Secure and Efficient Testing of IEC 61850-Based Protection and Control Systems

Agenda

What are the issues and challenges during testing
(focus on maintenance testing)

Requirements for testing IEC 61850-based PACS

Doble's simulation test devices and software tools

Testing Issues and Challenges

- "**Software switches**" replace conventional physical test switches for **isolating injected signals and outputs** of device under test (DUT) from the rest of the system in normal service

- Test signals (SV and GOOSE) are seen by DUT as well as devices in normal service – a **major security concern**

- Similar GOOSE messages from Test Sets and Real IEDs (under test and in normal service) are difficult to be differentiated by testers and by some IEDs (Edition 1)

- Test Isolation features of IEC 61850 are not understood by most testers

- Existing packet sniffing tools are difficult to use for data visualization by testers

- Issuing of control sequences through generic MMS client tools is extremely difficult from the data model IED explorer tree and list views

3

Testing Issues and Challenges

- A complete substation and its system configuration description file (SCD) can contain 100s of IEDs and it is difficult to manage the test scenarios

- Some substations have been designed with little regard to testing

- Configuring some complex tests is often times a trial-and-error process

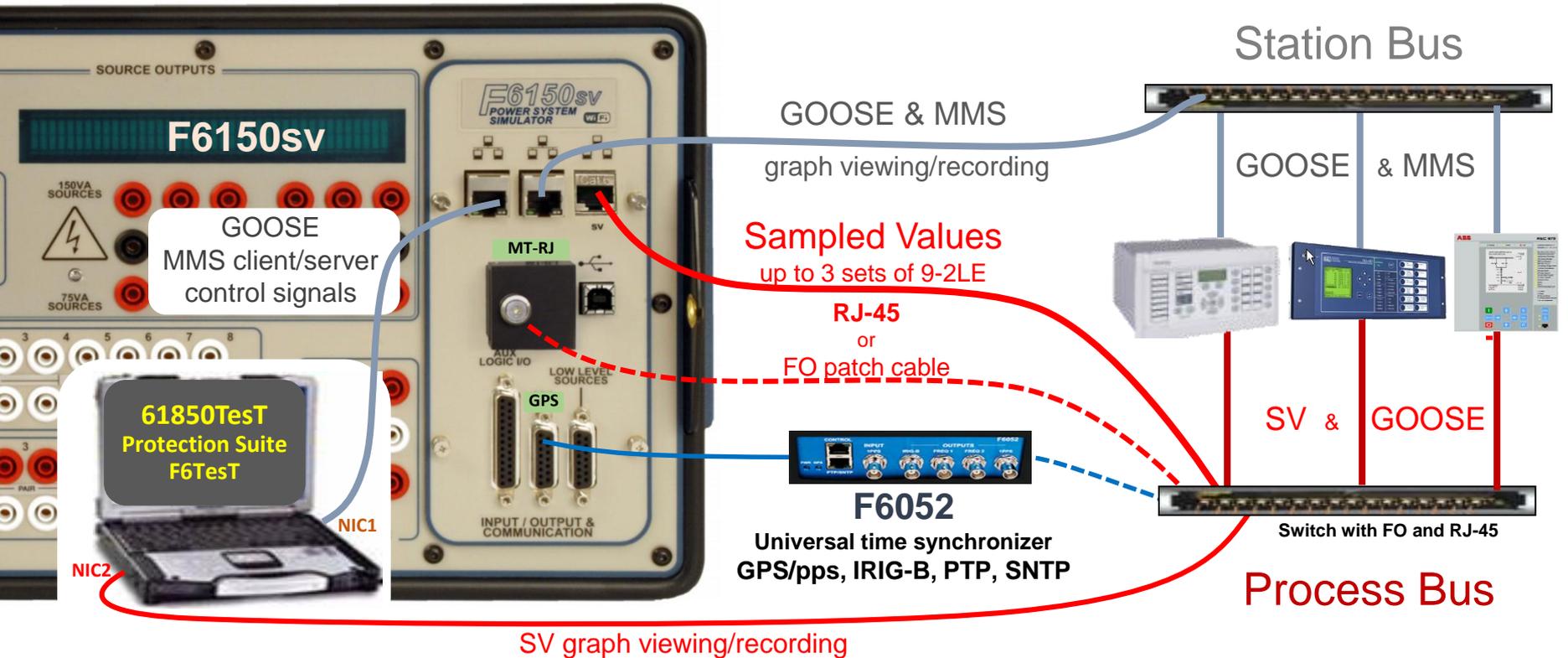- **No room for errors** when doing maintenance **testing in a live substation**

Testing Issues and Challenges

- A single IED can have **numerous** protection & control functions
- Many functions can share a **common trip output**. How to test a specific protection element (e.g., Zone 2 AB loop, Neutral OC stage 2, etc.) if the **element of interest is not in the dataset**
- **Not allowed to change** protection settings or re-map I/O signals for maintenance

- Some schemes have functional elements that are **distributed across multiple physical IEDs**
- Some protection functions require 2 or more simultaneous sets of sampled values
- Some **hybrid systems** use both conventional voltages and currents and sampled values

Testing Requirements and Doble Solutions

- Import SCL files; read data model and configuration from IEDs; compare files
- Scan network for GOOSE & SV messages
- Mask complexity of IEC 61850 from user
- Easy setup of test configuration for SV publishing and GOOSE subscription and publishing.
- Real-time data visualization
  - Tabular list of selected signals
  - Annunciator panel with widgets
  - Oscillography (SV, GOOSE, Reports)
- Record SV and data (GOOSE, Reports) in COMTRADE files; Viewer/Analysis module
- Logging of GOOSE, Report and Polling data

- User-friendly MMS Client w/ descriptive semantic information
- Easy-to-use interface for
  - control of breakers and other controllable objects
  - preparing the IEDs for simulation and testing
- GOOSE simulator for publishing and subscription; with programmable logic
- Support IEC 61850 testing and isolation features
- Default to secure simulation/quality states
- Save and re-use Configuration Setup files and Test Plans that have been fully verified to be working correctly – This ensures security, avoids errors during actual testing and improves efficiency and management of the testing process

