# CDOAN-IEC60870

IEC 60870-5-101 and 60870-5-104 Protocol Tester
Release 1.0.11
February 17, 2022

*www.cdoancal.com*

TPILB

# Contents

# Introduction

CDOAN-IEC60870 is a Windows-based application designed to generate, capture, and test communication between IEC 608705-101 protocol devices, or between IEC 608705-104 protocol devices. Version 1.0.8 was released on 20-January-2022.

The application can be configured to operate over serial communication channels or TCP/IP network ports:

- When serial communication is selected, the application operates with IEC 60870-5-101 protocol
- When network communication is selected, the application operates with IEC 60870-5-104 protocol

In either mode, the program can:

- Operate as a controlling station
- Operate as a controlled station
- Listen for communication between active controlling and controlled stations

## Protocol Support

| IEC 60870-5 Protocol Support | | |
|---|---|---|
| **General** | Adjustable timers | Periodic scan period |
| | | Background scan period |
| | Counters | Modes A, B, C, and D |
| | | Internal freeze interval is adjustable for applicable modes |
| | Single points | Can be configured for normal (M_SP_NA_1) or packed (M_PS_NA_1) format |
| **ASDU** | Process Information in Monitor Direction | Display support: Interpretation of all types<br>Controlled station: Simulation of all types except protection equipment ASDUs (M_EP_TA_1, M_EP_TB_1, and M_EP_TC_1) |
| | Process Information in Control Direction | Display support: Interpretation of all types<br>Controlling station: Can transmit all types<br>Controlled station:<br>• Responds to all types<br>• Can link reception of a command to a similar "monitor direction process information" ASDU |
| | System Information in Monitor Direction | Display support: Interpretation of all types<br>Controlled Station: Generates "End of Initialization" on startup |
| | System Information in Control Direction | Display support: Interpretation of all types<br>Controlling Station:<br>• Ability to send all types except "Reset Process"<br>• Test command sent with time with when using 60870-5-104<br>• Test command sent without time when using 60870-5-101<br>Controlled Station: Responds to all types |
| | Parameter in Control Direction | Display support: Interpretation of all types<br>Controlling Station: No support for transmission<br>Controlled Station:<br>• Responds to all types<br>• Parameter information is not otherwise processed |
| | File transfer | Display support: Interpretation of all types<br>Controlling Station: No support<br>Controlled Station: No support |
| **60870-5-104** | Adjustable | T1, T2, and T3 times |
| | | K and W parameters (Message send/receive limits) |
| **60870-5-101** | Sizes | Data link address, common address, object address, and cause of transmission |
| | Data Link Address | Enterable, supports only one controlled station |
| | Background scans | Configurable to report in class 1 or class 2 |
| | Adjustable timers | Response timeout |
| | | Class poll frequency |
| | Balanced mode | Not supported in the current release |

## Views

The application presents information in seven views

## Config

- Select network or serial mode
- Specify IP addresses and communication ports
- Request and enter licensing information

## IEC

- Enter protocol configuration settings
- Select ASDU types for inclusion in the Event Log view

## Controlling Station

- Build a list of messages to be sent when operating as a controlling station

## Controlled Station

- Enter a list of points to be used when operating as a controlled station
- Configure applicable points as periodic or not
- Enter point values, simulation parameters, and quality codes
- Link "process information in the control direction" to "process information in the monitor direction"
- Make changes in real time to generate events

## Messages

- Show communication messages and message counts

## Events

- Show events for each detection of an "enabled" ASDU type sent from a controlled station. ASDU types are enabled from the IEC view and include:
  - All process information ASDUs containing time tags
  - All control ASDUs
  - All parameter ASDUs
  - Interrogation ASDUs
  - End of initialization ASDU
  - Clock synchronization ASDU sent with a spontaneous cause of transmission

## Point List

- Show all points reported from a controlled station including responses to controls

## Installation

CDOAN-IEC60870 is installed from a single setup file called CDOAN- CDOAN-IEC60870-setup.exe. it is digitally signed to CDOAN.

