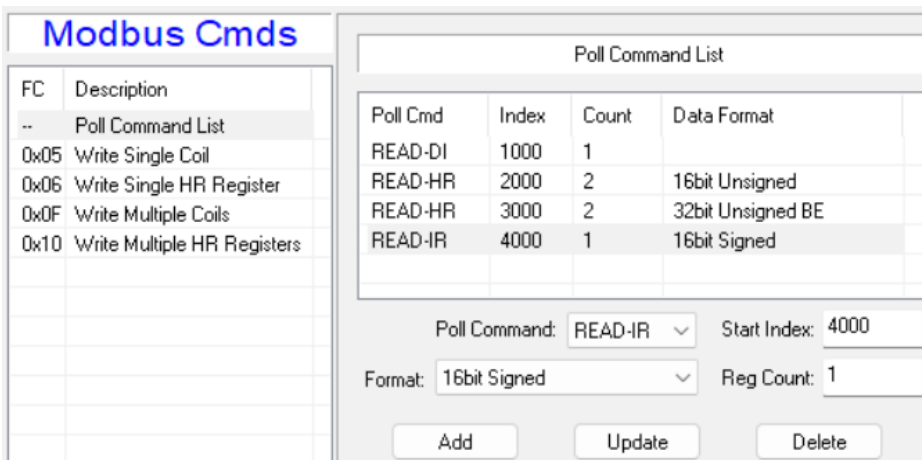
- Slave Address: Sets the Modbus slave address
- Poll interval: Sets the slave polling interval in seconds
- Reply Timeout: Sets the reply timeout in seconds

13.3 Advanced Configuration



- Re-Connect timeout: Sets TCP or serial re-connect timeout in seconds
- Log point updates: Enables or disables logging of data point updates

13.4 Modbus Commands



This window is used to build a polled command list – a series of polled command that are periodically sent to the modbus server to poll it for data. Select Poll Command List on the left, then use Add, Update, Delete buttons on the right to build the poll list. Use Poll Command, Format, Reg Count, and Start Index fields to setup each poll command.

This view is also used to select and set Write commands to the modbus server (Coils and HR registers)

14 HART Master

The screenshot displays the VestaTel SCADA Multi-Protocol Simulator interface for the HART Master. It is divided into several sections:

- HART Master Status:** Shows Link Status (UP) and Log Level (Debug). It includes checkboxes for Protocol Trace, Hex Dump, and Expert, along with an Apply button.
- HART Master Configuration:** Contains a General Polling section and a Polling Configuration section. The Polling Configuration section lists HART Device Addresses to poll (0-15) with checkboxes. Dev Addr 0 and 1 are selected.
- HART Device Data Points:** A table showing Slave Addr, Var Type, Variable Value, and Update Time for various variables.
- Log Window:** Displays a list of log entries with Time, Level, and Text.

Slave Addr	Var Type	Variable Value	Update Time
0	PV (Primary Variable)	1.124000	2024.01.11.19:39:52.534
0	SV (Secondary Variable)	2.456000	2024.01.11.19:39:52.534
0	TV (Tertiary Variable)	3.789000	2024.01.11.19:39:52.534
0	QV (Quaternary Variable)	4.000000	2024.01.11.19:39:52.534
1	PV (Primary Variable)	11.111111	2024.01.11.19:39:53.588
1	SV (Secondary Variable)	11.222222	2024.01.11.19:39:53.588
1	TV (Tertiary Variable)	11.333333	2024.01.11.19:39:53.588
1	QV (Quaternary Variable)	11.444444	2024.01.11.19:39:53.588

14.1 General Configuration

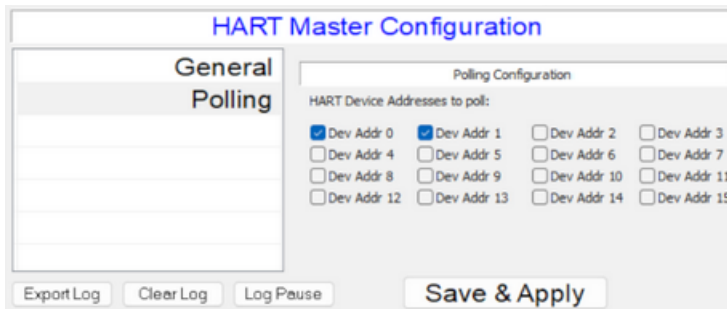
The HART Master Configuration dialog box is shown, focusing on the General Configuration section. The settings are as follows:

