Grid Automation Products

ITT600 SA Explorer
Integrated Testing Tool
User Manual
ITT600 SA Explorer Ver. 2.1

© Hitachi Energy 2021. All rights reserved.

EU Declaration of Conformity REC650

Document identity

Revision C

Declaration
We Hitachi Energy Sweden AB, SE-721 59 Västerås, Sweden, declare under our sole responsibility that the family of apparatus:

Bay Control Type: REC650, Ver. 1.0 acc. to Product Guide 1MRK 511211-BEN to which this declaration relates is in conformity with the following relevant Union harmonization legislations:

Directives
2014/30/EU EMC Directive
Official Journal of the EU (L96, 29/03/2014, p. 79-106)
2014/35/EU Low Voltage Directive
Official Journal of the EU (L96, 29/03/2014, p. 357-374)

Application of the objects
The product is intended for use in the industrial environment and to protect high voltage or high-power apparatus, and thus normally used in a harsh electromagnetic environment near high voltage apparatus.

Harmonized Standards
References to the relevant harmonized standards or other technical specifications to which conformity is declared:

EN 60255-26: 2013 Electromagnetic compatibility requirements
EN 60255-27: 2014 Product safety requirements

Authorization
Signed for and on behalf of:
Marko Kovacic (PM)

Date
Copyright

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

Hitachi Energy is a registered trademark of Hitachi Energy Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Warranty

Please inquire about the terms of guarantee from your nearest Hitachi Energy representative.
Disclaimer

We reserve the right to make technical changes or modify the contents of this document without prior notice.

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guarantee properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity, applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This document has been carefully checked by Hitachi Energy but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments in no event shall Hitachi Energy be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

Important notice

Experience has shown that reliable operation of our products is assured, providing the information and recommendations contained in these Operating Instructions are adhered to.

It is scarcely possible for the instructions to cover every eventuality that can occur when using technical devices and systems. We would therefore request the user to notify us directly or our agent of any unusual observations or instances, in which these instructions provide no or insufficient information.

In addition to these instructions, any applicable local regulations and safety procedures must always be strictly observed both when connecting up and commissioning this equipment.

We expressly accept no responsibility or liability for any damage, which may result from operation of this equipment, even if no reference is made to the particular situation in the Operating Instructions.

ABB is a registered trademark of ABB Asea Brown Boveri Ltd. Manufactured by/for a Hitachi Energy company.
Table of contents

Section 1  Introduction..............................................................................................................5
  1.1  Scope of the document................................................................................................. 5
  1.2  Abbreviations and definitions....................................................................................... 5
    1.2.1  Abbreviations.............................................................................................................. 5
    1.2.2  Definitions.................................................................................................................. 6
  1.3  References...................................................................................................................... 6
  1.4  Overview......................................................................................................................... 7

Section 2  Configuration...................................................................................................... 9
  2.1  Network Interface Card settings.................................................................................... 9
    2.1.1  IP Address.................................................................................................................. 9
    2.1.2  Virtual LAN (VLAN).................................................................................................. 9
  2.2  Software firewalls......................................................................................................... 9
  2.3  VPN clients................................................................................................................... 10
  2.4  Changing OSI address parameters............................................................................... 11
  2.5  Debug and trace output configuration......................................................................... 11
  2.6  Ethernet switch configuration...................................................................................... 12

Section 3  Functionality...................................................................................................... 13
  3.1  ITT600 – Explore IEDs................................................................................................. 13
    3.1.1  Overview.................................................................................................................. 13
    3.1.2  Keyboard shortcuts................................................................................................. 13
    3.1.3  File Menu................................................................................................................ 14
    3.1.4  Edit menu............................................................................................................... 14
    3.1.5  Tools menu............................................................................................................. 15
    3.1.6  ITT600 SA Explorer options.................................................................................. 15
    3.1.7  Help menu............................................................................................................. 18
    3.1.8  Tree navigation panel............................................................................................. 18
      3.1.8.1  Tree View “By Subnetworks”........................................................................... 19
      3.1.8.2  Tree View “By Substation”............................................................................. 20
    3.1.9  Get Started Panel.................................................................................................... 22
    3.1.10  Main panel............................................................................................................ 22
      3.1.10.1  Object properties.......................................................................................... 22
      3.1.10.2  Dockable panes............................................................................................ 23
      3.1.10.3  Object details............................................................................................... 24
    3.1.11  Coloring rules........................................................................................................ 25
    3.1.12  Debug and logging information............................................................................ 26
    3.1.13  Working with IED configurations....................................................................... 27
      3.1.13.1  Working offline............................................................................................ 27
      3.1.13.2  Working online............................................................................................ 31
      3.1.13.3  Dynamic Data Sets...................................................................................... 45
      3.1.13.4  Read VMD Specific Variables of an IED..................................................... 50
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.15</td>
<td>Exporting IEDs to an SCD file.</td>
<td>65</td>
</tr>
<tr>
<td>3.1.16</td>
<td>Quick Checker.</td>
<td>66</td>
</tr>
<tr>
<td>3.1.16.1</td>
<td>Checking IED status.</td>
<td>66</td>
</tr>
<tr>
<td>3.1.16.2</td>
<td>Checking network devices status.</td>
<td>66</td>
</tr>
<tr>
<td>3.1.16.3</td>
<td>Status indicators.</td>
<td>67</td>
</tr>
<tr>
<td>3.1.16.4</td>
<td>Operation.</td>
<td>67</td>
</tr>
<tr>
<td>3.1.17</td>
<td>IED Status View.</td>
<td>69</td>
</tr>
<tr>
<td>3.1.17.1</td>
<td>Overview.</td>
<td>69</td>
</tr>
<tr>
<td>3.1.17.2</td>
<td>Functionality.</td>
<td>69</td>
</tr>
<tr>
<td>3.1.18</td>
<td>IED simulation.</td>
<td>72</td>
</tr>
<tr>
<td>3.1.18.1</td>
<td>Overview.</td>
<td>72</td>
</tr>
<tr>
<td>3.1.18.2</td>
<td>IED simulation options.</td>
<td>74</td>
</tr>
<tr>
<td>3.1.18.3</td>
<td>Start IED simulation.</td>
<td>76</td>
</tr>
<tr>
<td>3.1.18.4</td>
<td>IED Status View.</td>
<td>77</td>
</tr>
<tr>
<td>3.1.18.5</td>
<td>Stopping a simulated IED.</td>
<td>78</td>
</tr>
<tr>
<td>3.2</td>
<td>ITT600 – Explore Ethernet.</td>
<td>78</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Overview.</td>
<td>78</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Keyboard shortcuts.</td>
<td>79</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Toolbar.</td>
<td>80</td>
</tr>
<tr>
<td>3.2.4</td>
<td>Capture window.</td>
<td>81</td>
</tr>
<tr>
<td>3.2.5</td>
<td>Packet information.</td>
<td>82</td>
</tr>
<tr>
<td>3.2.6</td>
<td>Status bar.</td>
<td>82</td>
</tr>
<tr>
<td>3.2.7</td>
<td>Working with ITT600 – Explore Ethernet.</td>
<td>82</td>
</tr>
<tr>
<td>3.2.7.1</td>
<td>Working with capture files.</td>
<td>82</td>
</tr>
<tr>
<td>3.2.7.2</td>
<td>Capture network traffic.</td>
<td>82</td>
</tr>
<tr>
<td>3.2.7.3</td>
<td>Analyzing network packets.</td>
<td>84</td>
</tr>
<tr>
<td>3.2.7.4</td>
<td>The different filters.</td>
<td>88</td>
</tr>
<tr>
<td>3.2.7.5</td>
<td>Export captured packets to Excel.</td>
<td>92</td>
</tr>
<tr>
<td>3.2.7.6</td>
<td>Import captured packets from Excel.</td>
<td>93</td>
</tr>
<tr>
<td>3.2.7.7</td>
<td>Dump MMP PDUs.</td>
<td>93</td>
</tr>
<tr>
<td>3.2.7.8</td>
<td>Options and default settings.</td>
<td>93</td>
</tr>
<tr>
<td>3.2.8</td>
<td>Statistics.</td>
<td>94</td>
</tr>
<tr>
<td>3.2.9</td>
<td>Send capture file.</td>
<td>95</td>
</tr>
<tr>
<td>3.2.10</td>
<td>Send a packet.</td>
<td>96</td>
</tr>
<tr>
<td>3.2.11</td>
<td>Toggle relative/absolute time.</td>
<td>96</td>
</tr>
<tr>
<td>3.2.12</td>
<td>Find in packet data.</td>
<td>97</td>
</tr>
<tr>
<td>3.2.13</td>
<td>Protocol specific information.</td>
<td>98</td>
</tr>
<tr>
<td>3.2.13.1</td>
<td>MMS.</td>
<td>98</td>
</tr>
<tr>
<td>3.2.13.2</td>
<td>GOOSE/RGOOSE/Tunneled RGOOSE.</td>
<td>100</td>
</tr>
</tbody>
</table>
Section 4  Limitations........................................................................................................141
Section 5  Appendix........................................................................................................143
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Troubleshooting</td>
<td>143</td>
</tr>
<tr>
<td>5.2 ITT600 – Explore IEDs Default Address Parameters</td>
<td>143</td>
</tr>
<tr>
<td>5.2.1 Local Address</td>
<td>144</td>
</tr>
<tr>
<td>5.2.2 Remote Address</td>
<td>144</td>
</tr>
<tr>
<td>5.3 ITT600 – Explore Ethernet Supported Protocols</td>
<td>144</td>
</tr>
<tr>
<td>5.4 IEC 61850 Edition 2 features</td>
<td>145</td>
</tr>
<tr>
<td>5.4.1 Local Remote Handling Feature</td>
<td>145</td>
</tr>
<tr>
<td>5.4.2 Mode Behavior Handling</td>
<td>145</td>
</tr>
<tr>
<td>5.5 IEC 61850 Edition 2.1 features</td>
<td>146</td>
</tr>
<tr>
<td>5.5.1 GOOSE replay protection algorithm</td>
<td>146</td>
</tr>
</tbody>
</table>
Section 1  Introduction

1.1 Scope of the document

This document is the user manual for the ITT600 SA Explorer. As such it describes the functionality, configuration and operation of the product packages.

This manual does not include an introduction to the IEC 61850 standard. References to IEC 61850 and Substation automation can be found in Section "References".

1.2 Abbreviations and definitions

1.2.1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACP</td>
<td>Ethernet Capture File Format</td>
</tr>
<tr>
<td>ACSI</td>
<td>Abstract Communication Service Interface</td>
</tr>
<tr>
<td>BRCB</td>
<td>Buffered Report Control Block</td>
</tr>
<tr>
<td>CDC</td>
<td>Common Data Classes, see</td>
</tr>
<tr>
<td>DA</td>
<td>Data Attribute</td>
</tr>
<tr>
<td>DO</td>
<td>Data Object</td>
</tr>
<tr>
<td>DS</td>
<td>Data Set</td>
</tr>
<tr>
<td>FC</td>
<td>Functional Constraint</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GI</td>
<td>General Interrogation</td>
</tr>
<tr>
<td>GOOSE</td>
<td>Generic Object Oriented Substation Event</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>ITT</td>
<td>Integrated Testing Toolbox</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LN</td>
<td>Logical Node</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MMS</td>
<td>Manufacturing Message Specification</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>RCB</td>
<td>Report Control Block</td>
</tr>
<tr>
<td>RMS</td>
<td>Root Mean Square</td>
</tr>
</tbody>
</table>

Table continues on next page
### 1.2.2 Definitions

**Tip icon** indicates special advice. Examples:

- Recommendation for a system configuration that is not a strict requirement, but typically is advantageous.
- Alternative method for performing a function.

**Warning icon** indicates important advice that has to be followed.

- **Packet** An OSI layer 3 information unit transmitted in a frame
- **Frame** An OSI layer 2 information unit transmitted as a whole

### 1.3 References

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61850-1</td>
<td>Introduction and Overview</td>
</tr>
<tr>
<td>IEC 61850-7-3</td>
<td>Common Data Classes</td>
</tr>
<tr>
<td>IEC 61850-7-4</td>
<td>Compatible Logical Node Classes</td>
</tr>
<tr>
<td>IEC 61850-8-1</td>
<td>Mappings to MMS</td>
</tr>
<tr>
<td>IEC 61850-9-2</td>
<td>Sampled Values over ISO/IEC 8802-3</td>
</tr>
<tr>
<td>IEC 61850-90-4</td>
<td>Network Engineering Guidelines</td>
</tr>
<tr>
<td>IEC 62351-6</td>
<td>Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850</td>
</tr>
<tr>
<td>IEC 61869-9</td>
<td>Digital interface for instrument transformers</td>
</tr>
</tbody>
</table>

1.4 Overview

Integrated testing tool ITT600 SA Explorer is designed for easy diagnosis and troubleshooting of IEC 61850-based substation automation systems and applications.

It features convenient navigation, comprehensive presentation of application data, and support for system consistency check both on-line and off-line. This allows anybody to use the same tool to analyze and debug substation automation applications regardless of their level of knowledge of IEC 61850 communication.

The ITT600 SA Explorer tool offers facilities for exploring and analyzing the communication configuration of the protection and control IEDs (Intelligent Electronic Devices) and IEC 61850 communication in substation automation systems, including GOOSE messages. Its versatile functionality eliminates the need for multiple testing tools for different purposes, such as MMS browsers, and protocol and Ethernet analyzers.

The powerful features of ITT600 SA Explorer provide test engineers with access to any IEC 61850-compliant IED. The tool’s various functions allow efficient testing of the IED application and isolate the root cause of system communication problems. This significantly reduces testing and commissioning time.

ITT600 SA Explorer is easy to use, and does not require the skills of a data communication specialist. By translating the complex terminology of communication protocols into the standardized IEC 61850 language, it makes the essential information available to all users.

ABB’s comprehensive suite of tools for engineering, integration and testing supports you throughout the complete lifecycle of protection and control IEDs and IEC 61850-based substation automation systems. With many advanced features, the tools allow you to manage your installation efficiently in all situations from engineering and commissioning to operation and maintenance.

![Figure 1: ABB’s SA Tools landscape](image)

The ITT600 SA Explorer can be divided in five main parts:

**ITT600 – Explore IEDs** enables the user to either browse SCL file contents or retrieving the IEC 61850 related configuration from any compliant IED over the network. Its full-fledged IEC 61850 client allows to do various operations on multiple IEDs in parallel. Additionally, it provides the functionality to simulate one IED of the loaded SCL file.

**ITT600 – Explore Ethernet** is an easy to use protocol analyzer that supports SA related protocols. It is able to present the transmitted IEC 61850 data in a user readable form, without having a deep knowledge about the protocols. This functionality simplifies troubleshooting of communication problems significantly.

**ITT600 – Explore Models** enables the user to compare SCL related data. It does not matter whether two SCL compatible files or online data are compared. This functionality again simplifies troubleshooting because every configuration can be compared against a reference.
ITT600 – Explore GOOSE visualizes GOOSE data in an Oscilloscope style. Several individual Data Attributes sent in GOOSE frames can easily be compared and measured. This enables faster debugging and comprehension of distributed application logic using GOOSE.

ITT600 – Explore SV visualizes IEC 61850-9-2 LE data streams using a polar chart. Two different data streams can easily be visualized and compared at the same time. The Oscilloscope view shows current and voltage trends, allowing the user to inspect the content of each SV packet.

Figure 2 illustrates the wide variety of usages of ITT600 SA Explorer.
Section 2  Configuration

To ensure its full functionality, ITT600 requires that some general settings are checked.

2.1  Network Interface Card settings

Usually no special settings have to be made to the Network Interface Card (NIC). However, some models with their specific drivers need to be adjusted so they do not block specific packets.

2.1.1  IP Address

To be able to browse an IED, the NIC of the PC has to be configured to be in the same network as the IED. Usually this is done by configuring the same subnet mask and a similar IP address within the same subnet that the IED is using. See Figure 3.

![Figure 3: IP Addresses for an IED and ITT600 SA Explorer PC](Image)

The ITT600 SA Explorer PC should be in the same network as the IEDs, to be able to connect them.

2.1.2  Virtual LAN (VLAN)

Depending on the settings of the NIC, it might happen that the VLAN tags in the packets are discarded before the packet is passed to the capturing engine.

Refer to the vendor specific documentation on how to configure the NIC in a way that it is transparent.

2.2  Software firewalls

Software firewalls could also block specific packets. How to disable software based firewalls is described in its own user manual.
As a general rule, there is usually a Service that has to be stopped from the Windows Control Panel, or the firewall allows it to be disabled by a menu entry or an icon.

For correct MMS operation, port 102 also needs to be enabled. For MMS simulation, port 5007 also needs to be enabled.

It is not recommended to disable any firewall without informing the Network Administrator in your organization in advance. The firewall should only be disabled during testing sessions. It is not recommended to keep it disabled all the time. As well, if ITT600 SA Explorer is to be run on virtual machine, Windows Defender service may have to be turned off.

2.3 VPN clients

Some VPN clients might also interfere the packets capturing process. Again, disabling the VPN client can solve this issue.

Some VPN clients can be disabled by changing the used item on a connection in the network connection properties. An example is shown in Figure 4.