Tools for Testing IEC 61850-based PACS

Station Bus

GOOSE & MMS

graph viewing/recording

GOOSE & MMS

F6150sv

GOOSE
MMS client/server
control signals

Sampled Values
up to 3 sets of 9-2LE

RJ-45
or
FO patch cable

MT-RJ

61850TesT
Protection Suite
F6TesT

NIC1

NIC2

SV & GOOSE

F6052
Universal time synchronizer
GPS/pps, IRIG-B, PTP, SNTP

Switch with FO and RJ-45

Process Bus

SV graph viewing/recording

Test Features – **Isolation** during Maintenance

Test signals injected by test set should be:
- **Accepted only** by Devices *(IEDs or Logical devices)* under test (**DUT**)
- **Rejected** by devices that are in normal service

Simulation:
- Test set publishes SV and GOOSE messages with Simulation flag = true
- **DUT set to Simulation** will process messages with Simulation flag = true
- Devices in **normal service** (Simulation not set) will **not process** simulated messages

Output Signals of DUT
- Outputs signals should be accepted by other devices also under test
- **rejected** by other devices in normal service
- Hard-wired outputs of the DUT **blocked** from operating on the process

Mode/Behavior: – Test, Test/blocked
- GOOSE outputs of DUT are identified with q.test=true. They are **processed as valid** by other devices also **under test**
- Devices in normal service reject (or **process as Invalid**) signals with q.test=true.
Test/blocked mode: HW outputs **blocked**

IEC 61850 Test Simulation Features (Edition2)
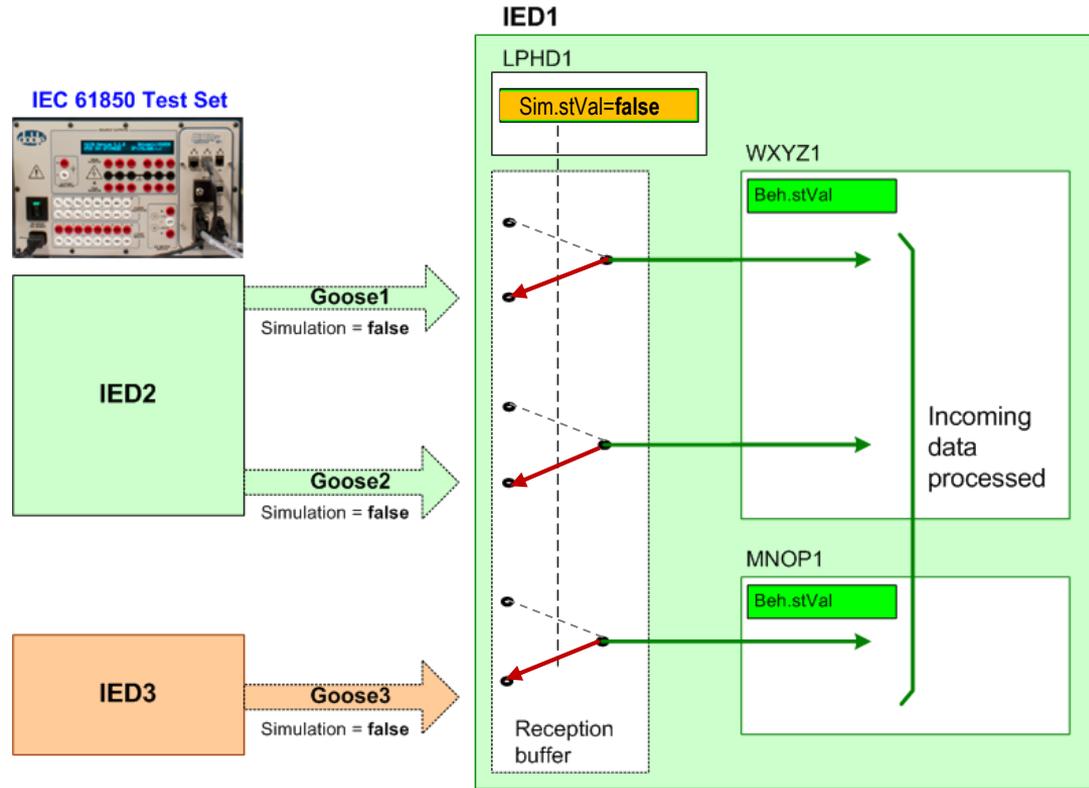
- Devices in <u>normal service</u> with Simulation=**false** will <u>process</u> GOOSE messages from real IEDs

9

IEC 61850 Test Simulation Features (Edition2)
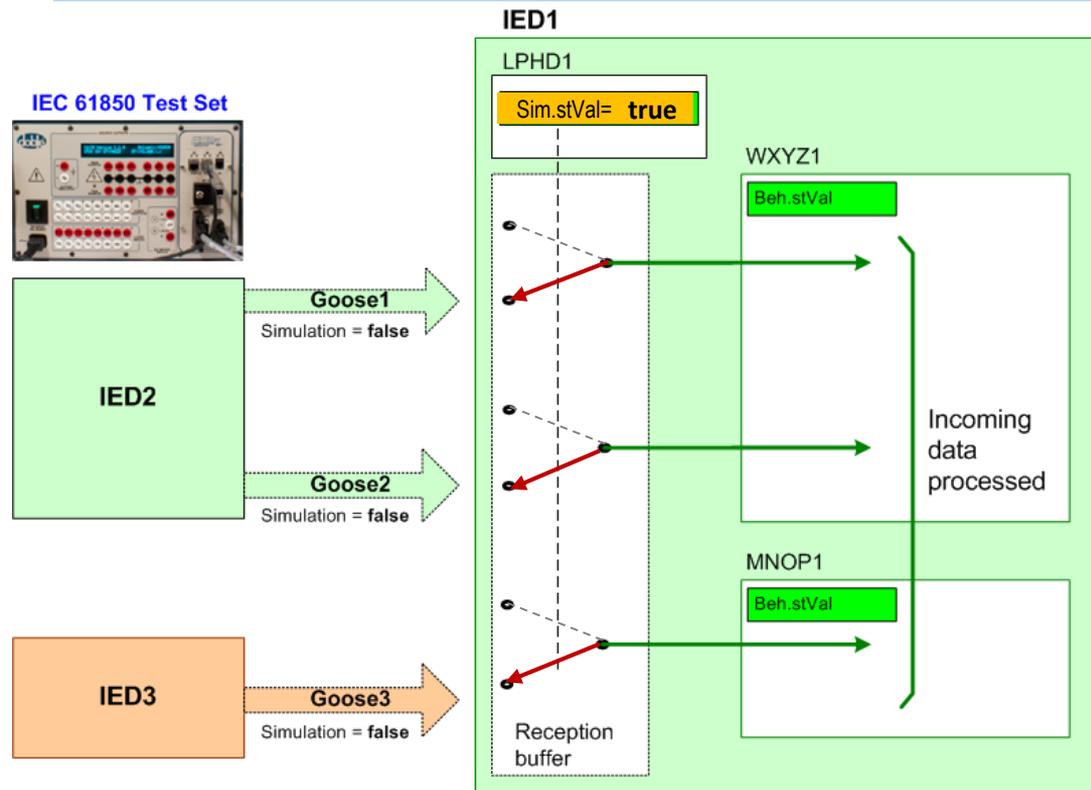
- Devices in <u>normal service</u> with Simulation=**false** will <u>process</u> GOOSE messages from real IEDs
- Device with Simulation changed to **true** will <u>still continue</u> processing GOOSE messages (with simulation flag = false) from real IEDs, if there are **no** simulated messages from the test set

