SIM-101

IEC 60870-5-101 SIMULATOR

USER MANUAL

English

sim-systems

SUMMARY

1. Overview

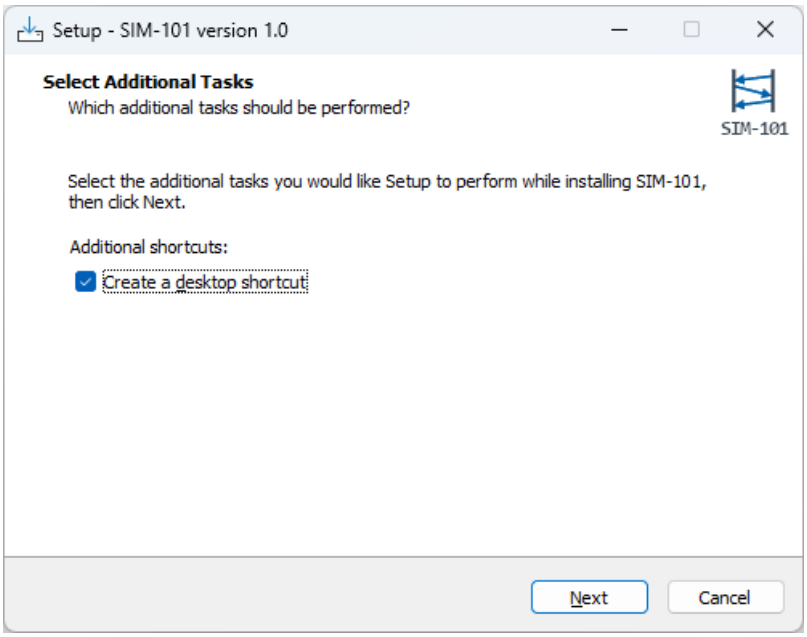
Developed by SIM-SYSTEMS, SIM-101 is a comprehensive IEC 60870-5-101 protocol simulation software for Windows. It offers a robust and flexible platform for emulating master and slave devices, enabling the simulation of realistic and comprehensive communication scenarios in SCADA systems.

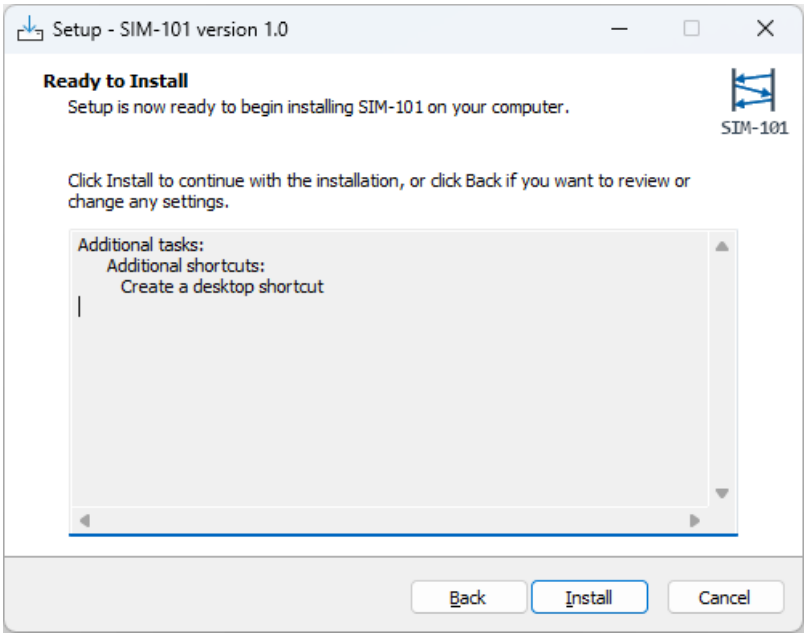
The SIM-101 goes beyond protocol simulation, also offering complete IEC 60870-5-101 communication line monitoring capabilities, an essential function for communication troubleshooting.

2. Installation

Installing the software is simplified, just follow the steps below:

- Run the installer.
- Click "Next" in the home window.
- Click "Install" in the next window.
- Wait for the installation to be completed.

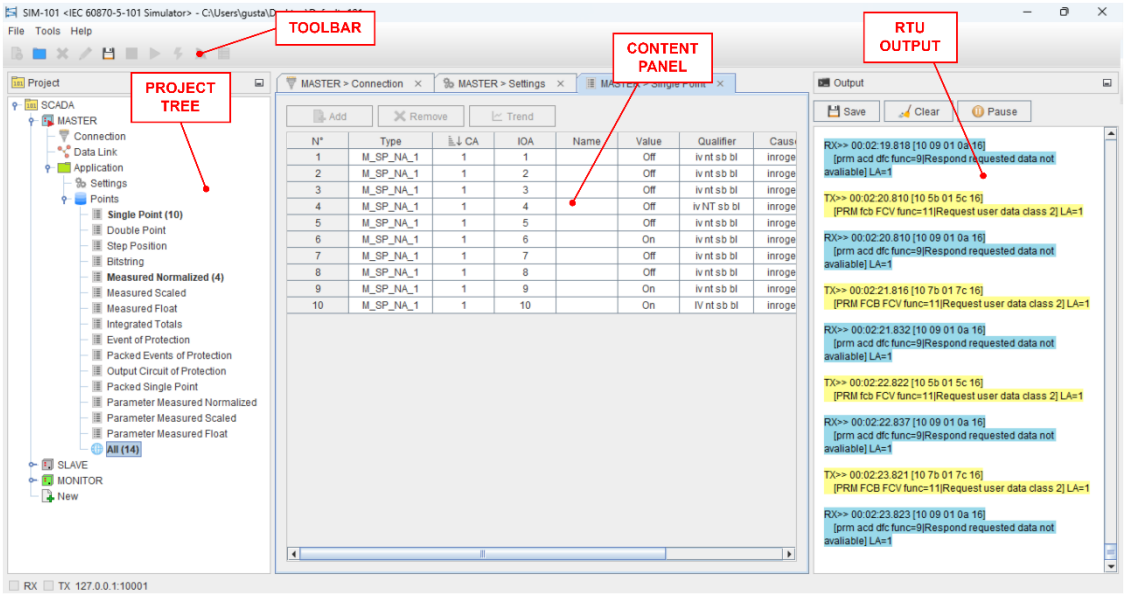




3. User Interface

The simulator's main interface is made up of four main components:

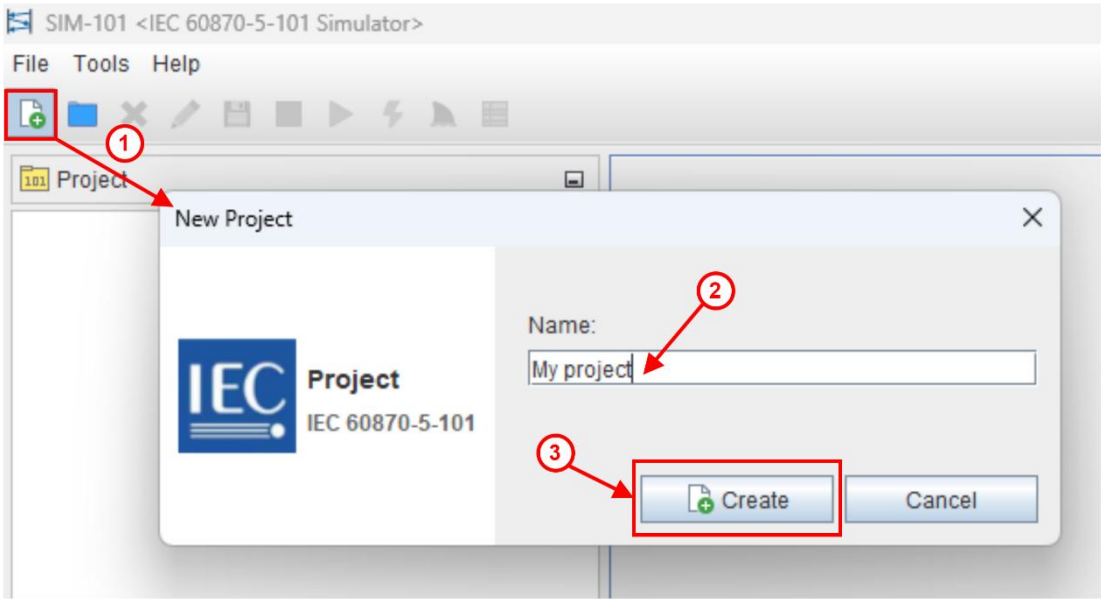
- **Project tree:** Project viewing area, containing the stations.
- **Content panel:** Viewing area of project items.
- **Rtu output:** Output terminal of the running station.
- **Toolbar:** Command bar and project management.



