Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, 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

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

Guarantee

Please inquire about the terms of guarantee from your nearest ABB representative.

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.

Any work such as insertion or removal of soldered jumpers or setting resistors, which may be necessary, may only be performed by appropriately qualified personnel.

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.
Disclaimer

This 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 ABB 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 ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.
# Table of contents

## 1 Introduction

1.1 Scope of the document ........................................... 1

1.2 Abbreviations and definitions .................................. 1

1.2.1 Abbreviations .................................................. 1

1.2.2 Definitions .................................................... 3

1.3 References ......................................................... 3

1.4 Overview ............................................................ 4

## 2 Configuration

2.1 Network Interface Card Settings ............................... 6

2.1.1 IP Address ..................................................... 6

2.1.2 Virtual LAN (VLAN) ......................................... 7

2.2 Software Firewalls ............................................... 8

2.3 VPN Clients ....................................................... 8

2.4 Changing OSI Address Parameters ........................... 9

2.5 Debug and Trace Output Configuration ........................ 9

2.6 Ethernet Switch Configuration ................................ 11

## 3 Functionality

3.1 ITT600 – Explore IEDs ........................................ 12

3.1.1 Overview ...................................................... 12

3.1.2 File Menu ..................................................... 13

3.1.3 Edit Menu ..................................................... 14

3.1.4 Tools Menu .................................................... 15

3.1.4.1 ITT600 SA Explorer Options ......................... 15

3.1.5 Help Menu ...................................................... 18

3.1.6 Tree Navigation Panel ....................................... 19

3.1.6.1 Tree View “By Subnetworks” .......................... 19

3.1.6.2 Tree View “By Substation” ............................ 20

3.1.7 Get Started Panel ............................................ 22

3.1.8 Main Panel ..................................................... 23

3.1.8.1 Object Properties ........................................ 23

3.1.8.2 Object Details ............................................ 24

3.1.9 Coloring Rules ................................................ 24

3.1.10 Debug and Logging Information .......................... 26

3.1.11 Working with IED Configurations ........................ 27

3.1.11.1 Working Offline ......................................... 28

3.1.11.1.1 Open an SCL File ................................... 28

3.1.11.1.2 Explore an SCL File ................................ 28

3.1.11.1.3 The Dataflow View .................................. 29

3.1.11.1.4 Representation ....................................... 30

3.1.11.1.5 Filtering ............................................... 30

3.1.11.1.6 Zooming ............................................... 31

3.1.11.1.7 Moving Elements .................................... 31

3.1.11.1.8 Navigation ............................................ 31

3.1.11.1.9 Fault Simulation ..................................... 33

3.1.11.1.10 Combination with Quick Checker .................. 33
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3</td>
<td>ITT600 – Explore GOOSE</td>
<td>125</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Overview</td>
<td>125</td>
</tr>
<tr>
<td>3.3.2</td>
<td>File Menu</td>
<td>125</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Tools Menu</td>
<td>126</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Help Menu</td>
<td>127</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Operation</td>
<td>127</td>
</tr>
<tr>
<td>3.3.5.1</td>
<td>Offline Mode</td>
<td>127</td>
</tr>
<tr>
<td>3.3.5.2</td>
<td>Online Mode</td>
<td>128</td>
</tr>
<tr>
<td>3.3.5.3</td>
<td>Adding Data to the Oscilloscope</td>
<td>129</td>
</tr>
<tr>
<td>3.3.5.3.1</td>
<td>Capture Time</td>
<td>129</td>
</tr>
<tr>
<td>3.3.5.3.2</td>
<td>Frame Time</td>
<td>129</td>
</tr>
<tr>
<td>3.3.5.4</td>
<td>Display with Loaded Configuration</td>
<td>130</td>
</tr>
<tr>
<td>3.3.5.5</td>
<td>Display without Loaded Configuration</td>
<td>131</td>
</tr>
<tr>
<td>3.3.6</td>
<td>Plot Legend</td>
<td>131</td>
</tr>
<tr>
<td>3.3.7</td>
<td>Status Colors</td>
<td>132</td>
</tr>
<tr>
<td>3.3.8</td>
<td>Quality Information</td>
<td>133</td>
</tr>
<tr>
<td>3.3.9</td>
<td>Source Information</td>
<td>134</td>
</tr>
<tr>
<td>3.3.10</td>
<td>Plot Information and Functions</td>
<td>134</td>
</tr>
<tr>
<td>3.3.11</td>
<td>Go to the Next Value Change</td>
<td>135</td>
</tr>
<tr>
<td>3.3.11.1</td>
<td>The ITT 600 – Explore GOOSE Toolbar</td>
<td>135</td>
</tr>
<tr>
<td>3.3.11.1.1</td>
<td>Zooming</td>
<td>135</td>
</tr>
<tr>
<td>3.3.11.1.2</td>
<td>Data Cursor and Synchronizing</td>
<td>136</td>
</tr>
<tr>
<td>3.3.12</td>
<td>Saving and Opening Configurations</td>
<td>137</td>
</tr>
<tr>
<td>3.4</td>
<td>ITT600 – Explore SV</td>
<td>138</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Overview</td>
<td>138</td>
</tr>
<tr>
<td>3.4.2</td>
<td>File Menu</td>
<td>139</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Tools Menu</td>
<td>139</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Help Menu</td>
<td>140</td>
</tr>
<tr>
<td>3.4.5</td>
<td>Operation</td>
<td>141</td>
</tr>
<tr>
<td>3.4.5.1</td>
<td>Online Mode</td>
<td>141</td>
</tr>
<tr>
<td>3.4.5.1.1</td>
<td>Phasor Display</td>
<td>143</td>
</tr>
<tr>
<td>3.4.5.1.2</td>
<td>Show and Ref Function</td>
<td>144</td>
</tr>
<tr>
<td>3.4.5.1.3</td>
<td>Logging the SV Packets</td>
<td>145</td>
</tr>
<tr>
<td>3.4.5.1.4</td>
<td>Stream Quality Information</td>
<td>147</td>
</tr>
<tr>
<td>3.4.5.2</td>
<td>Offline Mode</td>
<td>147</td>
</tr>
<tr>
<td>3.4.5.2.1</td>
<td>Trends</td>
<td>148</td>
</tr>
<tr>
<td>3.4.5.2.2</td>
<td>Statistics Analysis</td>
<td>149</td>
</tr>
<tr>
<td>3.5</td>
<td>ITT600 – Explore Models</td>
<td>150</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Overview</td>
<td>150</td>
</tr>
<tr>
<td>3.5.2</td>
<td>File Menu</td>
<td>150</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Help Menu</td>
<td>151</td>
</tr>
<tr>
<td>3.5.4</td>
<td>Toolbar</td>
<td>151</td>
</tr>
<tr>
<td>3.5.5</td>
<td>Model panels</td>
<td>151</td>
</tr>
<tr>
<td>3.5.6</td>
<td>Comparison panels</td>
<td>152</td>
</tr>
<tr>
<td>3.5.7</td>
<td>Comparing SCL Files</td>
<td>152</td>
</tr>
<tr>
<td>3.5.8</td>
<td>Comparing ITT600 – Explore IEDs Data with an SCL File</td>
<td>153</td>
</tr>
<tr>
<td>3.5.9</td>
<td>Comparison Filters</td>
<td>153</td>
</tr>
<tr>
<td>3.5.10</td>
<td>Comparison Results</td>
<td>155</td>
</tr>
<tr>
<td>3.5.11</td>
<td>Export differences to .xsl File</td>
<td>156</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.6</td>
<td>Software Update</td>
<td>157</td>
</tr>
<tr>
<td>4</td>
<td>Limitations</td>
<td>158</td>
</tr>
<tr>
<td>5</td>
<td>Appendix</td>
<td>159</td>
</tr>
<tr>
<td>5.1</td>
<td>Troubleshooting</td>
<td>159</td>
</tr>
<tr>
<td>5.2</td>
<td>ITT600 – Explore IEDs Default Address Parameters</td>
<td>160</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Local Address</td>
<td>160</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Remote Address</td>
<td>160</td>
</tr>
<tr>
<td>5.3</td>
<td>ITT600 – Explore Ethernet Supported Protocols</td>
<td>161</td>
</tr>
<tr>
<td>5.4</td>
<td>IEC 61850 Edition 2 features</td>
<td>161</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Local Remote Handling Feature</td>
<td>161</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Mode Behavior Handling</td>
<td>162</td>
</tr>
</tbody>
</table>
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 1.3 - References.