## Licensing

CDOAN- IEC60870 is licensed is two ways:

- License code installed on a PC based on hardware in the PC. This licensing form limits operation to the specific PC on which the license is installed. These licenses cannot be transferred to another computer.
- License code installed on a (customer provided) USB flash drive based on characteristics of that drive. Most (but not all) USB flash drives contain enough information to store a license file. A license installed on a USB drive enables operation on any PC in which the USB drive is installed. That is, a USB drive-based license allows operation on any PC, but only one at a time.

The CDOAN-IEC60870 startup screen shows active license information and contains a target to request a license from CDOAN.

- If you want a USB flash drive-based license, insert that drive into a USB port before starting this process
- Select the **Request License** target
- The application searches for a USB flash drive that contains enough characteristics to store a license. If one is found, a prompt is issued asking if that drive should be used. If more than one USB drive is inserted, only the first applicable USB flash drive is presented. Trial licenses cannot be installed on a USB drive, only permanent licenses can.
- Enter all requested data including the license type. A trial, available for free, operates for two-weeks
- The resulting license request information is saved to a "txt" file
- Email this file to [cdoancal@gmail.com](mailto:cdoancal@gmail.com)
- A license "txt" file will be sent by return Email

Restart CDOAN-IEC60870 and select the **Load License From File** target. If the license is to be installed on a USB flash drive, remove all other flash drives and insert the target drive before loading the license.

## Menu

The main menu contains five pull-down lists: *File, Edit, Views, Window,* and *Communication*. The edit pull-down differs depending on the active view.

### File
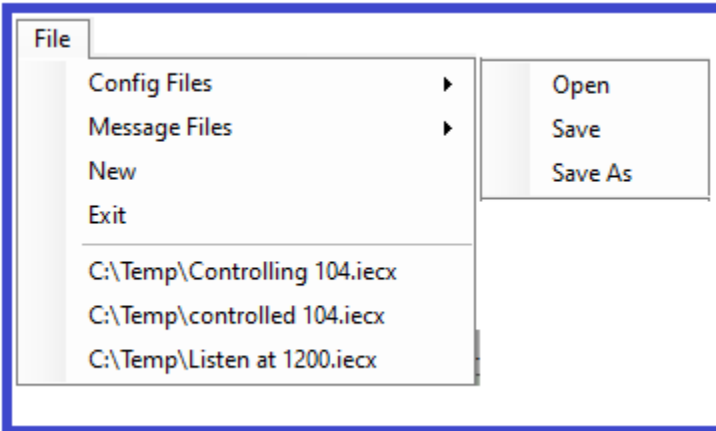


**Config File** is used to open or save a configuration file. The three most recently accessed files are also shown at the bottom of the menu and may be selected for a "Quick Open"

**Messages File** is used to open or save communication messages to or from the *Messages View.* The 500 most recently detected messages are retained in the *Messages View*

**New** resets all information in the application to initial states, including erasing entries made in other views

### Views
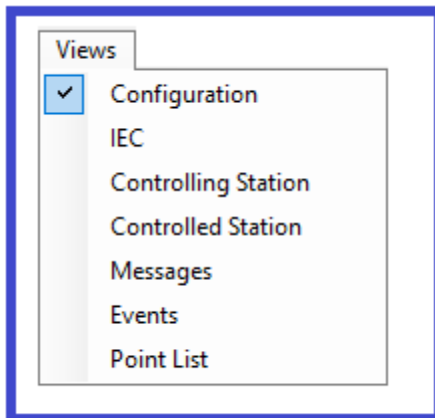


Used to request a view. Active views are identified by a checkbox to the left of the view name. Selecting a view that is not active causes the view to be shown. Selecting a "Active" view causes the view to close.