It is not recommended to disable any VPN Software without informing the Network Administrator in your organization in advance. The VPN Software should only be disabled during testing sessions. It is not recommended to keep it disabled all the time.

![Figure 4: Disabling a VPN client in the network connection properties](image-url)
2.4 Changing OSI address parameters

Some IED might need special OSI address parameters to be able to connect to the device. Usually the remote address parameters are defined in the SCL, or can be configured in the Create Server Dialog.

For a list of default address parameters, see section "ITT600 – Explore IEDs Default Address Parameters".

2.5 Debug and trace output configuration

ITT600 SA Explorer logs error messages and additional information during operation. See "Debug and logging information" for more information.

The logging functionality of ITT600 SA Explorer can be configured in the Options dialog. User can define the amount of information to be logged.

Changing the logger configuration could slow down the whole application and is therefore not recommend for in-experienced users.

![ITT600 SA Explorer Options](image)

**Figure 5:** Define Log Level
2.6 Ethernet switch configuration

ITT600 SA Explorer needs no special environment for operation. However, since switched networks are used in IEC 61850 SA systems, some basic configuration has to be followed to be able to capture network traffic between two endpoints.

Figure 6 shows a basic system setup in an abstract form. To capture the traffic between IED1 and the SCADA System, the Ethernet switch has to be configured in a way that it sends all traffic received on the port where the SCADA System is connected to the port the ITT600 SA Explorer notebook is connected. This is called **Port Mirroring**. Depending on the switch manufacturer, it can be configured in a different way.

![Figure 6: Basic SA system setup](image-url)
Section 3  Functionality

This chapter describes the different software components that are bundled together in ITT600 SA Explorer.

3.1 ITT600 – Explore IEDs

3.1.1 Overview

ITT600 – Explore IEDs enables the user to browse and display the IEC 61850 related parts of IEDs. This can be done online over the network or offline with a SCL compliant configuration file (typically a SCD file describing the whole substation). Further it allows the user to simulate one IEC 61850 IED.

The main user interface of the ITT600 – Explore IEDs application, as shown in Figure 7 is divided into four main areas:

• Menus (yellow)
• Tree Navigation (blue)
• Get Started Panel and Main Panel (red)
• Debug and Logging Information (green)

Figure 7: ITT600 SA Explorer main user interface

Four main menus are available within ITT600 – Explore IEDs for performing high-level operations and launching the other ITT600 parts. The following sections give an overview of the available functions. How those features can be used, is described in section "Working with IED configurations".

3.1.2 Keyboard shortcuts

ITT600 main window provides following keyboard shortcuts:
### 3.1.3 File Menu

The file menu provides access to the following operations (see Figure 8):

- Loading an IEDs configuration from a SCL compatible file
- Opening a SCD file that has been opened in the past (the Open Recent sub-menu)
- Inserting a recently added IED to navigation tree (the Open Recent IEDs sub-menu)
- Exporting browsed IEDs to an SCD file (only available when no SCD file was loaded).
- Exiting the program (the Exit menu item)

![Figure 8: ITT600 – Explore IEDs File menu](image)

### 3.1.4 Edit menu

The edit menu essentially serves as an alternative to the context menu of the tree navigation panel and provides access to the following operations (see Figure 9):

- Adding an IED to the root of the navigation tree (the Add IED... menu item) with a user-provided name
- Auto-detecting IEDs on the network and adding them to the root of the navigation tree
- Connecting all IEDs
- Disconnecting all IEDs
- Clearing the entire configuration (the Clear Tree menu item)
3.1.5 Tools menu

The tools menu provides access to the following functions (see Figure 10):

- Launching of ITT600 – Explore Ethernet
- Launching of ITT600 – Explore Models
- Launching of ITT600 – Explore GOOSE
- Launching of ITT600 – Explore SV
- Options

3.1.6 ITT600 SA Explorer options

The Options dialog allows the user to set different parameters related to operational behavior of the software. The options dialog box contains six tabs where the user can set parameters on different parts of ITT600 SA Explorer, namely:

- General
- IED Simulation
- Explore IEDs
- Explore Ethernet
- Explore GOOSE
- Explore SV

General Options and Explore IEDs Options are elaborated in this part. Tool specific options are described in their own dedicated sections.
General settings

The following parameters are tunable (see Figure 11):

- **Network adapter**: user can select available network adapters that are detected at the local computer. At least one network adapter should be selected to completely use all functionalities in ITT600 SA Explorer.
- **Language**: User can set the preferred language.
- **Files Directory**: User can select the path to store ITT600 SA Explorer files.
- **Display Local Time**: User can choose to display local time (adjusted to local computer time) or recorded (UTC) time.
- **Display time in microseconds**: user can choose the precision of time display.
- **Display Customer Names of SCD File**: Show the customer names in brackets after the logical name (SCD file has to be reloaded to activate this setting).
- **Check for Updates at Startup**: ITT600 will check if there is available new version at startup.
- **Show Debug Log**: Activating this parameter shows Debug and Logging Information in the overall ITT600 SA Explorer window.
- **Log File Path**: User can define the path to store the log files.
- **Logging Level**: Select whether to do a minimum or complete verbose logging. Verbose logging logs all the error, warning and informational logs.
- **Delete Log Files**: Deletes the available log files.
Explore IEDs settings

The following parameters are tunable (see Figure 12)

- **Number of Event List Entries**: User can define the number of event list entries and *Prefer desc* attribute over ‘d’ or ‘dU’.
- **View – Options**: User are offered the possibilities to show the following information:
  - Show dynamic Dataset configuration
  - Expand Data Attribute list view
  - Include Data Attribute in tree view
  - Display logical Devices hierarchically
- **MMS Client Timeout (ms)**: This setting can be used to set maximum time the user wants ITT600 SA Explorer to wait for the reply from IED.

Depending on the load of the IED, it may need longer time to response to an MMS query from ITT600 SA Explorer. When the time to wait for the IED’s response exceeds the define timeout, ITT600 SA Explorer will send out the next MMS query.

- **MMS File Transfer Wild Card**: This setting enables user to define a filtering for all files to be downloaded based on MMS query.
- **Default TLS port**: Default TLS port used to setup TLS connection.
- **MMS keepalive interval [sec]**: Time interval after ITT will perform MMS ‘status’ or ‘identify’ service query, depending which one is supported by an IED to keep MMS connection alive. It’s disabled while set to 0.
• Default orIdent: Per default the orIdent is "ITT", but it can be set to customer use.
• Default BRCB ResvTms: Time in sec for BRCB reservation, see chapter "Working with Buffered Reports".
• Ignore Control Block states for commands: Allow to send commands despite Control Block state (for testing purposes i.e. Trying to enable report without reservation)
• Perform IED status checks on disconnect: Enable to perform status checking on disconnecting from an IED, i.e test/test_blocked values.
• Turn on replay analysis: Disable/enable Replay protection analysis. See "GOOSE replay protection algorithm"
• Time deviation[ms]: The time margin for timestamp check, see "GOOSE replay protection algorithm"

3.1.7 Help menu

The help menu provides access to the following operations (see Figure 13)

• Viewing the help file associated with the ITT600 - Explore IEDs
• A legend of the used status colors (see also Figure 24)
• Check whether software updates are available
• Viewing the about screen

Figure 13: ITT600 – Explore IEDs Help menu

For a detailed version overview click on the Assembly Versions button in the About window.

3.1.8 Tree navigation panel

The tree navigation panel provides a hierarchical view of an IED as defined in a SCD file or as dynamically generated from a connected IED.

It is separated in two different views:

• IEDs by Subnetwork- In this view, IEDs are sorted according the Sub-network they are connected to. See Section "Tree View "By Subnetworks""
• IEDs by Substation- In this view, the IEDs and LNs are sorted according to which part of a Substation they belong to (usually a Bay). See Section "Tree View "By Substation". This view is only available if a SCD file was loaded. The substation layout related information cannot be retrieved from an IED online.

In general, this presentation provides a quick and easy way to navigate to specific objects within a given configuration and is targeted primarily at users having some background knowledge of IEC 61850 (see Section "References"). In brief, this navigation panel is useful when attempting to drill-down to a specific object within a configuration.

As an extra help to the user, a tooltip containing the functionality or the description of the element is given when the mouse pointer remains on a node. See Figure 14.
In addition to providing simple point-and-click navigation, the tree also exposes a large collection of user commands through its context-menus. To access the user commands available to a specific object within a configuration, simply right-click on the object in the tree navigation panel.

Most of the ITT600 functionalities are accessible over content sensitive context menus.

At the top of the tree, there is a toolbar with following options:

- Navigate through previously selected tree nodes.
- Group related tree nodes.
- Change display options.
- Search for tree elements containing specific text.

### 3.1.8.1 Tree View "By Subnetworks"

This view structures the IED’s according to the Subnetwork they are connected to. As a default, only IEC 61850 Networks (SCL type “8-MMS”) are displayed. By changing the Show only IEC 61850 Networks state, all available Subnetworks will be shown. See Figure 15.

In case some of the IEDs are not linked to the Communication Section of an SCD file, those IEDs are shown in the “IEDs without reference to Communication Section” IED folder.

Depending on the node clicked and state of the underlying elements, the tree context menu may contain following options:

- Adding a new IED to Subnetwork (the Add new IED to... menu item).
- Removing the added IED from the navigation tree (the Remove... menu item).
- Adding a SERVER to the added IED (the Add SERVER to... menu item).
- Modifying a selected SERVER (the Edit SERVER... menu item).
- Removing a selected SERVER from an IED (the Remove... menu item).
- Clearing the entire configuration (the Clear Tree menu item).
- Choosing naming style.
IEDs without a reference to the SCD communication section will be added to IEDs folder called “IEDs without reference to Communication section”.

As default only IEC 61850 related networks (network name contains 8-MMS) are shown.

3.1.8.2 Tree View “By Substation”

This view structures the IED’s according the Substation they are connected to. In case, some of the IEDs are not linked to the Substation Section of an SCD file, those IEDs will be shown in the IEDs without reference to S/S section IED folder. See Figure 16.
Figure 16: Tree view by substation (without and with customer names)

IEDs without a reference to the SCD substation section will be added to IEDs folder called IEDs without reference to S/S section.

In case an IED is referenced by more than one bay, the IED is shown in each bay. IEDs can be shown/hidden by the last button on the By substation toolbar.

A typical substation section can have the following subtree node structure:

- Substation level
  - Voltage level 1
  - Voltage level 2
    - LN reference x
    - LN reference y
    - ...
    - Bay 1
    - Bay 2
      - Conducting equipment
        - LN reference
        - ...
- IED
3.1.9 Get Started Panel

The Get Started panel is by default shown when ITT600 is started. This panel allows user to directly access the recently opened documents, files or IEDs in ITT600. See Figure 17. Additionally, each of the block titles is a clickable shortcut to the relevant part of the SA Explorer.

![Get Started panel](image)

Figure 17: Get Started panel

3.1.10 Main panel

The Main panel displays information pertaining to the currently selected object in the configuration. Most object viewers are divided into two distinct areas as shown in Figure 18.

3.1.10.1 Object properties

The header of the object properties area as shown in Figure 18 and Figure 19 provides the following information about any selected object (from left to right):

- An icon followed by the type of object currently being examined
- The name and path of the object being examined (where appropriate)
- An icon indicating the connection status of the object being examined.

The remaining portion of the object properties area displays information describing the currently selected object and its child objects.
3.1.10.2 Dockable panes

All panels of the main window are dockable, user can arrange them according to his preferences (in tabs, floating windows, unpinned panels, etc.). The layout is saved when ITT600 is closing. Main panel tabs can be rearranged to best display the required workspace. Dragging tabs to different areas of the window will show an outline indicating where the window will be moved to. This includes placing windows next to the edges of the main window, nesting inside of an existing window's space, or adding the window as a tab in a new or existing list of tabs. See Figure 20.
Tabs and tab headers can also be right-clicked to bring up their context menu. This allows for closing tabs, switching them to floating windows, or turning on auto hiding when the cursor is no longer over them. See Figure 21.

Double clicking an element on the tree will open a new tab for it. These tabs are not saved in layout and will not be restored on next ITT600 run. See Figure 22.

The object details area varies depending on which type of object is currently being examined and provides detailed information that relates to the selected object (an example can be seen on Figure 23).
3.1.11 Coloring rules

ITT600 – Explore IEDs uses different colors to show the state of IEDs contained in the tree view.

To get a list of the different colors, click on the Tree Navigation color Legend in the Help menu. See Figure 24 and Table 2.

![Figure 24: Legend of used colors in ITT600 – Explore Ethernet](image-url)
### Table 2: Detail legend of the used colors in ITT600 – Explore Ethernet

<table>
<thead>
<tr>
<th>Legend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online and in SCL</td>
<td>Data is available online (from a connected IED) and from the loaded SCD file.</td>
</tr>
<tr>
<td>Only available in SCL</td>
<td>The data is only available in the SCD file, but not in a connected server.</td>
</tr>
<tr>
<td>Only available online</td>
<td>The data is only available in the connected server, but not in the SCD file.</td>
</tr>
<tr>
<td>Misconfigured</td>
<td>Something in the configuration is wrong. This might happen if a value cannot be read from a server.</td>
</tr>
<tr>
<td>Invalid state</td>
<td>Indicates a node that has an invalid state and is neither configured in the SCL nor in the server (should not occur).</td>
</tr>
<tr>
<td>Report enabled</td>
<td>An enabled RCB (only RCBs that are enabled from ITT)</td>
</tr>
<tr>
<td>Report enabled by other client</td>
<td>An enabled RCB instance by other client</td>
</tr>
<tr>
<td>Report was once enabled</td>
<td>A RCB that was once enabled is colored differently.</td>
</tr>
<tr>
<td>Simulated</td>
<td>The IED is currently simulated</td>
</tr>
<tr>
<td>Simulation not possible</td>
<td>It is not possible to simulate a selected IED. This could be caused by an IP Address conflict in the network (e.g. another IED with the same IP Address is already online)</td>
</tr>
<tr>
<td>Undefined</td>
<td>Any other state apart of the described states here</td>
</tr>
<tr>
<td>Unsupported must understand element</td>
<td>It is used to indicate unknown Must Understand element as defined in IEC 61850 Edition 2</td>
</tr>
</tbody>
</table>

### 3.1.12 Debug and logging information

The bottom area of the ITT600 - Explore IEDs provides access to the debug log. To display debug information while the application is running simply check the **Show debug log** from the Tools – Options Main menu (See Figure and Figure). The log window can be cleared by clicking on the **Clear log list** button.

ITT600 SA Explorer allows user to define the verbosity of the logging information. A description on how to configure the output is provided in Section “Debug and trace output configuration”.

All the information that is shown in the debug log is also saved as log files. Depending on the verbosity of the logging, the size of these files can get quite big. At start-up of ITT600 SA Explorer the size of the log files is checked. In case the size of all files exceeds 100MB, the user will be prompted to delete the old files.

The log files can also be deleted manually by selecting the **Delete old log files** from the options menu.

#### Figure 25: Debug information controls

The debug information window allows filtering of specific message types by filter options (Figure) on each column and search logs containing specific text (custom complex filters are supported).
3.1.13 Working with IED configurations

There are two primary methods for working with IED configuration within the ITT600 – SA Explorer (see the following two sub-chapters):

- Browse an existing configuration by opening a SCD file Section "Working offline".
- Dynamically discover a connected IEDs configuration Section "Working online".

3.1.13.1 Working offline

Here is a simplified example of working with a SCD file. The sample SCD file used in this example is included with the installation and can be found in the following location:

[InstallDir] /Samples /SCD Files /DemoSysA.scd

Open an SCL file

To open an SCD file corresponding to the configuration you wish to work with, select Open SCD file… from the File menu. If you have already opened a SCD file earlier, select the recently opened SCL you like to work with from the Open Recent list under the File menu. See Figure 26.

![Figure 26: ITT600 – Explore IEDs loading a SCD file](image)

After selecting the SCD file, a busy mouse pointer will be shown and the file will be loaded.

- Loading a SCD file can be time consuming. A busy mouse pointer is shown during the loading phase.

Signed and encrypted files

Signed files are partially supported - only non-encrypted files can be opened. If the file has a signature, ITT600 will log a warning in the notifications panel that the signature cannot be verified. In the case of encrypted files, a warning dialog will be shown that file is encrypted and cannot be opened and an error will be logged in notifications panel.

Explore an SCL file

Once the SCL file is opened, you can expand the entire tree navigation panel by right-click on an IED and selecting the Expand all nodes item. You can navigate to the various objects of interest by simply selecting the object in the tree navigation pane. See Figure 27.

Depending on the selected tree view, the structure of the file will be shown either from a communication point of view, or from a substation layout point of view.
Figure 27: ITT600 – Expanding the Tree view

All nodes in the Tree represent IEC 61850 related data. The display will not differ between online and offline values. See Section "Working online" for detailed description of different display options and values.

The Dataflow View

The Dataflow view is a graphical representation of the Subnetwork tree combined with the Substation tree plus information about the data flow between IEDs.

The view is shown in a separate tab. See Figure 28.

Figure 28: Data Flow view tab

Representation

All IEDs from the selected Subnetwork are shown as green boxes, including information about the IED (see Figure 29):
• The IED Name (Bold)
• The IED Type
• The IP Address of the IED
• The Description of the IED

Figure 29: IED information

The IED information is taken from the loaded SCD file. In case the information is missing or unattractive, it has to be changed in the SCD file accordingly.

