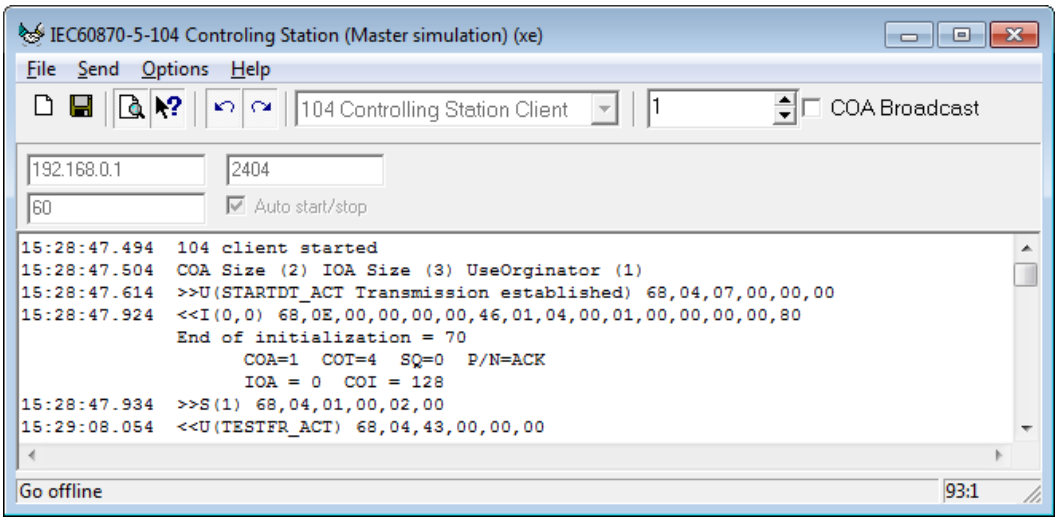
IEC60870 Controlling Station Simulation

IEC60870TT

Brodersen Test Tool for

IEC60870-5-101 and IEC60870-5-104 protocols

Version 2.60



Brodersen A/S, Islevdalvej 187, DK-2610 Roedovre, Denmark Tel: +45 45 35 26 27, Fax: +45 45 35 26 29, Email: 1
mail: sales@brodersen.com web: www.brodersen.com

Table of Contents

Introduction

The IEC60870 Master Simulator is a PC program that is used to test the IEC60870 protocol. It can run as 101 or 104 controlling station. The main usage of this simulator is to test communication against Brodersen RTU870 or Brodersen RTU32 running as 101 or 104 controlled stations.

The installation program installs the simulator and this PDF document into the Windows Start menu.

The Main Window

Following windows commands (controls and buttons) are available for both 101 and 104 protocols.

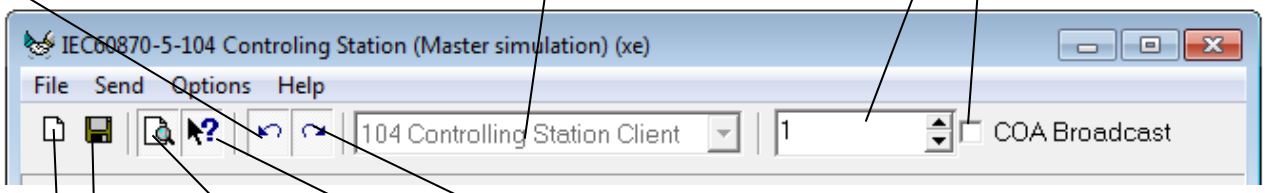
Go Online / Go Offline
When this button is pressed down, the simulator will attempt to connect to the RTU using the selected protocol.

When the simulator is online then the **Send** menu is enabled to send commands to the slave.

Protocol Selection
Selection between:
- 101 Master protocol
- 104 Client protocol
- 101 Sniffer

Common Address of ASDU or COA used by the send commands

Use COA broadcast address 0xFF or 0xFFFF



Show Link Transfer / Hide Link Transfer
When this button is down, all link layer transfer will be displayed in the message window together with the application layer.

Hide Frame Errors
Frame errors will not be shown in the message window when this button is pressed.

Save (Ctrl+S)
Save the messages to a text file.

New (Ctrl+N)
Used to clear the message window. It is also possible to right click the message window and select Clear

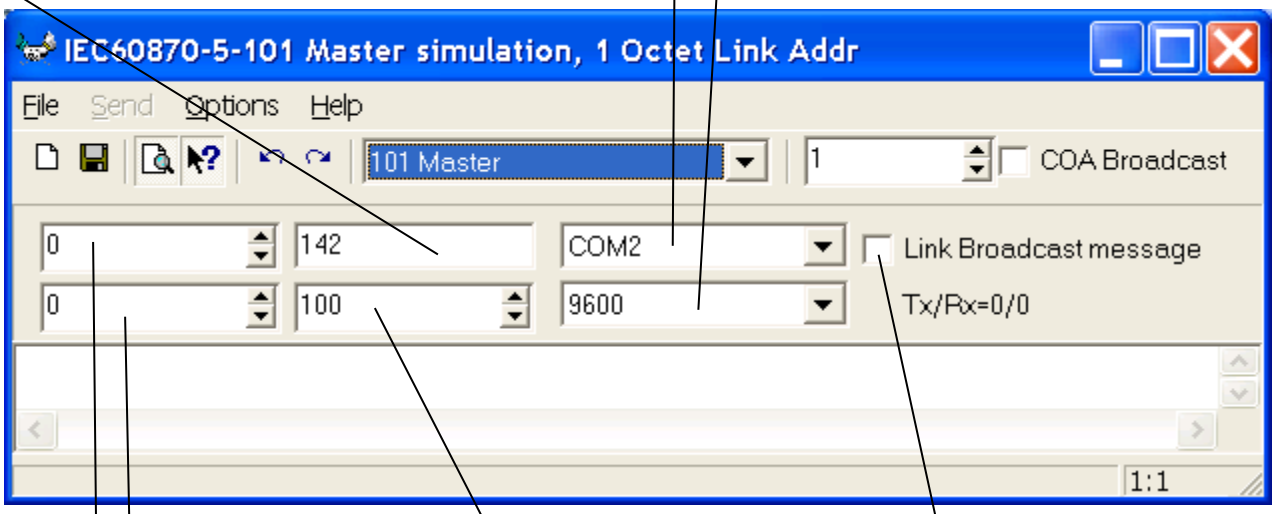
Lock View on Last Message. When pressed the message window will auto scroll down.