- COM Port: COM3
- Speed: 1200
- Data Bits: 8
- Parity: ODD
- Stop bits: 1
- Hardware Flow Control:
- Poll Interval (secs): 3
- Reply Timeout (secs): 2
- Max Poll Retries: 2

- **COM Port:** Sets the COM port number for operation over RS232
- **Data Bits:** Sets number of serial data bits

- Stop Bits: Sets number of serial stop bits
- Speed: Sets serial interface speed
- Parity: Sets serial interface parity
- Hardware Flow Control: Enables RTS/CTS flow control
- Poll Interval: Sets the device polling interval
- Reply timeout: Sets the maximum time to wait for poll reply
- Max poll retries: Sets the maximum number of times to retries polling

14.2 Polling Configuration



Dev Addr 0 to 15 – Configures the set of device addresses to poll

15 Event Log

Time	Level	Text
10:41:06.043	Debug	Dst:1024 Src:1 DIR:Control Primary FCB:0 FCV/DFC:0 FC:4
10:41:06.043	Debug	AC: FIN,FIR,SEQ=3 FC: CONFIRM
10:41:09.057	Debug	DNP3M DL TX (14): Unconfirmed User Data
10:41:09.057	Debug	Dst:1024 Src:1 DIR:Control Primary FCB:0 FCV/DFC:0 FC:4
10:41:09.057	Debug	AC: FIN,FIR,SEQ=4 FC: READ
10:41:09.061	Debug	DNP3M DL RX (49): Unconfirmed User Data
10:41:09.061	Debug	Dst:1 Src:1024 DIR:Monitor Primary FCB:0 FCV/DFC:0 FC:4
10:41:09.061	Debug	AC: FIN,FIR,CON,SEQ=4 FC: RESPONSE
10:41:09.061	Debug	DNP3M DL TX (5): Unconfirmed User Data
10:41:09.061	Debug	Dst:1024 Src:1 DIR:Control Primary FCB:0 FCV/DFC:0 FC:4
10:41:09.061	Debug	AC: FIN,FIR,SEQ=4 FC: CONFIRM
10:41:12.073	Debug	DNP3M DL TX (14): Unconfirmed User Data

This view area displays the event log which holds protocol transmit / receive messages and internal software events
Control buttons:

- Export Log: exports the content of the log to a text file
- Clear Log: clears the content of the log
- Pause Log: temporarily pauses logging
- Log Resume: resumes logging
- Compact / Full view: toggles the application windows from "Tall mode" where more of the event log is shown or "compact mode" (default)

The log severity and what is exactly logged in the the event log is controlled in the main screen area group of controls shown below

VestaTel SCADA Multi-Protocol Simulator :: INSTANCE 0 :: DNP3 CLIENT

Tools View About

DNP3 Master Status

Link Status	UP
App Layer Frags	RX 27690/TX 52156/Timeouts 0
TS Segments	RX 27765/TX 52156
DL Frames	RX 27769/TX 52161/CRC Errs 0

Log Level

Debug ▼

Protocol Trace

Hex Dump

Expert

Apply

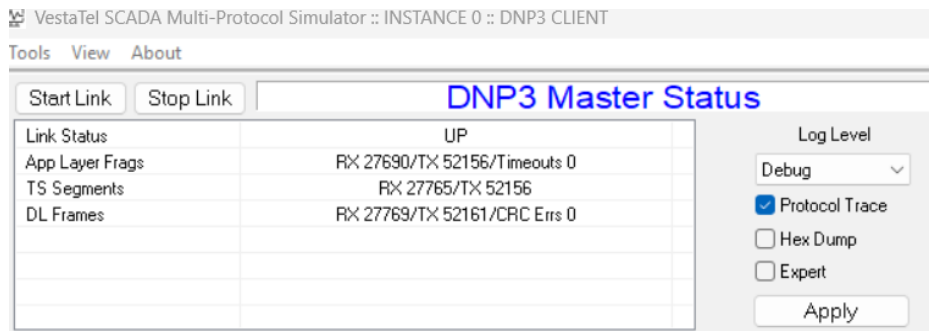
Log level: selects the maximum displayed severity

Protocol trace: log protocol decoded messages into event log

Hex Dump: logs the hex dump of received and transmitted protocol messages

Expert: maximum level of logging (system internal events, state transitions, etc)

16 Diagnostic Counters



This area of the program screen displays various protocol diagnostic counters that get updated during the operation, the content of the view changes depending on selected protocol.