4. Creating a project

To create a project, follow these steps:

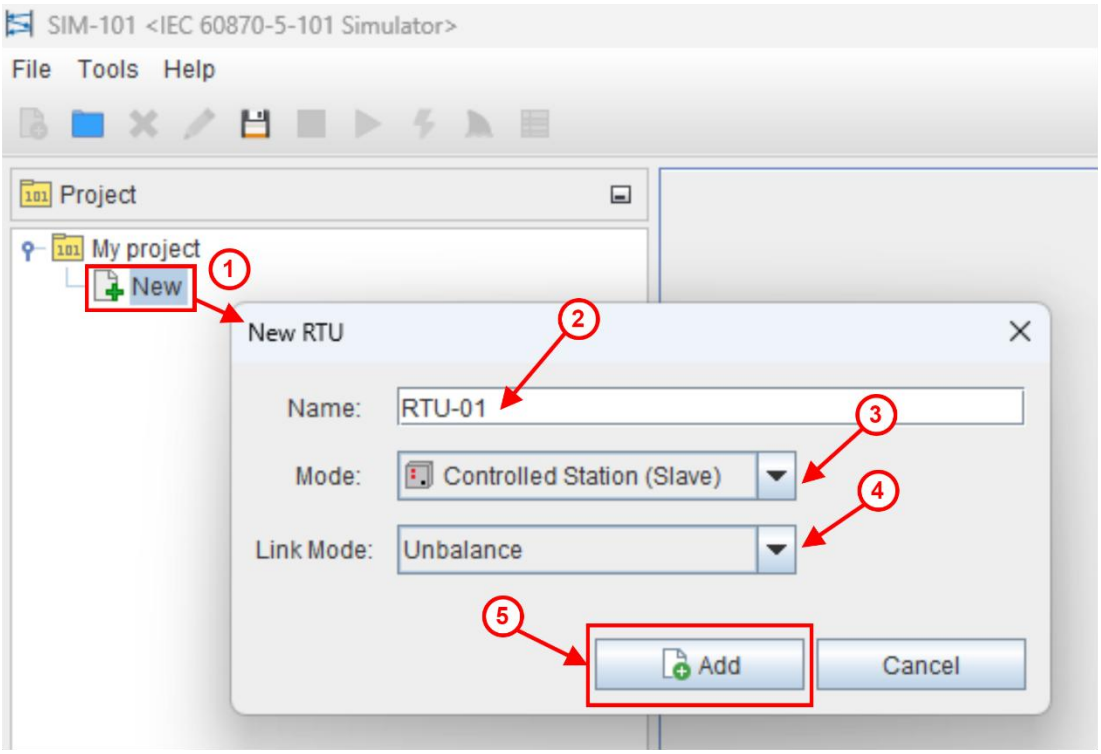
1. Click on the "New Project" button.
2. Fill in the name of the project.
3. Click on the "Create" button.



5. Adding a Station

To add a station to your project, follow these steps:

1. Click (x2) on the "New" icon.
2. Fill in the name of the station.
3. Select the mode of operation.
4. Select the link mode.
5. Click the "Add" button.



6. Settings

The simulator offers several configuration options, enabling tests of different scenarios. In this chapter, more details about the customizable parameters will be described.

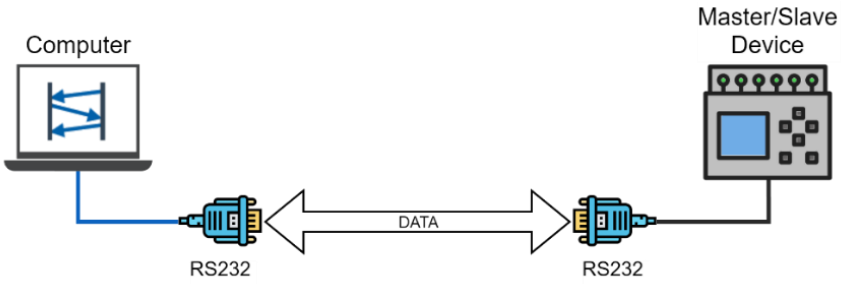
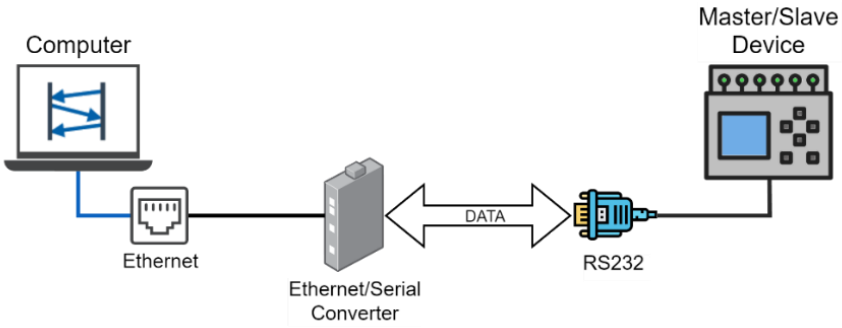
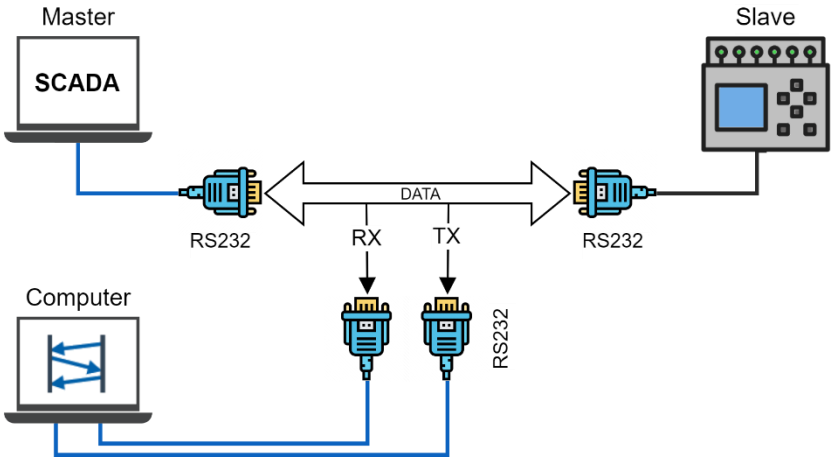
6.1 Connection

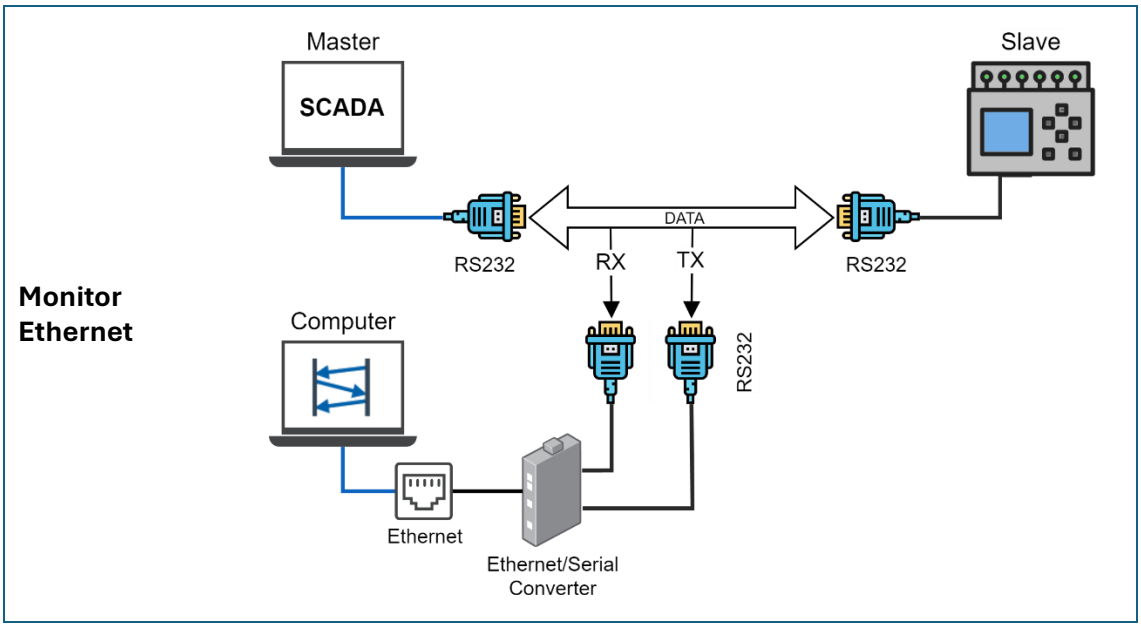
In general, devices that implement the IEC 60870-5-101 protocol use serial interfaces RS232, RS485 or other compatible industrial standard, however, modern equipment simply uses ethernet connections (IEEE 802.3) associated with media converters, knowing this, serial interface and TCP/IP options have been implemented.