IEC 61850 Test Simulation Features (Edition2)
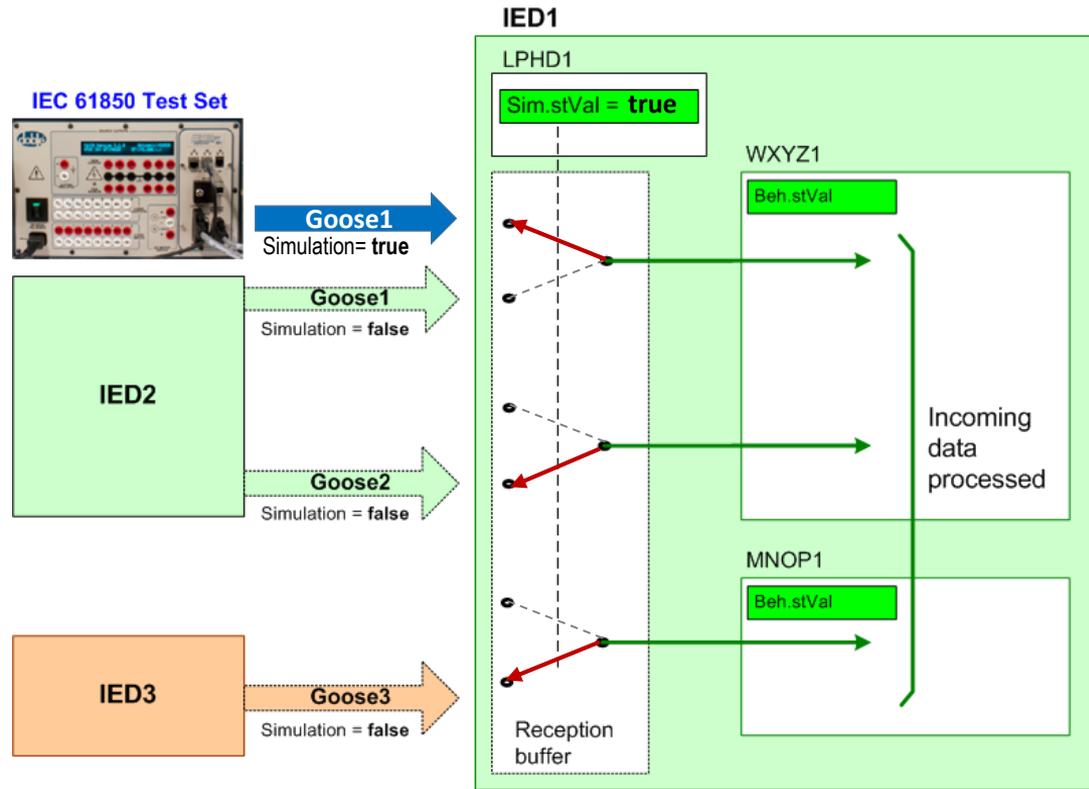
- Test set publishes GOOSE msgs with Simulation flag = true
- DUT with Simulation = true will
  - Start accepting messages with Simulation flag = true
  - Reject messages from real IED with Simulation flag = false

11

IEC 61850 Test Simulation Features (Edition2)
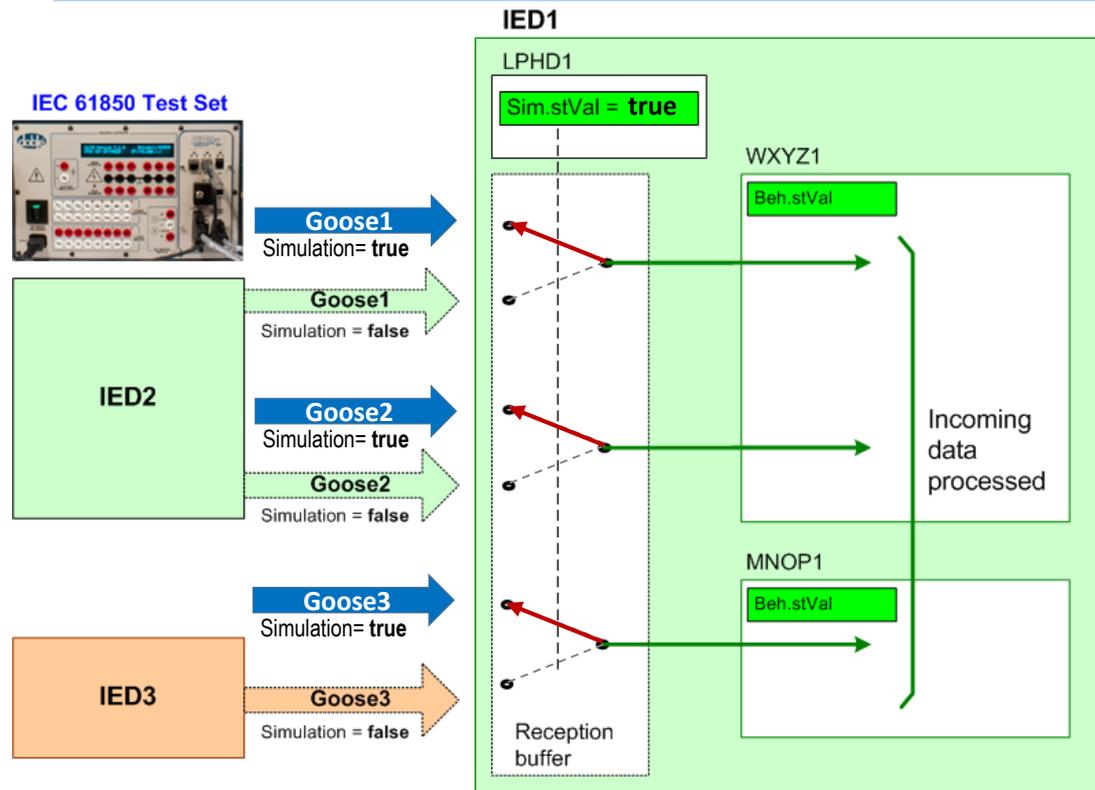
- Test set publishes GOOSE msgs with Simulation flag = true
- Devices in Simulation = true will accept incoming simulated messages with Simulation flag also set to true

- All GOOSE messages from the real IEDs (**Sim=false**) that have the same names as the simulated ones will now be rejected.