## Window



**Cascade** operates on all open views
**Tile** operates on all open views
**Undock** allows the selected window to float in the computer monitor, not constrained by the general display area
    for the application
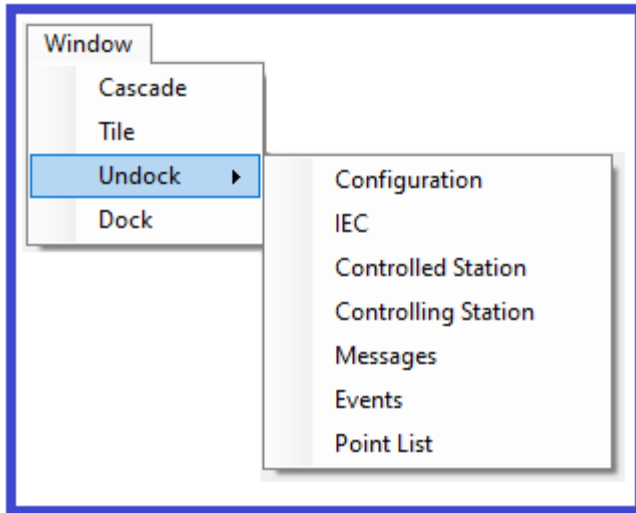**Dock** re-docks the window, reversing operation of a prior "Undock"

## Communication



**Controlling** starts operation as a controlling station. At least one message must be defined in the *Controlling* view.
**Controlled** starts operation as a controlled station. At least one point must be defined in the *Controlled* view.
**Listen** starts operation by listening to active ports or COM channels. Network listening can be filtered by entering
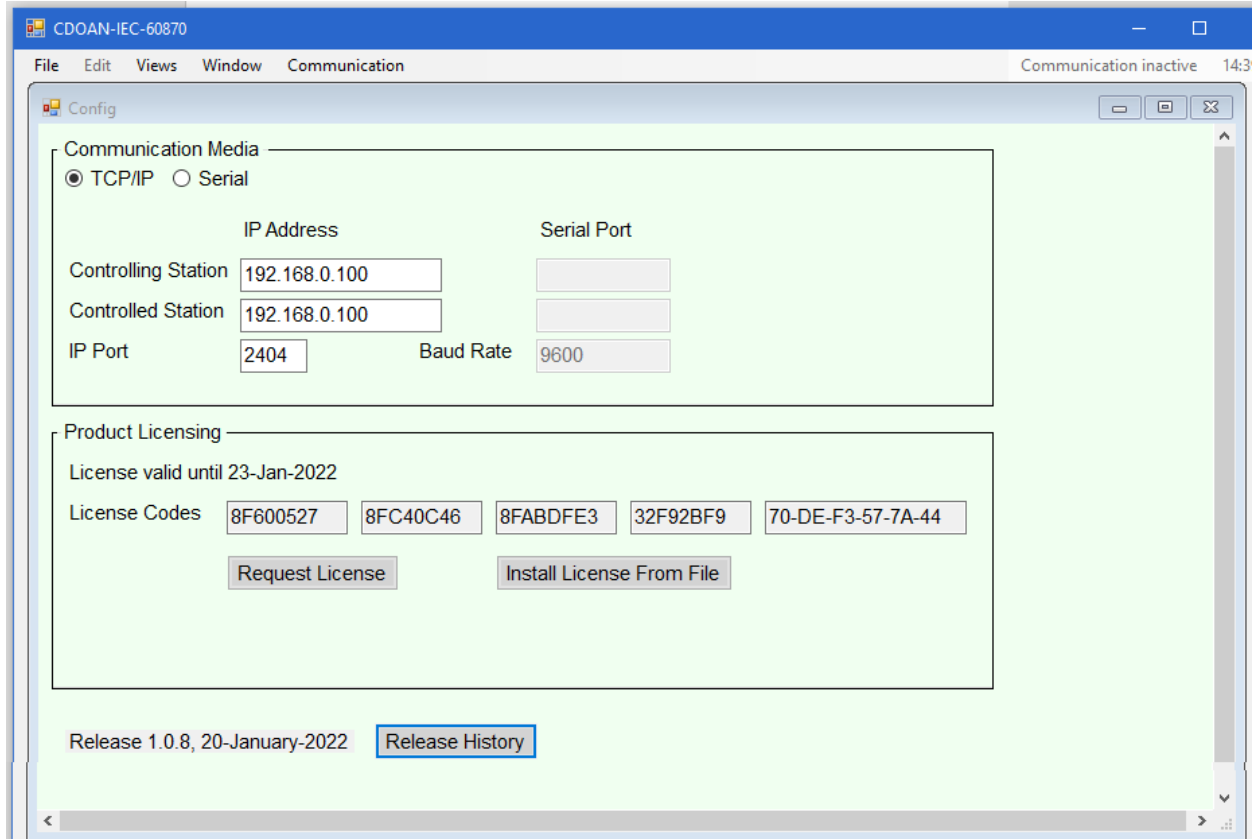    valid IP addresses on the Control view.