The Main Window in 101 Master mode

Slaves to Scan
It is possible to scan more than one slave by separting the Slave numbers with comma (,) e.g. 1,5,7. However it is not possible to send commands when more than one slave is scanned.

COMport to be used
Select a comport on your PC.

Baurate Settings for COMport



Trailing RTS Time
Leading and trailing RTS time are used in multidrop RS485 communication

Leading RTS Time
Leading and trailing RTS time are used in multidrop RS485communication

Read/Write turnover time (ms)
Sleep time before next request is sent after receiving last frame. Normally used in RS485 communication.

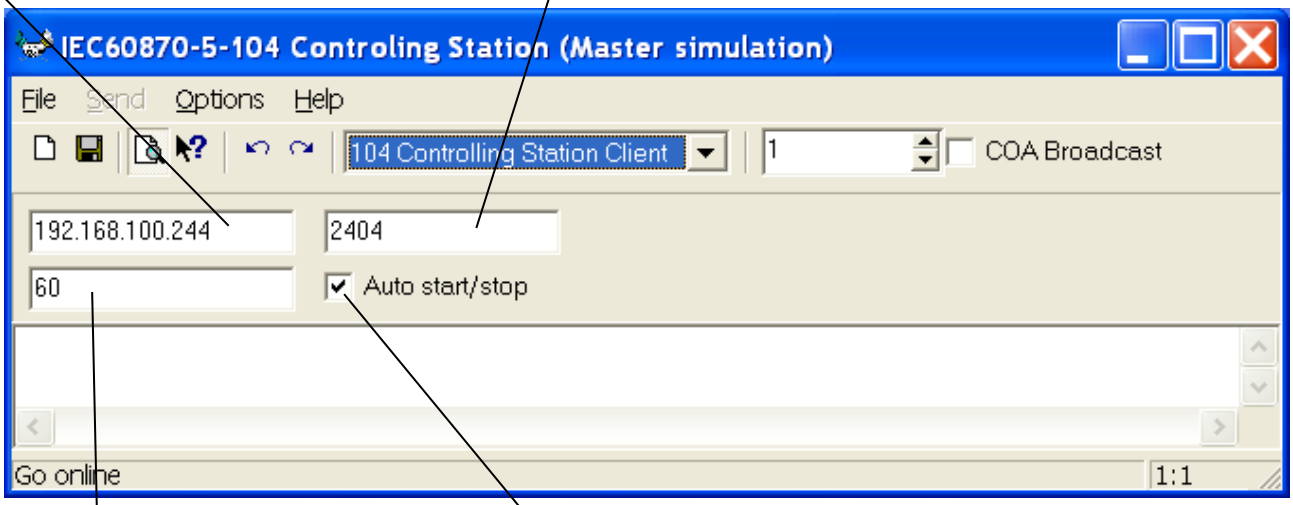
Broadcast Next Message

Link level broadcast for testing purpose.

The Main Window in 104 Controlling Station (Client) mode

IP or URL address
Here you enter the IP address of the controlled station you want to access.

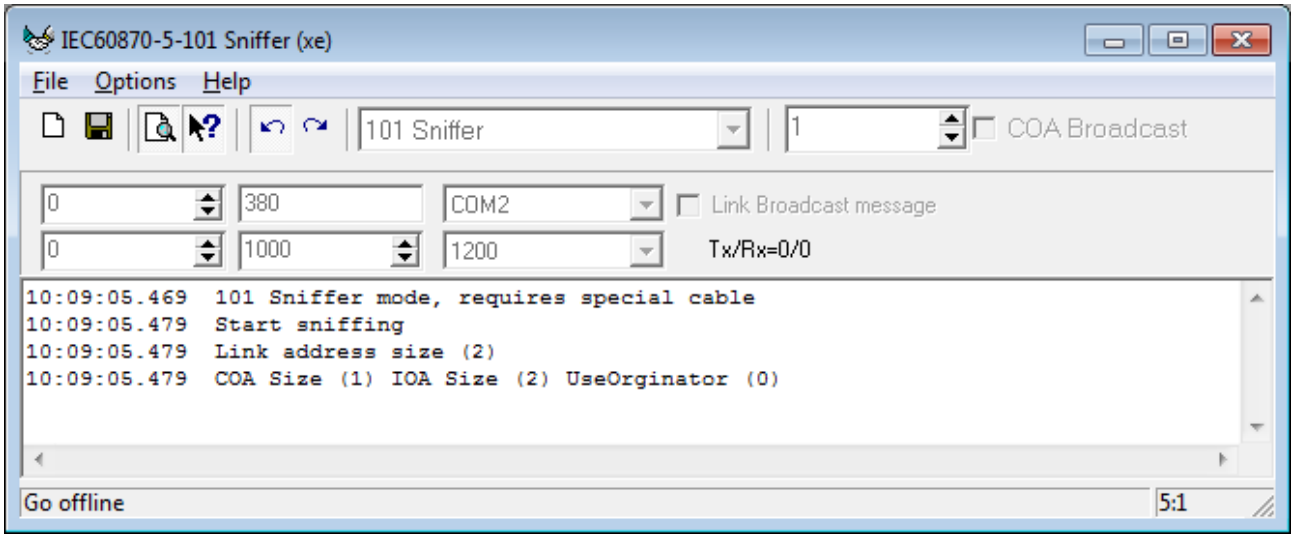
IP port number
The standard specifies port 2404 to be used.