The connection configuration of a station is accessed from the "Connection" menu, the parameters are as follows:

Serial	
Port	Serial port name It is case-sensitive.
Baud Rate	Speed of communication. 1200, 2400, 4800, 9600, 19200, 38400, 57600 ,115200 [bit/s]
Data Bits	Number of bits per frame. 5…8 [bit]
Parity	Frame parity. None, Odd and Even
Stop Bits	Number of stop bits. 1, 1.5, 2 [bit]
Flow Control	Flow control mode. None, RTS/CTS, Xon/Xoff
Max Idle Line	Maximum delay between frames. 0…9999 [ms] It is recommended to use at least 50 ms for serial connections and 250 ms for TCP/IP connections associated with media converters. Parameter should be increased if there are constant errors in "Frame format" and/or "Timeout".
TCP/IP	
Mode	TCP/IP connection option. Client, Server **Mode=Client** Initiates the TCP/IP connection to the remote station that is in server mode, suitable for master stations. **Mode=Server** Opens a TCP port and waits for connection, suitable for slave stations.
Ip Address	IP address. IPv4 and IPv6 support
Port	TCP port number.
Max Idle Line	Maximum delay between frames. 0…9999 [ms] It is recommended to use at least 50 ms for serial connections and 250 ms for TCP/IP connections associated with media converters. Parameter should be increased if there are constant errors in "Frame format" and/or "Timeout".

Below are examples of suggested connection topologies for each simulator operating mode.

Mode	Topology
Master/Slave Serial	
Master/Slave Ethernet	
Monitor Serial	



6.2 Data link

The station link settings are made via the "Data Link" menu, which groups the structure parameters of the IEC FT 1.2 frame.

Mode	Link operation mode. Unbalanced, Balanced **Mode=Unbalanced** In unbalanced mode, the controlled station only responds after a request, i.e. all communication is based on "question and answer". **Mode=Balanced** In balanced mode, the controlled station communicates spontaneously, i.e. communication is based on "notification and confirmation", in addition each terminal controls its link with the remote station.
Address Size	Number of octets of the station's physical address. 1, 2 [Octet]
Address	Physical address of the station. 1...254 (Address Size=1), 1...65534 (Address Size=2)
COT Size	Number of octets of the cause of transmission (TOC). 1, 2 [Octet] **COT Size=2** Second octet assigned to the originator address (AO)
CA Size	Number of octets of ASDU Common Address (CA). 1, 2 [Octet]
IOA Size	Number of octets of the information object address (IOA). 1..3 [Octet]
DIR bit	Transmission direction bit (balanced mode). **DIR bit=1** Control data for the controlled station. **DIR bit=0** Data from the controlled station to the control station.

6.3 Application

The following are the application settings for controlled stations, controllers, and monitors.

Slave	
Class 1 Event Buffer Size	Class 1 event buffer size. 0...50000 [events]
Class 1 Buffer Overflow	Class 1 event buffer overflow percentage. 0...100 [%] If the buffer occupancy percentage is higher than that adjusted in this parameter, the oldest events are discarded.
Class 2 Event Buffer Size	Class 2 event buffer size. 0...50000 [events]
Class 2 Buffer Overflow	Class 2 event buffer overflow percentage. 0...100 [%] If the buffer occupancy percentage is higher than that adjusted in this parameter, the oldest events are discarded.
Clock Sync Period	Maximum interval for receiving synchronization commands. 0...999999 [s] Clock Sync Period=0 Disabled If the station is not synchronized in the period established in this parameter, the events are generated with the invalid time stamp.
Short Pulse Duration	Pulse duration interval for commands received with the short pulse qualifier. 1... 999999 [ms]
Long Pulse Duration	Pulse duration interval for commands received with the long pulse qualifier. 1... 999999 [ms]
SBO Timeout	Maximum interval between select and execute commands. 1... 999999 [ms]
Background Scan Time	Interval between streams of background events. 1... 999999 [s]
Cyclic Transmission Time	Interval between transmissions of cyclical events. 1... 999999 [s]
Remote Link Expiration	Maximum interval without communication with the remote station (balanced mode). 1... 999999 [s] After the interval expires, the link is checked using the link state request command.
Reply Timeout	Maximum response range of the remote station. 1...999999 [ms]
Max Retry	Maximum number of transmissions. 1..32
Retransmission Time	Minimum interval for retransmission. 1...999999 [ms]
Double transmission	Enables/Disables dual streaming. Disable, Enable **Double transmission=True** the points are initially sent without a time stamp and with higher priority, later they are sent with the respective event stamp.
Default CA	Default ASDU Common Address (CA) value.

	1…254 (CA Size=1), 1…65534 (CA Size=2) The station will also assume the common ASDU (CA) addresses registered in the database points, however, these will be generated automatically.

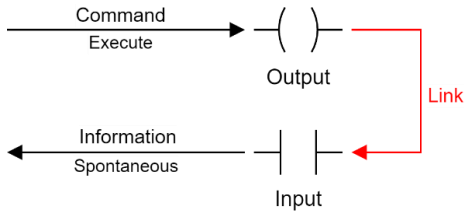
Master	
Polling Interval	Interval between data requests (unbalanced mode). 100…999999 [ms]
General Interrogation Interval	Interval between general interrogation (GI) requests. 0…999999 [s] **General Interrogation Interval=0** Disables cyclic sending of the command.
Counter interrogation Interval	Interval between counter interrogation (CI) requests. 0…999999 [s] **General Interrogation Interval=0** Disables cyclic sending of the command.
Acquisition of Integrated Totals	Meter acquisition mode used in meter interrogation (CI). Interrogation, Freeze and Interrogation, Freeze **Acquisition of Integrated Totals=Interrogation** Only reads locally frozen counters (IEC 60870-5-101 Mode B). **Acquisition of Integrated Totals=Freeze and Interrogation** freezes the meters and then reads them (IEC 60870-5-101 mode C). **Acquisition of Integrated Totals=Freeze** Only freezes the meters and waits for the spontaneous receipt of the frozen meters (Mode D of IEC 60870-5-101).
Freeze Command	Freeze command qualifier. Freeze Without Reset, Freeze with Reset, Reset
Clock Sync Interval	Synchronization interval of the controlled station. 0…999999 [s] **Clock Sync Interval=0** Disables cyclic sending of the command.
Command Timeout	Maximum interval for receiving acknowledgments (ACTCON and ACTTERM) of a command. 1…60 [s]
Remote Link Expiration	Maximum interval without communication with the remote station (balanced mode). 1… 999999 [s] After the interval expires, the link is checked using the link state request command.
Reply Timeout	Maximum response range of the remote station. 1…999999 [ms]
Max Retry	Maximum number of transmissions. 1..32
Retransmission Time	Minimum interval for retransmission. 1…999999 [ms]
Auto-Generated Database	Enables/Disables automatic database generation. **Auto-Generated Database=Disable** Enable the manual database modeling option.
Originator Address	Originator address (OA) assigned to the second octet of the transmission cause parameter (COT Size=2). 0…255

	Originator Address=0 Disables the addition of the originator address.
CA List	ASDU Common Address List (CA). 1...255 (CA Size=1), 1...65535 (CA Size=2) To add more of the common ASDU address (CA), use the hyphen (-) as the address separator.

Monitor	
Clock Source	Sets the station's time synchronization source. Internal, Line **Clock Source=Internal** Uses the internal clock (operating system). **Clock Source=Line** Used the controller station synchronization command to synchronize the internal clock.
Auto-Generated Database	Enables/Disables automatic database generation. Auto-Generated Database=Disable Enable the manual database modeling option. The database will not be generated automatically if **Data Link.Address=0 (Any),** i.e. all messages trafficked on the communication line will be decoded, but the points will not be added to the database.

6.4 Input and output link

The input and output link is a special function of the simulator for controlled stations, where it is possible to generate return events to the controller station, simulating a change in the field after the execution of a received command.