**Stop**. When communication is active, the three choices shown above are replaced by a single "Stop" option.

# Views

This section discusses each of CDOAN-IEC60870's seven views.

## Config

The Config view supports entry of general operational parameters and license information.



## Communication Media

**TCP/IP** enables network communication and IEC 60870-5-104 protocol. IP addresses and the IP port can be modified. The "Controlled Station" IP address is required when operating as a controlling station. No IP address is required when operating as a controlled station. A connection is accepted from any address. Either address entry is optional when operating in listening mode. However, if one is entered, both should be. They filter communication from other addresses.

**Serial** selection enables serial communication and IEC 60870-5-101 protocol. The "Controlled Station" serial port is required when operating as a controlling station. The "Controlling Station" serial port is required when operating as a controlled station. Both ports are required when operating in listening mode.

## Product Licensing

**Request License** is used to enter information about your PC and request a license, either trial of permanent. This action generates a "txt" file that should be emailed to support@cdoancal.com. The response will be a "txt" license file. The license will only work on the same computer that was used to generate the request.

**Install License From File** is used to install the license sent from CDOAN.

## Other

**Release History** shows a history of CDOAN-IEC60870 release dates, revision numbers, and what was changed

## IEC



Supports configuration of IEC protocol

### IEC 60870-5-104

Sets parameters used for IEC 60870-5-104 protocol only. These include timers T1, T2, and T3, and message count parameters K and W. When operating with 60870-5-104 protocol, current countdown values for each parameter are shown in the upper right portion of the program window,.

### IEC 60870-5-101

Sets parameters used for IEC 60870-5-101 protocol only. These include:
- Sizes for data link address, common address, object address, and cause of transmission
- Response timeout, in seconds. Used when operating as a controlling station
- Data link address
- Parameters for operation in balanced mode are shown, but balanced mode is not yet implemented

### Controlled Station

Sets parameters used only when operating as a controlled station
- **Periodic Scan** period for reporting points with a periodic cause of transmission
- **Background Scan** period for reporting points with a background scan cause of transmission. Points are sent with this cause only when not otherwise reported within the specified background scan period
- **Measured Event Deadband.** The integer value is used for normalized, scaled, and floating-point values
- **Event Time** is the size of the time field used to report time tagged events. 3-octet and 7-octet are supported. While 3-octet time tags are not part of 60870-5-104 protocol, they may be selected. When 3-octet time tags are configured with 60870-5-104, a warning is issued at the start of communication, allowing the user to change to the conformant 7-octet time setting.
- **Totals Acquisition Mode** allows selection of one of the four specified modes: A, B, C, or D. Selection of a new mode automatically updates the freeze type and interrogation type fields.
- **Local Freeze Period** is a time, in seconds, at which counters are locally frozen (modes A and B)

- **Select Required** defines whether controls require a select before an operate. If required, a negative confirm is sent if an operate occurs without a select. If not required, a select (if received) is still processed, but the operate is always processed regardless of the presence of a preceding select.
- **Report Single Points** configures reporting of single point in normal or packed mode. When packed mode is selected, the application verifies that all single points are configured at sequential object addresses.
- **Background Scan Class** identifies if ASDUs sent with a "Background Scan" cause of transmission are included in class 1 or class 2. (Applies only for 60870-5-101)

## Controlling Station

Configures items used only when operating as a controlling station. All apply only to 60870-5-101.