Im a live timeout in seconds for (TESTFR)
TESTFR are sent when no other communication is active on then link to keep the link open.

Auto start/stop
Used to control if the link should be active or inactive when connected.
When checked the master simulator will automatically send STARTDT_ACT when connecting to the controlled station to request active connection and when disconnecting STOPDT_ACT will be sent.
If not checked then an inactive connection will be made and STARTDT_ACT / STOPDT_ACT can be sent from the **Send** menu.

The Main Window in 101 Sniffer mode

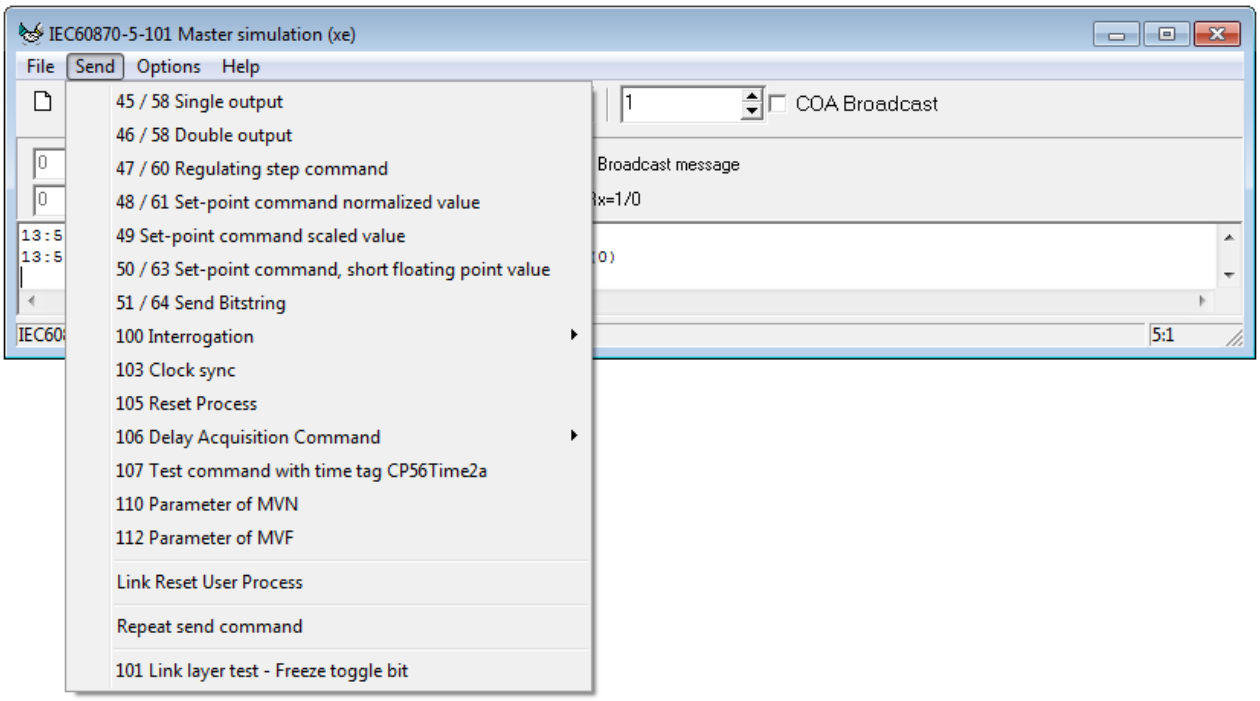


The test tool can run in a sniffer mode where it only listen and displays to what is sent on the specified COM port. This mode requires a cable where the transmit signals of both the master and server are redirected to the receive line on the sniffer computer. When in sniffer mode nothing is sent from the test tool.

The Send Menu for the IEC60870-5-101 protocol

When Master Simulator is online and connected to a Controlled Station the send menu can be used to send commands and parameters.