1.2 Abbreviations and definitions

1.2.1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</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>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</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>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>SA</td>
<td>Substation Automation</td>
</tr>
<tr>
<td>SCD</td>
<td>Substation Configuration Description</td>
</tr>
<tr>
<td>SCL</td>
<td>Substation Configuration Language</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNTP</td>
<td>Simple Network Time Protocol</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>SV</td>
<td>Sampled Values</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>URCB</td>
<td>Un-buffered Report Control Block</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VMD</td>
<td>Virtual Manufacturing Device</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
1.2.2 Definitions

**NOTE:** 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:** 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

- IEC 61850-1 (Introduction and Overview)
- IEC 61850-7-3 (Common Data Classes)
- IEC 61850-7-4 (Compatible Logical Node Classes)
- IEC 61850-8-1 (Mappings to MMS)
- IEC 61850-9-2 (Sampled Values over ISO/IEC 8802-3)
- IEC 61850-90-4 (Network Engineering Guidelines)

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 1.1. ABB’s SA Tools landscape
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 1.2 illustrates the wide variety of usages of ITT600 SA Explorer.
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 2.1.

172.17.1.200
255.255.255.0

172.17.1.1
255.255.255.0

NOTE: 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.

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

**WARNING:** 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 2.2.

**WARNING:** 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.
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 please refer to Section 5.2 - ITT600 – Explore IEDs Default Address Parameters.

2.5 Debug and Trace Output Configuration

ITT600 SA Explorer logs error messages and additional information during operation. Refer to Section 3.1.10 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.

**WARNING:** Changing the logger configuration could slow down the whole application and is therefore not recommend for inexperienced users.
Figure 2.3. 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 2.4 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 2.4. Basic SA system setup](image)

To be able to capture traffic from SCADA to IED1, the port IED1 is connected to (port #2) has to be mirrored to the port ITT600 SA Explorer PC is connected (port #8).
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). Furthermore, it allows the user to simulate one IEC 61850 IED.

The main user interface of the ITT600 – Explore IEDs application, as shown in Figure 3.1, is divided into four main areas:

- Menus (yellow)
- Tree Navigation (blue)
- Get Started Panel and Main Panel (red)
- Debug and Logging Information (green)
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 3.1.11 - Working with IED Configurations.

### 3.1.2 File Menu

The file menu provides access to the following operations (see Figure 3.2):

- 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)
- Exporting browsed IEDs to an SCD file (only available when no SCD file was loaded).
- Exiting the program (the “Exit” menu item)
3.1.3 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 3.3):

- Adding an IED to the root of the navigation tree (the “Add IED...” menu item) with a user-provided name
- Removing a selected IED from the root of the navigation tree (the “Remove IED” menu item)
- Auto-detecting IEDs on the network and adding them to the root of the navigation tree
- Adding a SERVER to a selected IED (the “Add SERVER...” menu item) with its access point(s)
- Modifying a selected SERVER (the “Edit SERVER...” menu item), i.e., modify its access point(s)
- Removing a selected SERVER from an IED (the “Remove SERVER” menu item)
- Connecting all IEDs
- Disconnecting all IEDs
- Clearing the entire configuration (the “Clear Tree” menu item)
3.1.4 Tools Menu

The tools menu provides access to the following functions (see Figure 3.4):

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

![Figure 3.4. ITT600 – Explore IEDs Tools menu](image)

3.1.4.1. 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 6 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

![Figure 3.5. ITT600 – Explore IEDs Options Dialog – General Settings](image)
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 above on Figure 3.5):

- **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 set where ITT600 SA Explorer stores files.
- **Display Local Time:** user can choose whether to show local time (adjusted to local computer time) or recorded (UTC) time.
- **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).
- **Show Debug Log:** activating this parameter shows Debug and Logging Information in the overall ITT600 SA Explorer window.
- **Log Panel Height:** this particular control is used to set the height of the Debug and Logging Information panel.
- **Log File Path:** user can define a path where all the log files are to be stored.
- **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:** delete available log files.

![Figure 3.6. ITT600 – Explore IEDs Options Dialog – Explore IEDs Settings](image)
Explore IEDs settings:
The following parameters are tunable (see above on Figure 3.6)

- **Number of Event List Entries**: user can define the number of event list entries
- **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
- **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.

**NOTE**: 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 orIdent**: per default the orIdent is “ITT”, but it can be set to customer use.
3.1.5 Help Menu

The help menu provides access to the following operations (see Figure 3.7):

- Viewing the help file associated with the ITT600 - Explore IEDs
- A legend of the used status colors (see also Figure 3.15)
- Check whether software updates are available
- Viewing the about screen

![Figure 3.7. ITT600 – Explore IEDs Help menu](image)

NOTE: For a detailed version overview click on the “Assembly Versions” button in the About window.
3.1.6  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 Subnetwork they are connected to. See Section 3.1.6.1 - 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 3.1.6.2 - 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 1.3 - 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 3.8.

![Figure 3.8. Tool tips in the tree views](image)

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.

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

3.1.6.1  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. Refer to Figure 3.9.
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.

**Figure 3.9. Tree view by subnetworks**

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>IEDs without a reference to the SCD communication section will be added to IEDs folder called “IEDs without reference to Communication section”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE:</td>
<td>As default only IEC 61850 related networks (network name contains 8-MMS) are shown.</td>
</tr>
</tbody>
</table>

### 3.1.6.2. 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 3.10.
Figure 3.10. Tree view by substation (without and with customer names)

**NOTE:** 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 checkbox at the bottom of the substation tree view.
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

3.1.7 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 3.11.

![Figure 3.11. Get Started panel](image-url)
3.1.8 **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 3.12.

3.1.8.1. **Object Properties**

The header of the object properties area as shown in Figure 3.12 and Figure 3.13 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.

![Figure 3.12. The different areas of the ITT600 - Explore IEDs main viewer panel](image)

![Figure 3.13. The header section of the object properties area](image)
3.1.8.2. Object Details

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 3.14).

![Object Attributes Table]

Figure 3.14. Various object detail panels

3.1.9 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 3.15 and Table 3.1.
**Chapter 3 Functionality**

**Figure 3.15. Legend of used colors in ITT600 – Explore Ethernet**

**Table 3.1: Detail legend of the used colors in ITT600 – Explore Ethernet**

<table>
<thead>
<tr>
<th>Color Description</th>
<th>Legend</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 ITT600 – Explore IEDs) will be colored differently to an inactive one.</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>SimulationNotPossible</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>
</tbody>
</table>
### 3.1.10 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 3.16 and Figure 3.17). The log window can be cleared by right clicking in the logger area and selecting “Clear” from the context menu.

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 2.5 - 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.