**Use Data Link Confirms** defines whether ASDU information sent in the control direction uses Data Link Confirm or Data Link No Confirm. Data link Confirm is normal and expected.

**Failure After [3] missing responses** causes the controlling station to reenter the startup state after a number of consecutive "no response" conditions from the controlled station

**Class 1/2 Polls** define the frequency a class 1 or class 2 message is sent. Options are to send one every 'x' seconds, or continuously. The "Continuous" option results in a class 1 or class 2 request sent whenever the line is idle. Regardless of the setting, any message other that a class 1 or class 2 request that is ready to be sent takes priority of a class 1 or 2 poll.

## Event Log ASDU Type

The application maintains an Event Log view that creates a one-line entry for every event received from the controlling station. An event is defined as any ASDU with a type corresponding to one of the ASDU types checked.

## Controlling Station

This view configures messages to be sent when operating as a controlling station. There are two parts to this table. Messages to send in a startup sequence, and messages to send after that sequence completes.

| Request | FirstTime | RepeatTime | CommonAddress | ObjectAddress | Value | Qualifier |
|---|---|---|---|---|---|---|
| Begin Startup Sequence | 0 | 0 | 0 | 0 | 0 | |
| STARTDT | 0 | 0 | 0 | 0 | 0 | |
| End Startup Sequence | 0 | 0 | 0 | 0 | 0 | |
| General Interrogation | 0 | 0 | 1 | 1 | | Station Global |

Messages in the startup sequence are processed as follows:

- They are sent at startup only.
- A subsequent message is not sent until the prior message gets an appropriate response. This may be a simple ACK (such as for Reset Link) or a CON (such as for STARTDT), or an application confirm or application termination message (if one is expected).
- The sole exception to this is for 60870-5-101 for Class 1, Class 2, or Class 1/2 entries. If such an entry appears immediately after a request expecting an application confirm or application termination message, then the defined Class sequence is sent until the expected response is received.
- 60870-5-101 controlling stations reenter the startup sequence after excessive response timeouts from the controlled station. The response timeout limit is set from the IEC view.
- When in the startup section, the tool bar at the top of the application (the one showing the time-of-day at the right) is shown with a dark background. The background changes to a lighter color when startup is complete.

### 60870-5-104

Messages automatically sent, even if not configured, include:
- StopDT when the connection is closed
- TestFR commands whenever the T3 timer expires
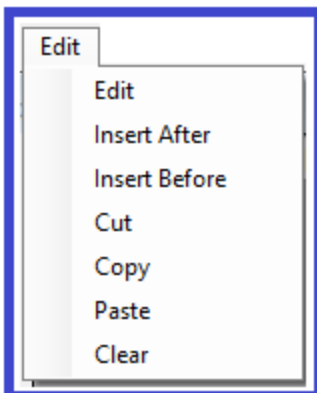- Supervisory commands as appropriate

### 60870-5-101

Messages automatically sent, even if not configured, include:
- Class 1 and/or class 2

## Configurable Messages

Messages are entered in a list starting from the edit menu.



