Study Committee B5 Colloquium
September 11-15, 2017
Auckland, New Zealand

PS1-103

PS1 - Challenges of design and maintenance of IEC 61850 based systems

# EXPERIENCES AND REQUIREMENTS FOR COMMISSIONING, TROUBLESHOOTING AND MAINTENANCE OF IEC 61850 STATIONS

| R HUGHES | P EDSTRÖM | A BONETTI | R DOUIB |
|---|---|---|---|
| Rod Hughes Consulting Pty Ltd | Vattenfall | FMTP Power AB | FMTP Power AB |
| Australia | Sweden | Sweden | Sweden |
| rgh@rodhughesconsulting.com | patrik.edstrom@vattenfall.com | andrea.bonetti@fmtppower.com | romain.douib@fmtppower.com |

## Summary

Commissioning and test is undoubtedly an area where we must not compromise, but rather improve, on our requirements to prove that the Substation Automation System is working correctly despite being more complex and less tangible in a virtual environment.

The challenge of an IEC 61850 LAN-based system is being able to “see” the proof and understand the meaning of that “proof”. Sniffer tools can show the series of 1’s and 0’s but this is “mere data, not information”. This can lead to safety issues, a bad quality of response to problems, risky mitigation plans and poor decisions.

In replacing wires with LAN messages, the traditional volts and amps multimeter needs to be replaced by reliable and user friendly LAN compatible tools, and be even more informative about what we are looking at. This paper outlines our experiences over the last 10+ years of supporting the application engineering, consulting and helping customers around the world to deal with network and application issues resulting from commissioning and test of IEC 61850 systems. We have outlined in this paper a set of specific information that needs to be derived from simple sniffing using advanced tools.

The paper therefore describes the issues of cyber security for connecting test devices, the requirements and benefits from use cases describing the technician being able to visualise information, identifying if the messages are in fact as expected from the SCL files, any missing or new messages compared to the SCL and any problems in the configuration of those messages and the benefits in being able to capture records and reports for further analysis and even comparison at the next round of testing.

## Keywords

IEC 61850, Testing, Visualisation, Real-time message validation, comparison SCL-sniff, comparison sniff-sniff

## 1. Introduction

When using a new technology, the methods and procedures used in the past can not always be directly extrapolated for the new technique. Equally, the new technology provides new methodologies that allow users to achieve the same goals of the previous routines. To understand how this can be done, it is necessary to find out the purpose of the previous procedures, and see how the new technique can be used to get the same outcome: the confidence that the system will operate reliably in-service.

Commissioning tests are performed in order to set-up the system until its functionality is confirmed. The maintenance tests are to verify that the system is still running correctly and are therefore a more restrictive subset of the commissioning tests. Figure 1 shows a schematic representation of the process involving commissioning and maintenance tests.

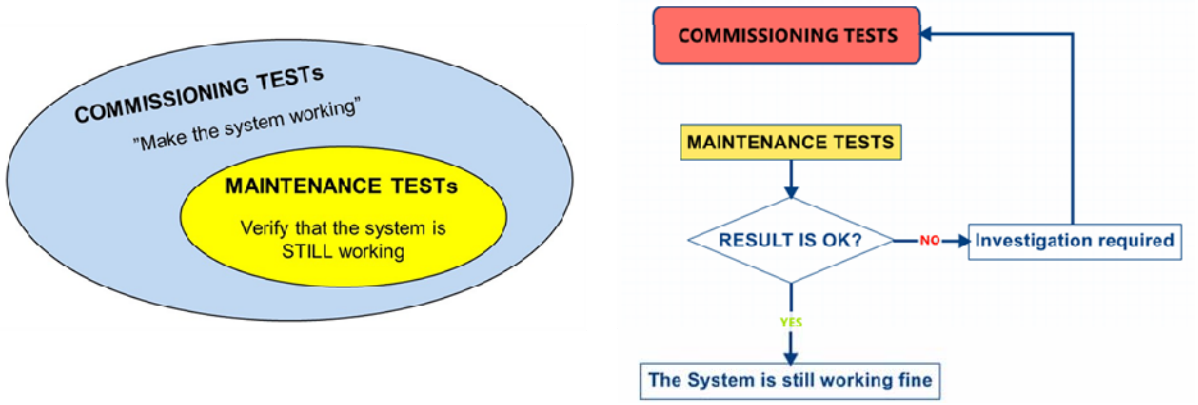


**Figure 1** – Commissioning and maintenance tests. Symbolic representation and flow diagram.

Maintenance procedures associated with older electromechanical and “wire-based” technologies demanded isolation of devices from the system and direct full testing of the devices to verify their operational status – an invasive procedure involving power system switching and outages for safety of the grid and personnel.