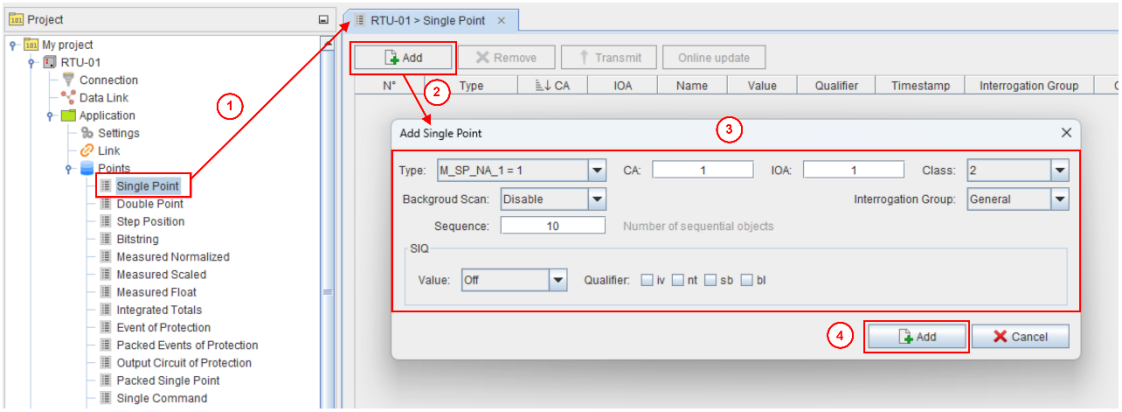
The following associations are possible:

Output	**Entry**
Single command	Single point
Double command	Double point
Regulating step command	Step position
Sepoint command	Measured value

7. Adding Objects to the Database

Database modeling is extremely simple, just follow the steps below to include an object or a sequence of objects.

1. Click (x2) the object group.
2. Click on the "Add" button.
3. Fill in the attributes of the object or sequence of objects.
4. Click the "Add" button in the include window.

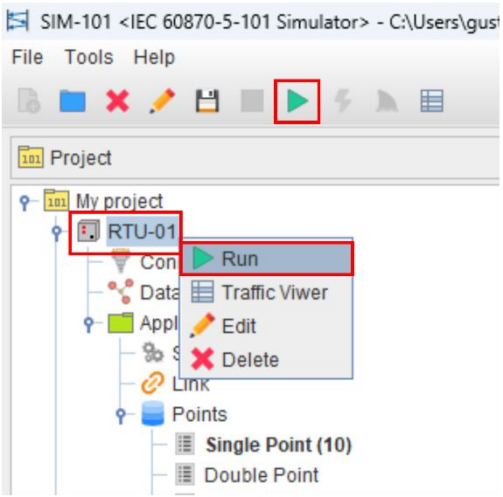


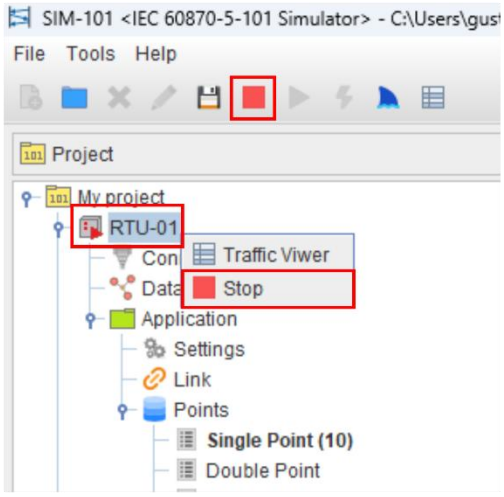
In the case of controlled stations, both inclusion and exclusion of objects can only be carried out with the station switched off. On the other hand, controller stations configured with a manual database generation option (Settings.Auto-Generated Database=Disable) can make changes with the station connected.

8. Starting and Stopping a Simulation

To start or stop the simulation of a station, select it in the project tree and click on the "Run/Stop" button in the toolbar.

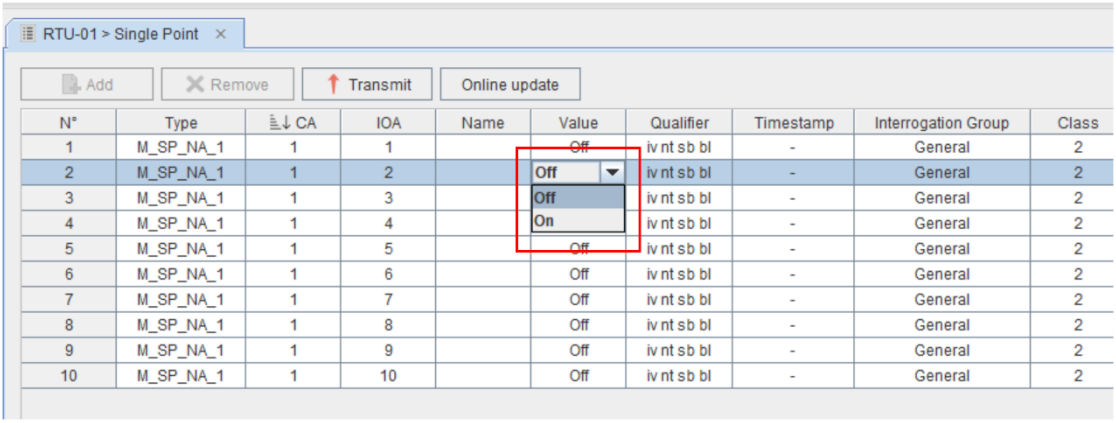
Another option is to right-click on the station icon and select "Run/Stop" from the menu.





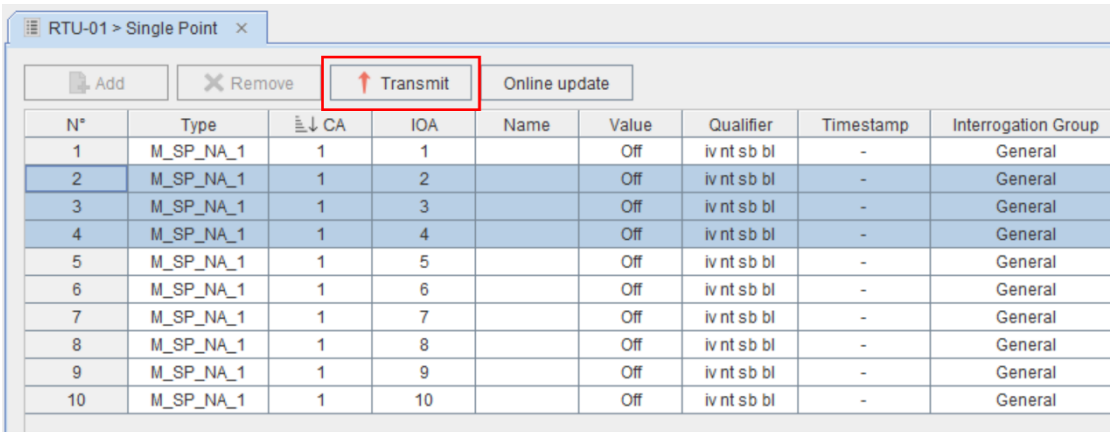
9. Generating events

There are four ways to generate events from the controlled station, the first of which is the generation of spontaneous events by change in the value or quality of the point, this type of event is triggered when the value or qualifier field of the object is changed in the point table.



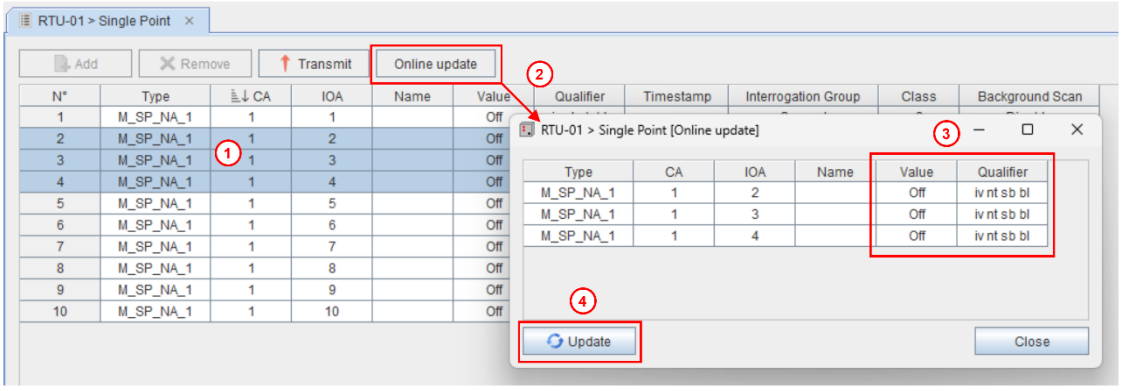
N°	Type	CA	IOA	Name	Value	Qualifier	Timestamp	Interrogation Group	Class
1	M_SP_NA_1	1	1		Off	iv nt sb bl	-	General	2
2	M_SP_NA_1	1	2		Off	iv nt sb bl	-	General	2
3	M_SP_NA_1	1	3		Off	iv nt sb bl	-	General	2
4	M_SP_NA_1	1	4		Off	iv nt sb bl	-	General	2
5	M_SP_NA_1	1	5		Off	iv nt sb bl	-	General	2
6	M_SP_NA_1	1	6		Off	iv nt sb bl	-	General	2
7	M_SP_NA_1	1	7		Off	iv nt sb bl	-	General	2
8	M_SP_NA_1	1	8		Off	iv nt sb bl	-	General	2
9	M_SP_NA_1	1	9		Off	iv nt sb bl	-	General	2
10	M_SP_NA_1	1	10		Off	iv nt sb bl	-	General	2

The second way is to generate spontaneous events without changing the point, in this case just select the points to which you want to generate the event and click on the "Transmit" button.