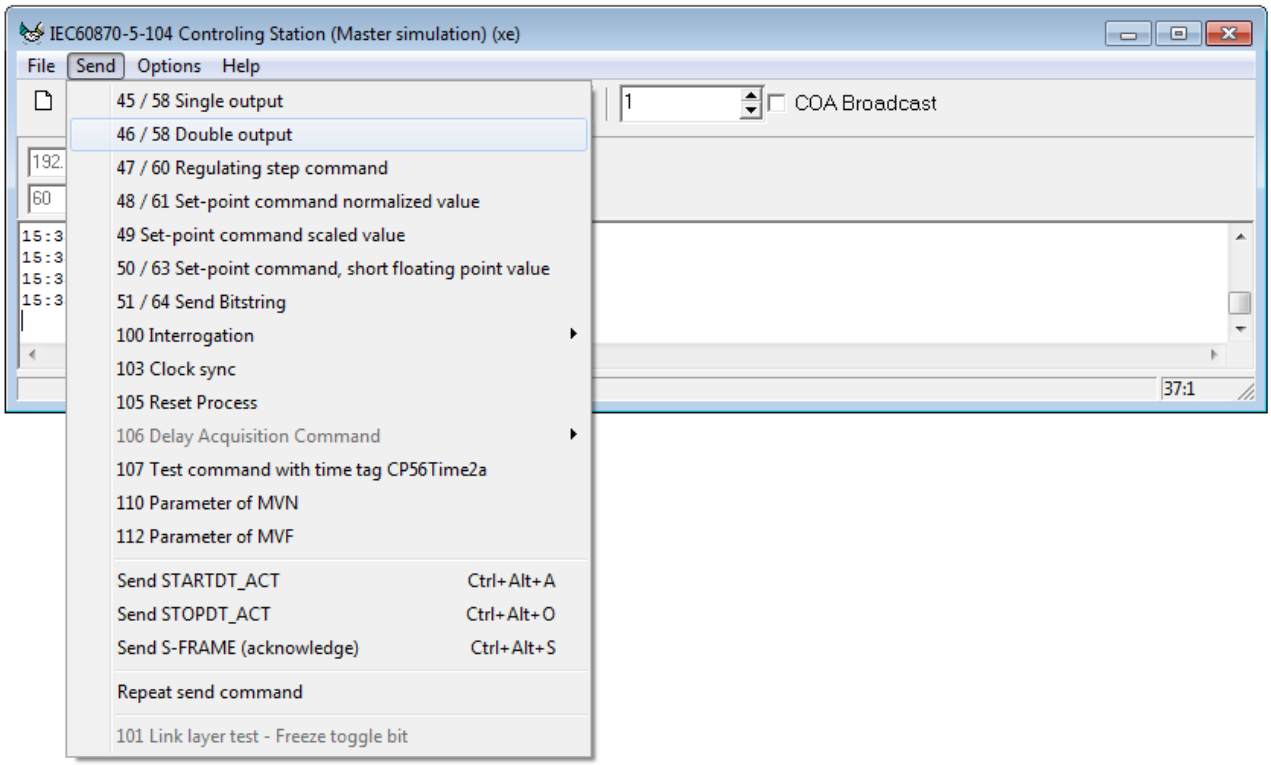
Send Menu for the 101 protocol simulation is shown below:



Link Reset User Process is only available in the 101 protocol. This send command will send the *Reset of user process* command number 1 to the slave.

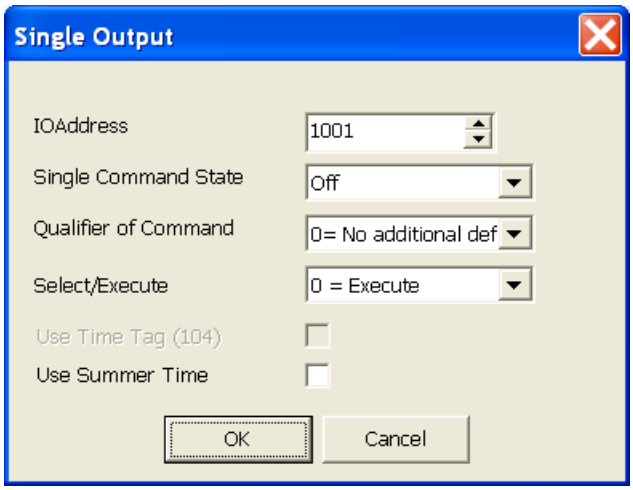
The Send Menu for the IEC60870-5-104 protocol

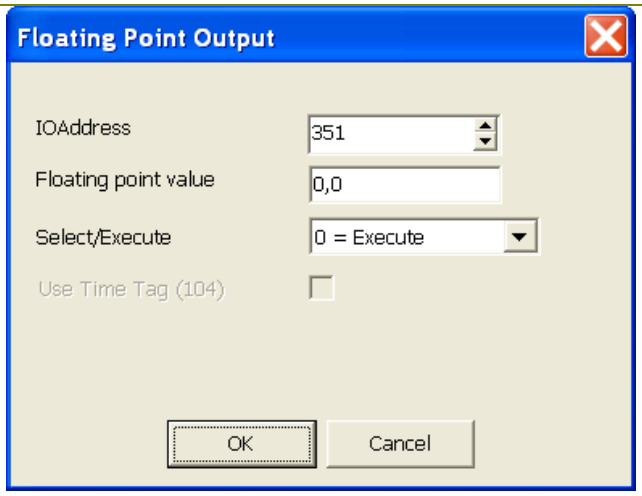
Send Menu for the 104 protocol simulation is shown below:



Send STARTDT_ACT / STOPDT_ACT / S-FRAME (acknowledge) are only available in the 104 protocol. They are primarily used when testing redundant connections to a 104 controlled station.

Many of the **Send** commands will display a small dialog box were all needed parameters for the actual command can be entered. Below are some of the dialog boxes shown e.g. single output (or command) and floating point setpoint.