This concept also applies to Sampled Values

Mode and Behavior of Logical Devices and Logical Nodes
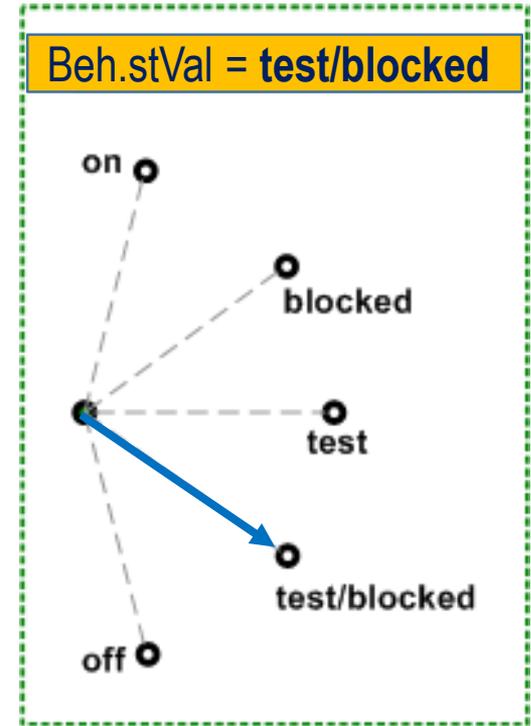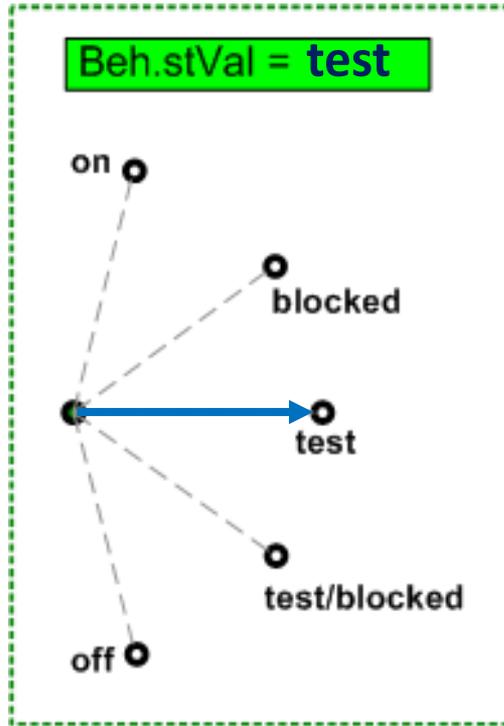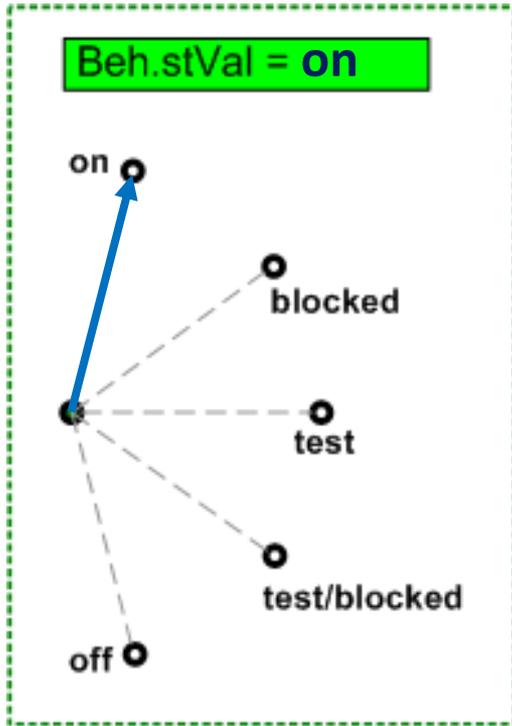
LD/LN Mode/Beh Inheritance

LNMode or nested LDMode XXXX.Mod	LDMode LLN0.Mod	LNBeh (read only) XXXX.Beh
on	on	on
on	blocked	blocked
on	test	test
on	test/blocked	test/blocked
on	off	off
blocked	on	blocked
blocked	blocked	blocked
blocked	test	test/blocked
blocked	test/blocked	test/blocked
blocked	off	off
test	on	test
test	blocked	test/blocked
test	test	test
test	test/blocked	test/blocked
test	off	off

LNMode or nested LDMode XXXX.Mod	LDMode LLN0.Mod	LNBeh (read only) XXXX.Beh
test/blocked	on	test/blocked
test/blocked	blocked	test/blocked
test/blocked	test	test/blocked
test/blocked	test/blocked	test/blocked
test/blocked	off	off
off	on	off
off	blocked	off
off	test	off
off	test/blocked	off
off	Off	off

The behavior of a function is controlled jointly by its superior hierarchical level as well as through its controllable object 'Mod'. To reach a definite behavior among these two access variants, the states are ordered by priority, where 'off' has priority over 'test' which has priority over 'on' . Test and blocked have the same priority resulting in test/blocked.