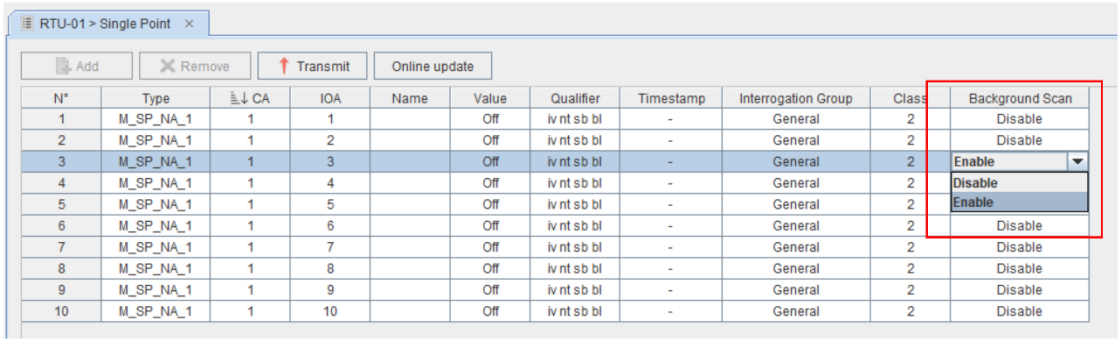


N°	Type	CA	IOA	Name	Value	Qualifier	Timestamp	Interrogation Group
1	M_SP_NA_1	1	1		Off	iv nt sb bl	-	General
2	M_SP_NA_1	1	2		Off	iv nt sb bl	-	General
3	M_SP_NA_1	1	3		Off	iv nt sb bl	-	General
4	M_SP_NA_1	1	4		Off	iv nt sb bl	-	General
5	M_SP_NA_1	1	5		Off	iv nt sb bl	-	General
6	M_SP_NA_1	1	6		Off	iv nt sb bl	-	General
7	M_SP_NA_1	1	7		Off	iv nt sb bl	-	General
8	M_SP_NA_1	1	8		Off	iv nt sb bl	-	General
9	M_SP_NA_1	1	9		Off	iv nt sb bl	-	General
10	M_SP_NA_1	1	10		Off	iv nt sb bl	-	General

The third way is the generation of spontaneous multi-point events by change in value or quality, for this select the objects of interest (1), click on the "Online update" button (2), make the changes in value and/or quality of the objects (3), then click on the "Update" button (4).



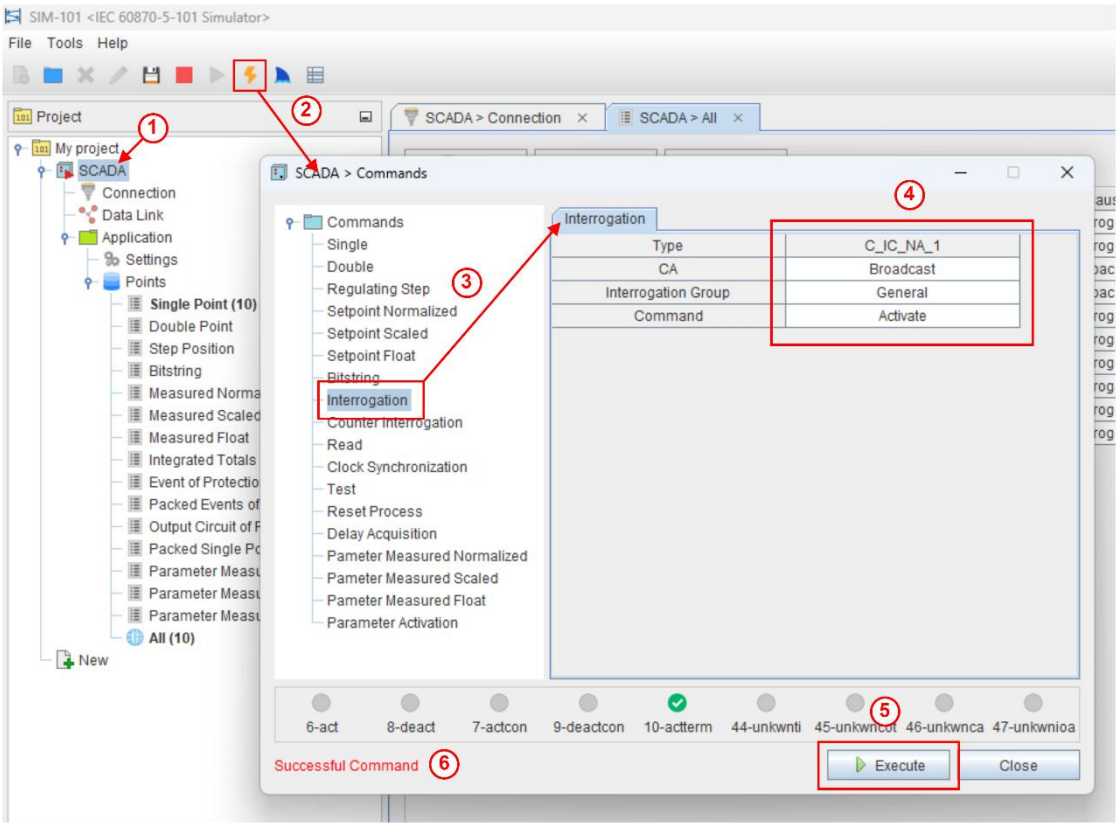
Finally, the last way to generate events is by activating the "Background Scan" or "Cyclic Transmission" function, this is done directly on the points table. Background Scan and Cyclic Transmission events are cyclical and the intervals are configured in the application settings.



10. Running Commands

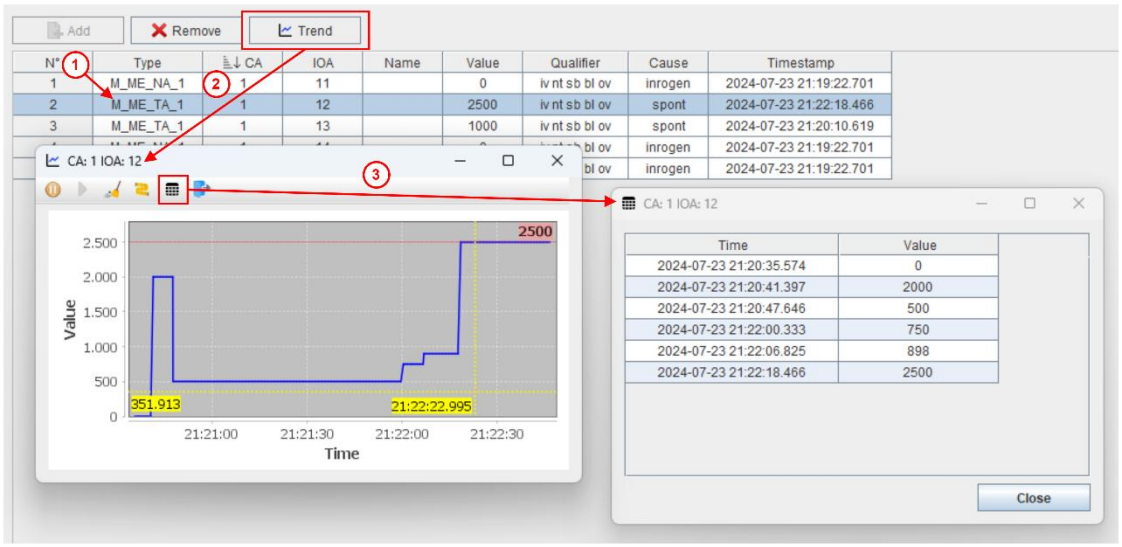
To execute a command from a controller station, simply follow the steps below:

1. Select the station.
2. Click on the "Command" button.
3. Click (x2) on the icon of the command you want to execute.
4. Fill in the parameters of the command.
5. Click on the "Run" button.
6. Wait for the command to return.