![NOTE: The log files can also be deleted manually by selecting the “Delete old log files” from the options menu.](image)
3.1.11 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 3.1.11.1 - Working Offline.
- Dynamically discover a connected IEDs configuration Section 3.1.11.2 - Working Online.
3.1.11.1. 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
```

### 3.1.11.1.1. 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 3.18.

![Figure 3.18. ITT600 – Explore IEDs loading a SCD file](image)

After selecting the SCD file, a progress bar will be shown and the file will be loaded.

**NOTE:** Loading a SCD file can be time consuming. A progress bar is shown during the loading phase.

### 3.1.11.1.2. Explore an SCL File

Once the SCL file is opened, you can expand the entire tree navigation panel by right-clicking on an IED and selecting the “Expand children” item. You can navigate to the various objects of interest by simply selecting the object in the tree navigation pane. See Figure 3.19.

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.
All nodes in the Tree represent IEC 61850 related data. The display will not differ between online and offline values. Refer to Section 3.1.11.2 - Working Online for detailed description of different display options and values.

3.11.1.3. 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, when a communication subnetwork is selected in the Subnetworks tree view. See Figure 3.20.
3.11.1.4. **Representation**

All IEDs from the selected Subnetwork are shown as green boxes, including information about the IED (see Figure 3.21):

- The IED Name (Bold)
- The IED Type
- The IP Address of the IED
- The Description of the IED

![Figure 3.21. IED information](image)

**NOTE:** 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

3.11.1.5. **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 3.22.

![Figure 3.22. Filters](image)
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”.

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

### 3.11.1.6. Zooming

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

### 3.11.1.7. Moving Elements

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

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

### 3.11.1.8. 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 3.23.
Figure 3.23. Navigating to a DS

**NOTE:** The DS is only selected in the Subnetworks tree, but the view does not automatically change to the object details.
3.11.1.9. **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 3.24.

![Figure 3.24. Simulate a failed IED](image)

**NOTE:** Right click on an IED to simulate it as failed.

The failed IED is shown in red, all affected IEDs are shown orange. See Figure 3.25.

![Figure 3.25. Failed and affected IEDs](image)

3.11.1.10. **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 3.1.15).

**NOTE:** Quick checker results are shown in the Dataflow diagram.
3.1.11.2. Working Online

3.1.11.2.1. Connect to IEDs and SERVERs

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

- Select “Connect All IEDs” from the subnetwork context menu either with or without enabling reports (see Figure 3.26).
- To connect one IED and its Servers, select “Connect this IED” from IED context menu
- To connect a Server, select “Connect this SERVER” from a SERVER context menu (see Figure 3.27).

![Figure 3.26. Connect to all IEDs and Enable Reports](image)
Chapter 3 Functionality

Figure 3.27. 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 3.1.11.10 - Dynamically Add IEDs to the Configuration.

NOTE: To specify different address parameters or Authentication Password, select Edit Server prior the connection attempt.

While the ITT600 - Explore IEDs connects to the specified IED a progress bar will be displayed – see Figure 3.28.

Figure 3.28. 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.

NOTE: No Reports are enabled. To obtain spontaneous data change from an IED, reports need to be enabled (see Section 3.1.11.2.17 - Manually Update Values from an IED).
3.11.2.2. **Connect SERVER as a specific client**

Connecting the SERVER as specific client will automatically enable all reports associated with that client (see Section 3.11.2.19 - Spontaneous Update of Values for more information about reports).

![Connect SERVER as a specific client](image)

**Figure 3.29. Connect as a specific client**
3.11.2.3. 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 3.30.

![Figure 3.30. Exploring an IED](image)

3.11.2.4. Simulate this Server

In general, ITT600 SA Explorer provides the functionality to simulate one IED. For details, refer to Section 3.1.16.

3.11.2.5. 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.

3.11.2.6. Disable All Substituted Values

Reset all Substituted Values will automatically set all “SubEna” Data Attributes to false, therefore disabling all substitution for the whole SERVER. See Figure 3.31.
3.11.2.7. Disable All Blocking Values

Reset all blockings Values will automatically set all "BLkCmd" Data Attributes to false, therefore disabling all blockings for the whole SERVER. See Figure 3.32.

3.11.2.8. Change Attributes of the IED

Depending on the functional constraint of the data attribute you click on, various modifications are possible. For instance, the d data attribute represents documentation and can be modified. If you double click the d data attribute, you can enter a new value for the d attribute.

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 3.33.
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).

**NOTE:** Data with functional constraint CO (Control) cannot be written/edited as shown in Figure 3.23. To write CO values, a Control Dialog will be shown. Refer to Figure 3.34. See Section 0 - Commands.

**WARNING:** 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.

**NOTE:** 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.
3.11.2.9. 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 3.35.

NOTE: Editing of Setting group values is not supported by all IEDs.

3.11.2.10. Changing Active Setting Group

To change the active Setting group, the corresponding value ("ActSG") of the SGCB has to be changed. See Figure 3.36.
3.11.2.11. 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 3.38.

![Figure 3.37. Selecting the active Setting group to be changed](image1)

Now individual values can be changed. See Figure 3.39.

![Figure 3.38. Changing Setting group values](image2)

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.

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

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

3.11.2.13. Select Before Operate Command

To operate a switch controlled by a real IED, a “Select-Before-Operate” (SBO) sequence according to Section 1.3 - References has to be sent to the device. This function is available from the Switch Control Dialog. See Figure 3.39.

![Switch Control (Select Before Operate) dialog](image)

Figure 3.39. Switch Control (Select Before Operate) dialog

3.11.2.14. Basic View

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.

3.11.2.15. Advanced View

The advanced view lets the experienced user change additional parameters. See Figure 3.40.
ITE 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.

**WARNING:** 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).

**WARNING:** 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.

### 3.11.2.16. Direct Commands

The Direct Command dialog looks slightly different to the SBO Command Dialog. See Figure 3.41.
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.

**WARNING:** Issuing Commands without cautious in a real station is dangerous!

Use this feature with extra caution!

### 3.1.11.2.17. 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 context menu. See Figure 3.42.

![Figure 3.42. Refreshing a value](image-url)
3.1.11.2.18. **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 3.43. This command will re-read all values from the server, thus this command might take some time.

![Figure 3.43. Refreshing the whole SERVER](image)

3.1.11.2.19. **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 1.3 - 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

**NOTE:** 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 3.1.11.6 - Process Event List for details).

### 3.1.11.20. Working with Unbuffered Reports

Unbuffered reports have to be reserved for most of the operations. See Figure 3.44.

**NOTE:** The URCB has to be reserved for the following operations as shown in Figure 3.45.

To reserve the URCB, simply click on the “Reserve URCB” command button

**NOTE:** 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.

**NOTE:** The data_set_name should always be included in order to decode the report.
Next, enable the URCB by clicking the “Enable RCB” button. The color of an enabled report will change. See Section 3.1.9 - Coloring Rules for a detailed list of all available status colors. See Figure 3.46.
Finally, to update all values, click the “Start General Interrogation” button. To disable the report, click “Disable URCB” and “Release URCB.”

**NOTE:** Received reports are displayed in the process event list (see Section 3.1.11.6 - 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.

### 3.11.2.21. Working with Buffered Reports

Buffered reports from the ITT600 – Explore IEDs are very similar to unbuffered ones. To find out more about the differences please refer to Section 1.3 - References. See also Figure 3.47.

**NOTE:** Buffered reports do not need to be reserved.
Figure 3.47. A BRCB
3.1.11.2.22. **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 3.48.

![Figure 3.48. Enable all possible reports of a Server](image)

**NOTE:** 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.

3.1.11.2.23. **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 3.49.
3.11.3. 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 3.50.

![Menu Entry](image)

**Figure 3.50. Create dynamic data sets**

**NOTE:** This functionality is only executable in online mode!

You must be connected to an IED which supports this function.