Arrows between the IEDs show the data flow. An arrow ending at an IED shows the received data. An arrow starting at an IED shows the information sent by the IED. Color legend of the arrow is shown as follows:

• Green: GOOSE
• Magenta: Buffered Reports
• Yellow: Unbuffered reports
• Blue: Sampled Values

Filtering

Depending on the applied filters, more or fewer communication service types are shown. Each service can be switched on and off using the buttons in the Toolbar. See Figure 30.

Figure 30: Filters

The “String Based Filter” is using the data set names to apply its filter. The ‘*’ character is used as wild card. For example:

StatUrg* is showing all communication related to any DS where the name starts with “StatUrg”.

String Based Filter is using the DataSet Name for its filter criteria.

Vlan dropdown list is visible when it's more than one vlan in selected subnetwork. Vlans selected on filter are highlighted.

Zooming

The Diagram can be zoomed using the Toolbar Button or pressing Ctrl and moving the mouse wheel.

Moving elements

Diagram elements such as IEDs or entire Bays can be moved by dragging and dropping the selected element on a new position.

IEDs can only be moved inside the Bay they belong to.

Navigation

The diagram can be used to navigate in the Subnetworks tree.
Clicking on an IED changes the view in a way that only related IEDs are shown. All other IEDs are greyed out. The clicked IED is selected in the Subnetworks tree.

Right clicking on a communication arrow, shows a context menu that can be used to select the chosen DS in the tree view. See Figure 31.

![Figure 31: Navigating to a DS](image)

The DS is only selected in the Subnetworks tree, but the view does not automatically change to the object details.

**Fault simulation**
The diagram can be used to visualize the impact of a failing IED.

An IED can be set as **Failed**, all dependent IEDs are marked as affected. Right click on an IED to simulate a failure. See Figure 32.

![Figure 32: Simulate a failed IED](image)

Right click on an IED to simulate it as failed.

The failed IED is show in red, all affected IEDs are shown in orange. See Figure 33.
Combination with Quick Checker
Quick checker results are also shown in the diagram. The check has to be performed from within the quick checker control (see Section "Quick Checker").

Quick checker results are shown in the Dataflow diagram.

3.1.13.2 Working online

Connect to IEDs and SERVERs
To connect to various IEDs and SERVERs, user can select from the following options:

- Select **Connect All IEDs in...** from the subnetwork context menu either with or without enabling reports (see Figure 34).
- To connect one IED and its Servers, select **Connect...** from IED context menu.
- To connect a Server, select one of the **Connect...** options from a SERVER context menu (see Figure 35).
Figure 34: Connect to all IEDs and Enable Reports

Figure 35: Connect to a SERVER of an IED

ITT600 – Explore IEDs will use the defined Address parameters for the connection. A description how to change the various address details can be found in Section "Dynamically add IEDs to the configuration".

To specify different address parameters or Authentication Password, select **Edit Server** prior the connection attempt.
While the ITT600 - Explore IEDs connects to all IEDs a progress bar will be displayed – see Figure 36.

**Figure 36:** ITT600 progress bar

During the connection phase, all MMS variables are browsed, the type information and the actual values are retrieved. The time it will take depends on the configuration of the IED and the different IED types.

No Reports are enabled. To obtain spontaneous data change from an IED, reports need to be enabled (see Section "Manually update values from an IED").

**Connect SERVER as a specific client**

Connecting the SERVER as specific client will automatically enable all reports associated with that client (see section “Spontaneous update of values” for more information about reports).

**Figure 37:** Connect as a specific client

**Connect to an IED over TLS**

To connect with IED over TLS proper configuration must be set on an IED. Selecting an IED in the navigation tree will show TLS configuration panel:

**Figure 38:** Configuring TLS connection
User has to be aware about specific IED TLS required settings, certificates etc.

In the panel user should:

- Add required client certificates in correct order
- Protocols: select correct supported protocols
- TLS port (0 – default TLS port from ITT main options will be used)
- Local IP: if required, IP address will be set on an NIC
- Server Name: if required by an IED validation

**Connection keep alive mechanism**

ITT600 allows enabling the MMS keep alive mechanism for an IED after client inactivity closes the connection. In the ITT600 main options -> Explore IEDs -> MMS Client Configuration section, keep alive interval can be set (with 0 as disabled). If enabled ITT600 will periodically perform an MMS 'status' or 'identify' service query, depending on which one is supported by the IED. Each MMS keep alive query is logged in notifications panel. In case neither are supported, ITT600 will log a warning in the notifications panel.

![MMS keep alive notifications](image)

The Keep alive notifications are logged when Verbose logging level is set in ITT600 main options

**Explore a connected IED**

Once the IED (or SERVER) has been successfully connected, you can click on various objects to view more detailed information. For instance, click on the Pos Data object located under the SCSWI1 logical node of the LD0 logical device. See Figure 40.

![Exploring an IED](image)

**Simulate this Server**

In general, ITT600 SA Explorer provides the functionality to simulate one IED. For details, see section "IED simulation".
Open Device Web Interface

The Open Device Web Interface context menu is used to automatically launch the connected device web interface (for each server) in the local default web browser if the device has a web interface.

Change attributes of the IED

Depending on the functional constraint of the data attribute you click on, various modifications are possible. If you double click a writeable data attribute, you can enter a new value for it, or pick one from the dropdown menu (if available).

Hitting the Enter key or the Write Button will write the value to the IED, the Escape key or the Cancel Button will cancel your changes. See Figure 41.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>Product definition</td>
<td>IED600</td>
<td>DC</td>
</tr>
<tr>
<td>serNum</td>
<td>IED serial number</td>
<td>Sample input</td>
<td>Write</td>
</tr>
<tr>
<td>swRev</td>
<td>Firmware version</td>
<td>ADD</td>
<td>UC</td>
</tr>
<tr>
<td>vendor</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 41: Changing a value of an IED

Depending on the type and FC of the data attribute you are attempting to change, various input methods will appear upon the second click of a given data attribute (provided the data attribute is writeable).

Data with functional constraint CO (Control) cannot be written/edited as shown in Figure 43. To write CO values, a Control Dialog will be displayed as shown in Figure 42. See "Commands".

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
<th>FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>subID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>subEna</td>
<td>Substitute enable</td>
<td>True</td>
<td></td>
</tr>
</tbody>
</table>

Figure 42: Changing different data types

Changing a value is not persistently saved in the IED. After restart of the IED your changes are lost. To save them persistently, you have to change the IED configuration file and reload the IED. This task will be different for different IED types.

It is up to the IEDs implementation whether to allow write operations or not. In case the IED does not allow such operations, an error message is logged in the Debug output section (like objectAccessDenied). These messages are generated by the IED.

Editing Setting Group values

Setting group values can be changed using IEC 61850 defined Services. The data and services are available in the Setting Group Control Block (SGCB). This control block is located in the LLN0. See Figure 43.
Editing of Setting group values is not supported by all IEDs.

Figure 43: SGCB of an IED

Changing Active Setting Group
To change the active Setting group, the corresponding value (ActSG) of the SGCB has to be changed. See the following figure.

Figure 44: Changing the active setting group

Editing Setting Group values
To edit individual values of a Setting group, this group has to be copied to the edit buffer. This is achieved by setting the EditSG value of the SGCB to the desired value. See Figure 45.
Now individual values can be changed. See Figure 46.

The three columns show the following values:

- **Active SG**: The value of the currently activated SG.
- **Editable SG**: The current value of the SG being edited.
- **New Value**: The new value that shall be assigned.

Changes to the values have to be confirmed with a **Confirm Edit Setting Group** Service. This ensures that all values have been accepted by the IED and are switched over at once.

To finally write new Setting group values to an IED, the Confirm Edit SG Values Button needs to be pressed.

Simulated IEDs do not support editing SGCBs.

**Commands**

Depending on the Control Model of a CDC a different control dialog will be shown.

**Select Before Operate command**

To operate a switch controlled by a real IED, a **Select-Before-Operate** (SBO) sequence has to be sent to the device. This function is available from the Switch Control Dialog. See Figure 47.
In the basic view, simple commands like Open and Close can be sent to the IED. Clicking on Open Switch or Close Switch will actually send a select (SBOw) command to the IED. After a positive confirmation an Execute dialog will pop up. By pressing Execute, operate (Oper) command is sent to the IED.

The advanced view lets the experienced user change additional parameters. See Figure 48.

IEC 61850 OrCat and OrIdent define the origin of the command. Default values are station control and ITT.

Setting the Test flag indicates a test command.

Removing the Synchro Check flag will bypass the synchrocheck functionality in the IED.
Overriding synchrocheck in a real station might cause severe damage to the primary equipment of the station! Use this feature with extra caution!

Removing the Interlock Check flag will bypass the interlocking calculation in the IED (if supported by the IED).

Overriding interlocking in a real station might cause severe damage to the primary equipment of the station! Use this feature with extra caution!

Setting the Continue after neg. resp. causes the dialog to show the Execute sub dialog although the selection command was confirmed negative. By using this feature, the behavior of an IED can be verified despite the selected command was not accepted.

**Direct commands**
The Direct Command dialog looks slightly different to the SBO Command Dialog. See [Figure 49](#).

![Direct Command dialog](image)

*Figure 49: Direct command dialog*

In this dialog there are less options available. Depending on the data type of the control value (ctrlVal) the input box changes to a drop down list for Boolean values.

Issuing Commands without caution in a real station is dangerous! Use this feature with extra caution!

**Manually update values from an IED**
The values are not refreshed in the GUI automatically. To refresh the view, the values have to be read from the connected server. To do this, simply right click on the object you want to refresh and click on the Refresh or Refresh all option in the context menu. See [Figure 50](#).
Refreshing content of a SERVER

It is also possible to refresh the whole content of a server with the Refresh this server’s contents command. See Figure 51. This command will re-read all values from the server, thus this command might take some time.

Spontaneous update of values

All spontaneous data changes in an IEC 61850 compliant IED are sent to clients in so-called reports. There are two different report types: buffered and unbuffered (for details see Section “References”). With the ITT600 SA Explorer both types can be controlled.

The following three steps are necessary to set up the reporting:

- Configure the Report control block (RCB)
- Enable the report
- Start a general interrogation (optional)

An unbuffered report will be set up as follows: Select an URCB (rcb_A from the LLN0 of P2KA1C1 in this example) and click the Reserve URCB button.
Enabling reports interferes with the SA system the IED is connected to. ITT600 – Explore IEDs acts as every other IEC 61850 client. For instance, if only three Clients can enable reports (this is a setting of the IED), ITT600 – Explore IEDs will use one of these client instances. In case there are already three clients that have enabled the report, it will not be possible to enable it by ITT600 – Explore IED.

When reports are enabled, all spontaneous updates are also logged in the process event list (see Section "Process Event List" for details).

**Working with Unbuffered Reports**

Unbuffered reports have to be reserved for most of the operations. See Figure 52.

The URCB has to be reserved for the following operations as shown in Figure 53.

To reserve the URCB, simply click on the **Reserve** command button.

If an RCB is already used by another client, it cannot be used with ITT600 – Explore IEDs. In this case, the command buttons will be disabled (grey).

Select the trigger options in the Control Block Options and change them to your needs or simply use the default settings.

The **data_set_name** should always be included in order to decode the report.

---

**Figure 52:** An Unbuffered Report Control Block
Next, enable the URCB by clicking the Enable button.

The color of an enabled report will change. See Section "Coloring rules" for a detailed list of all available status colors. See Figure 54.

Finally, to update all values, click the Start General Interrogation button. To disable the report, click Disable and Release.

Received reports are displayed in the process event list (see Section "Process Event List" - for a detailed description). They will be logged and automatically update the data contained in the report if the received values differ from the values currently stored in the internal data model.

The object details will be updated automatically as well.
Working with Buffered Reports

Buffered reports are very similar to unbuffered ones. To find out more about the differences, see section "References". See also Figure 55.

Figure 55: A Buffered Report Control Block

If the IED is IEC61850 Ed. 2.1 and ReportSettings service resvTms is 'true', ITT600 allows to reserve the BRCB:

Figure 56: BRCB with reservation commands

The default time for BRCB reservation is set according to ITT600 main options -> Explore IEDs -> Command handling section. The ResvTms is how many seconds the BRCB will be reserved for after disconnecting the client.
The IED is keeping BRCB reserved after client disconnection when the client will not release it before, otherwise the BRCB can be reserved by another client. ResvTms value 0 indicates that BRCB can be reserved, any positive value indicates that it is reserved by the client. For more information please refer to the IEC61850 Part 7-2 (2010; Edition 2)

**Enabling All Reports of a SERVER**

There is a simple way to activate all reports of a connected SERVER. The context menu of a SERVER contains an entry **Enable all possible RCBs** nested within the **Enable reports** entry.

This function will also automatically issue a General Interrogation command to the connected server. See **Figure 57**.

![Figure 57: Enable all possible reports of a Server](image)

Only one instance of each report is enabled (one report per different datasets). To enable the same report more than once, this has to be done manually.

**Disabling All Reports of a SERVER**

To disable all reports of a connected SERVER, simply use the context menu of a SERVER - **Disable all Reports**. See **Figure 58**.
3.1.13.3 Dynamic Data Sets

Some IEDs offer the possibility to create dynamic datasets while you are connected to the IED. These datasets can be connected to URCBs and corresponding events can be generated.

If this functionality is available on an IED, a menu entry is visible in the context tree menu of the ITT600 SA Explorer. See Figure 59.

Figure 59: Create dynamic data sets

This functionality is only executable in online mode!
You must be connected to an IED which supports this function.

This functionality only supports non persistent data sets!

Activating the menu item Create dynamic data sets.. opens the following window. See Figure 60.
The window contains the following items:

- **Data tree**: selectable DO/CDC objects. CDC objects can be assigned to data sets.
- **Data filter**: filter option for selecting different kind of CDC items (e.g. show all Pos items).
- **Arrow buttons**: buttons for adding/deleting DS/DS entries to/from the internal configuration.
- **Predefined RCBs**: tree view of predefined RCBs/configured DS with DS entries.
- **Write to IED buttons**: buttons for applying the internal configuration to the IED.
- **Selection of tree items**: In the CDC tree view, multiple selection of tree items is possible. See Figure 61.
- **Status of CDC Objects**: CDC items which have been assigned to a DS are shown in green. See Figure 62.
- **Status of RCB/DS/DS entries**: Items added to the internal configuration, but not yet written to the IED, are shown in green. Items already written to the IED are shown in black. Modified items are shown in blue. Removed items are shown in red with strikethrough.

Pre-configured, empty URCBs must exist on the IED to add DS and DS entries. See Figure 61 and Figure 62.

Only one DS can be assigned to an URCB!
Figure 61: CDC tree view with multiple selection

Figure 62: CDC tree view: CDCs assigned to DS
Dynamic data sets are automatically named **ITT-DynDSxxx** to avoid duplicate names.

The creation of a dynamic data set consists of two steps:

- Add the data set with entries to the ITT600 internal configuration
- Write the internal configuration to the IED

The deletion of a dynamic data set consists of two steps:

- Delete the data set from the ITT600 internal configuration
- Write the internal configuration to the IED

**Adding Data Sets to the internal configuration**
Selecting items in the DO/CDC tree view and pressing one of the right arrow buttons adds the DS entries to the internal configuration.

**Deleting Data Sets from the internal configuration**
Selecting items in the RCB tree view and pressing one of the left arrow buttons deletes the DS entries from the internal configuration.

**Writing Data Sets to the IED**
There are two buttons which allow to write internal configuration to the IED. These button can be found above RCB tree view. See **Figure 65**.
Figure 65: RCB tree view menu

Status of successfully enabled RCBs and written DSs is shown in black. See Figure 66.

![Screenshot of RCB tree view menu]

- **SIPApplication/LLN0/A_URCB_1001**
  - **ITTDynDS001**
    - [ST] SIPApplication/LLN0.LEDRs
- **SIPApplication/LLN0/A_URCB_101**
  - **ITTDynDS002**
    - [ST] SIPApplication/LPHD0.Proxy
    - [ST] SIPApplication/LPHD0.PwrUp
    - [ST] SIPApplication/CALH0.GtAlm
- **SIPApplication/LLN0/A_URCB_1101**
  - **ITTDynDS003**
    - [ST] SIPApplication/LTMS0.TmSrc
- **SIPApplication/LLN0/A_URCB_1201**
  - **ITTDynDS004**
    - [ST] SIPQA1/XCBR1.8kCls
    - [ST] SIPQA1/XCBR1.8kOpn
    - [ST] SIPQA1/XCBR1.EEHealth
    - [ST] SIPQA1/XCBR1.Loc
    - [ST] SIPQA1/XCBR1.OpCnt
    - [ST] SIPQA1/XCBR1.Pos
    - [ST] SIPQA1/XCBR1.SumSwARs

Figure 66: RCB tree view with a DS written to IED

After this operation, the updated URCBs must be enabled in the Subnetwork/Substation tree view!

Deleting Data Sets from the IED

First delete the data set from the ITT600 internal configuration, then write the internal configuration to the IED. See Figure 67.