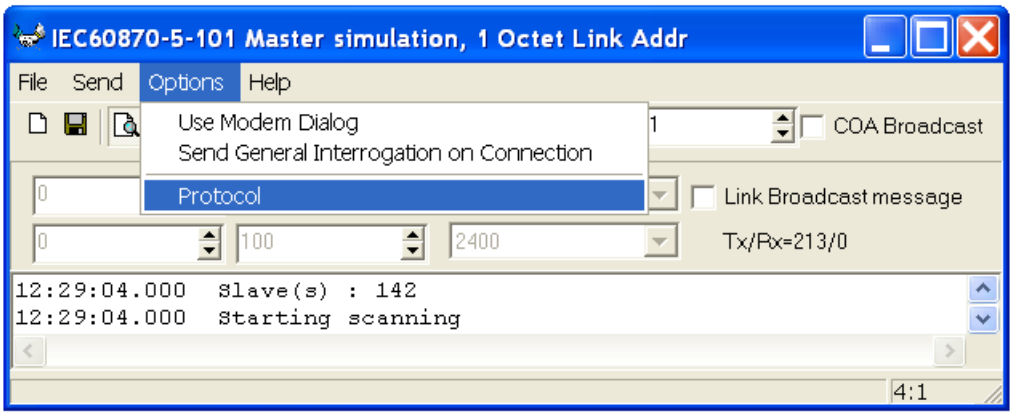




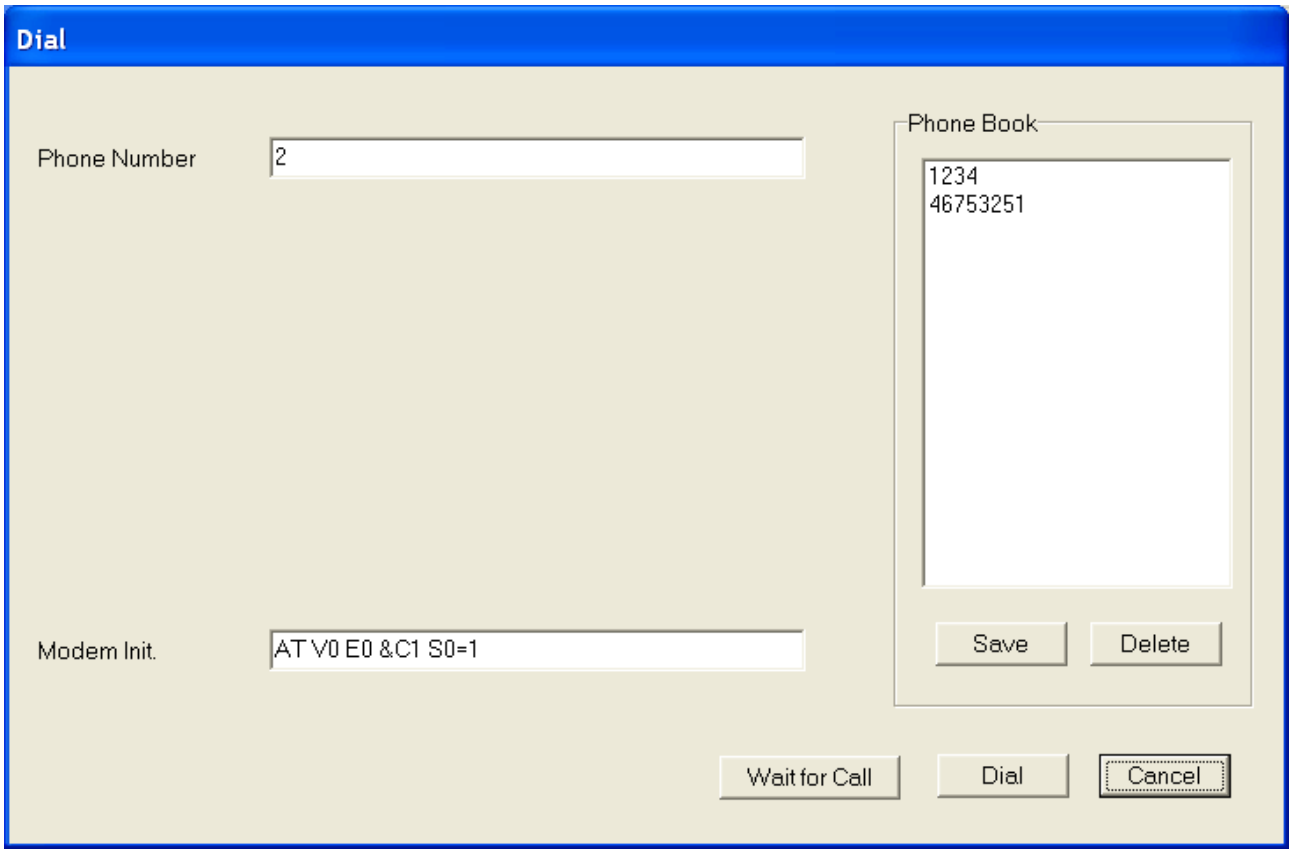
The Options Menu

The **Option** menu has three menu items:

- **Use Modem Dialog**
  - If this menu item is enabled then a dialog box with dial options and phone book will be displayed before a connection to a 101 slave is attempted via modem.
- **Send General Interrogation on Connection**
  - If this menu item is enabled then every time a new connection to controlled station is started a General Interrogation command=100 is sent to the controlled station.
- **Protocol**
  - This menu item opens a dialog box where some protocol options parameters can be entered.