**NOTE:** This functionality only supports non persistent data sets!

Activating the menu item ‘Create dynamic data sets..’ opens the following window. See Figure 3.51.
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 3.52.
- **Status of CDC Objects**: CDC items which have been assigned to a DS are shown in green. See Figure 3.53.
- **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.

**NOTE:** Preconfigured, empty URCBs must exist on the IED to add DS and DS entries. See Figure 3.54, Figure 3.55.

Only one DS can be assigned to an URCB!
Figure 3.52. CDC tree view with multiple selection

Figure 3.53. CDC tree view: CDCs assigned to DS

Figure 3.54. RCB tree view with new created DS entries
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

**NOTE:** Dynamic data sets are automatically named ‘ITT-DynDSxx’ to avoid duplicate names.
3.11.3.1. **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.

3.11.3.2. **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.
3.11.3.3. Writing Data Sets to the IED

There are two buttons which allow to write internal configuration to the IED. These buttons can be found above RCB tree view. See Figure 3.56.

![Figure 3.56. RCB tree view context menu](image)

Status of successfully enabled RCBs and written DSs is shown in black. See Figure 3.57.

![Figure 3.57. RCB tree view with a DS written to IED](image)

**NOTE:** After this operation, the updated URCBs must be enabled in the Subnetwork/Substation tree view!
3.11.3.4. 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 3.58.

![Figure 3.58. Deleting Data Sets from the IED](image)

3.11.3.5. Export Data Sets to SCD

New created data sets can be saved to an SCD file (see Section 3.11.3 - Exporting IEDs to an SC3 File).

3.11.3.6. Disconnecting from Server

When disconnecting, all created data sets will automatically be deleted.
3.11.4. **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 3.59.

![Figure 3.59. Read VMD specific variables of a Server](image)

**NOTE:** 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 3.61.
3.11.5. 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.
NOTE: If an IED does not support MMS file transfer, it might support FTP protocol. See Section 3.1.11.9 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 3.62.
All possible file operations are available over a context menu, or the control buttons. See Figure 3.63.

![MMS File Transfer Commands](image)

**Figure 3.63. The MMS file transfer commands**

**NOTE:** 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.

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

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

### 3.1.11.6. Process Event List

Changes in process values (also called events) are received by IEC 61850 reports. These changes are logged in the process event list as shown in Figure 3.64. 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.

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

![Figure 3.64. The Process event list](image)

Help on how to set up reporting is described in Section 3.1.11.2.19 - 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 3.65.

**NOTE:** The list can be exported to an Excel file by pressing the button 🖼️ “Export to Excel”.

**NOTE:** The list can be cleared by pressing the ❌ “Clear List Button”.

**NOTE:** The substation related information is only filled if the IED is connected to a substation/voltage level.

**NOTE:** The most recent event can be selected by pressing the button ⌚️ “Show most recent event”.

**NOTE:** The substation related columns can be shown/hided by pressing the button 🔌 “Show/hide functional names”.

**NOTE:** The auto sizing of the columns can be enabled/disabled by pressing the button 🔴 “Toggle auto / manual column sizing”.

**NOTE:** By pressing the right mouse button in the event list tab, you can navigate to the selected item in the active tree view.

**WARNING:** 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 3.2: 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 3.65. The Process event list details
3.11.7. 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 3.66.

**NOTE:** 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 3.1.11.2.19 - Spontaneous Update of Values.

The list is divided in several columns and has a toolbar providing some additional functionality. See Figure 3.67.

Table 3.3: Security Event list column description 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 3.3: 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</td>
<td>The timestamp of the DO (tagged in the IED)</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>
<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</td>
</tr>
<tr>
<td>Client</td>
<td>The associated client</td>
</tr>
</tbody>
</table>
3.11.8. **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.

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

![Figure 3.68. Point Value list](image)

Help on how to set up reporting is described in Section 3.1.11.2.19 - Spontaneous Update of Values.

The list is divided in 14 columns and has a toolbar providing some additional functionality.
Figure 3.69. Point Value list details

Table 3.4: 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</td>
<td>The timestamp of the DO (tagged in the IED)</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</td>
</tr>
</tbody>
</table>
### Chapter 3 Functionality

<table>
<thead>
<tr>
<th>Client</th>
<th>The associated client</th>
</tr>
</thead>
</table>

**NOTE:** The list can be exported to an Excel file by pressing the button "Export to Excel".

**NOTE:** The substation related information is only filled if the IED is connected to a substation/voltage level.

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

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

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

**NOTE:** 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.
3.11.9. **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 3.70. 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 3.71. 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 3.72.

![Figure 3.70. FTP Client](image1)

![Figure 3.71. FTP Username and password](image2)
3.1.11.10. **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 3.73.

Enter a meaningful name for the new IED and click “OK”. See Figure 3.74.
Figure 3.74. Adding an IED

To communicate with an IED, a SERVER has to be added. The Dialog will be shown automatically after the IED was created. See Figure 3.75.

![Create New SERVER](image)

Figure 3.75. 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 5.2 - ITT600 – Explore IEDs Default Address Parameters for more details on the address parameters or Section 2.4 - Changing OSI Address on how to change the address parameters).

To show the SERVER details, press the “Advanced >>” button in the create Server Dialog. See Figure 3.76.

![Create New SERVER](image)

Figure 3.76. Server details

**NOTE:** 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.

Refer Section 3.1.11.2 - Working Online for further information pertaining to what can be done with a connected IED.
3.1.12 Dynamically Discovering IEDs

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

From the "Edit" menu please 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 255.255.255.0
- Scanning the subnet of the computer the ITT600 - Explore IEDs software is running on. The subnet is detected automatically. See Figure 3.77.

![Figure 3.77. Detect IEDs](image)

Click next and wait for the following window to finish its activity. See Figure 3.78.

**NOTE:** 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.

![Image of ITT600 Discover IEDs]

**Figure 3.78. 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 3.79 and Figure 3.80.

![Image of ITT600 Discover IEDs]

**Figure 3.79. Found IEDs**
WARNING: 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.

3.1.13 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 3.81.
3.1.14 Exporting Single IED to an IID File

Data from dynamically added IEDs can be exported to an IID file. Once a file is opened in ITT600 – Explore IEDs, this menu item disappears. See Figure 3.82.

NOTE: Only dynamically added and browsed IEDs can be exported!
3.1.15 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 3.83.

![Quick Checker Tab](image.jpg)

Figure 3.83. Quick checker tab shown for Subnetwork AA1WA1

3.1.15.1 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 including 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.
3.1.15.2. 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.

3.1.15.3. Status Indicators

To indicate the different status, individual icons are used. See Table 3.5.

Table 3.5: Icon legend and description

<table>
<thead>
<tr>
<th>Icon type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>The values have not been checked, or are not up to date</td>
</tr>
<tr>
<td>✅</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>🚨</td>
<td>There are inconsistencies between the values loaded from SCL and the online values</td>
</tr>
<tr>
<td>❌</td>
<td>It was not possible to connect the IED or Server</td>
</tr>
</tbody>
</table>

3.1.15.4. 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 3.84.

Figure 3.84. 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 3.85.

![Figure 3.85. Quick checker countdown](image)

To reset the cyclical check, click the stop button. See Figure 3.86.

![Figure 3.86. Quick checker commands](image)

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.

**WARNING:** 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 3.87.
Figure 3.87. Quick checker commands
3.1.16 IED Status View

3.1.16.1. 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 chapter 3.1.17.4).

It is shown in its own tab when an IED or a sub node is selected in the tree view (see Figure 3.88).

![Figure 3.88. IED Status view](image)

3.1.16.2. 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 3.89. Functionality Filters](image)
The user can manually select certain attributes or use the “Select All” button.

![Figure 3.90. Select Attributes]

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.