Mode/Behavior, Data Quality and Processing

Mode/Behavior, Data Quality and Processing

Incoming GOOSE

Data items that have *q.test = false* will be *processed as invalid*
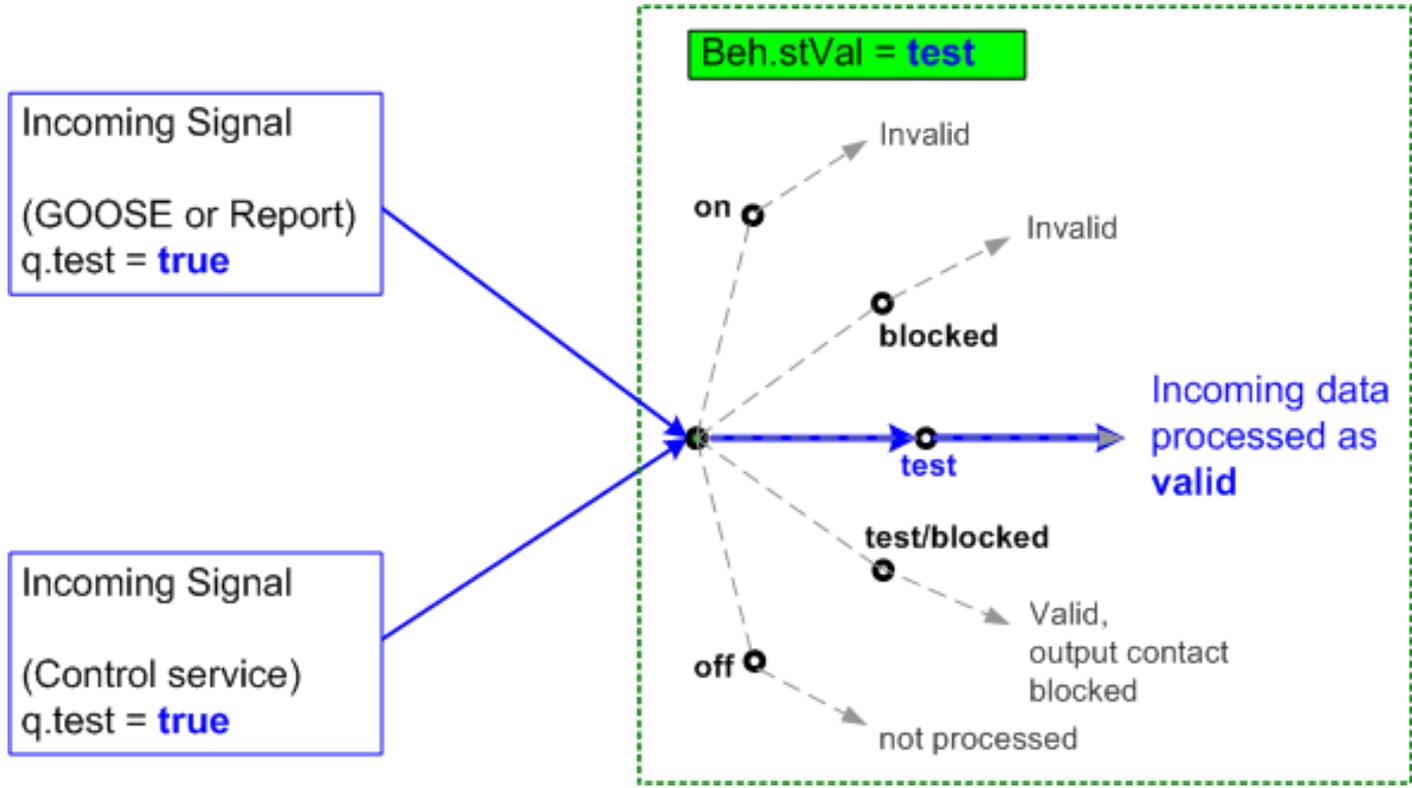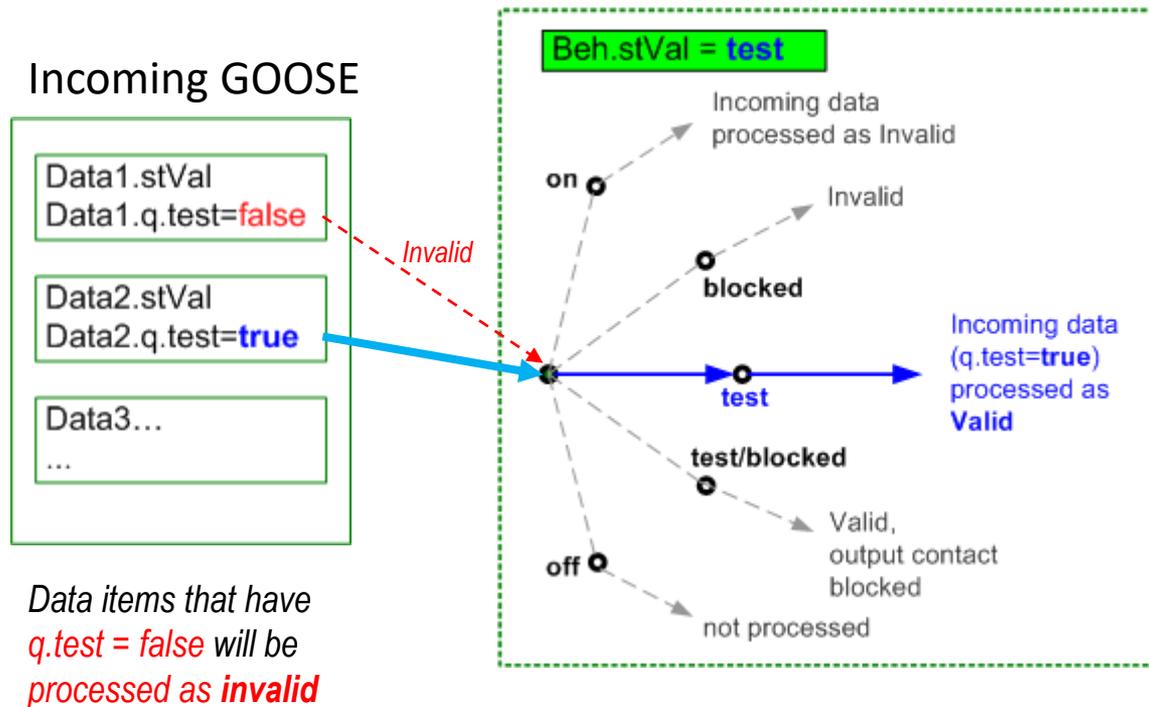
- LD/LN with Behavior = **test** or **test/blocked** will **process as valid** incoming data with **q.test = true**

- Data items with q.test=false (even from the same GOOSE message) will be rejected or **processed as invalid**