The Options | Modem Dialog

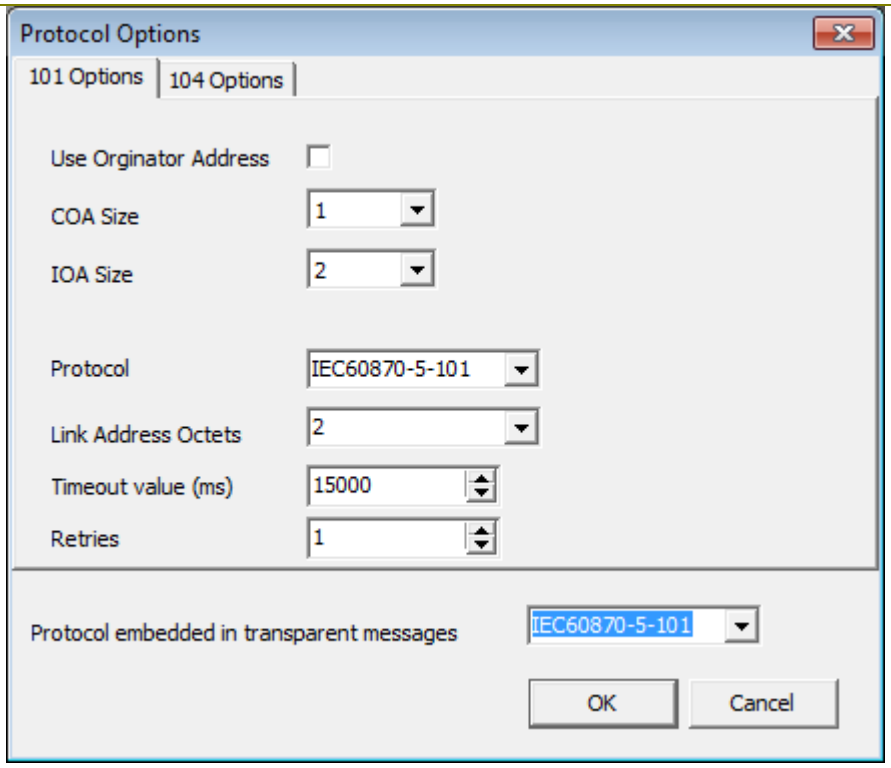


This dialog menu will pop up when you press the **Go online** button and the menu item **Options | Use Modem Dialog** is enabled.

The **Dial** button will initiate the modem using the Modem Init string and the dial the entered number.

The **Wait for Call** button will initiate the modem using the Modem Init string and then go into wait loop and wait for an RTU to dial in.

The Options | Protocol Menu | 101 Options



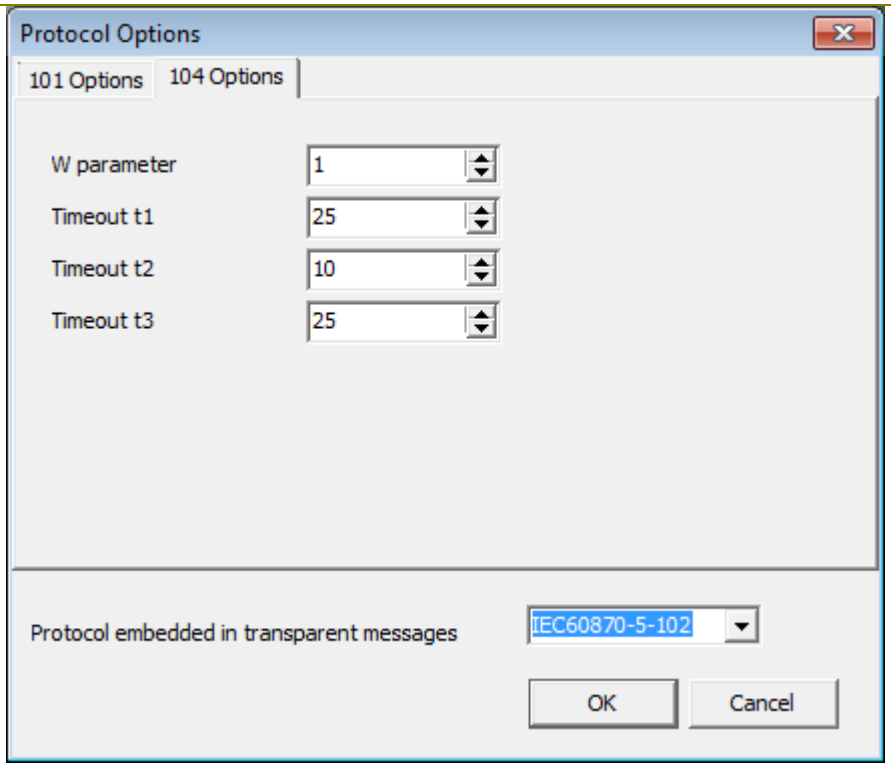
This dialog box allows you to adjust the different address sizes used in the 101 protocol. The sizes entered here must apply to the sizes programmed in the RTU.

The **Protocol** option should normally be IEC60870-5-101.

Brodersen Systems has implemented transparent message type in the private range in some of its RTUs. The option **Protocol embedded in transparent messages** can control how the simulator should display these transparent messages.