Once the system is based on numerical devices and they are in service, it makes a lot of sense to use the numerical technology to get information about the status of the system and its components as a “non-invasive” process. This is especially true given the higher degree of “virtual” aspects of the system in its configuration operation – after all, IEC 61850 is an engineering process to configure IEDs to communicate.

Key procedures for maintenance can now include non-invasive comparison actions: e.g. compare the previous proven correct status of the system with the current “unknown” status; if no differences are found, it can be concluded that the system is still running correctly, at least as previously proven before being placed into service. If there are some differences, some investigations are needed to find the cause of the difference. This activity can be seen as a sort of numerical “checksum” used in data transmission; the key is to identify which parts of the system are able to give a reasonable representation of its healthy or fail status in order to minimize the number of tests.

Experience has shown that maintenance and operation considerations should be included from the start of at the design phase in order to ensure efficient ownership and harmonization between substations supplied by different Systems Integrators. Just as “designing in” CT shorting and isolation links because they can’t be added when the system is in service, so must the testing requirements be considered even though the virtual environment is more flexible. Modifying the system configuration to enable a test is not necessarily testing the operational system and may be just lead to testing your modification!

A clear Utility strategy on the implementation of IEC 61850 is the key for successful operation, maintenance and future-proof substations. Things that are not mandatory in the IEC 61850 standard itself can easily become mandatory for a particular Utility or for a particular project. This is totally in accordance with the principles of the Standard as establishing an implementation “profile” for the particular Utility.

## 2. Key experiences

There are well over 10 thousand substations with various degrees of IEC 61850 implementation around the world. Naturally these have been thoroughly tested using various tools such as “network sniffers” (e.g. Wireshark) and the test set vendors analysis tools. The general experience of these tools is that they provide visualization of the bits on the wire, but very rarely any meaning for the purposes of :

- Showing the meaning of messages for the purposes of debugging
- Verifying the system has been correctly configured
- Verifying the system has not been modified since its last verification and performance tests
- Identifying system performance issues
- Aiding the use of test sets not supporting IEC 61850 functionality

### 2.1. Inspecting message headers

When we look at a typical GOOSE message “sniff”, we can see all the header information such as VLAN configurations, Multicast filters, Destination MAC Addressing, IP addresses and other aspects essential for correct operation of IEDs using LAN-based signals. We can even see the specific IE 61850 components in the message as defined in IEC 61850-8-1 Ed 2 Table A.1.

**Table A.1 – Encoding allData in Fixed-length GOOSE message – the GOOSE Header**

| Abstract Buffer Format according to IEC 61850-8-1 | | ASN.1 Tag for Data | ASN.1 Length | Comments |
|---|---|---|---|---|
| Attribute name | Attribute type | | | |
| goCBRef | Visible-string | 0x80 | | Length determined by SCL configuration |
| timeAllowedToLive | INT32U | 0x81 | 5 | 32 Bit Big Endian; unsigned; see Table A.3 |
| datSet | Visible-string | 0x82 | | Length determined by SCL configuration |
| goID | Visible-string | 0x83 | | Length determined by SCL configuration |
| T | UtcTime | 0x84 | 8 | 64 Bit timestamp as defined in 8.1.3.7 |
| stNum | INT32U | 0x85 | 5 | 32 Bit Big Endian; unsigned; see Table A.3 |
| sqNum | INT32U | 0x86 | 5 | 32 Bit Big Endian; unsigned; see Table A.3 |
| simulation | Boolean | 0x87 | 1 | 8 Bit set to 0 FALSE; anything else = TRUE |
| confRev | INT32U | 0x88 | 5 | 32 Bit Big Endian; unsigned; see Table A.3 |
| ndsCom | Boolean | 0x89 | 1 | 8 Bit set to 0 FALSE; anything else = TRUE |
| numDatSetEntries | INT32U | 0x8a | 5 | 32 Bit Big Endian; unsigned; see Table A.3 |

**Figure 2** – GOOSE Header elements IEC 61850-8-1 Ed 2 Table A.1

This information includes <<stNum>> which is incremented each time an element in the dataset changes value – this does not change in the subsequent retransmission “heartbeats”. This can therefore be used to identify if any state-changes have been missed.

The <<sqNum>> is reset to zero when <<stNum>> is incremented so a value of “45” would mean there have been 44 previous identical messages since the last dataset change. This can be used to check if all the retransmission messages have been received and in the correct order.