![Figure 3.91. Perform Command]

If the user wants to revert the changes, he can select all and press the “Highlight Differences” button. All rows that are different to its initial value are highlighted and selected.
**Chapter 3 Functionality**

**Figure 3.92. Highlight Differences**

NOTE: 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 3.93. 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.

![Disconnect Warning](image)

Figure 3.94. Disconnect IED
3.1.17 IED Simulation

3.1.17.1. Overview

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

**NOTE:** 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)

**WARNING:** 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.

**NOTE:** 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.

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. Refer to Figure 3.96 for command processing flow.

NOTE: 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 3.97.

NOTE: ITT600 allows several options for processing commands. These options can be set in the ITT600 SA Explorer Options Dialog.
The result of a received command is visualized in Figure 3.97. 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.

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).
3.1.17.2. 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 3.98.

![Figure 3.98. IED Simulation options](image)

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):**
- **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.

### 3.1.17.3. Start IED Simulation

**NOTE:** 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 show in Figure 3.99.

![Figure 3.99. Launching a simulated IED](image)

**NOTE:** 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”.

**WARNING:** 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 first informing your Network Administrator.

#### 3.1.17.3.1 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 3.100. IED simulation Tab](image)

#### 3.1.17.3.2 Functionality

On the upper part of this tab, statistical information about the simulated IED is shown – refer to Figure 3.100, 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.

3.1.17.3.3. 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: .

3.1.17.4. 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 3.1.16 on how to use the IED Status view.

![Figure 3.101. IED Status view for simulated IED](image)

3.1.17.5. Stopping a simulated IED

To stop an IED, click on the Stop Simulated IED context menu entry as shown in Figure 3.102.
NOTE: 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 or PCAP). 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 four areas (see Figure 3.103):

- Menus (yellow)
- Toolbar (blue)
- Capture window (green)
- Packet window and tabs, Status bar (red)

![Figure 3.103. Explore Ethernet main user interface areas](image)

3.2.2 File Menu

Through the “File” menu following of the ITT600 – Explore Ethernet functionality is accessible (see Figure 3.104):

- Reading captures in the format of ACP and PCAP files.
- Start and stop a network capture.
• 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.
• Dump all MMS PDUs found in MMS frames into a text file for further processing.
• The contents of the capture window can be printed.
• Exit the application. Note that this does not close or terminate the ITT600 – Explore IEDs window.

Figure 3.104. Explore Ethernet File menu

3.2.3 View Menu

The “View” menu allows the user to (see Figure 3.105):

• Clear all filters previously set in the capture window.
• Clear selected filters previously set in the capture window.
• Find packets with specific contents.

Figure 3.105. Explore Ethernet View menu

3.2.4 Tools Menu

The “Tools” menu provides access to the applications options and special functions as (see Figure 3.106):
• The ITT600 – Explore Ethernet options.
• Display statistics.
• Send ACP files.

![Explore Ethernet Tools menu](image)

**Figure 3.106.** Explore Ethernet Tools menu

The options - Figure 3.107 - dialog provides following configurable settings:

![Explore Ethernet Options Dialog](image)

**Figure 3.107.** Explore Ethernet Options Dialog

### 3.2.5 Help Menu

The “Help” menu provides access to the user manual and the about window (see Figure 3.108).

![Help menu](image)

**Figure 3.108.** ITT600 – Explore Ethernet Help menu

### 3.2.6 Toolbar Functions

The toolbar provides basically shortcuts for some of the menu entries described before. See Figure 3.109.
Figure 3.109. ITT600 – Explore Ethernet Toolbar
3.2.7 Capture Window

The capture window displays the captured (or read from file) network packets in a grid like style (see Figure 3.110). The available columns can be selected through the “Tools/Options” menu entry.

The full list of available columns is:

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

The packets can be filtered through a mouse click on the filter symbol. More information about filtering can be found in Section 3.2.10.4 - The Different Filters.

![Figure 3.110. ITT600 – Explore Ethernet display filters](image)

3.2.8 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 3.2.10.3 - Analyzing Network Packets - for detailed information.
3.2.9 Status Bar

The status bar contains information about the application’s state:

- The mode (Running | Stopped).
- The capture source (File Name | NIC name).
- Amount of captured.
- Amount of captured bytes.
- Time.

3.2.10 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 3.2.10.3.4 - Analyzing Network Packets - Analyzing MMS Packets without a Loaded Configuration and Section 3.2.10.3.5 - Analyzing Network Packets - Analyzing MMS Packets with a Loaded SCL File respectively.

3.2.10.1 Working with Capture Files

On the “File” menu click on the “Open Capture” entry. In the displayed standard file open dialog, select the file you want to open.

---

**NOTE:** ITT600 – Explore Ethernet uses the same capture file format as other Ethernet Protocol Analyzers (e.g. Wireshark, Packetyzer, 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 five opened files can be accessed with the “Open Recent” list. Drag and drop a file from Windows Explorer is also supported.
3.2.10.2. **Capture Network Traffic**

3.2.10.2.1. **The Capture Wizard**

To start a capture select the appropriate file menu entry or press the button in the toolbar (See Section 3.2.2 - File Menu and Section 3.2.6 - Toolbar Functions). A wizard will guide you through the capture process (see Figure 3.111):

![Figure 3.111. Capture Settings Wizard – Step 1](image)

3.2.10.2.2. **Network Interface Card Selection**

On the first page 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.

NOTE: To capture all packets seen by the NIC the “Capture packets in promiscuous mode” has to be checked!
3.2.10.2.3. **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.

**NOTE:** If you specify a filename, the extension “acp” 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.

**NOTE:** Increase the buffer size in the wizard if packets are lost. Lost packets will be indicated in the “Statistics” dialog (see 3.2.11 - Statistics).

3.2.10.2.4. **Capture Filters**

Packets have to match the capture filter, to be shown in ITT600 – Explore Ethernet.

**NOTE:** 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 please refer to Section 3.2.10.4 - The Different Filters.

After pressing the “Next >” button the second step windows is displayed (see Figure 3.112):
More specific capture filters can be defined and the Filter will be displayed in the WinPcap syntax.

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

The step three of the wizard enables users to define the duration of the capture timing (see Figure 3.113).
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 “Finish” button, the capture will be started. New packets will be added to the grid and can be selected for further analysis.
3.2.10.2.5. **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.

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

3.2.10.3. **Analyzing Network Packets**

During or after a capture operation, network packets can be analyzed by accessing single packet rows in the capture window (Figure 3.114). 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 5.3 - 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.

3.2.10.3.1. **Detail Network Packets Columns Information**

The details column of the capture window is only updated when it is selected in the Options menu.

When the option is selected, the column will be filled when a capture is stopped or a capture file is opened. Since this feature requires a detailed analysis of each packet it requires some time.

However, this feature is of great help when e.g. only specific MMS packets should be displayed.

Only Substation Automation related protocols are reflected in this column.

**NOTE:** The Details column is only updated, when the option is active. Updating needs some time.
3.2.10.3.2. **General View**

Every packet can be shown in the general view as shown in Figure 3.114. 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.

![Figure 3.114. Display of a network packet](image-url)
3.2.10.3.3. IEC 61850 Related Protocol View

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 3.115

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).

NOTE: A list of supported protocols can be found in Section 5.3 - ITT600 – Explore Ethernet Supported Protocols.

3.2.10.3.4. 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 3.116 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 3.1.11.1.1 - Open an SCL File or connect the IED as described in Section 3.1.11.2.1 - Connect to IEDs and SERVER.

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

3.2.10.3.5. Analyzing MMS Packets with a Loaded SCL File

After the correct SCD file is loaded, the report data can be fully decoded. See Figure 3.117. 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 Section 3.2.4 - Tools Menu). See Figure 3.118.

WARNING: 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 3.116. An MMS report without a loaded SCD file

Figure 3.117. Decoding of all report values