![Screenshot of deleting data sets from IED]

Figure 67: Deleting Data Sets from the IED
Export Data Sets to SCD
New created data sets can be saved to an SCD file (see Section "Exporting IEDs to an SCD file").

Disconnecting from Server
When disconnecting, all created data sets will automatically be deleted.

3.1.13.4 Read VMD Specific Variables of an IED

VMD specific variables are MMS variables that are not in the scope of IEC 61850 objects. Some IEDs provide status information that is mapped to such variables.

To read those variables from an IED, select Read VMD Specific Variables from the Server’s Context Menu. See Figure 68.

![Figure 68: Read VMD specific variables of a Server](image)

Not all IEDs might support VMD variables. It is vendor specific Information that is not in the IEC 61850 scope.

VMD specific variables are not updated automatically. To refresh those variables, fetch them again from the IED. See Figure 69.
3.1.13.5 Working with files (MMS file Transfer)

Files contained in SERVER can be retrieved by ITT600 – Explore IEDs. It depends on the IED whether this service is supported. Furthermore, it also depends on the IED which files are available over MMS file transfer.

Usually only disturbance recorder files, but no configuration files can be retrieved with MMS File transfer.

If an IED does not support MMS file transfer, it might support FTP protocol. See Section "Embedded FTP Client" for information how to use ftp within ITT600 - Explore IEDs.

An IED supporting MMS file transfer will show a specific user control when the MMS file transfer node is selected in the tree view. See Figure 70.

Figure 70: MMS file transfer component
All possible file operations are available over a context menu, or the control buttons. See Figure 71.

The MMS file transfer node is only shown, if the IED supports MMS file transfer.

To get files from the IED, select a file and click the Download button or the Get file context menu entry.

Deleting files from the MMS Server might be limited. If the file delete service is not supported, the Delete button will be disabled.

Delete File is not supported by all IEDs or on some IEDs only the oldest file can be deleted.

MMS File transfer is only supported from an IED to ITT600 SA Explorer. No files can be uploaded to an IED.

### 3.1.13.6 Process Event List

Changes in process values (also called events) are received by IEC 61850 reports. The changes and commands sent from ITT(with different background) are logged in the process event list as shown in Figure 72. To switch to the event list, select the Process Events tab.

Only changes will be logged in the Event List. The list will not be saved persistently when ITT600 – Explore IEDs is closed. However, it is possible to save the received values into a Microsoft Excel® spreadsheet.

It is also not the intention of this list to have long term storage for updated process values, it should rather support the user during troubleshooting sessions.

Only a value change will be logged. Value updates (with the same value) are not logged.
Figure 72: The Process event list

Help on how to set up reporting is described in Section "Spontaneous update of values".

The list is divided in 12 columns and has a toolbar providing some additional functionality. The explanation of each column is presented in next table and Figure 73.

- The list can be exported to an Excel file by pressing the button Export to Excel.
- The list can be cleared by pressing the Clear List button.
- The substation related information is only filled if the IED is connected to a substation/voltage level.
- The most recent event can be selected by pressing the Show most recent event button.
- The substation related columns can be shown/hided by pressing the Show/hide functional names button.
- The auto sizing of the columns can be enabled/disabled by pressing the Toggle auto / manual column sizing button.
- By pressing the right mouse button in the event list tab, you can navigate to the selected item in the active tree view.
- The list is limited to 20000 entries! Once the limit is reached, new events will not be displayed in the list. However, the values are still updated.
Table 3: Event list column description

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>A sequential event number</td>
</tr>
<tr>
<td>Info</td>
<td>Additional information about the event: Q = Bad quality of the logged DO</td>
</tr>
<tr>
<td></td>
<td>T = Time quality bad of the logged DO</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The timestamp of the DO (tagged in the IED)</td>
</tr>
<tr>
<td>Source IED</td>
<td>The IED that sent this event</td>
</tr>
<tr>
<td>Substation</td>
<td>The substation this DO belongs to</td>
</tr>
<tr>
<td>Voltage</td>
<td>The voltage level this DO belongs to</td>
</tr>
<tr>
<td>Bay</td>
<td>The bay this DO belongs to</td>
</tr>
<tr>
<td>Conducting equipment</td>
<td>The conducting equipment this DO belongs to</td>
</tr>
<tr>
<td>IEC 61850 Path</td>
<td>The IEC 61850 designation of the DA</td>
</tr>
<tr>
<td>Description</td>
<td>A textual description of the DA. Taken from</td>
</tr>
<tr>
<td></td>
<td>• The “d” Attribute of the DO</td>
</tr>
<tr>
<td></td>
<td>• The SCL desc of the DA (if available)</td>
</tr>
<tr>
<td></td>
<td>• The SCL desc of the DO (if available)</td>
</tr>
<tr>
<td>Value</td>
<td>The value of the DA</td>
</tr>
<tr>
<td>Client</td>
<td>The associated client</td>
</tr>
</tbody>
</table>

Figure 73: The Process event list details

3.1.13.7 Security Event List

The IEC 61850 LN GSAL is used to make security related activities available. In case reports with GSAL content is received, this information is presented in a specific list.

To view the captured security events, change to the tab Security Events. See Figure 74.

Only a value change will be logged. Value updates (with the same value) are not logged.

Help on how to set up reporting is described in Section "Spontaneous update of values".
The list is divided in several columns and has a toolbar providing some additional functionality. See Figure 75.

Figure 74: Security events list tab

Table 4 provides information that is contained in the security events list. The description of the toolbar button features can be found in section Process event list.

Table 4: Security Event list column description

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>A sequential security event number</td>
</tr>
<tr>
<td>Timestamp/Timestamp(local)</td>
<td>The timestamp of the DO (tagged in the IED)/The same timestamp displayed in user’s local time(depends on options configuration)</td>
</tr>
<tr>
<td>IED</td>
<td>The IED that has sent this event</td>
</tr>
<tr>
<td>Substation</td>
<td>The substation this DO belongs to</td>
</tr>
<tr>
<td>Voltage level</td>
<td>The voltage level this DO belongs to</td>
</tr>
<tr>
<td>Bay</td>
<td>The bay this DO belongs to</td>
</tr>
<tr>
<td>Conducting equip-</td>
<td>The conducting equipment this DO belongs to</td>
</tr>
<tr>
<td>IEC 61850 Path</td>
<td>The IEC 61850 designation of the DA</td>
</tr>
<tr>
<td>Event Text</td>
<td>The resolved security event text</td>
</tr>
<tr>
<td>addInfo</td>
<td>The content of the DO attribute addInfo</td>
</tr>
<tr>
<td>User Name</td>
<td>The resolved user name of the DO attribute addr</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the source</td>
</tr>
<tr>
<td>Cnt</td>
<td>The security event counter index</td>
</tr>
</tbody>
</table>

Table continues on next page
### 3.1.13.8 Point Value List

Process values are shown in the Point Value List Tab. Values are automatically updated. Only values which belong to the selected Tree view object’s scope are displayed. To switch to the point value list, select the **Point Value List** tab.

Only updateable values will be displayed in the point value list. The list will not be saved persistently when ITT600 - Explore IEDs is closed. However, it is possible to save the received values into a Microsoft Excel © spreadsheet.

It is also not the intention of this list to have long term storage for updated process values, it should rather support the user during troubleshooting sessions.

Only updateable values are displayed i.e. values for which reporting has been enabled.

![Point Value List](image)

**Figure 76: Point Value list**

Help on how to set up reporting is described in Section "Spontaneous update of values".

The list is divided into 14 columns and has a toolbar providing some additional functionality.
### Figure 77: Point Value list details

#### Table 5: Point Value list column description

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>A sequential security event number</td>
</tr>
<tr>
<td>Timestamp/Timestamp(local)</td>
<td>The timestamp of the DO (tagged in the IED)/The same timestamp displayed in user's local time (depends on options configuration)</td>
</tr>
<tr>
<td>IED</td>
<td>The IED that has sent this event</td>
</tr>
<tr>
<td>Substation</td>
<td>The substation this DO belongs to</td>
</tr>
<tr>
<td>Voltage level</td>
<td>The voltage level this DO belongs to</td>
</tr>
<tr>
<td>Bay</td>
<td>The bay this DO belongs to</td>
</tr>
<tr>
<td>Conducting equipment</td>
<td>The conducting equipment this DO belongs to</td>
</tr>
<tr>
<td>IEC 61850 Path</td>
<td>The IEC 61850 designation of the DA</td>
</tr>
<tr>
<td>Event Text</td>
<td>The resolved security event text</td>
</tr>
<tr>
<td>addInfo</td>
<td>The content of the DO attribute addInfo</td>
</tr>
<tr>
<td>User Name</td>
<td>The resolved user name of the DO attribute addr</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the source</td>
</tr>
<tr>
<td>Cnt</td>
<td>The security event counter index</td>
</tr>
<tr>
<td>Sev</td>
<td>The severity of the security event</td>
</tr>
<tr>
<td>Description</td>
<td>A textual description of the DA. Taken from - The “d” Attribute of the DO</td>
</tr>
<tr>
<td>Client</td>
<td>The associated client</td>
</tr>
</tbody>
</table>

The list can be exported to an Excel file by pressing the button [Export to Excel].
The substation related information is only filled if the IED is connected to a substation/voltage level.

The substation related columns can be shown/hided by pressing the button Show/hide functional names.

The auto sizing of the columns can be enabled/disabled by pressing the button Toggle auto / manual column sizing.

By pressing the right mouse button in the point value list tab, you can navigate to the selected item in the active tree view.

You can toggle on/off the refreshing of the Point value list by pressing this button. When the refreshing of the list is off, the values are no longer automatically updated.

### 3.1.13.9 Embedded FTP Client

Obtaining files from an IED might also be possible using the FTP protocol. However, this functionality is not part of IEC 61850 and is not mandatory for all IEDs.

When a Server node is selected in the Tree view, the FTP Client control is shown in the lower right area. See Figure 78. To connect a FTP server, a password is required. The username and password has to be provided in the following connection dialog as seen in Figure 79. If the Username is left blank, anonymous login will be used. After successful connection, all FTP commands are available via the command buttons, or the context menu. See Figure 80.

![FTP Client](image)

**Figure 78:** FTP Client
The default directory where the files are saved locally is \[installation dir]\ABB\ITTSAExplorer\Files\[IED Name].

The FTP server’s response is not standardized. It might happen that some Servers cannot be connected using this FTP client.

3.1.13.10 Dynamically add IEDs to the configuration

The ITT600 - Explore IEDs also has the ability to dynamically generate the configuration of a connected IED without having the corresponding SCD file for it.

Right-click on the tree navigation panel and select the Add IED… item. See Figure 81.
Figure 81: Adding a new IED to the tree

Enter a meaningful name for the new IED and click OK. See Figure 82.

Figure 82: Adding an IED

To communicate with an IED, a SERVER has to be added. The add dialog contains section for server information. See Figure 83.
Figure 83: Adding a Server to an IED

Enter the IP address of the IEDs main server, a Server name and click OK.

Additionally also detailed address parameters could be specified. Otherwise default parameters are used (see Section "ITT600 – Explore IEDs Default Address Parameters" for more details on the address parameters. See Section "Changing OSI address parameters" on how to change the address parameters).

To show the SERVER details, press the Addresses expander button. See Figure 84.
A Subnetwork is automatically generated, and the IED is added to the Subnetwork. To add an IED to an already existing Subnetwork, the Subnetwork has to be selected before clicking the Add IED menu item. IEDs can only be added to a Subnetwork node.

See Section "Working online" for information pertaining to what can be done with a connected IED.

Dynamically added IEDs have a different icon ( ) than IEDs from an SCD file ( ).

### 3.1.14 Dynamically discovering IEDs

The ITT600 - Explore IEDs allows dynamically detecting and adding IEDs from a LAN.

From the Edit menu select Autodetect IEDs....

A wizard will be started to guide you through the auto detection.

From the first of three wizard panes select the IP address scanning method. The following alternatives are available to the user:
• Scanning an IP range: Scans the network between two specified IP addresses
• Scanning a subnet (with a specific subnet mask). Note that this is currently restricted due to performance and practical reasons to 255.255.x.y
• Scanning the subnet of the computer the ITT600 - Explore IEDs software is running on. The subnet is detected automatically. See Figure 85.

![ITT600 Discover IEDs](image)

**Figure 85:** Detect IEDs

Click next and wait for the following window to finish its activity. See Figure 86.

You can always cancel the scanning. Depending on the number of IP Addresses to scan, this might take some time!
Canceling the scanning does not remove the discovered IEDs.
Figure 86: Status of the detection

Click **Next >** for the final selection window.

All found IEDs are shown in the left list.

The user can now choose to add one or more of the detected IEDs to the IED list on the right side of the windows. See Figure 87 and Figure 88.

Figure 87: Found IEDs
The auto-detection pings all specified IP addresses. If an answer is received it will try to open a MMS connection with this address. Since a lot of specific traffic is generated by the PC, an intrusion detection system or a network administrator might be alerted. It is not recommended to use this feature on corporate LANs without informing your network administrator first.

### 3.1.15 Exporting IEDs to an SCD file

Data from dynamically added IEDs can be exported to a SCD file. Once a file is opened in ITT600 – Explore IEDs, this menu item disappears. See Figure 89.

Only dynamically added and browsed IEDs can be exported!

It is not possible to merge existing configuration files with browsed IED data. Once a file is opened, the **Export** menu item will disappear!
3.1.16 Quick Checker

The Quick Checker functionality enables a fast overview of the communication on a particular IEC 61850 network, both on the IEDs and as well on network devices. For checking the network devices configuration, communication section in the SCD file must be filled.

It is shown in its own tab when a Subnetwork is selected in the tree view. See Figure 90.

![Figure 90: Quick checker tab shown for Subnetwork AA1WF1](image)

3.1.16.1 Checking IED status

Available IEDs from the selected Subnetwork are listed in a tree structure including some common attributes.

All selected IEDs are checked for defined mandatory values:

- Each logical device’s NamePlate includes the following data attributes:
  - Configuration Revision (configRev)
  - Description (d)
  - Software Revision (swRev)
  - Vendor (vendor)

- Each Report Control Block for its configuration revision

In case of inconsistencies to the expected values loaded from the SCD file, different status information will be shown.

3.1.16.2 Checking network devices status

In addition to checking IEDs, ITT600 SA Explorer provides a functionality to help user in discovering faulty network configuration. This function is able to detect configuration and wiring errors. This
functionality is made possible if all related network devices are modelled properly according to IEC 61850-90-4 in the SCD file.

### 3.1.16.3 Status indicators

To indicate the different status, individual icons are used. See Table 6.

<table>
<thead>
<tr>
<th>Icon type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Info" /></td>
<td>The values have not been checked, or are not up to date</td>
</tr>
<tr>
<td><img src="image" alt="Check" /></td>
<td>The connection to the IED or Server could be established, all values are as defined in the SCD file</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>There are inconsistencies between the values loaded from SCL and the online values</td>
</tr>
<tr>
<td><img src="image" alt="Error" /></td>
<td>It was not possible to connect the IED or Server</td>
</tr>
</tbody>
</table>

### 3.1.16.4 Operation

After opening the quick checker, all IEDs are marked with the Information Icon, which means the values have not yet been updated.

To run an initial check, click on the Run button of the toolbar.

All possible operations are available from the tool bar buttons. See Figure 91.

**Figure 91:** Quick checker toolbar

Another option is to run the check in a defined time interval (5 min).

If the time interval is selected, a countdown that indicates remaining time until the next check will be triggered. See Figure 92.

**Figure 92:** Quick checker countdown

To reset the cyclical check, click the stop button. See Figure 93.
This feature is useful during system setup or commissioning start, since it gives a quick overview which IEDs are in service and whether the correct configuration is loaded.

The quick checker will first ping all specified IP addresses. If an answer is received it will try to open an MMS connection with this address. Since a lot of specific traffic is generated by the PC, an intrusion detection system or a network administrator might be alerted. It is not recommended to use this feature on corporate LANs without informing your network administrator first.

The quick checker results can be exported into a Microsoft Excel® spreadsheet. The Excel spreadsheet will contain two worksheets, one containing some general information and another containing the actual results as shown in Figure 94.

![Figure 94: Quick checker commands](image)
3.1.17 IED Status View

3.1.17.1 Overview

The IED Status view shows the complete IED status in respect to its testing configuration. It works for connected IEDs but also for simulation of an IED (see section "IED Status View").

It is shown in its own tab when an IED or a sub node is selected in the tree view (see Figure 95).

![Figure 95: IED Status view](image)

3.1.17.2 Functionality

The user can choose from different functionality filters such as Blocking, LPHD.Sim, Substitution and IED Testing Status. According to the selected filter the corresponding attributes will be shown in the grid.

![Figure 96: Functionality Filters](image)

The user can the manually select certain attributes or use the Select All button.
In the next step the user can select a new value and perform a bulk command to all selected items. The attributes will then change to the new value.

If the user wants to revert the changes, he can select all and press the Highlight Differences button. All rows that are different from initial value are highlighted and selected.
To highlight the initial value (value that was active when connecting to the device), select the column Initial Value from the grid field chooser.

User can then revert changes to its initial value.