17 Automation Features

There are two automation features that may be useful in testing that SCADA Multi-Protocol Simulator supports:

17.1 Running multiple instances from a script

It is possible to launch multiple instances of the simulator application in server or client mode from a Windows bat file (script). An example script called multiserv.bat is provided with the installation (which by default can be found in [c:\VestaTel-Scadasim](#) folder).

Currently running up to :

- 100 instances simultaneously is supported when running under Professional License
- 10 instances are supported for Trial / Evaluation mode
- 4 Instances are supported for Personal License

Example multiserv.bat starts 100 instances giving the base TCP listening port 2404 which increments for each instance.

A prepared base configuration file (IEC104 server mode) should be located in the running directory (scada-sim.cfg).

You can use the following procedure:

1. Start the application normally and select the required protocol, click save apply – that will be your base configuration
In case of IEC104 the TCP server port is 2404 which shall be your base TCP listening port
2. Copy cfgX/scada-sim.cfg .. (X depends on which instance was started, could be 0, 1 etc.)
3. Edit multiserv.bat for your needs – adjust N to the number of instances required, etc.
4. Run multiserv.bat from command line (cmd.exe) – you must be in the working folder (C:\VestaTel-Scadasim)

Content of multiserv.bat:

```
@echo off
setlocal enabledelayedexpansion

REM === USER CONFIGURATION ===
set N=100
set BASE_CFG=scada-sim.cfg
set EXE=scadasim.exe
set BASE_PORT=2404
```

```

set DELAY_SEC=1

for /L %%i in (0,1,%N%-1) do (

set CFG_DIR=cfg%%i

if not exist "!CFG_DIR!" (
    mkdir "!CFG_DIR!"
)

copy /Y "%BASE_CFG%" "!CFG_DIR!\%BASE_CFG%" >nul

set /A PORT=%BASE_PORT% + %%i

echo Launching instance %%i on port !PORT! ...

start "" "%EXE%" ^
    -i %%i ^
    -p !PORT!

REM === Delay between launches ===
timeout /t %DELAY_SEC% /nobreak >nul

)

echo All instances launched.
    
```

The multiserv.bat calls the scadasim.exe in "batch mode" passing the command line arguments to it. The following command line arguments are supported:

Argument	Examples	Comment
-i <instance number>	scadasim.exe -i 0 scadasim.exe -i 56	Causes the application to run a specific instance (numbered from 0 to Max)

		where Max is 100 for Professional license, 4 for the Personal License and 10 for Evaluation / Trial mode.
- p <TCP port>	scadasim.exe -i 3 -p 2404 scadasim.exe -i 4 -p 2405 scadasim.exe -i 5 -p 2406	Override the TCP listening port in configuration with the given port If the base configuration file is a SCADA Master / Client, then this is a remote TCP port
-l <IP address>	scadasim.exe -i 3 -p 2404 -l 0.0.0.0	This allows binding the instance to a specific local IP address or in case of the client, this overrides the configured remote IP address.

17.2 Command line interface

While running, VestaTel SCADA Multi-Protocol Simulator supports accepting commands from a command line application called simcmd.exe (found in the installation directory).

Command syntax: simcmd.exe <arguments>

Currently the following commands arguments are supported:

- i <instance> - directs the command to a specific running instance of the application
- c <command> - send the command to the specified running instance

Currently <command> must be in the following format:

setpoint:ix=<point index>;val=value

This command changes the data point value of the application running in server mode. Point index starts from 0 and runs to the last data point displayed in the application data points window.

Examples:

```

Git CMD
c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=0;val=0
Sending to Instance 1, cmd [setpoint:ix=0;val=0]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=4;val=1
Sending to Instance 1, cmd [setpoint:ix=4;val=1]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=4;val=2
Sending to Instance 1, cmd [setpoint:ix=4;val=2]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=4;val=3
Sending to Instance 1, cmd [setpoint:ix=4;val=3]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=8;val=10
Sending to Instance 1, cmd [setpoint:ix=8;val=10]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=16;val=123
Sending to Instance 1, cmd [setpoint:ix=16;val=123]
OK

c:\VestaTel-Scadasim>simcmd.exe -i 1 -c setpoint:ix=24;val=123.5
Sending to Instance 1, cmd [setpoint:ix=24;val=123.5]
OK

c:\VestaTel-Scadasim>
    
```

18 VENDOR INFORMATION

Developed by VestaTel

www.vestatel.eu

info@vestatel.eu

Registered in Poland

NIP: 6040233038

REGON: 522919182