This also applies to Control service messages

16

Doble Solutions

for

Testing IEC 61850-based Protection and Control Systems

GOOSE Messages and Datasets

- Import SCL file or discover IEDs
- Add custom labels for easy identification, esp. for GGIO data items
- Select data items for
  - Use as Inputs/Outputs
  - Viewing in live data
- For GOOSE simulation
  - Set Sim flags
  - Set data q.bits
  - Verify default data values

18

Configuring Doble F6150sv test set for Signal Inputs(GOOSE Subscription)

- Map selected data signals to **Inputs** (GN#) of F6150sv test set
- Verify "compare" values signal triggering for use during testing

Substation	F6 Input	F6 Output	PC GSE Simulator	Subscription Mapping	Notes

Dataset items available

GSE control block reference	Dataset name	GSE application ID	Label ▲	Details from SCL file	Item no.	Data type
SV_EFACECIO/LLN0GOEFA_L500_Go61	DSforGo61	EFA_L500_61	EFA DOBLE Start Fault	USER.GGIO1.Ind02.stVal(ST)	3	Boolean
SV_EFACECIO/LLN0GOEFA_L500_Go61	DSforGo61	EFA_L500_61	EFA PTOC.Str	PROT.PHOC1PTOC1.Str.general(ST)	7	Boolean
SV_EFACECIO/LLN0GOEFA_L500_Go61	DSforGo61	EFA_L500_61	EFA PTRC.Op	PROT.SPTRC1PTRC1.Op.general(ST)	9	Boolean
SV_EFACECIO/LLN0GOEFA_L500_Go61	DSforGo61	EFA_L500_61	EFA RBRF.OpEx	PROT.SPBF1RBRF1.OpEx.general(ST)	5	Boolean
SV_EFACECIO/LLN0GOEFA_L500_Go61	DSforGo61	EFA_L500_61	EFA Reset Demo	CTRL.CSWI1.OpCls.general(ST)	11	Boolean
SV_NRPIGO01/LLN0GOgocb1	dsGOOSE1	NR_PCS902_A1	NR DOBLE Fault Start	PIGO01.GOOUTGGIO1.Ind2.stVal(ST)	2	Boolean
SV_NRPIGO01/LLN0GOgocb1	dsGOOSE1	NR_PCS902_A1	NR Reset Demo	PIGO01.GOOUTCSWI1.OpCls.general(ST	3	Boolean
SV_NRPIGO01/LLN0GOgocb0	dsGOOSE0	NR_PCS902_A0	NR PTOC2.Str	PIGO01.PTOC2.Str.general(ST)	2	Boolean
SV_NRPIGO01/LLN0GOgocb0	dsGOOSE0	NR_PCS902_A0	NR PTOC2.Op	PIGO01.PTOC2.Op.general(ST)	4	Boolean
SV_NRPIGO01/LLN0GOgocb0	dsGOOSE0	NR_PCS902_A0	NR PTRC.Op	PIGO01.PTRC1.Op.general(ST)	5	Boolean

Dataset item assigned   ➕ **Add below**

F6 Instrument	ID	Label	Details from SCL file	GSE control block reference	Dataset name	GSE application ID	Item no.	Data type	Compare	Value
F6150	GN1	EFA DOBLE Start Fa	USER.GGIO1.Ind02.stVal(ST)	SV_EFACECIO/LLN0GOEFA_L500_Go6	DSforGo61	EFA_L500_61	3	Boolean	=	1
F6150	GN2	NR DOBLE Fault Sta	PIGO01.GOOUTGGIO1.Ind2.stVal(ST)	SV_NRPIGO01/LLN0GOgocb1	dsGOOSE1	NR_PCS902_A1	2	Boolean	=	1
F6150	GN3	EFA Reset Demo	CTRL.CSWI1.OpCls.general(ST)	SV_EFACECIO/LLN0GOEFA_L500_Go6	DSforGo61	EFA_L500_61	11	Boolean	=	1
F6150	GN4	NR Reset Demo	PIGO01.GOOUTCSWI1.OpCls.general(ST)	SV_NRPIGO01/LLN0GOgocb1	dsGOOSE1	NR_PCS902_A1	3	Boolean	=	1
F6150	GN5	EFA PTOC.Str	PROT.PHOC1PTOC1.Str.general(ST)	SV_EFACECIO/LLN0GOEFA_L500_Go6	DSforGo61	EFA_L500_61	7	Boolean	=	1
F6150	GN6	EFA PTRC.Op	PROT.SPTRC1PTRC1.Op.general(ST)	SV_EFACECIO/LLN0GOEFA_L500_Go6	DSforGo61	EFA_L500_61	9	Boolean	=	1
F6150	GN7	EFA RBRF.OpEx	PROT.SPBF1RBRF1.OpEx.general(ST)	SV_EFACECIO/LLN0GOEFA_L500_Go6	DSforGo61	EFA_L500_61	5	Boolean	=	1
F6150	GN8	NR PTOC2.Str	PIGO01.PTOC2.Str.general(ST)	SV_NRPIGO01/LLN0GOgocb0	dsGOOSE0	NR_PCS902_A0	2	Boolean		

Configuring Doble F6150sv test set for Signal Output Simulation (GOOSE Publishing)

- Map selected GOOSE data signals to logic **Outputs** (GP#) of test set

- Verify "True value" and "False value" for signals simulated during testing

Configuring F6150sv test set for Simulation of Sampled Values

- Define multiple SV sets for Substation
- Select and simulate up to 3 sets of SV (9-2 LE) simultaneously for each test
- Set or reset Simulation flag
- Time synchronization
  - Automatic Sync (based on GPS signal)
  - Override to make Local & Global
  - Override to make Unsynchronized
- Set Quality bits –
  - Test, Validity, etc.