Figure 100: Revert changes

When disconnecting the IED, the user will be informed if there are still any active Blockings, Substitutions or Testing. User can then continue or abort and use Revert functionality to reset to initial value.

Figure 101: Disconnect IED
3.1.18 IED simulation

3.1.18.1 Overview

ITT600 – Explore IEDs has the ability to simulate one IEC 61850 based IED.

Only the data communication part of an IED can be simulated. The application logic of the simulated IED is implemented according the IEC 61850 standard but might be different to a real IED. This is especially the case for non-ABB IEDs.

A test with a simulation helps when the focus of the test is on the data communication (e.g. Signal tests to SAS or protocol converters).

A test with a simulation never replaces the test with the real IED and the attached process.

The configuration of the simulated IED is based on the loaded SCD file. All Data Attributes of the IED can be changed in order to simulate any possible value. In case the DA is also configured for IEC 61850 reporting, the change of a value will automatically sent to a connected client. Depending on its configuration, the updated value will also be sent via GOOSE communication service.

Since the GOOSE Sender is running on a PC in a non-deterministic environment, it cannot be guaranteed that the sender’s real time behavior will be the same as from an IED. But it is guaranteed that updated GOOSE information will be transmitted within the tmax frame.

A connected MMS client or GOOSE subscriber will not determine a communication difference to a real IED.

When a simulated IED receives a command from a connected client, it executes the command and updates the related value according to the command.

Figure 102: Sending of changed value in simulated IED

When a simulated IED receives a command from a connected client, it executes the command and updates the related value according to the command.
In case a command to operate a Circuit Breaker or Disconnector is received, the simulation will process the command and change the position of the switch object according the command value. See Figure 102 for command processing flow.

The SCD file used in ITT600 must contain a proper Substation Section including links from Primary Equipment (e.g. CBR) to Logical Nodes of an IED (so called LNode References).

The command is processed according the simulated IED behavior shown in Figure 103.

ITT600 allows several options for processing commands. These options can be set in the ITT600 SA Explorer Options Dialog.

Figure 103: Command processing
The result of a received command is visualized in Figure 103. It shows a SBO command received on the SCSWI1.Pos. This command will result in the change of the assigned LNs to the command value – in this example it will close the CB. Also the position indication values of the XCBR that are assigned to the same CB are updated.

![Figure 104: Simulated IED behavior](image)

Commands to other LN classes are handled in a similar way. The value of the command (usually the ctlVal Data Attribute) is applied to the corresponding status value (e.g. the stVal Attribute).

### 3.1.18.2 IED simulation options

Before the IED simulation can be started, it is important to review the various options related to IED simulation in the ITT600 SA Explorer Options Dialog. See Figure 105.
Figure 105: IED simulation options

The following settings are possible in this option section:

- **Launch delay (ms):** this parameter defines the wait time until the simulated IED is launched.
- **Do not assign IP address of simulated IED:** this option keeps the current IP address of the machine and will not add the IED's IP address to network interface card. This might lead to not being able to connect to a simulated IED.
- **Do not remove IP address of simulated IED:** usually when simulation of IED is stopped, the respective IP address is removed from the network interface card. This option allows to avoid this removal.
- **Automatically add missing Report Trigger Options (Ed.1 Server only)**
- **Enable strict Ed. 2.1 RCB reservation:** enable/disable if simulated IED should behave according Ed. 2.1 for RCB reservation
- **Show IED simulator window:** when the checkbox is enabled, a separate window that shows the process of simulated IED is shown
- **Minimize IED simulator window:** the simulated IED windows is hidden by default
- **Send simulated GOOSE (GOOSE Header Simulation Bit on):** All GOOSE messages sent from a Simulated IED will have the GOOSE Header Simulation Bit set to true.
- **Command handling:** This section can be used to adapt the internal IED simulation logic. Depending on this options, commands will be processed differently, to allow more possibilities during system testing.
3.1.18.3 Start IED simulation

The simulation can only be activated for one IED at the time.

The IED simulation can be started by selecting Simulate this IED from the IEDs context menu as shown in Figure 106.

The simulation can only be started if the simulated IEDs IP address is not reachable on the network. If the IED that shall be simulated is available, it has to be disconnected first to avoid addressing conflicts.

When launching an IED, several steps are performed:

- The IP address of the simulated IED is assigned to the chosen network adapter.
- A simulated IED is started as its own windows process.
- MMS communication simulation is started.
- GOOSE communication simulation is started.
- All values are set initially to off, 0 or false.
- All Quality Attributes are set initially to good.
- Control Authority of the simulated IED is set to remote.

Your PC will send multicast frames. An Intrusion Detection System or a Network Administrator might be alerted. You should not use ITT600 SA Explorer’s IED simulation on corporate LANs without informing your Network Administrator.

IED simulation tab

If the simulated IED is started, one can select the IED simulation tab to easily change simulated values in the Point to Point Testing grid.
The substation or communication tree can be used to navigate to the different equipment. The Point to Point Testing grid shows all simulated Primitive Data Attributes of the selected node in the tree (e.g. in the next figure all PDAs of the object QB1 are displayed in the grid).

Figure 107: IED simulation Tab

**Functionality**

On the upper part of this tab, statistical information about the simulated IED is shown as in Figure 107. This includes MMS and GOOSE communication statistic counters.

In the lower pane, each simulated PDA can be changed (value, timestamp, and quality) by clicking on the magenta cells.

The columns on the right indicate if the PDA sends Goose and/or MMS (Client name is indicated in the header).

Right click on a PDA offers navigation to the referenced item in the Main tree.

**Grid usage**

Use column chooser by clicking on the top left field of the grid to show more columns (e.g. PDA quality, FC …). To export the grid view to Excel, press the button on top of the grid.

To show functional name columns press the following button:

To disable the auto sizing of the columns press:

HMI aspect handling is provided by the following buttons:

### 3.1.18.4 IED Status View

Similar as for the connected IEDs, the IED Status view can also be used for a simulated IED. Follow the description in chapter "IED Status View" on how to use the IED Status view.
3.1.18.5 Stopping a simulated IED

To stop an IED, click on the Stop Simulated IED context menu entry as shown in Figure 109.

Stopping the simulated IED removes the IP address of the simulated IED from the Network Adapter.

3.2 ITT600 – Explore Ethernet

3.2.1 Overview

ITT600 – Explore Ethernet is a protocol analyzer that is focused on IEC 61850 and other SA System related protocols.

Network traffic can be captured online or it can be loaded from files providing a defined format (ACP, PCAP, PCAPNG). This format is also widely used with other network sniffing tools based on WinPCap (e.g. Wireshark).

This means that ITT600 - Explore Ethernet is compatible with capture files saved from other Network Sniffers.
The ITT600 – Explore Ethernet Application User Interface is divided into three areas (see Figure 110):

- Toolbar (blue)
- Capture window (green)
- Packet details: Packets stack, SA related details, Raw data and ASCII data, Status bar (red)

![Explore Ethernet main user interface areas](image)

**Figure 110:** Explore Ethernet main user interface areas

Grid layout is fully customizable. User can arrange columns visibility and their positions according to his preferences. Layout is saved after window is closed and restored while reopening.

![Explore Ethernet grid layout customization](image)

**Figure 111:** Explore Ethernet grid layout customization

3.2.2 **Keyboard shortcuts**

Explore Ethernet main window provides following keyboard shortcuts:
Table 7: Explore Ethernet

<table>
<thead>
<tr>
<th>Accelerator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + O</td>
<td>Open capture file</td>
</tr>
<tr>
<td>Ctrl + Shift + O</td>
<td>Open recent capture file</td>
</tr>
<tr>
<td>Ctrl + S</td>
<td>Save (visible) packets to capture file</td>
</tr>
<tr>
<td>Ctrl + Shift + S</td>
<td>Save all packets to capture file</td>
</tr>
<tr>
<td>Ctrl + F</td>
<td>Find packet</td>
</tr>
<tr>
<td>Ctrl + R</td>
<td>Start new capture/stop capturing, Stop loading file</td>
</tr>
<tr>
<td>Ctrl + Shift + R</td>
<td>Start capture with previous settings</td>
</tr>
<tr>
<td>Ctrl + P</td>
<td>Print</td>
</tr>
<tr>
<td>Ctrl + Shift + P</td>
<td>Preview print</td>
</tr>
</tbody>
</table>

3.2.3 Toolbar

Following Toolbar functionalities are accessible (see Figure 112):

- Start and stop a network capture.
- Start capture with last wizard settings
- Open capture file
- Save all packets being captured or only those currently in the view of the capture window through filter operations.
- Save the captures together with the corresponding SCD file which describes the SA environment the network capture was taken.
- Export the contents of the capture window to an Excel file for further processing.
- Import captures from an Excel file.
- ZIP packets with SCD
- Dump all MMS PDUs found in MMS frames into a text file for further processing.
- Send captured file
- Find packet
- Clear all filters
- Print
- Print preview
- Options
3.2.4 Capture window

The capture window displays the captured (or read from file) network packets in a grid (see Figure 113). The available columns can be selected through the Toolbar.

The full list of available columns is:

- Packet number
- Source and destination server
- Source and destination MAC address
- Recording date and time
- Source and destination IP
- Full packet data size
- Application, and transport layer of the packet
- Details of the packets

Packets can be filtered using the fields just below each column header. More information about filtering see Section "The different filters".

Figure 113: ITT600 – Explore Ethernet display filters
3.2.5 Packet information

The packet information section displays the information about the selected packet in different views. Depending on the selected packets protocol type, some elements will not be shown. See Section "Analyzing network packets" for detailed information.

3.2.6 Status bar

The status bar contains information about the applications state:

- Mode (Running | Stopped)
- Current capture filter
- Capture source (File Name | NIC name)
- Average packet size
- Amount of captured bytes
- Amount of captured packets

3.2.7 Working with ITT600 – Explore Ethernet

ITT600 – Explore Ethernet is tightly bound to its host Application ITT600 – Explore IEDs. Thus Explore Ethernet depends on the configuration previously loaded in Explore IEDs. An example of both cases – a matching configuration and one that does not match are shown in Section "Analyzing MMS Packets without a loaded configuration" and Section "Analyzing MMS packets with a loaded SCL file" respectively.

3.2.7.1 Working with capture files

Click on the Open Capture. In the displayed standard file open dialog, select the file you want to open.

ITT600 – Explore Ethernet uses the same capture file format as other ethernet protocol analyzers (e.g. Wireshark, Packetizer, Analyzer, etc.) thus the files are compatible and a file that was captured with Ethereal can also be opened with ITT600 – Explore Ethernet.

The last opened files can be accessed with the Open Recent list. Drag and drop a file from Windows Explorer is also supported.

3.2.7.2 Capture network traffic

The Capture Wizard
To start a capture select the appropriate button in the toolbar (See Section "Toolbar"). A wizard will guide you through the capture process (see Figure 114):
Figure 114: Capture Settings Wizard

Network Interface Card selection
The NIC has to be selected. Choose the adapter from where you want to capture traffic.

If you deselect the **Capture packets in promiscuous mode** entry, only packets with the destination or source address of the selected adapter will be captured.

To capture all packets seen by the NIC the **Capture packets in promiscuous mode** has to be checked! This setting changes the NIC working mode and affects other Explore tools (GOOSE, SV) and also other applications (i.e. wireshark) and vice versa – i.e to capture GOOSE packets promiscuous mode has to be enabled, when Wireshark will start capture and will disable this setting, packets won’t be captured in ITT600.

Automatic capture file splitting
To limit the memory usage of ITT600 – Explore Ethernet, a capture file can be specified. After the defined limit is reached, a capture file will be generated automatically. A file will only be generated if the limit has reached. The old packets will be removed from the grid and will be available only in the file.

If you specify a filename, the extension **pcapng** and a counter indicating how many files have been created will automatically be added. A file will only be generated if the limit has reached.

The buffer size indicates the buffer of the underlying capture engine. If you realize packet losses, increasing the buffer might help.

Increase the buffer size in the wizard if packets are lost. Lost packets will be indicated in the **Statistics** dialog and in the status bar (see "Statistics").

Capture filters
Packets have to match the capture filter, to be shown in ITT600 – Explore Ethernet.
Capture filter block the packets in the capturing engine. Packets that do not match
the capture filter, will never be shown in ITT600 – Explore Ethernet.

In the lower part of the window, you can define capture filters based on IP or MAC address. For more
information on how to define capture filters, see section "The different filters".

More specific capture filters can be defined and the Filter will be displayed in the WinPcap syntax.

Do not check/select any of the IEC 61850 related protocols capture filter, if all
network traffic should be captured!

The wizard enables users to define the duration of the capture timing.

Define a start time when the capture should be started or a time interval for how long the capture
should run.

The capture can also be stopped if certain situations occur:

- A defined number of packets received.
- A defined amount of data received.
- Ignore packets with a minimal size.

After pressing the Submit button, the capture will be started. New packets will be added to the grid
and can be selected for further analysis.

Start capture without using the wizard

It is also possible to start a capture without following the wizard. To do so, press the button in
the toolbar. Using this start method, the last wizard settings will be used.

Use the button to start a capture without the wizard, using the last defined
settings.

3.2.7.3 Analyzing network packets

During or after a capture operation, network packets can be analyzed by accessing single packet
rows in the capture window (Figure 115). In the packet window, one or two tabs are displayed
depending on the application type of the packet. For packets other than IEC 61850 related protocols
(A detailed list of supported protocols is defined in Section "ITT600 – Explore Ethernet Supported
Protocols") only the raw network data tab is displayed. It contains three resizable sections.

On the left side, packet properties are displayed in a property grid. The user can select to display the
contents in either alphabetical order or sorted by packet contents. The actual properties being
displayed depends on the packet type.

The middle section displays the packet contents in hexadecimal format and the right panel presents
the ASCII representation of the hexadecimal data.

General View

Every packet can be shown in the general view as shown in Figure 115. The window is divided into
four sections:

- Section 1 - Selected packet.
- Section 2 - Properties of the selected packet.
- Section 3 - Hex display of the packet’s content.
- Section 4 - ASCII display of the packet’s content.
For IEC 61850 relevant packets, a second tab **Substation Automation related Protocol** is displayed taking focus in front of the raw network data tab.

This tab also consists of four panels, but the information shown is protocol specific. See **Figure 116**.

The panels are:

- Section 1 - Selected packet.
- Section 2 - SA properties of the selected packet.
- Section 3 - Analyzed packet content (IEC 61850 style for MMS).
- Section 4 - Printed packet information (MMS PDU or details).

A list of supported protocols can be found in Section "ITT600 – Explore Ethernet Supported Protocols".
Analyzing MMS Packets without a loaded configuration

To analyze MMS packets it is necessary to load the IED configuration in the ITT600 – Explore IEDs prior starting the ITT600 – Explore Ethernet.

Otherwise it is not possible to decode all the data contained in the frame. This applies especially to reports.

Figure 117 shows an example of a MMS report without the loaded configuration. It is not possible to assign the received values to a data attribute.

It does not matter for ITT600 – Explore Ethernet, whether this configuration was loaded from a SCD file or retrieved online.

To load a SCD file follow the steps defined in Section "Open an SCL file" or connect the IED as described in Section "Connect to IEDs and SERVERs".

Without a loaded configuration it is not possible to decode reports correctly. A message will give you a hint on this.

Analyzing MMS packets with a loaded SCL file

After the correct SCD file is loaded, the report data can be fully decoded. See Figure 117. Loading a SCD file enables also other additional features: the source and destination server names are displayed. As an addition the servers can also be highlighted in ITT600 – Explore IEDs. To switch on this feature select Server Highlight in the Tools menu. See Figure 118.

ITT600 – Explore Ethernet tries to resolve the server names also based on MAC Address. After startup it sends out reverse ARP request for all defined Servers in the SCD, to generate a mapping table between MAC Address and Server Name. Since a lot of specific traffic is generated by the PC some Intrusion Detection System or a Network Administrator might be alerted. It is not recommended to use this feature on corporate LANs without informing your Administrator first.

Figure 117: An MMS report without a loaded SCD file
With each new selection of a packet, the servers will be marked in the Explore IEDs if found. To enable the Trace Server Communication feature, it has to be selected in the Options dialog as well (see Figure 134).

Enabling the trace all packets between a server and client (actually between two IP Addresses) will be highlighted. An example is shown in Figure 120. It is also possible to show the functional names and object description. This is done by enabling such features in the Option dialog. See Figure 121.
3.2.7.4 The different filters

ITT600 – Explore Ethernet uses different filters. Depending on the desired operation one type or the other is more appropriate.

**Capture filters**

Capture filters are working very close to the hardware and are used by the capture engine. Thus, packets that are not matching the filter will not be shown.

A capture filter cannot be changed during a capture. To apply a new filter, a new capture has to be started.

The advantage of capture filters is that the amount of captured packets can be minimized.
Capture filters only apply on online captures.

If a capture filter is specified, only packets that match this filter will be captured and shown in the application.

Capture filters are available for IP addresses, MAC addresses and port numbers.

**Examples:**

The following example - Figure 123 - will capture all traffic from the three IP addresses, no matter whether it is the source or destination address:

![Capture filter based on IP addresses](image1)

**Figure 123:** Capture filter based on IP addresses

Values can always be separated by semicolons or commas.