**Edit** edits the currently selected entry

**Insert After** inserts a new entry after the currently selected entry
**Insert Before** inserts a new entry before the currently selected entry

The process for inserting or editing a new request starts with the following menu.
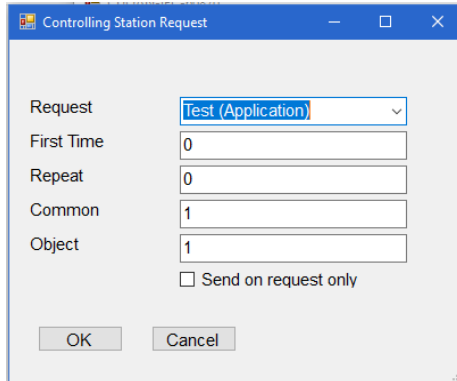
**Request Type**
The following request types are configurable.

| | | | |
|---|---|---|---|
| • Both Protocols | Test (Application) | Single Command | Setpoint Normalized |
| | General Interrogation | Double Command | Setpoint Scaled |
| | Counter Interrogation | Regulating Step Command | Setpoint Float |
| | Read | Biststring Command | Time Sync |
| | | | |
| • 60870-5-104 | StartDT | | |
| | | | |
| • 60870-5-101 | Reset Link | Reset User | Request Link Status |
| | Test Link | Class 1 | Class 2 |
| | Class 1/2 | | |

Note that there are three "Class" entries for IEC 60870-5-101.
- Class 1 will send a Class 1 request regardless of the state of the ACD flag
- Class 2 will send a Class 2 request regardless of the state of the ACD flag
- Class 1/2 will send a Class 1 request if the last response from the controlled station had the ACD bit set, or a Class 2 request otherwise

**First Time** is the time the message is sent for the first time in "seconds after startup". A value of '0' causes the message to be sent immediately.
**Repeat** is the repetition time for retransmission after the first transmission. A value of '0' causes the message to not be repeated the first transmission
**Common** is the common address of ASDU
**Object** is the object address
**Send on Request Only** checkbox configures to message to be sent only when on a user request. In this case, the "First Time" and "Repeat" entries are ignored. When running, each message is associated with a **SEND** button. The message is sent once evert time the button is selected.

After entering all information and selecting OK, the user is prompted for more information appropriate for each request type. The end result may be something like this:
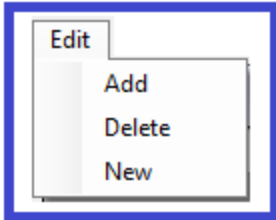
| SendNow | Request | FirstTime | RepeatTime | CommonAddress | ObjectAddress | Value | Qualifier |
|---------|---------|-----------|------------|---------------|---------------|-------|-----------|
| Send | Begin Startup Seque... | 0 | 0 | 0 | 0 | 0 | |
| Send | Reset Link | 0 | 0 | 0 | 0 | 0 | |
| Send | Time Sync | 0 | 0 | 1 | 0 | | |
| Send | Class 1 | 0 | 0 | | | | |
| Send | General Interrogation | 0 | 0 | 1 | 1 | | Station Global |
| Send | Class 1 and 2 | 0 | 0 | | | | |
| Send | End Startup Sequence | 0 | 0 | 0 | 0 | 0 | |
| Send | General Interrogation | 030 | 030 | 1 | 1 | | Station Global |
| Send | Class 1 and 2 | 0 | 0 | | | | |

Note the "Send" buttons. Those are shown only when communication is active.

## Controlled Station

This view configures points in the controlled station. When operating as a controlled station, communication messages are generated automatically according to the point configuration.

Points are entered through the edit menu.



Selecting "Add" generates the following menu



All points entered are assigned to the same common address entered at the top of the menu. Points can be configured in different common addresses by running the dialog more than once.

For each ASDU type to configure, enter a starting object address and the number of points. Repeat for all ASDU types to define.

- Within each ASDU type, points are created with sequential object addresses. To generate object addresses out of sequence for the same ASDU type, run the dialog a second time
- Process information in monitor direction points (left column) can be categorized as periodic. Periodic points are sent at the configured period scan period (IEC View) and excluded from Interrogation responses.
- Process information in control direction points (right column) need to be defined only to successfully process a command from the controlling station. Commands for non-configured points generate a "Unknown Object Address" response
- The same object address cannot be used for more than one point, even for different ASDU types. The editor verifies this after entry and removes duplicates.

