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
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

- **F6150sv**
  - GOOSE & MMS graph viewing/recording

- **GOOSE & MMS**
  - Sampled Values up to 3 sets of 9-2LE
  - SV graph viewing/recording

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

- **Station Bus**
  - GOOSE & MMS

- **Process Bus**
  - SV & GOOSE
  - Switch with FO and RJ-45

- **61850TesT** Protection Suite F6TesT
  - GOOSE MMS client/server control signals
  - FO or RJ-45 patch cable

- **Un**
  - GPS/SV & GOOSE

- **NIC1**
  - MT-RJ

- **NIC2**
  - GPS

- **SV & GOOSE**
  - F6TesT

- **NIC1**
  - MT-RJ

- **NIC2**
  - GPS

- **Switch with FO and RJ-45**
## Test Features – **Isolation** during Maintenance

### Test signals
- **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 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:
- 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**
Devices in **normal service** with Simulation=\texttt{false} will **process** GOOSE messages from real IEDs.
Devices in normal service with Simulation=false will process GOOSE messages from real IEDs.

Device with Simulation changed to true will still continue processing GOOSE messages (with simulation flag = false) from real IEDs, if there are no simulated messages from the test set.
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
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

Beh. stVal = on

Beh. stVal = test

Beh. stVal = test/blocked
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

Incoming Signal
(GOOSE or Report) 
q.test = true

Incoming Signal
(Control service) 
q.test = true

Beh.stVal = test

Invalid
on
Invalid
blocked

Incoming data processed as valid
test

off
Valid, output contact blocked
test/blocked
not processed
Mode/Behavior, Data Quality and Processing

• LD/LN with Behavior = **test** or **test/block** 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**

*Data items that have q.test = false will be processed as invalid*

*This also applies to Control service messages*
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
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
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.

Import SCL files
MMS Client – Data Model, Read/Write, Control, Reports

Watch window – Automatically polls and updates selected data

Client Simulator

Server Simulator

View IED Details and Configuration reports

Discover remote IED

Select IEDs for communication

Save as SCL file

Control operation

Data Name | Data Description | Value Description | Value | Type
---|---|---|---|---
CB1XCBR1.ST.Pos.stVal | Status value of data | Closed | 2(10) | CODEDENUM
CB1XCBR1.ST.Pos.q | Quality of the attribute(s) representing the value of data | | | 
CB1XCBR1.ST.Pos.t | Timestamp of the last change in data value or quality | | | 

Description of values and enumerations

Watch window

Client activity log

Write to server

©2018 Doble Engineering Company. All Rights Reserved
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

Annunciator view - with animated widgets
(user configurable); Detects if GOOSE is missing

Watch windows in Client/Server – Local + Global

Oscillograph views – GOOSE, Report, SV; Save COMTRADE

Logging view- GOOSE & Reports + dataset details
Server Simulator

• Use for simulating missing IEDs during any testing phase

• Use to simulate special test conditions

Table simulation

Direct input

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

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

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

- 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

- Develop automated test plans
  - Normal and test conditions

- 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

- 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