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 “Tools” menu as well (see Section 3.2.4 - Tools Menu).

Enabling the trace all packets between a server and client (actually between two IP Addresses) will be highlighted. An example is shown in Figure 3.119. 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 3.120.
3.2.10.4. The Different Filters

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

3.2.10.4.1. 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.

NOTE: If a capture filter is specified, only packets that match this filter will be captured and shown in the application.
NOTE: Capture filters are available for IP addresses, MAC addresses and port numbers.

**Examples:**

The following example - Figure 3.121 - will capture all traffic from the three IP addresses, no matter whether it is the source or destination address:

![Figure 3.121. Capture filter based on IP addresses](image)

NOTE: Values can always be separated by semicolons or commas.

Capture filters can be combined, see next example:

![Figure 3.122. Combined Capture filter](image)

In this example all packets with the source IP address of 10.41.25.78 AND the specified source or destination address are captured.

NOTE: Values in the same field are always combined in an OR condition, whereas different lines will be combined as AND condition. See Figure 3.123 for more details.

The complete filter will be shown on step two of the wizard:

![Figure 3.123. Filter combinations](image)
NOTE: Used capture filters are shown in the status bar. See Figure 3.124.

Figure 3.124. Status bar showing used capture filters.

3.2.10.4.2. 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 3.125:

It is also possible to define customized filters. Select “Custom” in one of the rows and define your own filter. See Figure 3.126. With a specified combination, as shown in Figure 3.127, 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 3.128 - will only show reports.

**NOTE:** Used View Filters are shown with a blue filter icon.
Applied view filters are indicated with a blue filter icon in the title row, see Figure 3.129.

![Figure 3.129. Indication of used filter](image)

View filters can be reset by choosing “All” from the filters drop down menu, or by selecting the “Clear Filter...“ from the View menu. See Figure 3.130.

![Figure 3.130. Reset view filters from the main menu](image)

3.2.10.5. 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 3.131.

![Figure 3.131. Several packets in an exported Excel file](image)

**NOTE:** Raw packet data are hidden after the last column.
NOTE: Export to Excel does not contain the related SCD file.

3.2.10.6. 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.

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

3.2.10.7. 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.

3.2.10.8. Options and Default Settings

Several default values can be set in the “Options” dialog. See Figure 3.132. User can define his own grid views, define network adapter settings or select specific capture files (e.g. GOOSE, sampled values or MMS).
3.2.11 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

**NOTE:** 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 3.133.
Figure 3.133. Protocols statistics

All connections are also recorded in the tab “Connections”. See Figure 3.134.

Figure 3.134. Connections statistics

3.2.12 Send ACP File

ITT600 – Explore Ethernet allows a replay of a captured file (*.acp). The dialog to this feature is shown in Figure 3.135.
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 state.

**NOTE:** This function does not take the real time tags of the packet into account. All packets will just be sent out as fast as possible.

**WARNING:** 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 in advance.

### 3.2.13 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 3.136). A dialog including the packet data and the contained addresses will show up (Figure 3.137). Next, select the appropriate adapter from the list and define how many times the packet should be transmitted.

**WARNING:** 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.
3.2.14 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 3.138 and Figure 3.139.
3.2.15 Find in Packet Data

Identifying packets with a specific content can be time consuming. The “Find in Packet Data” dialog 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 3.140.

After inserting the search string, press “Mark all” to highlight all packets, or click the “Find Next” button to select the next packet that matches the search string.

The selection shown in Figure 3.141 highlights all packets containing the string “RPT” (all IEC 61850 reports).
3.2.16 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.

3.2.16.1. 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 3.142 shows an example of a request/response pair.

The Details column (see Section 3.2.10.3 - Analyzing Network Packets-) also shows the invoke ID. This makes it easy to find “matching pairs”.

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

IEC 61850 Commands are mapped to MMS write requests. They will be acknowledged by a positive or negative command response. Figure 3.142 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 3.143.

3.2.16.1.2. 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.
3.2.16.1.3. **Segmentation or Fragmentation**

Since MMS messages can be larger than the maximal Ethernet frame length, the message has to be segmented into several frames. ITT600 - Explore Ethernet reassembles those frames and displays the message in one piece. Reassembled packets are indicated as shown in Figure 3.144.

![Figure 3.144. Segmented MMS message](image)

3.2.16.1.4. **Several MMS Messages in one Packet**

In contrary to segmentation, several short messages can be packed together in one packet. In this case ITT600 – Explore Ethernet will indicate it as seen in Figure 3.145.

![Figure 3.145. Message count](image)

3.2.16.2. **GOOSE**

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.

**NOTE:** 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 3.146
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 shown as hexadecimal value (as it is defined in the SCD file also).

**Figure 3.146. GOOSE Analyzer showing inconsistencies**
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. Up to 10 individual signals can be compared at the same time, synchronized to each other.

The GUI is divided in four main areas as shown in Figure 3.147:

- Main menu (yellow)
- Toolbar (blue)
- Signal selection (green)
- Oscilloscope (red)

![Figure 3.147. ITT600 – Explore GOOSE main user interface](image)

3.3.2  File Menu

The file menu provides basically the same functions as the toolbar (see Figure 3.148):

- Open a capture file
- Open a recently opened capture file
- Open a plot file containing a previously saved configuration
- Open a recently opened plot file
- Save the current configuration into a plot file
- Deleting the IED and GOOSE signal selection
- Starting / Stopping an online capture
Chapter 3 Functionality

3.3.3 Tools Menu

The Tools menu provides access to the options dialog. See Figure 3.149 and Figure 3.150.
3.3.4 Help Menu

The help menu provides access to (see Figure 3.151):

- User guide.
- Show plot legend.
- The about screen.

![Figure 3.151. ITT600 – Explore GOOSE Help menu](image)

3.3.5 Operation

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 3.2.10.2.

3.3.5.1 Offline Mode

To display offline GOOSE data, the capture file has to be opened using the File menu or the Toolbar. See Figure 3.152.

![Figure 3.152. Opening a capture file](image)

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. Refer to Section 3.1.11.1.1 - Open an SCL File or Section 3.1.11.2.1 - Connect to IEDs and SERVER.
3.3.5.2. **Online Mode**

The online mode listens basically on a specified NIC and processes all received GOOSE frames. The list of IEDs is dynamically updated when new IEDs sending GOOSE frames are detected on the network.

To start an online session, click on the Capture/Start menu entry or the toolbar button. See next figures Figure 3.153 and Figure 3.154.

**Figure 3.153. Start an online session from toolbar**

![Start an online session from toolbar](image1.jpg)

**Figure 3.154. Start an online session from menu**

As a second step, the used NIC has to be defined in the dialog as shown in Figure 3.155.

![Selecting the network interface for online mode](image2.jpg)

**Figure 3.155. Selecting the network interface for online mode**

The details of the selected adapter are shown in a tool tip.

In case previously recorded data should be kept, check the “Keep already captured data” checkbox.
3.3.5.3. **Adding Data to the Oscilloscope**

To add a specific signal to the oscilloscope – see Figure 3.157, first select the time base that should be used.

3.3.5.3.1. **Capture Time**

This time is assigned when the packet was received by the capturing engine.

3.3.5.3.2. **Frame Time**

This time is set by the IED when the GOOSE frame is transmitted and is contained in the header of the frame.

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

As a second step, simply double-click the attribute that should be displayed.

**NOTE:** Double click on an attribute in order to add it to the oscilloscope display.

NOTE: 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.

A running capture is indicated with a progress bar and a counter is indicating how many different IEDs sending GOOSE are found. See Figure 3.156.
Chapter 3 Functionality

[Image of a computer screen showing signals on an oscilloscope]

Figure 3.157. Signals added to the oscilloscope

**NOTE:** A maximum of 20 individual signals can be displayed at once.

Only sequential data can be displayed in the oscilloscope. It is also a limitation that the minimum time interval between two data entries is 100ns. Data with a smaller time interval cannot be displayed and will be omitted. See Figure 3.158.

[Image of a computer screen displaying information about non-sequential data]

Figure 3.158. Information of non-sequential data

3.3.5.4. **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 3.159.