After configuration is complete, a list of all configured points are shown in the table, sorted in common address and object address order.

| Common | Object | Type | | Value | AltVal Link | Time | Periodic | BL | SB | NT | IV | OV | CY | CA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 2 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 3 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 4 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 5 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 6 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 7 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 8 | Single Point | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 11 | Measured Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 12 | Measured Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 13 | Measured Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 14 | Measured Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 100 | Single Cmd | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 200 | Setpoint Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | 201 | Setpoint Normalized | ⌄ | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Information can be entered for each point to impact how each is reported to the controlling station.

Fields are:
- Value is the current value for the input (monitor direction) point. It is not used for control direction points
- AltVal Link
    - For monitor direction points, specifies an alternate value. The value and alternate values are alternated every "Time" period, in seconds, as entered in the "Time" column.
    - For control direction points, specifies a link to an object address of a monitor direction point of the same basic type. For example, a Single Command can link to a Single Point. When a linkage is established and a command processed, the value/state of the command is copied to the monitor direction point, which is then reported with a "Caused By Remote Command" cause of transmission
- The periodic check box identifies a monitor point as one to be reported with a periodic cause of transmission
- The other check boxes set quality flags. Only those applicable to the corresponding ASDU type are processed.

Entries made:
- Before active communication starts are applied when started
- During active communication, are applied immediately and cause an event to be generated
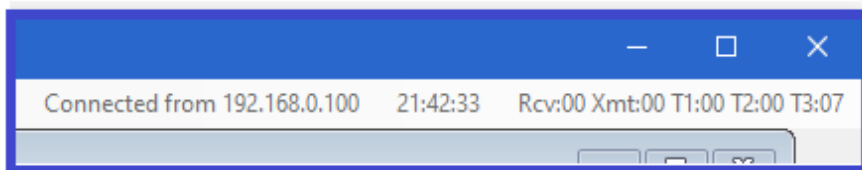
Messages
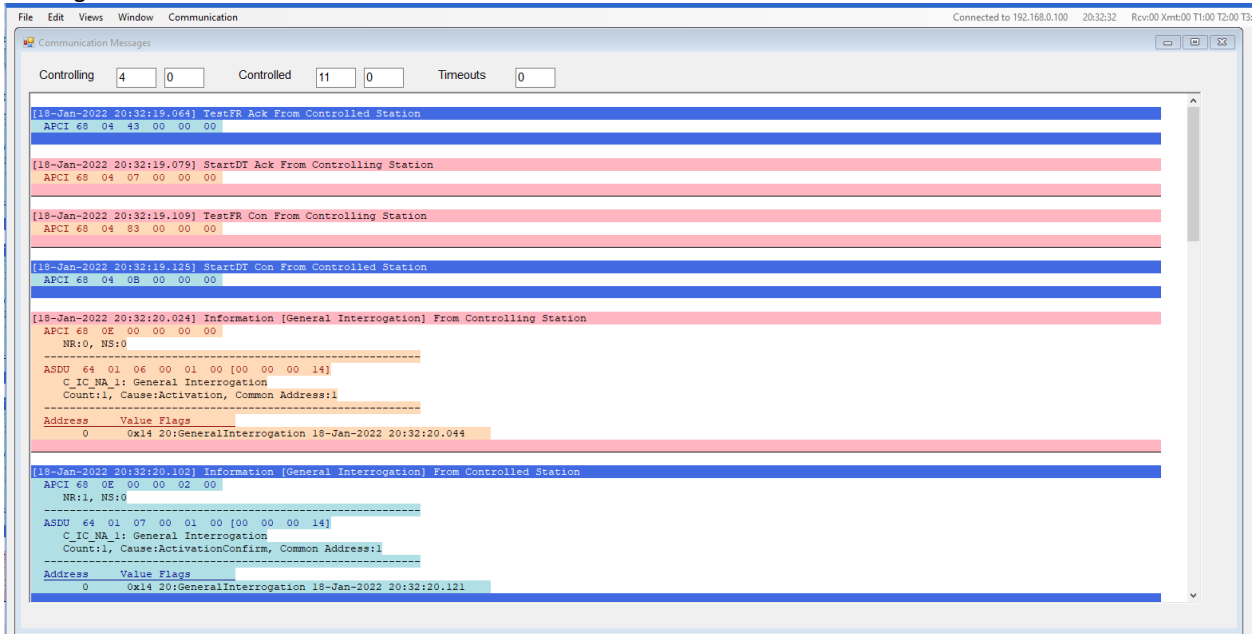