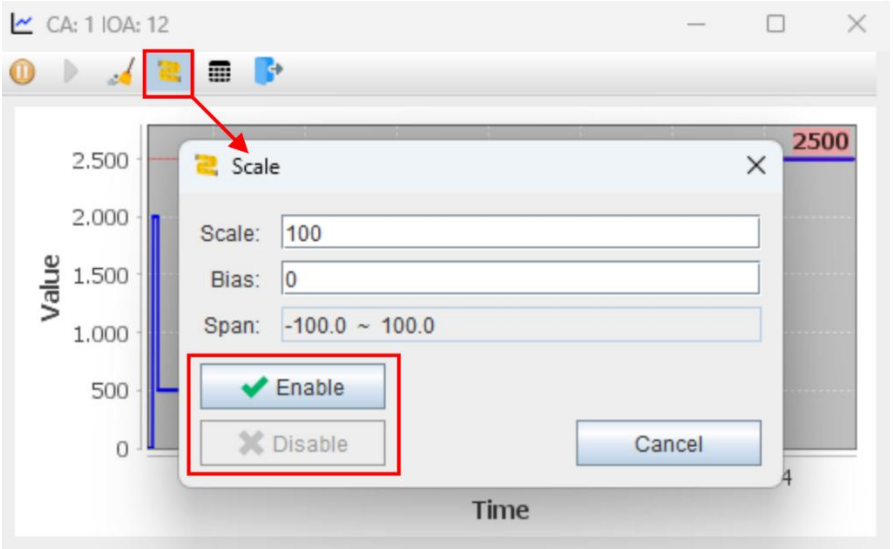
11. Graphical display

In the simulator there is the functionality of graphic visualization of a supervised point, for this just select a single point in the point table (1) and click on the "Trend" button (2), then the window with the graphic information of the point and real time will open, it is also possible to view the list of events that make up the graph, by clicking on the "Table" button (3).



Normalized points (M_ME) can be scaled directly on the chart via the "Scale" button, and the parameters are:

Parameter	Description	Count
Scale	Positive Scale Background	32767
Bias	Value refers to zero	0



12. Protocol Capture

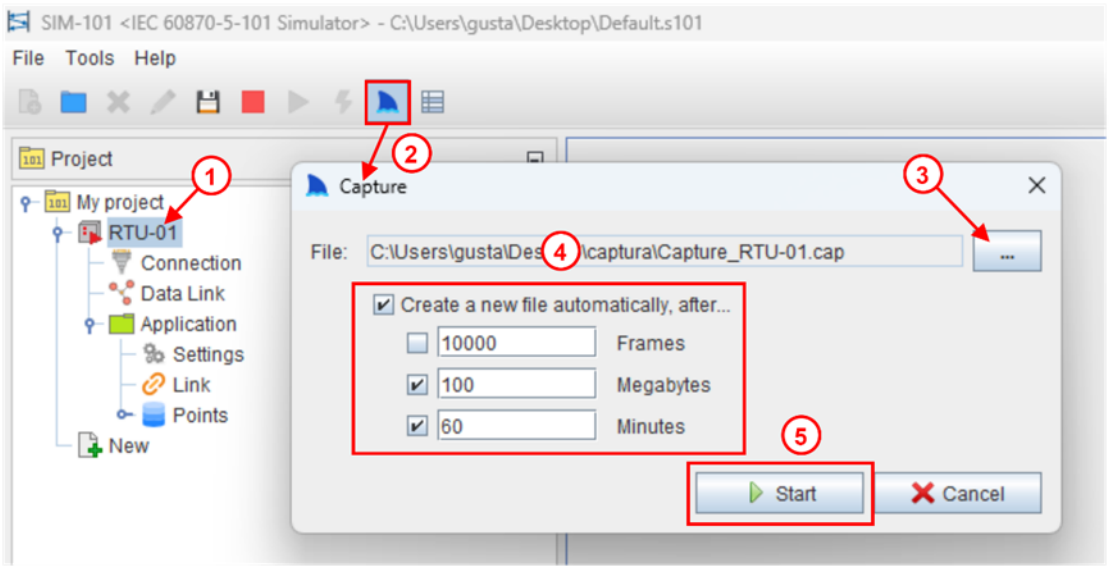
The tool offers protocol capture functionality with persistence on disk, which enables subsequent analysis, especially when monitoring the communication line.

The automatic file creation function uses the "OR" logic, that is, if one of the conditions has been met, a new file will be created to continue recording.

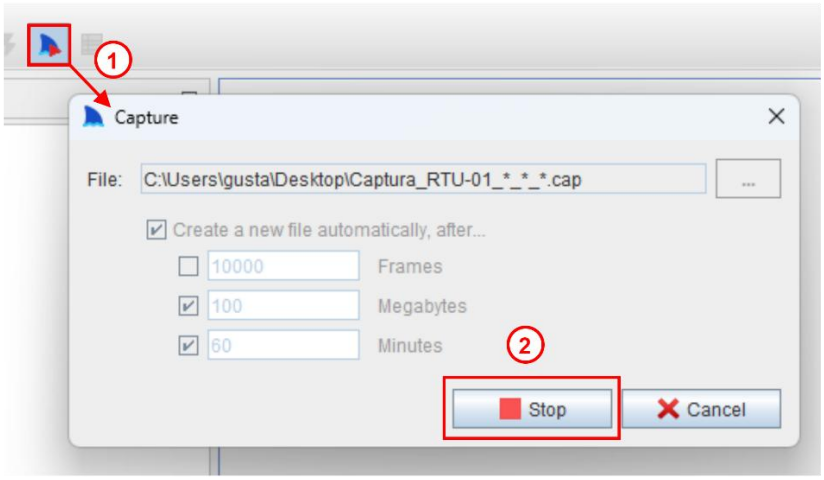
Although the protocol capture can be saved in a single file, it is advisable to create files up to 100Mb to optimize the analysis tool.

To start the protocol capture, you need to follow the steps below:

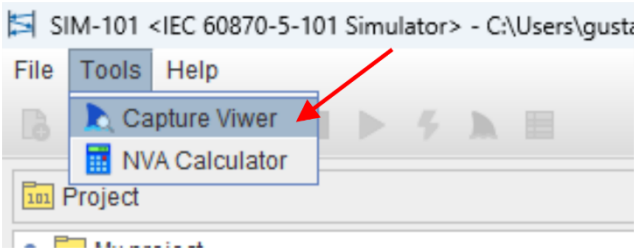
1. Select the station.
2. Click on the "Capture" button.
3. Select the recording file.
4. Select the archiving policy.
5. Click on the "Start" button.



To stop the capture, click the "Capture" button (1) and then click the "Stop" button (2).

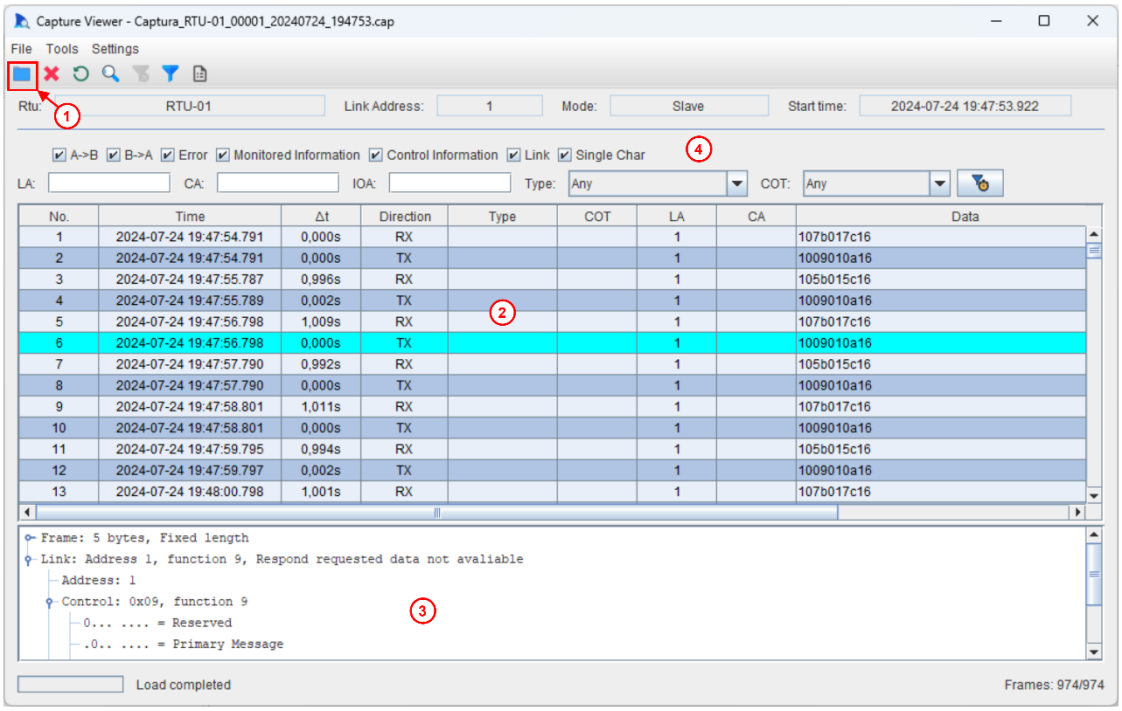


The visualization and analysis of the capture is carried out through the "Capture Viewer" tool that can be accessed through the "Tools" menu.