3.3.5.5. 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 3.160.

3.3.6 Plot Legend

From the help menu, the plot legend can be opened, displaying the different color codes used in the plot (see Figure 3.161):
### 3.3.7 Status Colors

Some of the attributes (like Quality Types) will be shown in grey color, meaning this data type cannot be shown in the oscilloscope. See Figure 3.162.

**NOTE:** Quality values cannot be displayed as individual values. The quality information is added to the related value.

If the configuration revision check between the online data and the SCD fails, the color of the attribute in the oscilloscope changes. Figure 3.163 shows a signal with a matching configuration revision, Figure 3.164 shows a mismatch. Figure 3.165 indicates an online capture (light blue color).

![Figure 3.162. Quality data type colored grey](image)

![Figure 3.163. Red indicates that configuration revision check is fine](image)

![Figure 3.164. Orange indicates that the check failed](image)

![Figure 3.165. Light blue indicates an online capture](image)
NOTE: Mismatches between the expected configuration revision from ITT600 – Explore IEDs and the actual received value are indicated.

3.3.8 Quality Information

As described earlier, 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 3.166, Figure 3.167, and Figure 3.168.

In addition to the color code, bad quality of signals (Invalid, Questionable or Reserved) is represented by a waved brushed style.

![Figure 3.166. Invalid quality of signals is shown as yellow area](image)

![Figure 3.167. Questionable quality of signals is shown as brown area](image)

![Figure 3.168. Reserved quality of signals is shown as white area](image)

NOTE: Quality information is incorporated in the related value.
3.3.9 Source Information

The source information is incorporated in the related value. Source of a signal (Substituted, Test) is displayed as shown in Figure 3.169 and Figure 3.170.

![Figure 3.169. Substituted source of signals is shown as brushed area](image1)

![Figure 3.170. Test source of signals is shown as brushed area](image2)

**NOTE:** Source information is incorporated in the related value.

3.3.10 Plot Information and Functions

There are a lot of functions provided by the oscilloscope 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 3.171:

![Figure 3.171. Dots indicating reception time](image3)
3.3.11 **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 there is a context menu available to jump to the next or previous value change. The functions can also be called by pressing the shortcut keys “Ctrl + N” / “Ctrl + P”. See Figure 3.172.

![Figure 3.172. Find next or previous value change](image)

3.3.11.1 **The ITT 600 – Explore GOOSE Toolbar**

The oscilloscope toolbar provides access to all major functions of the oscilloscope (see Figure 3.173):

![Figure 3.173. ITT600 - Explore GOOSE oscilloscope toolbar](image)

3.3.11.1.1 **Zooming**

It is possible to zoom in / out or define a zoom region by using the zoom box tool.
3.3.11.2. **Data Cursor and Synchronizing**

The data cursor can be used to measure the time or the value at a specific point in the plot. See Figure 3.174.

![Figure 3.174. Data cursor switched on (plots are synchronized)](image)

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

**NOTE:** Plots should be synchronized to compare the different values.

The data cursor has different modes, so also a time period can be measured. To change the data cursor's behavior, right click the cursor's tool tip and change the settings. See Figure 3.175 and Figure 3.176.
3.3.12 Saving and Opening Configurations

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

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.

NOTE: Oscilloscope configurations can be saved and re-loaded.

Figure 3.175. Changing the Data Cursor

Figure 3.176. Measuring time period between two signal states
3.4 ITT600 – Explore SV

3.4.1 Overview

ITT600 – Explore SV shows SV data capture from live streams or captured in a capture file previously logged. There are two ITT600 – Explore SV working mode, namely online and offline working mode.

- **Online working mode**: ITT600 – Explore SV captures SV packets from the user selected network adapter and displays the current and voltage phasor of a given stream within a polar chart. A maximum of 2 streams can be selected at a time and subsequently two polar charts, each represents a selected stream, are displayed. During the SV packets capturing, a user is also able to log the received SV packets to the disk by using the logging functionality.

- **Offline working mode**: ITT600 - ExploreSV loads the SV packets captured during online working mode, allowing for each available stream to display the voltage and current trends obtained out of the SVs. 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.

The ITT600 – ExploreSV is divided in five main areas as indicated with different colors (see Figure 3.177):

- Main menu (yellow).
- Toolbar (blue).
- Stream selection (green).
- Polar chart (red).
- Trend display – oscilloscope (purple)
3.4.2 File Menu

The file menu provides basic functionalities, namely (see Figure 3.178):

- Configure log file name to allow the user to set the folder location and the filename of the logged files.
- Open recently opened file that contains logged SV packets.

3.4.3 Tools Menu

The Tool menu provides the possibility for the user to set different parameters related to ITT600 – Explore SV via the Options panel (see Figure 3.179 and Figure 3.180):
The following parameters can be customized in ITT600 – Explore SV:

- **Enable Offline Analysis**: when this check box is ticked, ITT600 – Explore SV activates the offline analysis part. This allows user to perform analysis on the SV packets in an offline mode.
- **Buffer size**: to enable offline analysis, it is required to store some SV packets. 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.
- **Log file destination**: with this parameter, user can specify his/her preferred place to store the log files for the SV packets.

### 3.4.4 Help Menu

The help menu provides access to (see Figure 3.181):

- Phasors legend, providing information related to line style and colors of the displayed phasors.
- User guide.
- The about screen.
3.4.5 Operation

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

3.4.5.1. Online Mode

The online mode listens to a user specified NIC and processes all captured SV packets from selected streams and shows them in the form of phasor display as seen in Figure 3.182. The list of available streams is dynamically updated when new SV packets belonging to never-seen-before streams are detected on the network.

Figure 3.182. ITT600 – Explore SV – two streams are selected and the polar diagrams are shown

To start an online session, first select the proper NIC, and then click on the Capture toolbar button. See Figure 3.183.
While capturing, it is possible to enable file logging. This operation writes each received SV packet to file(s).

In order to show the phasor of the receiving streams, clicking on one of the detected streams, and subsequently a polar diagram is shown to show the phasors of the selected stream. A maximum of two streams can be selected at a time. When two streams are selected, two polar diagrams are shown. See Figure 3.184.

When displaying two streams, the displayed phasors are calculated using the same SV packet number (Sample Count) for both streams. There is a chance that the two streams are not synchronized and attempts to synchronize fails. In this case, the phasors are displayed but with a red background to indicate this anomaly. See Figure 3.184.

To stop an online capture, click on the Stop Button in the toolbar. This action switches the system to offline mode, allowing the user to analyze the SV packets belonging to the captured streams.

A summary of the overall functionalities in the online mode can be seen in Figure 3.185.
3.4.5.1.1. Phasor Display

The current and the voltage phasors from a selected stream are displayed 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 sliders – see Figure 3.186. In addition to magnitude and angle, each phasor provides additional information on the quality.

There are three line representations related to phasor, namely:

- Good, displayed as solid line: all the values used for calculating this phasor were good quality.
- Bad quality, displayed as line: at least one of the values used for calculating this phasor was bad quality
- Missing point, displayed as line: since phasor is calculated using 80 values, missing point quality is set if these 80 values belong to SV packets that are not sequential.
The table on the right side of the polar chart summarizes the following information (see Figure 3.187):

- Color of the phasor
- Logical name of the channel
- RMS value as Magnitude
- Phase Angle
- Quality
  - Green: when all the quality bits of all packets are set to 0.
  - Yellow: when any of the following quality bit, namely Test, OperatorBlocked, Source-Substituted, and Derived is set to 1, and quality validity is good.
  - Red: when quality validity is either Invalid, Reserved, or Questionable.

- Quality Details

Figure 3.187. Table represents summary of a selected stream

3.4.5.1.2. Show and Ref Function

At each channel, there are two checkboxes corresponding to the following functions respectively (see Figure 3.188):

- **Show checkbox**: show/hide a channel. In the offline mode, this show/hide checkbox impacts the related channel in the trends. For example, if a user unchecks the show checkbox for the channel related to Voltage phase 1, the channel related to Voltage phase 1 will be hidden.
• **Ref checkbox**: only one channel can be set as reference at a time. 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.

**NOTE**: If two streams are displayed at the same time, 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 the other stream. In this way, it is possible to compare the angle difference between the channels belonging to different streams. However, with two streams selected for displaying at the same time, the 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 the same streams.

![Figure 3.188. Behavior when a Ref checkbox is selected. Observe the Phase column](image)