MMS Client – Data Model, Read/Write, Control, Reports

Control User Interface

- Test sequences of control operations with ease
  - **Non-expert mode** hides/disable buttons and fields and allows only valid operations
  - **Expert mode** enables everything and allows testing of invalid sequences

- Filters for easy selection of objects
- Support all control models –
  - **status** only
  - **direct** with normal or enhanced security
  - **SBO (select-before-operate)** with normal security
  - **direct** with enhanced security
  - **SBO** with enhanced security
- Test control operations with checks of **interlocking** and **synchronization**
- Perform tests with IEDs in test mode with the control sequence **Test flag** set
- Status info of requests and responses
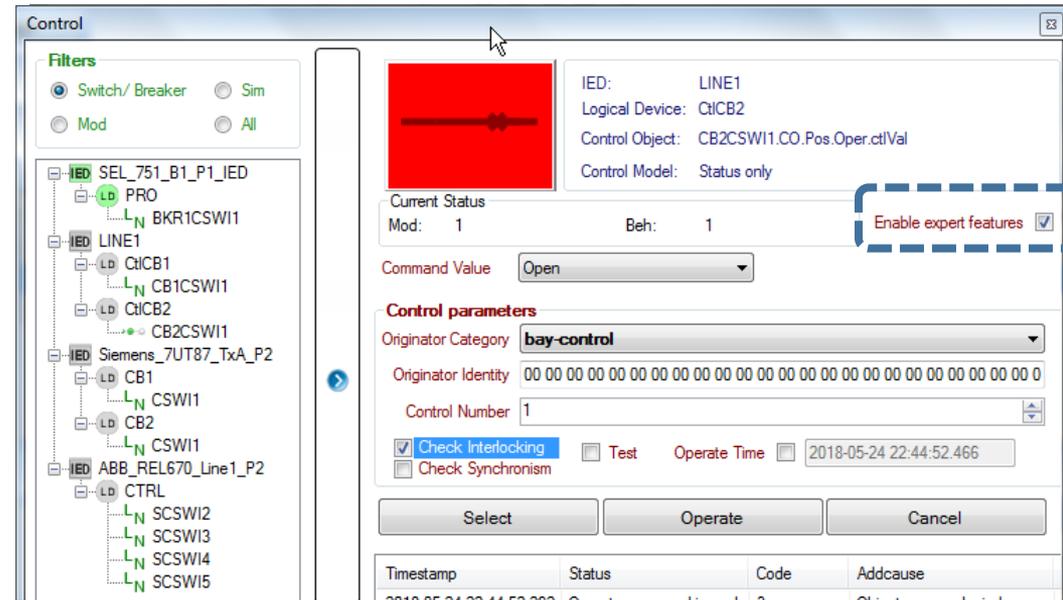
User Control of IED's modes for Testing

- LD or LN.Mod
  - on (1)
  - blocked (2)
  - test (3)
  - test-blocked (4)
  - off (5)

- LPHD.Sim
  - false (0)
  - true (1)

Real-time Data Visualization and Recording – GOOSE, Reports, Sampled Values

Live Tabular view - Selected signals only or All signals
Identify identical sources (real & test); Sim = true or false

Watch windows in Client/Server – Local + Global

Oscillograph views – GOOSE, Report, SV; Save COMTRADE
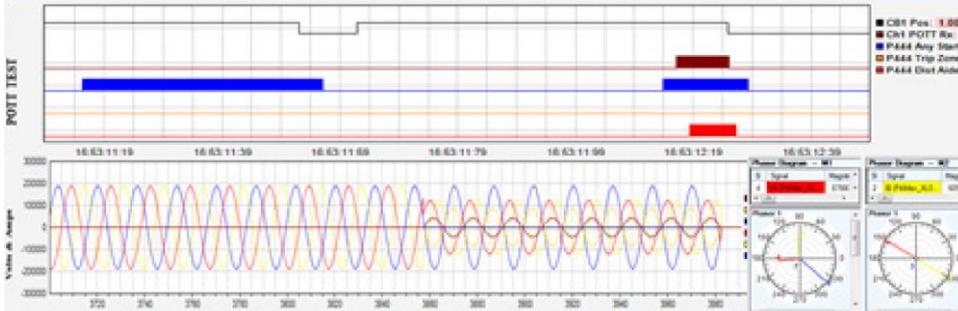
Annunciator view - with animated widgets
(user configurable); Detects if GOOSE is missing

Logging view- GOOSE & Reports + dataset details

ny. All Rights Reserved

Server Simulator

Table simulation

Direct input

Script simulation: Performs subscription, logic / math processing, and publishing

- **Use for simulating missing IEDs during any testing phase**
- **Use to simulate special test conditions**