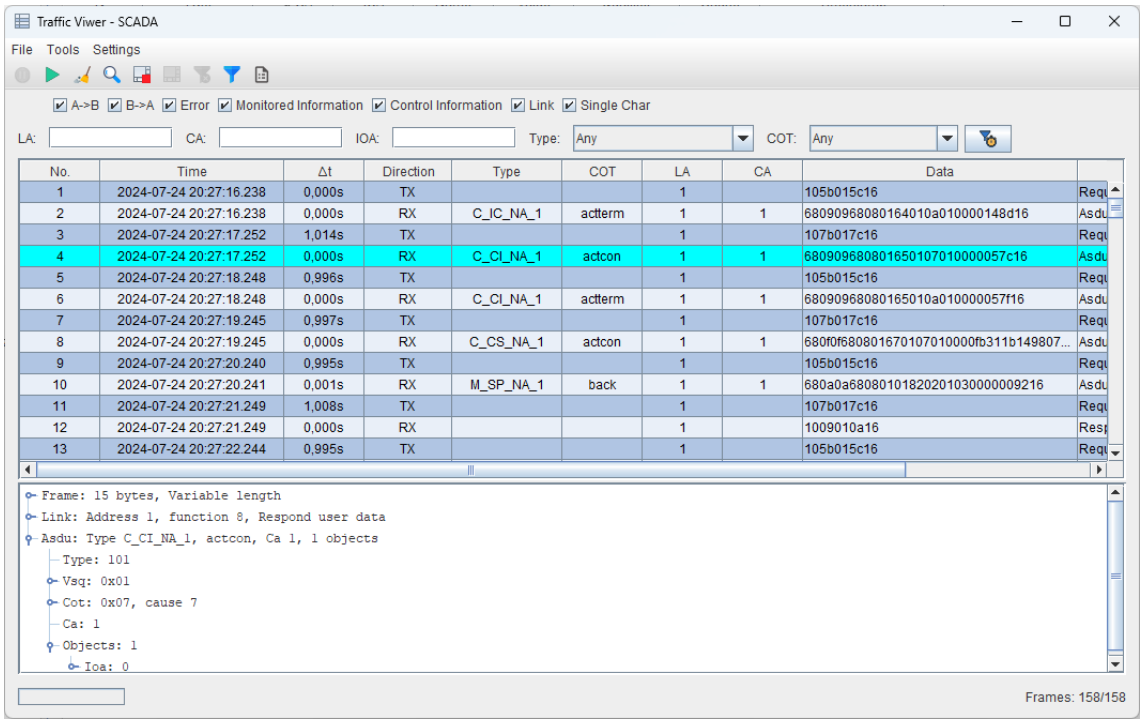
To view the contents of a capture, load the capture file via the "Open" button (1).

In the capture viewer, the traffic is displayed in the form of a table (2), being detailed in the panel below (3) when selected. In addition, several filters (4) can be applied to facilitate the analysis of a failure, for example, or the occurrence of an event.

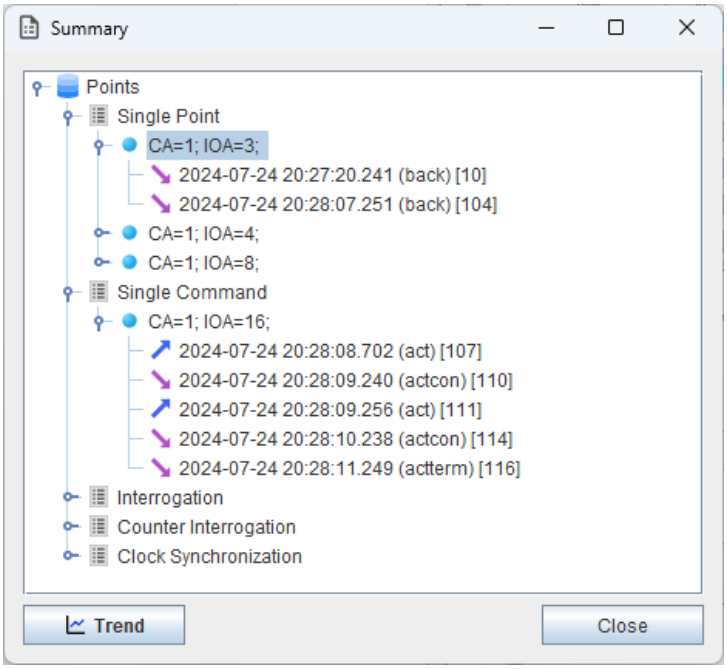


13. Traffic Viewer

In addition to the station's exit terminal, it is possible to view the traffic through the "Traffic Viewer" tool, it is like the "Capture Viewer" tool, with basically the only difference being the fact that it is in real time.



The traffic viewer also has an extremely useful function called "Summary", it summarizes the events in a hierarchical model, making it easy to search by type and address of the object.

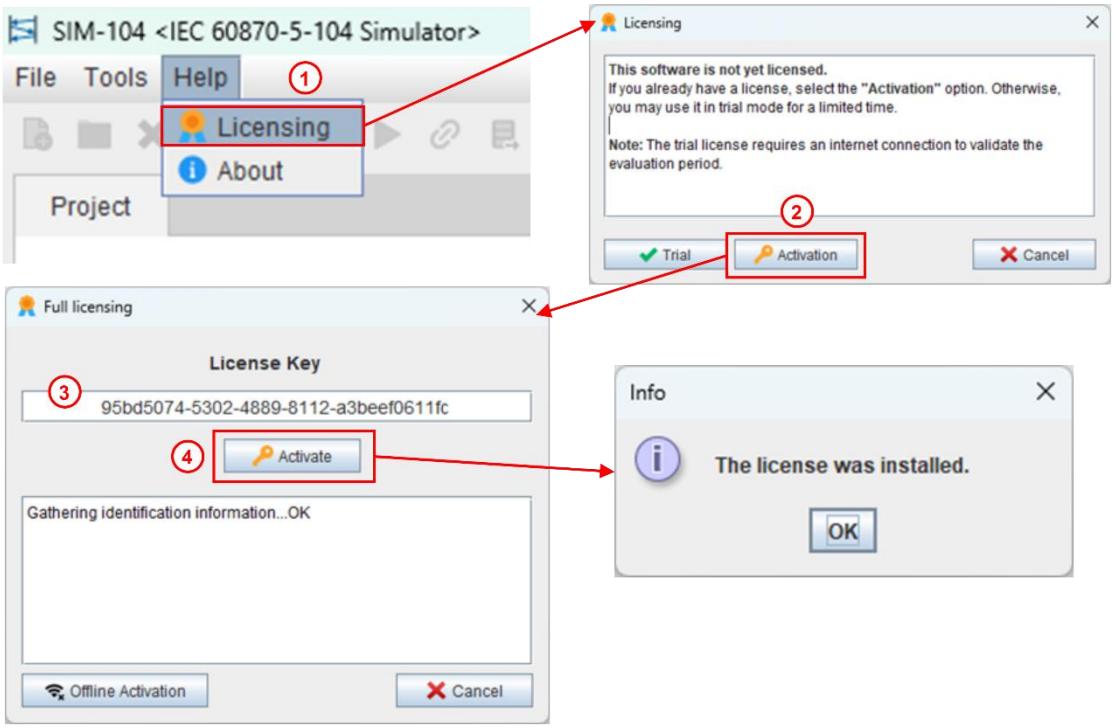


14. Licensing

SIM-101 is software licensed by Sim-Systems, so for full use of the simulator it is necessary to license it.