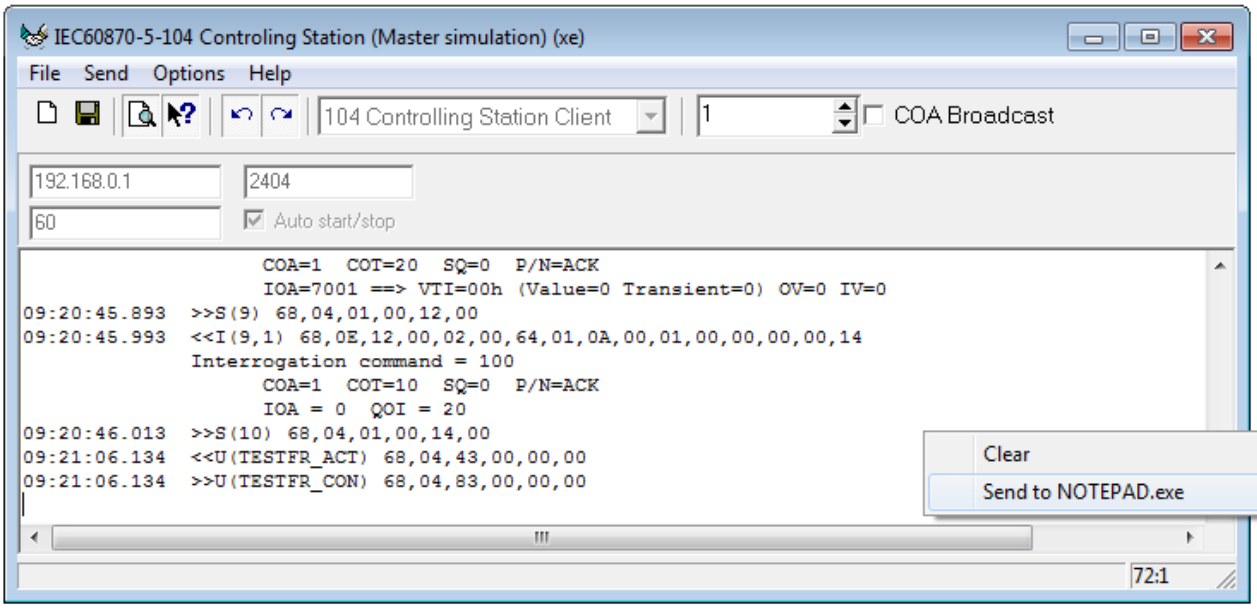
The Options | Protocol Menu | 104 Options

This dialog box allows you to adjust the different parameters and timeouts used in the 104 protocol. The timeouts and parameters entered here must apply to what is programmed in the RTU.



The Message window

The message window shows all messages transmitted and received by the simulator.