Capture filters can be combined, see next example:

![Combined capture filter](image2)

**Figure 124:** Combined capture filter

In this example all packets with the source IP address of 10.140.20.152 and the specified source or destination address are captured.

Values in the same field are always combined in an OR condition, whereas different lines will be combined as AND condition. See Figure 125 for more details.

The complete filter will be shown on step two of the wizard:
Used capture filters are shown in the status bar as shown in the following figure.

![Figure 126: Status bar showing used capture filters.](image)

**View Filters**

View filters simply rearranges the already captured packets. No packets will be deleted or ignored. The packets that do not match the filter will not be displayed.

View filters can be changed even if a capture is in progress.

View filters can be applied on online capture and also on capture files.

**Examples:**

The following example shows how to set a view filter for MMS - [Figure 127](image).

```
Data Size | Application | Transport | Data
---|---|---|---
284 | MMS (Custom) |  | S
54 | MMS (Blanks) |  | S
284 | MMS (NonBlanks) |  | S
284 | MMS |  | S
```

**Figure 127: Defining a new filter**

It is also possible to define customized filters. Select **Custom** in one of the rows and define your own filter. See [Figure 128](image) With a specified combination, as shown in [Figure 129](image) only MMS packets with a data size larger than 70 bytes are displayed.
Custom view filter is very powerful. It can also be used to filter only for specific contents, which is useful when applied to the Details column. The following filter - Figure 130 - will only show reports.
3.2.7.5 Export captured packets to Excel

The captured packet data can be exported into a Microsoft Excel file (select menu File | Export to Excel) for further processing. The Excel file has the format as shown in Figure 133.
Raw packet data are hidden after the last column.

Export to Excel does not contain the related SCD file.

### 3.2.7.6 Import captured packets from Excel

Captured data can be reimported from Microsoft Excel file into the capture window. A suitable SCD file must be loaded in the Explorer.

If columns in an exported Microsoft Excel files are moved or deleted, the reimport will fail!

### 3.2.7.7 Dump MMP PDUs

This feature will save all MMS PDUs into a text file for further evaluation. Only MMS packets will be contained in the file.

This feature is helpful when a sequence of MMS packets have to be analyzed by an experienced user.

### 3.2.7.8 Options and default settings

Several default values can be set in the Options dialog. See Figure 134. User can set some view options, define network adapter settings or select specific capture files (e.g. GOOSE, sampled values or MMS).
3.2.8 Statistics

ITT600 – Explore Ethernet provides some basic statistical information. General statistics shows the basic counters:

- How many packets are received
- How much data is received
- Start / Stop times
- How many packets are lost

In case packets are lost, increasing the buffer size will help.

It also gives an overview of all captured protocols and their percentage of the total. See Figure 135.
Figure 135: Protocols statistics

All connections are also recorded in the Connections tab. See Figure 136.

Figure 136: Connections statistics

3.2.9 Send capture file

ITT600 – Explore Ethernet allows a replay of a captured file. The action bar to this feature is shown in Figure 137.

Figure 137: Sending an capture file bar

Select the appropriate adapter from the list and define how many times all packets should be transmitted. During sending a progress bar will inform the user about the progress status.
FPS option allows user to set how many frames should be sent per second, however it is not guaranteed because of the Windows OS limitations. Default value 0 will cause that packets will be sent out as fast as possible.

This function does not take the real time tags of the packet into account.

Packets with remote addresses are sent from your local NIC. An intrusion detection system or a network administrator might be alerted. It is not recommended to use this feature on corporate LANs without informing your Network Administrator first.

### 3.2.10 Send a packet

A single captured packet can as well be resent to the network. Right-click a packet and select “Send Packet” from the context menu (see Figure 138). An action bar including the packet number will show up (see Figure 139). Next, select the appropriate adapter from the list and define how many times the packet should be transmitted.

A packet with remote addresses is sent from your local NIC. An intrusion detection system or a network administrator might be alerted. It is not recommended to use this feature on corporate LANs without informing your network administrator in advance.

![Send Packet context menu](image1)

**Figure 138:** Send Packet context menu

![“Send Packet” action bar](image2)

**Figure 139:** “Send Packet” action bar

### 3.2.11 Toggle relative/absolute time

When analyzing packet time stamps, it can be helpful to see relative time stamps. This option can be switched on/off by the menu item in the context menu. See Figure 140 and Figure 141.
3.2.12 Find in packet data

Identifying packets with a specific content can be time consuming. The Find Packet bar will help in this case.

The search mechanism uses the whole packet data (including MAC and IP addresses). There are two options: searching for ASCII based values or hexadecimal values. See Figure 142.

If Mark all options is selected, all packets matching search criteria are highlighted, clicking the Find Next/Prev button or pressing Enter key will select the packet that matches the search string, user can also decide if search should be case sensitive.

The selection shown in Figure 143 highlights all packets containing the string RPT (all IEC 61850 reports).
3.2.13 Protocol specific information

Analyzing different protocols still needs knowledge about the protocols itself. ITT600 – Explore Ethernet tries to display the information in a form that is easy to understand even for non-network experts.

It is not the scope of this manual to give an introduction in the various supported protocols. Nevertheless, some hints and basic protocol analysis techniques are shown in this chapter.

3.2.13.1 MMS

MMS is used for IEC 61850 vertical communication between IEDs (Servers) and different clients (e.g. SCADA Systems).

It is a connection oriented client/server protocol that is embedded in a TCP/IP stream. Every client request is answered by the server with a separate response. To find the response to a given request, every MMS message contains a so called “Invoke ID”. This is a unique ID (an integer number) for each pair. Figure 144 shows an example of a request/response pair.

The Details column (see Section “Analyzing network packets”) also shows the invoke ID. This makes it easy to find “matching pairs”.

![Figure 144: MMS request with Invoke ID](image)

Every MMS message has an Invoke ID. This is identification for request / response message pairs.

**Commands**

IEC 61850 Commands are mapped to MMS write requests. They will be acknowledged by a positive or negative command response. Figure 144 shows an example of a positive command response. As described in the former section, the only way to check, which command is acknowledged, is to analyze the InvokeID.

A negative response will be followed by a so called “LastApplError” report. This report contains the reason why the command has failed (the AddCause field).

Since a report does not contain an Invoke ID, the LastApplError refers always to the last command. See Figure 145.
Reports

Reporting is the mechanism used in IEC 61850 to send spontaneous data from IEDs to clients.

All data that has to be sent to a client has to be configured in a DS. The DS itself is then referenced by a RCB. Clients have to enable the RCB with specific options to receive the data changes from an IED.

Segmentation and fragmentation

MMS messages can be larger than the maximal Ethernet frame length, in that case the message has to be segmented into several frames on TCP level and/or fragmented on the TPKT/COTP level from OSI protocol. If packet is segmented on TCP level - Data packet will appear under TCP payload in Packets stack panel and additional information in Details column will be shown on the packets grid:

Fragments list in Data fragment for TCP segmentation show only TCP level fragments. If MMS is fragmented on higher level, the fragments list will not contain it. MMS fragment may also be not segmented on TCP level.
IsSegmented property indicates if TCP packet is segmented on TCP level, however the last segment does not contain segmentation flag. IsLast property in Data fragment indicates if the fragment is the last one and IsAssembled indicates if all fragments are correctly assembled - depending on which level Data fragment is displayed.

At the end, MMS message may be assembled from both tcp segments and OSI level TPKT/COTP fragments. MMS message, if segmented and/or fragmented will contain Fragments property with all the packet fragments, see Figure 147.

![Figure 147: Assembled segmented and fragmented MMS message](image)

MMS message is displayed only on the last, correctly assembled packet.

### 3.2.13.2 GOOSE/RGOOSE/Tunneled RGOOSE

GOOSE is a multicast service that is sent cyclically. During normal operation (no values are changing) the frames are sent with the defined maximum time $T_{\text{max}}$. As soon as a value changes that is defined in the GCB's referenced DS it will be sent with minimum time $T_{\text{min}}$ and the pattern repeats.

Each GOOSE frame contains header information and data (according the DS). When capturing GOOSE packets, some consistency checks are made by ITT600 – Explore Ethernet.

Various values of the GOOSE message are compared with the values loaded in ITT600 – Explore IEDs (e.g. from an SCL File). Inconsistencies are shown in the detailed view. This is a hint that the IED is not configured with the same SCD that is loaded. See Figure 148.
RGOOSE/Tunneled RGOOSE are GOOSE packets sent over UDP protocol with destination port 102, GOOSE details are the same as in ethernet GOOSE.

The GOOSE Header contains a so called APPID. Depending on this number an IED decides whether to process the frame or not. The APPID is show as hexadecimal value (as it is defined in the SCD file also).

3.2.14 Replay protection

Explore Ethernet, if the Replay protection analysis is turned on, will display analysis result in the packet details panel and in the details column on the packets grid as shown in following figure:

Replayed GOOSE packets are shown in grid with additional information in packet details section.

For more details about GOOSE replay analysis see "GOOSE replay protection algorithm"
3.3 ITT600 – Explore GOOSE

3.3.1 Overview

ITT600 – Explore GOOSE shows GOOSE data contained in a capture file related to a common time axis. Individual signals can be compared at the same time, with an option to synchronize them.

Explore GOOSE captures GOOSE, RGOOSE and Tunneled RGOOSE packets

The Figure 150 of main window show following panels.

- Toolbar
- Discovered IEDs tree
- Plots
- Packet details
- Legend
- Status bar

Figure 150: ITT600 – Explore GOOSE main user interface

3.3.1.1 Keyboard shortcuts

Explore GOOSE main window provides following keyboard shortcuts:

<table>
<thead>
<tr>
<th>Accelerator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + O</td>
<td>Open capture file</td>
</tr>
<tr>
<td>Ctrl + Shift + O</td>
<td>Open recent capture file</td>
</tr>
<tr>
<td>Ctrl + S</td>
<td>Save plots</td>
</tr>
<tr>
<td>Alt + O</td>
<td>Open plots</td>
</tr>
</tbody>
</table>

Table continues on next page
3.3.1.2 Toolbar

The toolbar provides access to the basic functionality of Explore Goose (see Figure 151). It allows the user to:

- Open a capture file
- Open a recently opened capture file
- Open a plot file containing a previously saved configuration
- Save the current plot configuration a file
- Clear the current IED list and GOOSE signals
- Refresh captured data to match a newly-loaded model
- Access ITT600 Options
- Select the Network Interface Card used for GOOSE capture
- Start/stop an online capture
- Toggle whether to keep already captured data after capture restart

Figure 151: ITT600 – Explore GOOSE toolbar

3.3.1.3 Options Menu

The Options menu provides access to the options dialog. See Figure 152.
### 3.3.2 Working with Explore GOOSE

ITT600 - Explore GOOSE is using saved capture files including GOOSE frames for displaying the contained values. Additionally, an online mode is available.

A capture file can be created with ITT600 – Explore Ethernet and is described in Section "Capture network traffic" or external third-party tool which can export captured packets to any of pcap supported capture file formats.

#### 3.3.2.1 Offline Mode

Click on the Open Capture. In the displayed standard file open dialog, select the file you want to open.

ITT600 – Explore IEC61850 GOOSE uses the same capture file format as other ethernet protocol analyzers (e.g. Wireshark, Packetizer, Analyzer, etc.) thus the files are compatible and a file that was captured with Ethereal can also be opened with ITT600 – Explore IEC61850 GOOSE.

The last opened files can be accessed with the Open Recent list. Drag and drop a file from Windows Explorer is also supported, see Figure 153.
After the file has been parsed, a list containing all IEDs sending GOOSE traffic is generated. Selecting an IED will show all contained GOOSE DataSets taken from the GOOSE Control Block references. This view will be different whether a configuration has been loaded in ITT600 – Explore IEDs previously. See Section "Open an SCL file" or Section "Connect to IEDs and SERVERs".

Online Mode

The online mode captures traffic on the specified Network Interface Card and processes all received GOOSE frames. By default it enables promiscuous mode on the NIC. The list of IEDs is dynamically updated when new IEDs sending GOOSE frames are detected on the network.

To start an online session, select the desired NIC in the dropdown, then press Start capture. See Figure 154.

In case previously recorded data should be kept, check the Keep already captured data checkbox.
In case multiple sessions are combined (the *Keep already captured data* feature is switched on), the data is connected with a straight line even though data changes might have happened during the paused time.

Explore GOOSE by default starts capture with promiscuous *Promiscuous* mode which may affect other tools and applications (i.e. wireshark) if this mode was not enabled.

To stop an online capture, click on the **Stop** Toolbar Button.

### 3.3.2.3 Discovered IEDs

The tree view allows navigating, selecting and searching for data attributes captured or loaded from a file:

![Discovered IEDs tree](image)

*Figure 156: Discovered IEDs tree*

The tree view shows the following hierarchy of items:

- IED name
- GCB (DataSet): goCBRef from captured packet and DataSet name
- DataSet group
- Data attribute and the number of packets

Data attribute level displays functional name and/or description according to View settings in Explore Ethernet options.

There are three types of DataSet groups:

- **DataSet attributes**: contains attributes from captured GOOSE packet which match the DataSet from a loaded model
- **Not matched to DataSet**: contains attributes from captured GOOSE packet which do not match DataSet in the loaded model (i.e. wrong number attributes, wrong types)
- **DataSet missing**: contains attributes from captured GOOSE packet when the GCB cannot be found in the loaded model, or when there is no loaded model
Data attributes may end up not matching to missing DataSet group if:

- the goCBRef from the GOOSE packet is not found in the loaded model
- model is not loaded
- loaded model is different than the one in real/simulated IED

Some of the attributes (like Quality) will be displayed as gray, meaning this data type cannot be shown in the plot. See Figure 157.

![Figure 157: Quality data type colored grey](image)

Quality values cannot be displayed as individual values. The quality information is part of the related value.

Each attribute has an icon indicating the value type, see Figure 168.

### 3.3.2.4 Display with loaded configuration

When the matching configuration is loaded, a list of available IEDs and the contained GoCBs are displayed. The list of attributes is grouped by the GOOSE Control Block (basically its dataset) they are contained in.

Every IED includes its description and all Data Set items are listed with the full IEC 61850 name as shown in Figure 158.

![Figure 158: GOOSE IED and attribute selection](image)

### 3.3.2.5 Display without loaded configuration

Without a loaded configuration, only basic information found in the GOOSE frame can be used to identify the individual IEDs and their attributes. Such an example is shown in Figure 159.

![Figure 159: GOOSE IED and attribute selection – without loaded configuration](image)
3.3.2.6 Simulated and real packets

Goose packets from the same GCB are treated separately depending on the simulation bit on packet header. The additional info is added to GCB name if GCB is simulated.

Figure 160: GOOSE packets grouped depending on simulation bit

3.3.2.7 Plots

Plot can be opened with two time settings:

- Capture time
- Frame time

Frame time
This time is set by the IED when change of one of the attribute triggers the GOOSE to be sent and is contained in the header of the frame.

- Frame time represents the time set by the IED and is included in the received frame.
- Capture time represents the time when the frame was recorded and is set by the PC.

Capture time
This time is assigned when the packet was captured on the selected network interface card.

Double clicking an attribute will open a plot using capture time by default. It can be also opened with the context menu.

Capture time is the default one, to open plot with frame time use context menu of the attribute.
3.3.2.8 Plot Information and functions

There are a lot of functions provided by the plot display. First thing that should be noted is that each dot in the plot indicates that a value was received at that time. Since GOOSE is a cyclical service and the values are resent even if they have not changed, this is indicated in Figure 162.

3.3.2.9 Go to the next value change

Sometimes it is cumbersome to find the next change of a specific value, especially if the plot is zoomed or a long time period is shown. For this reason, the plot toolbar and Overview Pane are available to enable easier navigation. The user can choose to navigate between. See Figure 163.
3.3.2.10 The Explore GOOSE plot toolbar

The plot toolbar provides access to all major functions (see Figure 164):

- Pause: when online capture is on, updates of plot can be paused to zoom and analyze the GOOSE packet
- Copy image to clipboard: plot image is copied to the clipboard
- Toggle overview pane: show/hide overview pane
- Toggle data cursor: show/hide data cursor
- Toggle plots synchronization: turn on/off synchronization of plots
- Previous data point: navigates to previous data point
- Next data point: navigates to next data point
- Navigation mode: allows to switch between navigation modes:
  - Data change – default mode, navigates between value and/or quality change of data point
  - Data point – navigates between data points

Figure 163: Go to next or previous value change

Figure 164: ITT600 - Explore GOOSE plot toolbar
3.3.2.11 Zooming

It is possible to zoom in/out or define a zoom region by using the slider on the bottom of each plot, or using the Overview Pane tool. See Figure 165.

![Figure 165: ITT600 - Explore GOOSE overview pane](image)

This tool also lets the user change the default mouse drag functionality between panning the plot view, or zooming to selection.

3.3.2.12 Data cursor and plots synchronization

The data cursor can be used to measure the time or the value at a specific point in the plot. See Figure 166.

![Figure 166: Data cursor switched on (plots are synchronized)](image)

To compare the different signal, it is important that the plots are synchronized.

Plots should be synchronized to compare the different values.

3.3.2.13 Saving and opening plots configuration

Any plots configuration can be saved into a plot file. This file will contain the captured data, as well as the opened plots configuration.