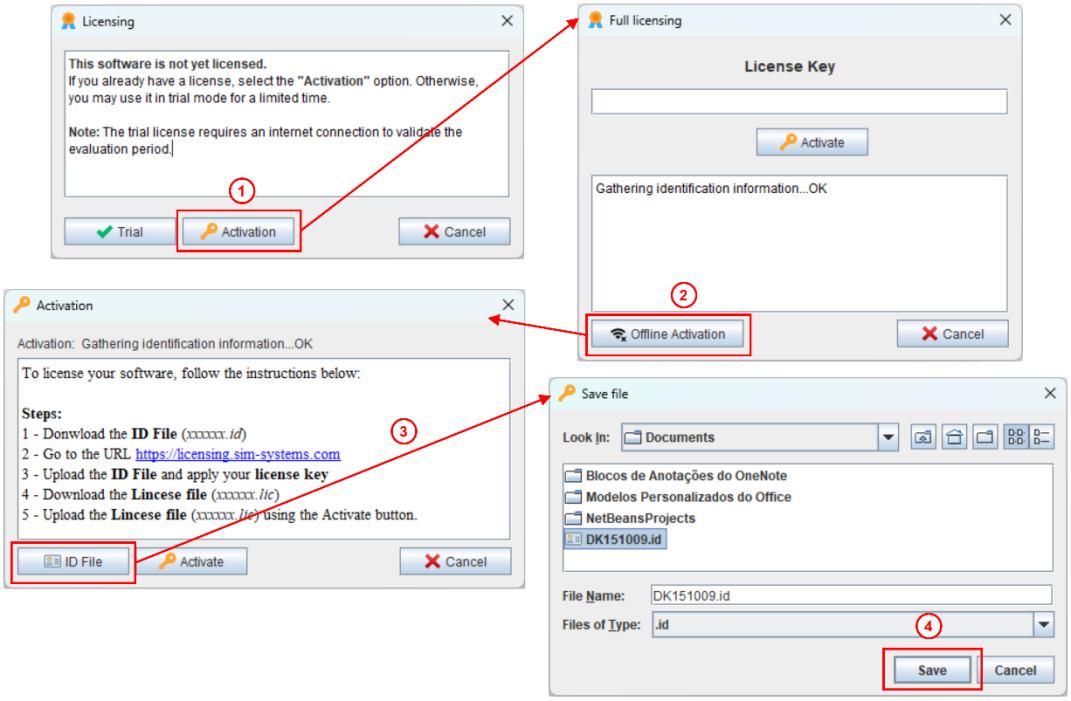
Licensing can be carried out online or offline for machines that do not have internet access. Online licensing is very simple, just follow the instructions below:

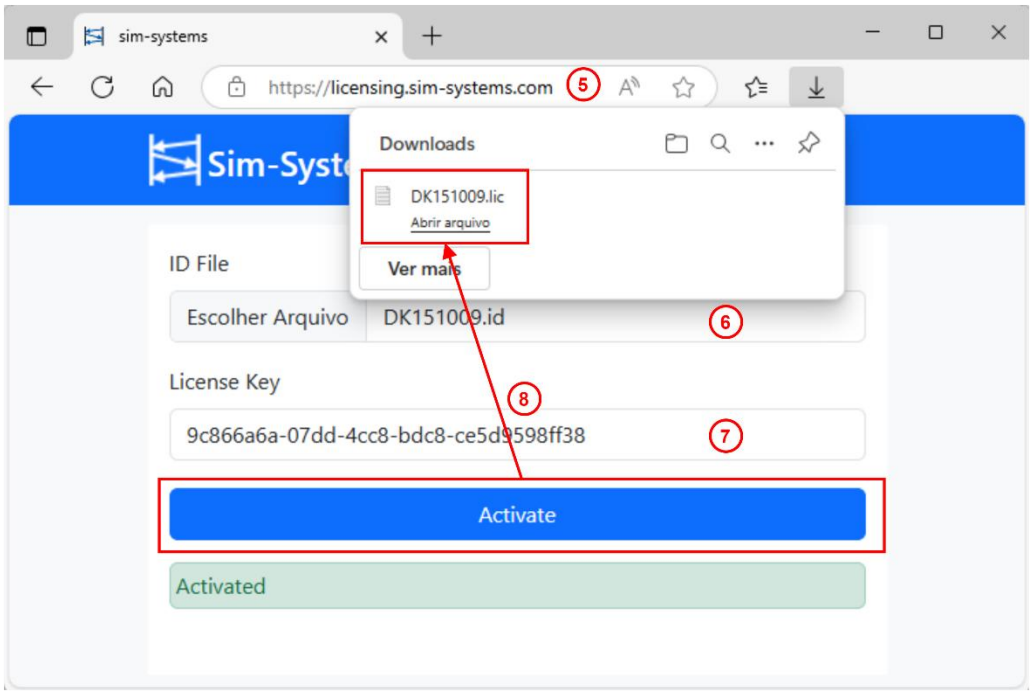
1. Access the "Help" menu and select the "Licensing" submenu.
2. Click on the "Activation" button.
3. Fill in the "License Key" field with the purchased key.
4. Click on the "Activate" button.

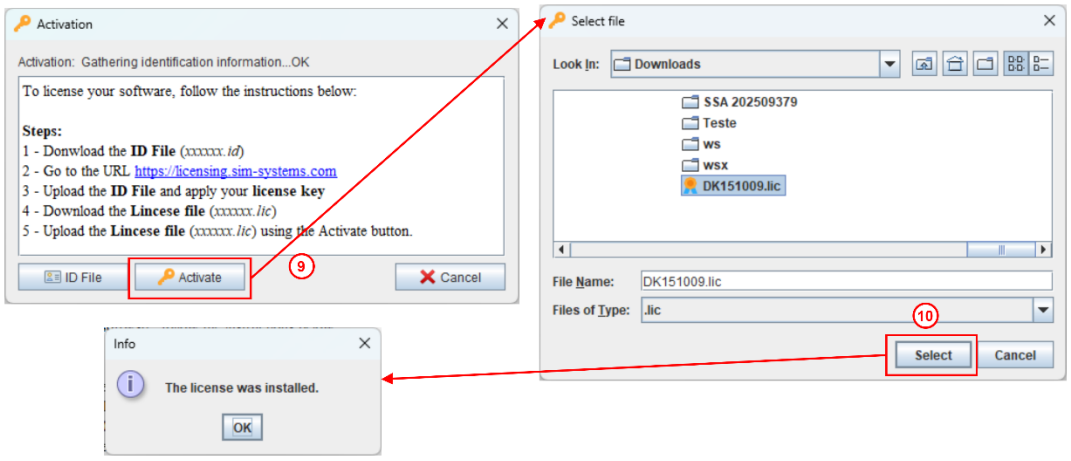


For offline licensing, perform the following steps:

1. Click on the "Activation" button in the licensing window.
2. Click on the "Offline Activation" button.
3. Click on the "ID File" button.
4. Save the machine's identification file.
5. Access the webpage https://licensing.sim-systems.com.
6. Select ID file (.id).
7. Fill in the "License Key" field with the purchased key.
8. Click on the "Activate" button then the license file (.lic) will be downloaded.
9. In the activation window, click on the "Activate" button.
10. Select the licensing file (.lic).


Licensing
This software is not yet licensed.
If you already have a license, select the "Activation" option. Otherwise, you may use it in trial mode for a limited time.
Note: The trial license requires an internet connection to validate the evaluation period.
1
Trial
Activation
Cancel
Full licensing
License Key
Activate
Gathering identification information...OK
2
Offline Activation
Cancel
Activation
Activation: Gathering identification information...OK
To license your software, follow the instructions below:
Steps:
1 - Donwload the ID File (xxxxxx.id)
2 - Go to the URL https://licensing.sim-systems.com
3 - Upload the ID File and apply your license key
4 - Download the Lincese file (xxxxxx.lic)
5 - Upload the Lincese file (xxxxxx.lic) using the Activate button.
3
ID File
Activate
Cancel
Save file
Look In: Documents
Blocos de Anotações do OneNote
Modelos Personalizados do Office
NetBeansProjects
DK151009.id
File Name: DK151009.id
Files of Type: .id
4
Save
Cancel


sim-systems
https://licensing.sim-systems.com
5
Downloads
DK151009.lic
Abrir arquivo
Ver mais
Sim-Syst
ID File
Escolher Arquivo
DK151009.id
6
License Key
8
9c866a6a-07dd-4cc8-bdc8-ce5d9598ff38
7
Activate
Activated


Activation
Activation: Gathering identification information...OK
To license your software, follow the instructions below:
Steps:
1 - Donwload the ID File (xxxxxx.id)
2 - Go to the URL https://licensing.sim-systems.com
3 - Upload the ID File and apply your license key
4 - Download the Lincese file (xxxxxx.lic)
5 - Upload the Lincese file (xxxxxx.lic) using the Activate button.
ID File
Activate
Cancel
9
Select file
Look In:
Downloads
SSA 202509379
Teste
ws
wsx
DK151009.lic
File Name:
DK151009.lic
Files of Type:
.lic
10
Select
Cancel
Info
The license was installed.
OK