26

PC-based GOOSE Simulator

Subscribe to GOOSEs from IEDs.
Map data items to simulator virtual inputs

IED/GOOSE Simulator

Perform mathematical and logical operations using scripts

Manually change output values

Publish GOOSEs with data values from calculated results, and/or

from manually entered values
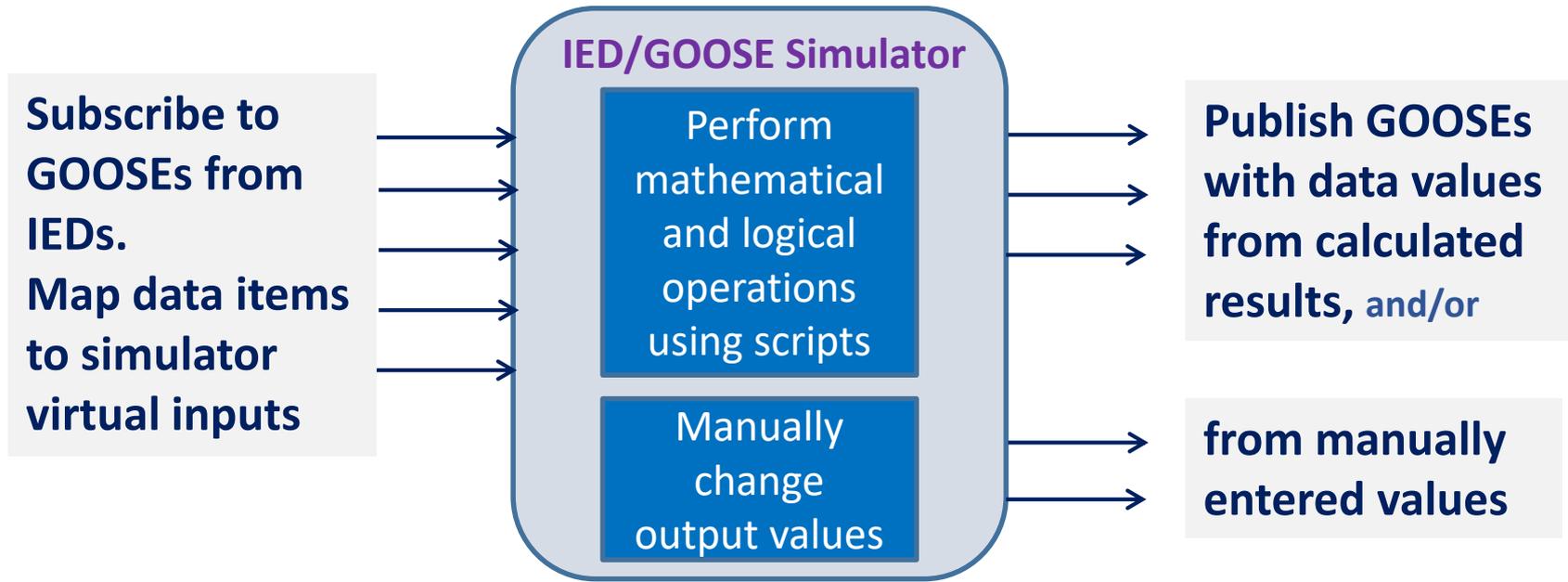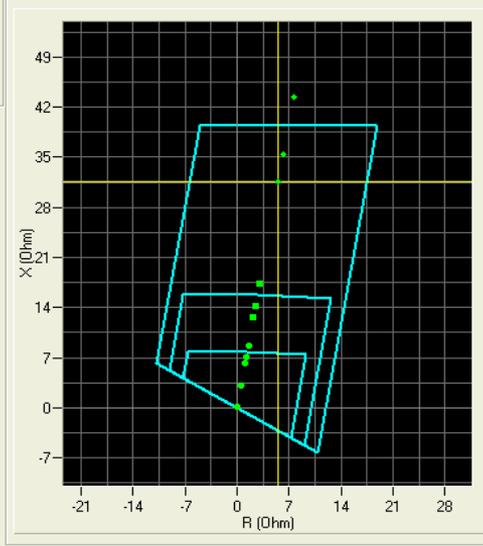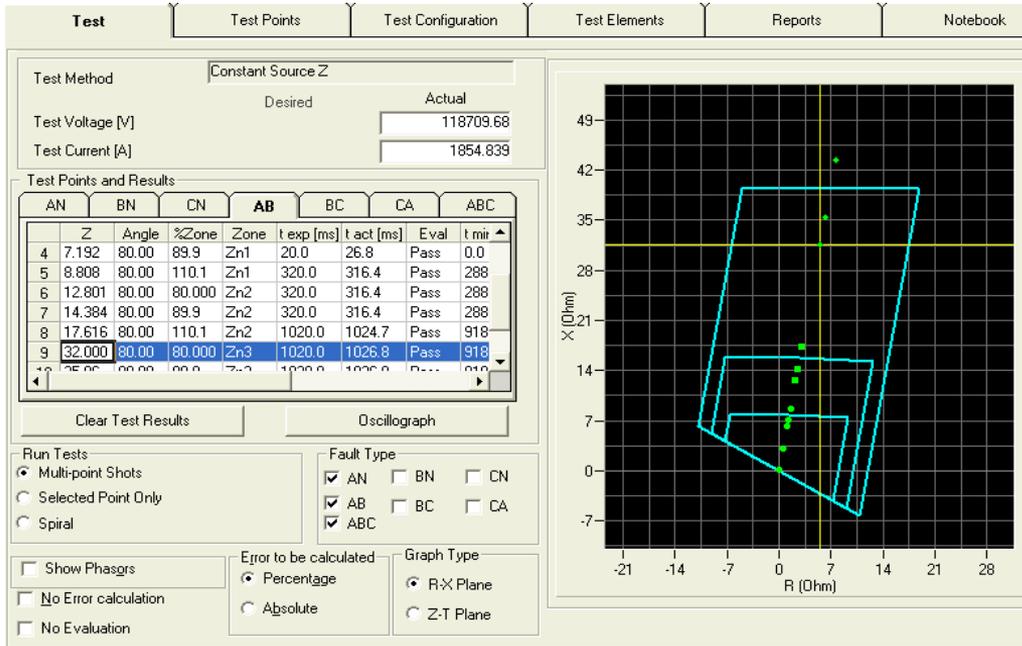
- **Use for simulating multiple missing IEDs during any testing phase**
- **Use for simulating various test conditions**

Protection Test software solutions

- Visual modeling and testing to verify settings and characteristics
- Avoid changing settings and signal mappings
- Smart testing targets specific functional elements by applying correct voltages and currents
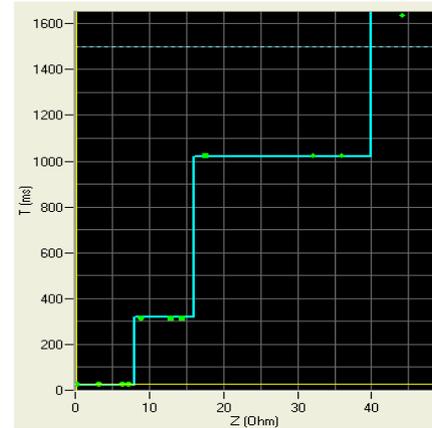
- Automatically identifies the elements that operated based on measured operate times and/or status of data signal

Protection Test software solutions

Protection Suite sw

- Power system models

- Transient testing

Test Preparation for Ensuring Security and Efficiency

- **Import SCD file**
- **Identify standard or similar sub-systems**
- **Divide substation into manageable sub-systems**

  - Identify and select related IEDs for each PAC sub-system
  - Matrix of GOOSE messages and signals
    - Publishing
    - Subscriptions/external references
  - SV messages and subscribing IEDs, functions

- **Develop 61850 Test configuration files**
- **System conditions**
  - **Normal**
  - **Simulation / Test**

  - Map GOOSE Signals to F6150sv Logic I/O
  - Simulation: sequence tables and scripts
  - Live Data visualization and recording (GOOSE, SV, Report)
  - Client config. for control, report, watch/polling

  - Take special attention to test isolation and security to prevent inadvertent operation of devices in normal operation while performing test on other devices.
  - Thoroughly test and vet configuration files and test plans
  - Document configuration files and test plans and provide clear procedures and instructions for test personnel

- **Develop automated test plans**
- **Normal and test conditions**

  - Functional element tests
  - Multi-element tests of main functions
  - Fault conditions and control sequences
  - Multi-IED scheme tests

- **Collection of well-organized files and test plans**
- **Select, use, reuse applicable files and plans for:**

  - Factory Acceptance Tests
  - Commissioning tests
  - Maintenance tests

  Fully tested and properly documented configuration and test files promotes efficiency and ensures security during testing