To save a configuration, use the Save Plots file menu entry or the toolbar button.

A configuration can be opened by using the Open Plots functionality. Since the file includes the plot data, it can also be opened on another PC.
Plots configurations can be saved and reloaded.

### 3.3.2.14 Packet details

By clicking on the packet marker on the plot, the Packet details panel will show decoded GOOSE packet. In the title panel the capture time of the packet is additionally displayed:

![Packet details panel](image)

**Figure 167: Packet details panel**

The details section contains four categories:

- General: decoded packet values with GOOSE Pdu
- Model check: details about compatibility with loaded model
- Data set: listed DS attributes decoded from packet
- Analysis: result of Replay protection analysis (if enabled)

### 3.3.2.15 Legend

Legend is divided into four categories which defines the packet data point:

- Quality validity marker colors
- Source shapes
- Config Rev mismatch outline (if model is not loaded each packet is marked)
- Analysis indicators

and Data attribute value types icon on the Discovered IEDs tree:
**Config Rev mismatch outline**

If the configuration revision check between the online data and the SCD fails, individual nodes gain a purple outline. **Figure 169** shows a signal with a matching configuration revision, **Figure 170** shows a mismatch.

**Quality information**

Quality information cannot be added as individual signals. The quality information is incorporated in the related value. Bad quality of a signal (Invalid, Questionable or Reserved) is displayed as shown in **Figure 171**, **Figure 172** and **Figure 173**.

**Mismatches between the expected configuration revision from ITT600 – Explore IEDs and the actual received value are indicated.**

**Figure 169:** No outline indicates that configuration revision check is fine

**Figure 170:** Purple outline indicates configuration revision mismatch

**Figure 171:** Invalid quality of signals is shown as yellow

**Figure 172:** Questionable quality of signals is shown as brown
Quality information is incorporated in the related value.

**Source information**
The source information is incorporated in the related value. Source of a signal (Substituted, Test) is displayed as shown in Figure 174 and Figure 175.

The source information is incorporated in the related value.

**Analysis indicators**
When the Replay analysis is turned on and the GOOSE packet analysis fails, the data point changes to either Replayed or Security failed marker, additionally if the next packet is not captured within Time Allowed To Live (TAL) time, the TAL expired indicator is placed on the plot:

For more details about GOOSE replay analysis see "GOOSE replay protection algorithm".
3.4 ITT600 – Explore SV

3.4.1 Overview

ITT600 – Explore SV shows SV data captured from live streams or read from a capture file. Explore SV supports 61869-9, IEC 61850 9-2 and 9-2 LE standards. There are two ITT600 – Explore SV working modes, namely online and offline working mode. Explore SV allows to analyse simulated and not simulated streams separately.

- **Online working mode**: ITT600 – Explore SV captures packets from the user selected network adapter and displays the current and voltage phasors of a given stream within a polar chart. During the packets capturing, a user is also able to log the received packets to the disk by using the logging functionality.

- **Offline working mode**: ITT600 - Explore SV allows to load packets from a capture file recorded during online mode, from external third party packets sniffer or internal buffer captured during online working mode allowing for each available stream to display the voltage and current trends and phasors. Moreover, it is possible to explore the content of each SV packet and display the current and voltage phasors related to that given moment in time. Explore SV switches to offline mode right after stopping the online capture.

Main Explore SV window is divided in three areas: (see Figure):

- Toolbar
- Detected streams list
- Streams view

![ITT600 – Explore SV main user interface](Figure)

Main window areas (panes) are dockable and it's layout is saved when the Explore SV window is closed and restored when opened.

ITT600 – Explore SV is a resource intensive application. It is highly recommended to set the power management of the computer to full performance in order to achieve smooth operation of the tool. Furthermore, when the application is running on a laptop, it is highly recommended to run it with the AC power supply and not solely on battery power.
3.4.1.1 Keyboard shortcuts

Explore SV main window provides following keyboard shortcuts:

<table>
<thead>
<tr>
<th>Accelerator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + O</td>
<td>Open capture file</td>
</tr>
<tr>
<td>Ctrl + Shift + O</td>
<td>Open recent capture file</td>
</tr>
<tr>
<td>Ctrl + R</td>
<td>Start/stop capturing</td>
</tr>
<tr>
<td>Ctrl + Shift + R</td>
<td>Start/stop recording</td>
</tr>
<tr>
<td>Left/Right Arrow</td>
<td>Navigate between samples</td>
</tr>
<tr>
<td>Ctrl + Left/Right Arrow</td>
<td>Go to first/last sample</td>
</tr>
</tbody>
</table>

3.4.1.2 Toolbar

The toolbar allows to switch between online and offline modes:

Figure 178: Online mode

Figure 179: Offline mode

The online mode allows to:

• Select NIC to be used for capture the streams
• Start/Stop capture
• Save the captured packets to file

The offline mode allows to:

• Open capture file
• Open recent capture file

3.4.1.3 Explore SV options

The main Explore SV options are accessible from main ITT window menu (Tools -> Options) in the Explore SV section (see Figure 180):
The following parameters can be customized in ITT600 – Explore SV:

- **Enable Offline Analysis**: when enabled, ITT600 – Explore SV activates the offline analysis part. This allows user to perform analysis of the SV packets in an offline mode after online capture is stopped. If option is disabled then user have possibility to analyze only last 1000 captured samples which is the minimal buffer size for online mode.

- **Buffer size**: to enable offline analysis, it is required to store some SV packets in the memory. Storing more SV packets enables an analysis to a more granular level and vice versa. When less packets are persisted, the quicker the software responds to input and vice versa.

  The buffer size is set per SV stream, setting large buffer size will utilize more PC memory.

- **Log file destination**: with this parameter, user can specify his/her preferred place to store the log files for the SV packets.

### 3.4.2 Working with Explore SV

ITT600 – Explore SV provides two different working modes: online mode and offline mode.

#### 3.4.2.1 Online mode

The online mode listens on a selected NIC and processes all captured SV packets from selected streams and shows them in the stream view. The list of available streams is dynamically updated when new SV packets belonging to never-seen-before streams are detected on the network.

To start an online session, first select the proper NIC and then click on the **Start capture** toolbar button. See Figure 181.
While capturing, it is possible to enable recording captured packets to file by pressing Start recording toolbar button. This operation writes each received SV packet to file(s).

**Detected streams list**
The list of detected streams allows user to select stream for capture, open stream to view values, align streams etc.

- **Checkbox to select stream for capturing**: The size of the buffer is taken from the main Explore SV options, if ‘offline analysis option’ is enabled. If this option is disabled, Explore SV will use minimal buffer required to calculate online values. If stream is not selected for capturing, if stream will be opened the values won't be calculated and updated. When sample rate is not determined, the checkbox is disabled.

  - **Samples rate**: determined by the smpCnt field in the SV packet which will arrive with correct value (Sampling rates and publishing rates are described in 61869-9)

  - **Stream descriptor edit button**:
    - **green information icon**: indicates that stream is matching to the definition found in the loaded model (SCD file) or is 9-2 LE (contains four currents, four voltages and either one ASDU or eight ASDU's)
    - **Orange warning icon**: indicates that there is no definition of the stream in loaded model or is not like 9-2 LE and user should edit the descriptor so the values will be correctly calculated.

- **Stream name**:
  - **Gray color**: indicates that stream is not selected to be captured
  - **Black color**: indicates that stream is not opened and is being captured
  - **Green color**: indicates that stream is opened
  - **Can contain additional information**.

---

**Figure 181**: ITT600 – Explore SV - starting online capture

**Figure 182**: Detected streams in online mode
• [Simulated]: if stream has simulation bit set
• [HSR Lane]: if stream is sent over HSR frames

• Stream frequency:
  • Black color: indicates that frequency is calculated from the captured samples
  • Red color: indicates that frequency cannot be calculated (i.e wrong measurement values)
  • Orange color: indicates that stream frequency was overridden in descriptor editor

• Show/Hide icon: allows to open/close the stream. It is also possible to use left mouse double click.

• Icon indicating if stream is:
  • online (green checkmark icon): packets are captured from the NIC
  • offline (red exclamation icon): no new packets were captured (i.e stream is not sent by merging unit anymore)

Streams list context menu allows to:

• Open/close stream
• Align stream with another stream
• Close stream alignment

Figure 183: Online mode context menu

Editing stream descriptor
Explore SV allows to edit stream definition in case definition was not found in the loaded model, there is no model loaded or if found stream definition is not correct (stream name matches but in fact user knows the stream has different definition).
Editor allows to:

- Set the channel name
- Set the channel type (current or voltage)
- Set the channel phase
- Override frequency

The most important for correct values calculations is the type of the channel. The standard defines the scale used to recalculate the raw measurement values from the SV ASDU:

- 0.001 for currents
- 0.01 for voltages

The neutral phase is omitted in frequency calculation. If stream is already opened - editor contains additional button ‘apply’ - to save the changes and re-open stream. If stream is not opened, the changes are applied immediately after editor is hidden.

Overriding frequency is useful when it cannot be calculated from the values (red color) but user knows which frequency should be used. The default frequency used in calculation in case it is not overridden and not calculated is 50Hz.

**Stream view**
The detected stream can be opened to view the values and calculated phasors. Views will be updated if the stream is also selected for capture:
The view consists of two sections:

- Phasors view
- Channels view

Phasors view
Displays calculated phasors in a polar chart using an absolute scaling system. There are two different scales, i.e., one for the current and another one for the voltage. Each phasor is divided by its...
own full-scale and the resulting value is used as phasor magnitude. User can adjust the values of each of the full-scale using the appropriate slider in the settings:

![Phasors view settings](image)

**Figure 186: Phasors view settings**

There are four line representations related to phasors quality:

- **Good**, displayed as solid line: all the values used for calculating this phasor were good quality.
- **Invalid**, displayed as dashed line: at least one of the values used for calculating this phasor had quality validity different than good.
- **Warning**, displayed as dotted line: at least one of the values used for calculating this phasor was different than good and quality validity was good.
- **Missing point**, displayed as line dashed with double dots: at least one of the values which should be used for calculating this phasor was missing.

**Channels view**

Channels view consists of stream name and additional information:

![Channels view](image)

Samples additional information:
The S.Sync filed in this view is not a SmpSync value from sample, but the minimum value from all samples used to calculate the phasor. The number of samples used to calculate the phasor is calculated as Samples Rate divided by Frequency (calculated/overridden/or default 50Hz).

Table with the channels values:

<table>
<thead>
<tr>
<th>Channel</th>
<th>RMS</th>
<th>Angle</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCTR1.Amp</td>
<td>1010.53 A</td>
<td>11.62°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR2.Amp</td>
<td>996.85 A</td>
<td>132.53°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR3.Amp</td>
<td>989.89 A</td>
<td>251.39°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR4.Amp</td>
<td>0.00 A</td>
<td>0.00°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR1.Vol</td>
<td>222.32 kV</td>
<td>11.62°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR2.Vol</td>
<td>219.31 kV</td>
<td>132.53°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR3.Vol</td>
<td>217.78 kV</td>
<td>251.39°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR4.Vol</td>
<td>0.00 kV</td>
<td>0.00°</td>
<td>Good</td>
</tr>
</tbody>
</table>

Figure 187: Channels table

Channels table consists of:

- Checkbox to show/hide channel
- Channel name
- Values:
  - Calculated RMS and angle
  - Instantaneous (raw) values
- Qualities
- Settings, which allows to:
  - Switch between RMS/angle and instantaneous (raw) values
  - Change precision of displayed values
Context menu: set/unset channel as reference

Multiple streams view
Explore SV allows to view multiple streams at once with the option to show them separately:

![Multiple streams opened](image)

**Figure 188:** Multiple streams opened

Align the streams together (two streams can be aligned, but is allowed to align multiple pairs) using the context menu 'align with' on the detected streams list:
Aligned streams are placed next to each other and the top bar is shown indicating the alignment. Streams are aligned by frequency, sampled values and SmpCnt from the samples. If the values are not matched, the phasors view will change the color indicating that streams are not synched:
Figure 190: Not synched streams

Ref Function
Channels list allows to select the channel as a reference via the context menu:

<table>
<thead>
<tr>
<th>Channel</th>
<th>RMS</th>
<th>Angle</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCTR1.Amp</td>
<td>1000,00 A</td>
<td>238,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR2.Amp</td>
<td>1000,00 A</td>
<td>358,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR3.Amp</td>
<td>1000,00 A</td>
<td>118,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TCTR4.Amp</td>
<td>0,00 A</td>
<td>0,00°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR1.Vol</td>
<td>220,00 kV</td>
<td>238,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR2.Vol</td>
<td>220,00 kV</td>
<td>358,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR3.Vol</td>
<td>220,00 kV</td>
<td>118,50°</td>
<td>Good</td>
</tr>
<tr>
<td>TVTR4.Vol</td>
<td>0,00 kV</td>
<td>0,00°</td>
<td>Good</td>
</tr>
</tbody>
</table>

Figure 191: Use channel as reference

If a channel is set as a reference, its phase angle is set to 0°, and it is used as “a reference” for calculating phase angle of the other channels.
If two streams are displayed in align mode, by setting a channel as reference, the phase angle of the reference channel is used as “a reference” for calculating the phase angles of channels of both streams. In this way, it is possible to compare the angle difference between the channels belonging to different streams. However, user can select different channels to use as reference, one for each stream. In this particular case the channel reference is considered only for all the channels belonging to that stream.

**Recording the SV Packets**

It is possible to record SV packets to file during online capture. To activate this function, click on the “Start Recording” button on the toolbar to start writing to file all the packets captured.

The maximum size of each logged file is fixed to ensure that the file size is not too large for further operation. During logging, when file size reach ~116MB, a new file is created as a container for the next recorded packets.

### 3.4.2.2 Offline mode

Users have two possibilities to display SV data in offline mode:

- Run an online capture and open the captured stream after stopping - the detected streams list is cleared from streams which were not selected to be captured at all (or simply do not contains any captured packets). After stop of online capture, the Explore SV is switched to offline mode

- Load a capture file (open new or recently opened file).

The detected stream list is similar to online mode, but is lacking the offline/online icon indication and the checkbox to select stream to be captured and contains option to save the stream packets to file.

Multiple streams can be opened to view, one in main window and others in separate windows:

![Figure 192: Two streams opened in offline mode](image)

Offline views contains trends view and details panel with statistics and selected sample details (multiple samples can belong to one packet - the sample is in fact the ASDU). The phasors are calculated based on the selected sample.

The phasor view and channels view are described in online mode section.
Offline mode does not allow to align the streams.

**Trends**

ITT600 – Explorer SV provides an integrated feature to show the trend of the voltage and current. Trend display shows at the same time both current and voltage values and qualities. If stream contains only one type of channel - the second one is hidden. To navigate through the trend graph, navigation panel and zoom in/out function are provided. Left and right buttons of the navigation panel can be used to access the samples. Besides that, when the play button is clicked, the cursor of the Trend display will be moved automatically and each sample will be shown sequentially. Additionally, based on the level of zoom currently used, the voltage and current trends are displayed as continuous lines or as data points. This functionality allows the users to have a proper level of details based on the required zoom.

User can move the axes or just click over any current/voltage point in the trend in order to display the detailed information of the current SV packet and this is shown on the left section of the trend display – in the Analyzed 9-2 packet tab (see Figure 193). Additionally, the particular point selection in the trend display will trigger the visualization of current and voltage phasors in a polar chart. Each point in both the current and the voltage trends are calculated based on the data from the channels of data, i.e for 9-2 three channels for the 3 phases plus the neutral one. By clicking the checkbox in the channels view it is possible to hide/show that channel in the trend and phasor views.

![Figure 193: ITT600 – Explore SV – Trend display and data analysis part](image1)

While the missing points are represented red dot style in the continuous line view; when the view changed to a data points, this missing points are shown as empty space (see Figure 194).

![Figure 194: ITT600 – Explore SV – Missing points are shown in the trend displays](image2)

Bad channels are shown zigzag style fill under trend line (see Figure 195).
Figure 195: ITT600 – Explore SV – Bad channels are shown in the trend displays

The trend display update may decrease with the number of samples in stream.

Statistics analysis
ITT600 – Explore SV provides several functionalities to dig deeper into the quality of the packets. The statistical information is available only in the offline mode. The details panel allows to view:

• Stream statistics
• Packet details

In packet view user can evaluate in detail the content of each particular packet that is used to construct a point in the graph.
Figure 196: Packet details view

In stream mode user can browse through statistics which shows a summary of the collected samples including information such as quality, anomalies, missing points and ranges in which master clock ID and stream sync values were changed.

Stream details view consist of statistics list with counter of entries inside each category (number of ranges)
Figure 197: **Selected stream statistic with counter of its entries**

After selecting any category user can see a list of entries. Each entry consists of the amount of consecutive samples which fit to selected category and range of sample numbers in which that samples was captured. After selection of specific entry inside statistics category application will navigate to the first sample from selected range.

- Sample numbers used in showing range for statistics entries includes missing samples so it could not necessarily match sample numbers in capture file, also packets can contain more than one ASDU and so the number of packets in capture file will be different than the number of samples.

- Statistics are calculated per sample so in case when we’ll have for example more than one channel with test quality coming from one sample it will be still treated as one and will not cause any additional entries in statistics.