### 3.4.5.1.3. Logging the SV Packets

It is possible to log SV packets to file during online capture. To activate this function, click on the Log to file button at the toolbar to start writing to file all the packets captured during the online execution. Logging will disable the stream selection in order to ensure logical continuity. The followings show different possibilities regarding logging the SV packets:
If one stream is selected for display and a user starts to log to file, the logged file will hold all SV packets belonging to that given streams.

If two streams are selected for displaying and user starts to log to file, the logged file will hold all SV packets belonging to one of the selected streams.

If the user starts to log to file when no stream is selected, all SV packets belonging to all the streams will be logged to file. For this reason, when the user starts to log, the streams selection is disabled in order to prevent uninterested stream packet is recorder in the same file. Such event could lead to misleading situations when the file is loaded back.

**NOTE:** 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 1 million of SV packets are recorded, a new file is created as a container for the next recorded packets. The maximum file size is 138Mbytes.
3.4.5.1.4. **Stream Quality Information**

Quality information cannot be added as individual signals. The quality information in the phasor display is represented in different types of line and different symbols as shown below - Figure 3.189. Refer to Section 3.4.5.1.1 - Phasor Display for the interpretation of the color.

![Figure 3.189. Legend for Phasors Display quality](image)

3.4.5.2. **Offline Mode**

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

- Run an online capture and process data acquired during online mode.
- Load a previously logged file, directly or using the recently opened file feature.

After the file is parsed, a list containing all available streams is generated. Selecting a particular stream will show current trends, voltage trends, and a statistical report (Statistics tab – ref. Section 3.4.5.2.2) that holds several data and allow the user to display the most relevant information.
3.4.5.2.1. Trends

ITT600 – Explorer SV provides an integrated features to show the trend of the voltage and current. Trend display displays at same time both current and voltage values and qualities. To navigate through the trend graph, zoom in/out function is provided. Additionally, based on the level of zoom currently used, the voltage and current trends are displayed as continuous lines or as a succession of dots. 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 right section of the trend display – in the Analyzed 9-2 packet tab (see Figure 3.191). 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 4 channels of data, namely 3 channels for the 3 phases plus the neutral one. By the right hand side of the trend displays, the legend highlights the mapping between each channel and its color. By clicking the name of the channel in the legend is possible to hide/show that channel in the trend and its phasor.

Figure 3.190. Trend display and data analysis part
### 3.4.5.2.2. Statistics Analysis

ITT600 – Explore SV provides several functionalities to dig deeper into the quality of the packets. The statistical information is shown only in the offline mode. On the right section of the trend displays, users can find the statistical analysis section (see Figure 3.191). At the Statistics tab, users can see a summary of the collected samples showing information such as anomalies, lost samples and quality information of the collected samples. If there is a missing point, users can click on a particular missing point entry, and the trend displays will show the time frame where the packet is missing (see Figure 3.192). At the Analyzed 9-2 packet tab, users can evaluate in detail the content of each particular packet that is used to construct a point in the graph.

![Figure 3.191. ITT600 – Explore SV – Statistical analysis section](image1)

![Figure 3.192. ITT600 – Explore SV – Missing points are shown in the trend displays](image2)
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 3.193):

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

![Figure 3.193. ITT600 - Explore Models main user interface](image)

3.5.2 File Menu

The file menu provides basic functionalities, namely (see Figure 3.194):

- Load the models.
- Exit the application.

![Figure 3.194. ITT600 - Explore Models File menu](image)
3.5.3 Help Menu

The Help menu provides Model Functionalities (see Figure 3.195).

![Figure 3.195. ITT600 - Explore Models Help menu](image)

3.5.4 Toolbar

Toolbar provides buttons to navigate through the compared model and comparison results, namely (see Figure 3.196)

- Load left and right model for comparison.
- Compare models.
- Move to next or previous difference.
- Export the differences to .xsl file.

![Figure 3.196. ITT600 – Explore Models Toolbar](image)

3.5.5 Model panels

The two model trees will display the structure of the IEC 61850 model contents (see Figure 3.197).

![Figure 3.197. ITT600 - Explore Models with loaded models](image)
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 3.198).

![Figure 3.198. Comparison result window](image)

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.

**NOTE:** 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.

After both models are loaded you have to select a node on each side (see Section 3.5.7 - Comparing SCL Files). The “Compare” toolbar button becomes enabled. Clicking this button will show a dialog with filters (for detailed explanations about the filters please refer to Section 0). Click OK to proceed with the comparison.

**NOTE:** 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 3.199.
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.

**NOTE:** 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 3.200) 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
  o Ignore differences in access point addresses. Access point addresses (IP, MAC ... addresses) are not checked.
  o 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.
  o Ignore short address differences. Different short addresses will not be taken into account.
• Control Block Filters: provides comparison filters for various control block attributes

NOTE: 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.

Error! Reference source not found. shows an example that the IP address of the compared IEDs are different.

Figure 3.201. 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 3.201). 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
- Only available in the left model
- Available in both models, but there is a difference

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.

**NOTE:** To export the differences to .xsl file both models have to 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 3.202. An example of .xsl export information page.**

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

**Figure 3.203. An example of .xsl export information page**
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 (ref. Section 3.1.5). 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 3.204.

![Figure 3.204. Check for Updates windows – no update is available](image_url)

Figure 3.204. Check for Updates windows – no update is available
Chapter 4 Functionality

4 Limitations

For limitations see the release notes.
### Appendix

#### 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.</td>
</tr>
<tr>
<td></td>
<td>Check whether you have a running VPN client on the PC and disable it.</td>
</tr>
<tr>
<td></td>
<td>Check the NIC settings.</td>
</tr>
<tr>
<td></td>
<td>Refer to chapter 2 - Configuration</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.</td>
</tr>
<tr>
<td></td>
<td>Refer to chapter 2 - Configuration</td>
</tr>
<tr>
<td></td>
<td>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.</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 “Ignore Type difference” flag in the “Explore SCL” 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.</td>
</tr>
<tr>
<td></td>
<td>The NIC configuration cuts off the VLAN tags from the frames.</td>
</tr>
</tbody>
</table>
Chapter 5 Functionality

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refer to chapter 2 - Configuration</td>
<td></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. Refer to: Section 3.1.11.2.17 - Manually Update Values from an IED and Section 3.1.11.2.19 - Spontaneous Update of Values.</td>
</tr>
<tr>
<td>No entries are logged in the process event list.</td>
<td>Reporting is not set up. Refer to: Section 3.1.11.2.19 - Spontaneous Update of Values</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>
</table>
| MMS           | Manufacturing Message Specification  
Communication protocol for IEC 61850 |
| (R)STP        | (Rapid) Spanning Tree Protocol.  
Protocol used by switches to determine alternate (redundant) routes |
| GOOSE         | Generic Object Oriented Substation Event  
The IEC 61850 “real time” protocol for bay to bay communication |
| NTP           | Network time protocol.  
Used for time synchronization of IEDs and clients. |
| IEEE1588 (PTP) | Precise time protocol.  
Used for time synchronization of SV Servers. |
| SNMP          | Simple Network Management Protocol  
Diagnostic information about network nodes. |
| SV            | Sampled Values  
Sampled Values according IEC 61850 |
| IEC60870-5-104 | IEC SA Protocol for SCADA / NCC connections |
| PRP           | Parallel Redundancy Protocol |
| DNP3.0 / TCP  | Distributed Network Protocol over TCP Protocol between RTUs and SCADA Systems |
| Modbus / TCP  | Modbus Protocol over TCP Protocol between RTUs / PLCs and SCADA Systems |

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 find 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