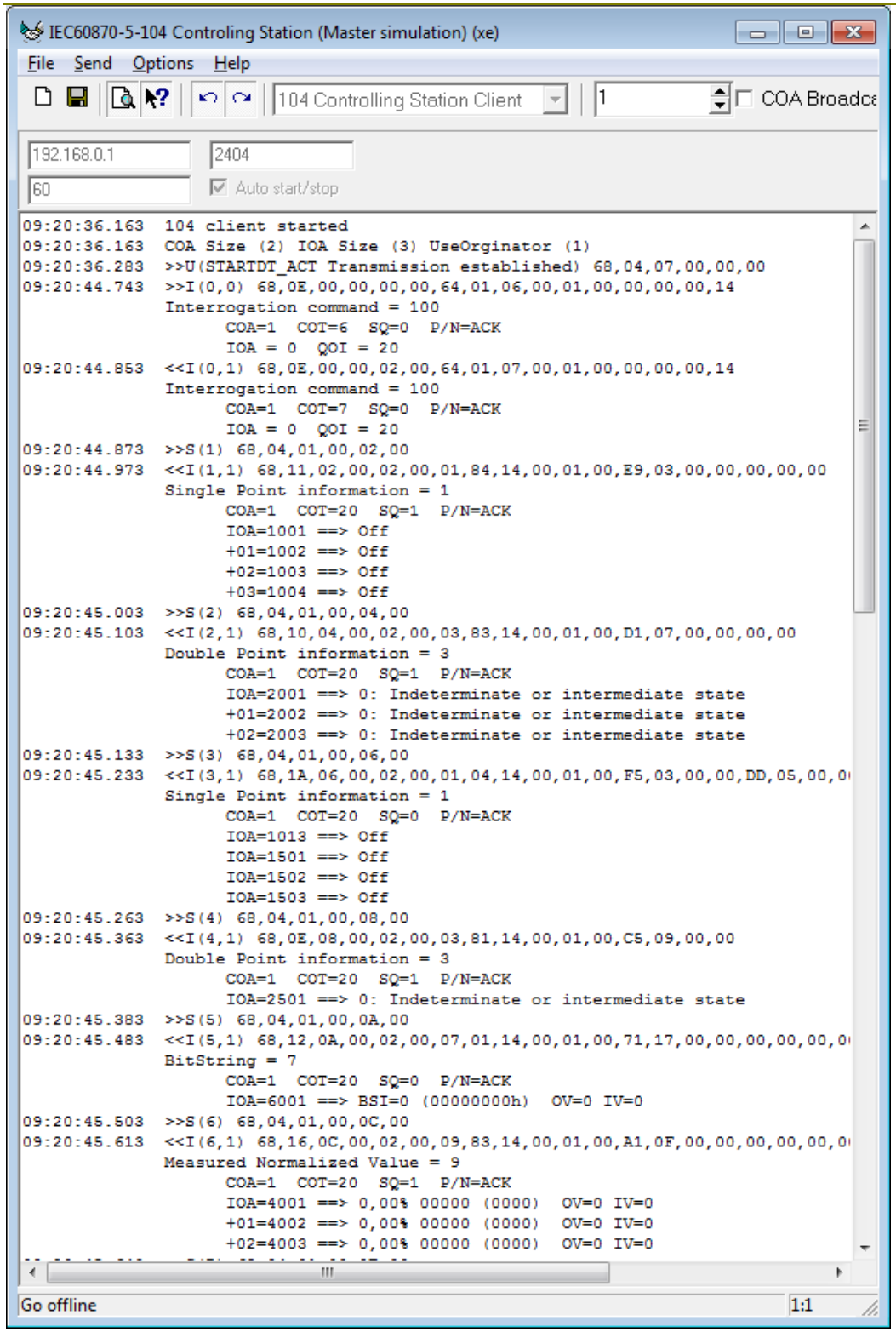


If you right click the message window then a small menu appears where you can choose:

- to clear the message window and discard all messages
- or send all the messages to NOTEPAD

Getting a snapshot into NOTEPAD gives you an option to save the messages to a file, print them and make a search for specific messages.

Below is an example of message window containing some different messages.


IEC60870-5-104 Controling Station (Master simulation) (xe)
File Send Options Help
104 Controlling Station Client
1
COA Broadca
192.168.0.1
2404
60
Auto start/stop
09:20:36.163 104 client started
09:20:36.163 COA Size (2) IOA Size (3) UseOrginator (1)
09:20:36.283 >>U(STARTDT_ACT Transmission established) 68,04,07,00,00,00
09:20:44.743 >>I(0,0) 68,0E,00,00,00,00,64,01,06,00,01,00,00,00,00,14
Interrogation command = 100
COA=1 COT=6 SQ=0 P/N=ACK
IOA = 0 QOI = 20
09:20:44.853 <<I(0,1) 68,0E,00,00,02,00,64,01,07,00,01,00,00,00,00,14
Interrogation command = 100
COA=1 COT=7 SQ=0 P/N=ACK
IOA = 0 QOI = 20
09:20:44.873 >>S(1) 68,04,01,00,02,00
09:20:44.973 <<I(1,1) 68,11,02,00,02,00,01,84,14,00,01,00,E9,03,00,00,00,00,00
Single Point information = 1
COA=1 COT=20 SQ=1 P/N=ACK
IOA=1001 ==> Off
+01=1002 ==> Off
+02=1003 ==> Off
+03=1004 ==> Off
09:20:45.003 >>S(2) 68,04,01,00,04,00
09:20:45.103 <<I(2,1) 68,10,04,00,02,00,03,83,14,00,01,00,D1,07,00,00,00,00
Double Point information = 3
COA=1 COT=20 SQ=1 P/N=ACK
IOA=2001 ==> 0: Indeterminate or intermediate state
+01=2002 ==> 0: Indeterminate or intermediate state
+02=2003 ==> 0: Indeterminate or intermediate state
09:20:45.133 >>S(3) 68,04,01,00,06,00
09:20:45.233 <<I(3,1) 68,1A,06,00,02,00,01,04,14,00,01,00,F5,03,00,00,DD,05,00,0
Single Point information = 1
COA=1 COT=20 SQ=0 P/N=ACK
IOA=1013 ==> Off
IOA=1501 ==> Off
IOA=1502 ==> Off
IOA=1503 ==> Off
09:20:45.263 >>S(4) 68,04,01,00,08,00
09:20:45.363 <<I(4,1) 68,0E,08,00,02,00,03,81,14,00,01,00,C5,09,00,00
Double Point information = 3
COA=1 COT=20 SQ=1 P/N=ACK
IOA=2501 ==> 0: Indeterminate or intermediate state
09:20:45.383 >>S(5) 68,04,01,00,0A,00
09:20:45.483 <<I(5,1) 68,12,0A,00,02,00,07,01,14,00,01,00,71,17,00,00,00,00,00,0
BitString = 7
COA=1 COT=20 SQ=0 P/N=ACK
IOA=6001 ==> BSI=0 (00000000h) OV=0 IV=0
09:20:45.503 >>S(6) 68,04,01,00,0C,00
09:20:45.613 <<I(6,1) 68,16,0C,00,02,00,09,83,14,00,01,00,A1,0F,00,00,00,00,00,0
Measured Normalized Value = 9
COA=1 COT=20 SQ=1 P/N=ACK
IOA=4001 ==> 0,00% 00000 (0000) OV=0 IV=0
+01=4002 ==> 0,00% 00000 (0000) OV=0 IV=0
+02=4003 ==> 0,00% 00000 (0000) OV=0 IV=0
Go offline
1:1

Version history

New in version 2.60

- Group interrogation to group 1 to 16, implemented. Prior versions did support general interrogation to group 0 only.
- Added a sniffer function for the IEC60870-5-101 protocol. Requires a special cable.
- IEC60870-5-101 timeout and retry can be adjusted in the Option dialog window.
- Delay Acquisition Command 106 added.
- The older versions did require PCs with COM port installed. If a COM port was not found the master test tool could not start. This is now corrected and COM ports are now longer required to start the test tool.