**Saving stream to file**

In offline mode user have possibility to save each stream to file by clicking "Save to file" icon localized next to show/hide stream. It allows user to choose destination path and will save all packets originated from selected stream to capture file.
3.5 ITT600 – Explore Models

3.5.1 Overview

ITT600 – Explore Models provides functionality to compare two different SCD files or even an IED online configuration with a SCD file.

The GUI can be divided into four main areas (See Figure 199):

- Main menu (red).
- Toolbar (blue).
- Comparison results (green).
- Models to be compared (yellow).
3.5.2 File Menu

The file menu provides basic functionalities, namely (see Figure 200):

- Load the models.
- Exit the application.

![ITT600 - Explore Models File menu](image)

Figure 200: ITT600 - Explore Models File menu

3.5.3 Help Menu

The Help menu provides Model Functionalities (see Figure 201).

![ITT600 - Explore Models Help menu](image)

Figure 201: ITT600 - Explore Models Help menu

3.5.4 Toolbar

Toolbar provides buttons to navigate through the compared model and comparison results, namely (see Figure 202):

![ITT600 - Explore Models Toolbar](image)

Figure 199: ITT600 - Explore Models main user interface
• Load left and right model for comparison.
• Compare models.
• Move to next or previous difference.
• Export the differences to .xsi file.

Figure 202: ITT600 – Explore Models Toolbar

3.5.5 Model panels

The two model trees will display the structure of the IEC 61850 model contents (see Figure 203).

Figure 203: ITT600 - Explore Models with loaded models

3.5.6 Comparison panels

The comparison panels will display the result of the model comparison in the left tree and details in the right panel to the user (see Figure 204).
### 3.5.7 Comparing SCL Files

ITT600 - Explore Models compares SCD files by loading the files in its internal representation – the model.

To compare two SCD files they have to be loaded to the models first. One way of doing it is selecting the load function from the File Menu.

Another way is to right click in each of the model windows and selecting the Load SCL model context menu.

- If you have already loaded an SCD file in the ITT600 – Explore IEDs prior starting ITT600 – Explore Models, the left model (model 1) will always be taken from the Explore IEDs.

- While ITT600 is loading SCL model it automatically corrects some formatting issues such as trailing spaces, prohibited signs etc. In that case when we open model comparison window with model already loaded, it looks in the same way as the one loaded in ITT600. While loading second model to compare we use the same corrections to avoid getting differences between the same files. However this can cause the situation when the displayed values will not match the actual ones in SCL. In case you want to compare raw/unmodified data as it is in SCL you need to reload left model as first step after opening comparison window or start it without model loaded in ITT600.

After both models are loaded you have to select a node on each side (see Section "Comparing SCL Files"). The “Compare” toolbar button becomes enabled. Clicking this button will show a dialog with filters (for detailed explanations about the filters, see Section "Comparison Filters"). Click OK to proceed with the comparison.
When comparing two substation nodes, the tool will compare the two different substation section elements.
To compare all IEDs, select the all IEDs folder. To compare individual IED, select one IED on each side. See Figure 205.

![Image](ITT600 - Explore Models)

**Figure 205:** One IED on each side is selected to be compared

### 3.5.8 Comparing ITT600 – Explore IEDs Data with an SCL File

To compare the data contained in ITT600 – Explore IEDs with another SCD file, the data has to be loaded before starting ITT600 – Explore Models.

The left model of ITT600 – Explore Models will always contain the data from ITT600– Explore IEDs.

To compare online data from an IED with an SCD file, connect to the IED first (the configuration will be uploaded) and then start ITT600 – Explore Models. The left model is automatically set to the model from ITT600 – Explore IEDs.

### 3.5.9 Comparison Filters

Comparison filters (see Figure 206) are useful if two different configurations are compared, but there have to be differences. For example, two typical (identical from the IEC 61850 configuration point of view) IEDs are compared. They are the same but they must have different addresses. Thus, the access point addresses have to be excluded from the comparison.
The available filters are listed as follows:

- **Functional constraint filters**
  - Ignore differences in Status (FC = ST) values. Status values (positions, binary inputs etc.) are not considered as differences. This is often desired if comparing online and SCL models.
  - Ignore differences in analog (MX) values. The same as status values, but for measurements.
  - Ignore differences for different trigger options. Different trigger options (DataChange, QualityChange, etc.) will be ignored.
  - Ignore differences in extended definitions (FC = EX).
  - Ignore differences in configuration (FC = CF) values.
  - Ignore differences in description (FC = DC) values.
  - Ignore differences in sample value (FC = SV) values.

- **Other filters**
• Ignore differences in access point addresses. Access point addresses (IP, MAC … addresses) are not checked.
• Ignore type differences when comparing enums to INTs. Online data type representation can differ from SCL. Since it is not possible to receive everything contained in the SCL from an IED, data type differences will occur.
• Ignore short address differences. Different short addresses will not be taken into account.
• Control Block Filters: provides comparison filters for various control block attributes

To compare online data from an IED with an SCD file, “Ignore type differences when comparing enums to INTs” should be used.

3.5.10 Comparison Results

The results of the comparison are shown in a simple way:

- **Bold** font means: There is a difference on a node below.
- **Red** font means: There is a difference on this node.
- **Orange** font means: There is a difference in the data types.

*Figure 207* shows an example that the IP address of the compared IEDs are different.

![Figure 207](image)

*Figure 207: An example of comparing two SCD files using ITT600 – Explore Model*

Clicking on the red node will show more information about the difference (shown in *Figure 207*). This detailed information cannot be displayed all the time, sometimes it will remain empty.

If something is missing in one model it will be shown in the result with a different icon:

- ![Only available in the right model](image)
- ![Only available in the left model](image)
- ![Available in both models, but there is a difference](image)

Furthermore, different values will be shown in red color and different types are shown in orange.
Since ITT600 - Explore Models does not know which model is correct, it is up to the user to do further investigation. ITT600 – Explore Models clearly indicates that the two files are not identical.

3.5.11 **Export differences to .xsl File.**

The comparison result can be exported via the export button into selected location.

To export the differences to .xsl file both models must be loaded and comparison has to be completed.

The report consists of two pages, first contains the export information: Date when export was made, models used and the author of the report.

![Figure 208: An example of .xsl export information page](image)

Second page is the comparison results, which displays node name, path, type and the difference information.

![Figure 209: An example of .xsl export information page](image)

3.6 **Software Update**

It is possible to check for a new version of the ITT600 SA Explorer via the Check for Updates menu in the Help main menu (see Section "Help menu"). Simply click on the menu and a window will appear on whether an update is available or the software is up-to-date. See Figure 210.
Figure 210: Check for Updates windows – no update is available
Section 4  Limitations

For limitations see the release notes.
### 5.1 Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible reasons and solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No packets received</td>
<td>Check whether you have enabled a firewall on the PC and disable it. Check whether you have a running VPN client on the PC and disable it. Check the NIC settings. Some protocols, like i.e GOOSE requires the Promiscuous mode to be enabled on selected capture NIC. See section &quot;Configuration&quot;</td>
</tr>
<tr>
<td>Packets are only received in one direction</td>
<td>Check whether you have a running VPN client on the PC and disable it. See section &quot;Configuration&quot; Check the properties of the network connection and the adapter.</td>
</tr>
<tr>
<td>No connection to IED possible</td>
<td>Try to ping the IED first. If it responds to the ping but it but it cannot be connected by Explore IEDs, check the OSI addresses. Windows (or third party) firewall may block the connection.</td>
</tr>
<tr>
<td>IED does not respond to ping.</td>
<td>To be able to ping an IED the PC has to be in the same network. This means both devices need the same subnet mask and a similar (not the same!) IP address.</td>
</tr>
<tr>
<td>Capturing packets from an IED is not possible.</td>
<td>If you want to capture frames from an IED that are sent to a SCADA, you have to run the analyzer on the SCADA PC or connect the PC with the analyzer with a hub between the SCADA PC and the IED or enable port mirroring on the switch.</td>
</tr>
<tr>
<td>ITT600 – Explore Models shows lots of INT / enum errors</td>
<td>Enable the &quot;Ignore Type difference&quot; flag in the &quot;Explore SCL&quot; if you compare online data with an SCD file.</td>
</tr>
<tr>
<td>Only GOOSE frames are captured with ITT – Explore Ethernet</td>
<td>Port mirroring functionality in the switch is not enabled. Thus only broadcast / multicast frames are received.</td>
</tr>
<tr>
<td>No VLAN tags are contained in frames</td>
<td>Some switches do not support VLANs. The NIC configuration cuts off the VLAN tags from the frames. See section &quot;Configuration&quot;</td>
</tr>
<tr>
<td>Changing of switch positions in the IED will not update the data in ITT600 – Explore IEDs.</td>
<td>Enable the RCB to get an automatic update of the data in the tree view, or update the data manually. See section &quot;Manually update values from an IED&quot; and &quot;Spontaneous update of values&quot;</td>
</tr>
<tr>
<td>No entries are logged in the process event list.</td>
<td>Reporting is not set up. See section &quot;Spontaneous update of values&quot;</td>
</tr>
<tr>
<td>Reports cannot be enabled</td>
<td>Are there free RCBs? Check how many clients are already connected to the IED, and, if necessary, disconnect one of them.</td>
</tr>
</tbody>
</table>

### 5.2 ITT600 – Explore IEDs Default Address Parameters
5.2.1 Local Address

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSI TSEL</td>
<td>00,01</td>
</tr>
<tr>
<td>OSI SSEL</td>
<td>00,01</td>
</tr>
<tr>
<td>OSI PSEL</td>
<td>00,00,00,01</td>
</tr>
<tr>
<td>OSI AP Title</td>
<td>1,3,9999,33</td>
</tr>
<tr>
<td>OSI AE Qualifier</td>
<td>33</td>
</tr>
</tbody>
</table>

5.2.2 Remote Address

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSI TSEL</td>
<td>00,01</td>
</tr>
<tr>
<td>OSI SSEL</td>
<td>00,01</td>
</tr>
<tr>
<td>OSI PSEL</td>
<td>00,00,00,01</td>
</tr>
<tr>
<td>OSI AP Title</td>
<td>1,3,9999,33</td>
</tr>
<tr>
<td>OSI AE Qualifier</td>
<td>23</td>
</tr>
</tbody>
</table>

5.3 ITT600 – Explore Ethernet Supported Protocols

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMS</td>
<td>Manufacturing Message Specification Communication protocol for IEC 61850</td>
</tr>
<tr>
<td>(R)STP</td>
<td>(Rapid) Spanning Tree Protocol. Protocol used by switches to determine alternate (redundant) routes</td>
</tr>
<tr>
<td>(R-)GOOSE</td>
<td>(Routable) Generic Object Oriented Substation Event. The IEC 61850 “real time” protocol for bay to bay communication</td>
</tr>
<tr>
<td>NTP</td>
<td>Network time protocol. Used for time synchronization of IEDs and clients.</td>
</tr>
<tr>
<td>IEEEE1588 (PTP) - V1 and V2</td>
<td>Precise time protocol. Used for time synchronization of SV Servers.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol Diagnostic information about network nodes.</td>
</tr>
<tr>
<td>(R-)SV</td>
<td>(Routable) Sampled Values Sampled Values according IEC 61850, IEC 61869</td>
</tr>
<tr>
<td>IEC60870-5-104</td>
<td>IEC SA Protocol for SCADA / NCC connections</td>
</tr>
<tr>
<td>PRP</td>
<td>Parallel Redundancy Protocol Partially supported, not all sub-types of supervision packets are decoded</td>
</tr>
<tr>
<td>DNP3.0 / TCP</td>
<td>Distributed Network Protocol over TCP Protocol between RTUs and SCADA Systems</td>
</tr>
<tr>
<td>Modbus / TCP</td>
<td>Modbus Protocol over TCP Protocol between RTUs / PLCs and SCADA Systems</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ICMP          | Internet Control Message Protocol  
Partially supported, not all sub-types of packets are decoded |
| IEEE 1344     | IEEE Synchrophasers for Power Systems transmission protocol (superseded by IEEE C37) |
| LLCP          | Logical Link Control Protocol |
| HSR           | High-availability Seamless Redundancy |
| VLAN          | Virtual Lan |
| SPA           | SPA-Bus ASCII-based protocol for serial communication |

### 5.4 IEC 61850 Edition 2 features

#### 5.4.1 Local Remote Handling Feature

The local / remote handling in IEC 61850 was focused on conventional bay level local/remote functionality. IEC 61850 Edition 2 introduces some more data objects which allow a better modelling of station/network level’s local remote functionality and separation of the key used to set local mode from the functions in local mode. Due to these additional data objects, the following two optional data objects have been introduced in all logical nodes that can send commands:

- **LocKey**: SPS, represents the (state of the) local / remote key which can be sent – for instance via GOOSE – to all logical nodes to switch between local and remote state. The Loc attribute is mandatory on all controllable functions. The LocKey is an optional feature on LLN0. In addition, Loc is optional at LLN0 as well.
  
The status change on LocKey always influences the Loc on the same LN (if there is one). In case the LocKey is located on LLN0, the status change will influences the Loc on LLN0 and the Loc on all LNs related to the same RootLD and not having its own LocKey.

- **LocSta**: SPC, represents the station local state and thus switches between station and network center command mode. It is possible to launch command from station level, and thus this state can be switched via the communication from some station level client. The command to change the LocSta always influences the LocSta status on the same LN. If it is located in LLN0, its status will be used by other LNs related to same RootLD.

To decide if a command is allowed to be executed from control authority perspective, the status of relevant Loc and LocSta has to be taken into account.

Additional information can be found in IEC 61850 - 7.4 Edition 2 Annex B.

#### 5.4.2 Mode Behavior Handling

Unlike in IEC 61850, Mod and Behavior is now precisely described.

In IEC 61850, it is up to the vendor to decide on how an IED behaves in case the IED is set in Test Mode or when the IED receives Data with quality Bit Test set. The only condition is that the behavior is described in the related documentation (PIXIT).

In IEC 61850 Edition 2, Mod and Behavior is clearly described how the IED has to behave in case a LN or LD is set into a certain Mod. This is one of the most significant improvement that is introduced in IEC 61850 Edition 2. As opposed to IEC 61850, IEC 61850 Edition 2 defines clearly that switching between the modes should only happen as a result of an operator command to the data object Mod.
This feature was introduced to improve the testing capabilities in IEC 61850 systems. Several use cases for testing engineers, commissioning engineers and maintenance people could be seen. Details could be found in IEC 61850 - 7.4 Edition 2 Annex A.

5.5 IEC 61850 Edition 2.1 features

5.5.1 GOOSE replay protection algorithm

Replay protection analysis is implemented for GOOSE/R-GOOSE with limited security checks in both Explore GOOSE and Explore Ethernet.

Current version of ITT600 explorer is able to parse the PDU security extension but is limited to perform full security checks and verifications by the lack of KDC - Key Distribution Center.

GOOSE replay protection is configured by following settings:

![Replay analysis options]

- **Time deviation [ms]**: checks if difference between timestamp in received goose packet and local time is in range of this value. Value 0 indicates that checking is disabled - any PDU timestamp is correct.

  **If time deviation is enabled, it is important that PC time clock where ITT is running is synchronised with IED time clock, otherwise the time deviations should be increased or disabled so the analysis will not treat most of the packets as replayed.**

Figure below shows the workflow of replay protection according to IEC 62351.
Figure 212: Goose replay state machine

For detailed description of the state machine please refer to the IEC 62351-6:2020.

The packets are analysed per GoCBRef and simulation bit pair - packets with the same GoCBRef but different simulation bit are processed separately.

Below is the simplified description of the replay protection analysis:

1. Wait for next packet
2. Check the capture time:
   If this is first analyzed packet or the TAL expired: values are reset to initial state (values of last stNum, last sqNum, expected timestamp of next packet)
3. Security Check:
   3.1. If any of the following is fulfilled:
      a. Model is not loaded in ITT
      b. Packet is not matched to any GCB in loaded model
      c. Matched GCB has no security enabled (not expected by configuration)
      d. Matched GCB has security enabled (expected by configuration) and packet contains security extension
      e. Presence of security extension in packet does not differ from previous packet
      
      Security check passes and proceed to step 4
   3.2. If security extension is expected by configuration and packet does not contain it: Security check fails and proceed to step 1
   3.3. If presence of security extension differ from previous packet: Security check fails and proceed to step 1
4. If stNum increased check the packet frame time (timestamp in GOOSE Pdu):
4.1. If time deviation check is disabled or packet frame time is in range [Capture time - time deviation; Capture time + time deviation]: time check passes, proceed to step 5

4.2. Time check fails: packet is replayed, proceed to step 1

5. If stNum equals 0: not replayed, update last values and proceed to step 1

6. If stNum is lower than last stNum or stNum is the same but sqNum does not increased: packet is replayed, proceed to step 1

7. Not replayed, update last values and proceed to step 1

Reset to initial state means that analyser does not expect any value of stNum, sqNum or next packet within TAL time
Hitachi Energy Sweden AB  
Grid Automation Products  
SE-721 59 Västerås  
Phone +46 (0) 10 738 00 00  
E-Mail: contact-us@hitachienergy.com  

https://hitachienergy.com/substation-automation

1/1  

© Hitachi Energy 2021. All rights reserved.