The messages view shows communication messages and statistics. Messages from the controlling station are shown in shades of red. Messages from the controlled station are shown in shades of blue.

Statistics at the top of the view show messages from the Controlling station (good messages to the left and those with errors to the right), the same for messages from the Controlled station, and finally, timeouts (messages from the controlling station where a response was expected, but not received).

The top right of the screen shows the connection status and, for 60870-5-104, receive and transmitted message counts, and current T1, T2, and T3 timer values.
- The transmitted message count is the number of messages sent by the controlled station and not confirmed. This field is valid only when operating as a controlled station.
- The received message count is the number of messages received from the controlled station and not confirmed. This field is valid only when operating as a controlling station.

This area of the screen may be hard to see in the picture above. Here it is, larger.

## Event Log

The Event log view contains a single line entry for every occurrence of an enabled ASDU type in a message sent from a controlled station. ASDU types are enabled, for inclusion in the event log, from the IEC view.

```
[18-Jan-2022 21:46:13.122] General Interrogation Index:0, Cause:ActivationConfirm, Flags:20:GeneralInterrogation , Value:0x14, At:18-Jan-2022 21:46:13.120
[18-Jan-2022 21:46:13.398] General Interrogation Index:0, Cause:ActivationTermination, Flags:20:GeneralInterrogation , Value:0x14, At:18-Jan-2022 21:46:13.398
[18-Jan-2022 21:46:21.110] Single Cmd Index:9, Cause:ActivationConfirm, Flags:Select, On, Short Pulse , Value:0x85, At:18-Jan-2022 21:46:21.108
[18-Jan-2022 21:46:21.131] Single Point Event (7-Octet Time) Index:1, Cause:CausedByRemoteCommand, Flags: , Value:On, At:18-Jan-2022 21:46:21.074
[18-Jan-2022 21:46:21.229] Single Cmd Index:9, Cause:ActivationConfirm, Flags:Execute, On, Short Pulse , Value:0x05, At:18-Jan-2022 21:46:21.227
[18-Jan-2022 21:46:21.277] Single Point Event (7-Octet Time) Index:1, Cause:CausedByRemoteCommand, Flags: , Value:On, At:18-Jan-2022 21:46:21.192
```

## Point List

The point list shows all process information points in both the monitor and control directions. Points are shown highlighted for five seconds whenever detected.

| Link Adrs | Common Adrs | Object Adrs | ASDUType | Cause | Value | Flags | Time |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | Single Point | BackgroundScan | On | | |
| 0 | 1 | 2 | Double Point | BackgroundScan | On | | |
| 0 | 1 | 3 | Step Position | BackgroundScan | 3 | | |
| 0 | 1 | 4 | Bitstring | BackgroundScan | 0x4 | | |
| 0 | 1 | 5 | Measured Normalized | BackgroundScan | 5 | | |
| 0 | 1 | 6 | Measured Scaled | Spontaneous | 0 | | 18-Jan-2022 21:50:58.221 |
| 0 | 1 | 7 | Measured Float | BackgroundScan | 7 | | |
| 0 | 1 | 9 | Single Cmd | ActivationConfirm | 0x05 | Execute, On, Short Pulse | 18-Jan-2022 21:46:21.227 |