Both of these pieces of information can be used in testing of so-called “bumpy” networks, e.g. RSTP, where messages may disappear for a few tens to 100’s of ms or more during ring re-convergence periods. It is also a useful performance indication for so-called “bumpless” networks defined under IEC 62439-3 where messages would normally arrive at one port before the other, but may suddenly change due to network issues. Hence it is still important to verify how little that “bump” is, indeed that the recovery or “bumpless” mechanism works.

### 2.2. The Meaning of Time

Time synchronisation is not absolutely necessary for Protection function related GOOSE - the system will work with all IEDs running independent clocks. In fact most system integrators do not include the event time stamp in the GOOSE message e.g. the <<PTOC.Op.t>> information of when the <<PTOC.Op.stVal>> changed from 0-to-1 or vice versa. That is reasonably logical as “wire-based” electromechanical and electronic “conventional” protection relays have worked for decades without knowing what time it was when the relay operated!

Sampled Values (IEC 61850-9-2), MUST have better than 1microsecond COHERENCY of time synch across all Merging Units. This is because the 1-second sampling windows in all IEDs must start at precisely the same instant and so the subscribing IEDs know that sample number “2345” in each message was taken at the same instant. IEEE 1588 v2 PTP and associated IEC/IEEE 61850-9-3 Profile is really the only option to achieve this. However the actual <<yyyy/mm/dd hh:mm:ss:000:000>> time stamp of the sample is irrelevant. Time stamps of the samples are not even included in the SV frame as they would just make each message far too long for the latency requirements and bandwidth of the networks.

However in LAN based system tests, there is an inherent interest in time – the time of the event and the time taken to deliver the information to the next IED that uses the information.

The “infamous” 4 millisecond GOOSE latency is critical to ensuring protection system performance. Looking at one sniffed message, we can see the message includes the <<T>> that THIS particular message was created. If the IED and the sniffing test set is synchronised to the same clock, some analysis can be undertaken to verify the network latency. Timing tests of which message arrives before another is dependent on where the sniff is done in the network relative to the connection of the two publishers.

However <<T>> is totally irrelevant to when the last event change of state happened. It might be possible to some very extensive maths based on <<sqNum>> telling you how many retransmissions of the same status have occurred. However if the message has several elements, you would only calculate the time since any one of the elements last changed state, e.g. the last change of the dataset may relate to element #5 which changed state “three days ago” which of course may not be the element you are testing right now. Moreover, if an IED has two changes of state in the dataset say 100 ms apart, they each would cause a new <<stNum>> and start a new GOOSE fast retransmission cycle.

Testing and debugging is highly reliant on knowing when something happened, at least relative to some other event. However most GOOSE configurations we have come across don’t include the time stamp of the last change of each element in the data set. That would need one time stamp for each element which would quickly explode the overall length of the GOOSE message. This would be counter-productive for the normal in service 4 ms latency requirements of the network. Whilst it may be possible to reconfigure the IEDs to add extra test-specific GOOSE messages with time stamps, this would clearly interfere with overall network performance, and of course we are no longer testing the in-service configuration.

## 2.3. Inspecting datasets

Just “seeing” the messages does not help to visualise the relative timing of events during the sniffing process. New tools are needed to detect and display changes of state of specific elements, and in particular being able to focus on specific GOOSE from a specific IED amongst the dozens /hundreds of different GOOSE appearing on the network

We can even see the value of the elements as 0 or 1, but the message itself does not tell us what that 0/1 represents in a functional perspective as the value of a IEC 61850-7-3 “Single Point Status” <<PTRC.Op.stVal>> or half of a “Double Point Status” <<XCBR.pos.stVal>> or perhaps one bit in a 32-bit time stamp! Every message and every sniff must therefore be analysed with some form of documentation of the SCL configuration files to hand making it very difficult to quickly verify and debug the system operation.

Tools are needed to “record” the sniffed GOOSE identification such that the next time you visit the site, the sniff will be identified with the same names as used previously.

## 2.4. Using “legacy” test sets

Of course we cannot gloss over the fact that over the decades of “conventional” wire-based protection systems, we have acquired a significant fleet of “conventional” test sets that have no direct interface and capability for dealing with IEC 61850 communication mechanisms. New IEC 61850 capable test sets are a significant additional cost and hence we need additional tools that aid in use of conventional test sets with IEC 61850 systems in hybrid arrangements.

As seen in the following diagram, the overall test equipment has to provide mechanisms for:

- Inject current/volts
- Measure current/volts
- Monitor status (open/closed, on/off, ..)
- Publish GOOSE / SV
- Subscribe to GOOSE / SV (to start/stop tests and measure time)
- Interpret GOOSE / SV (for humans)

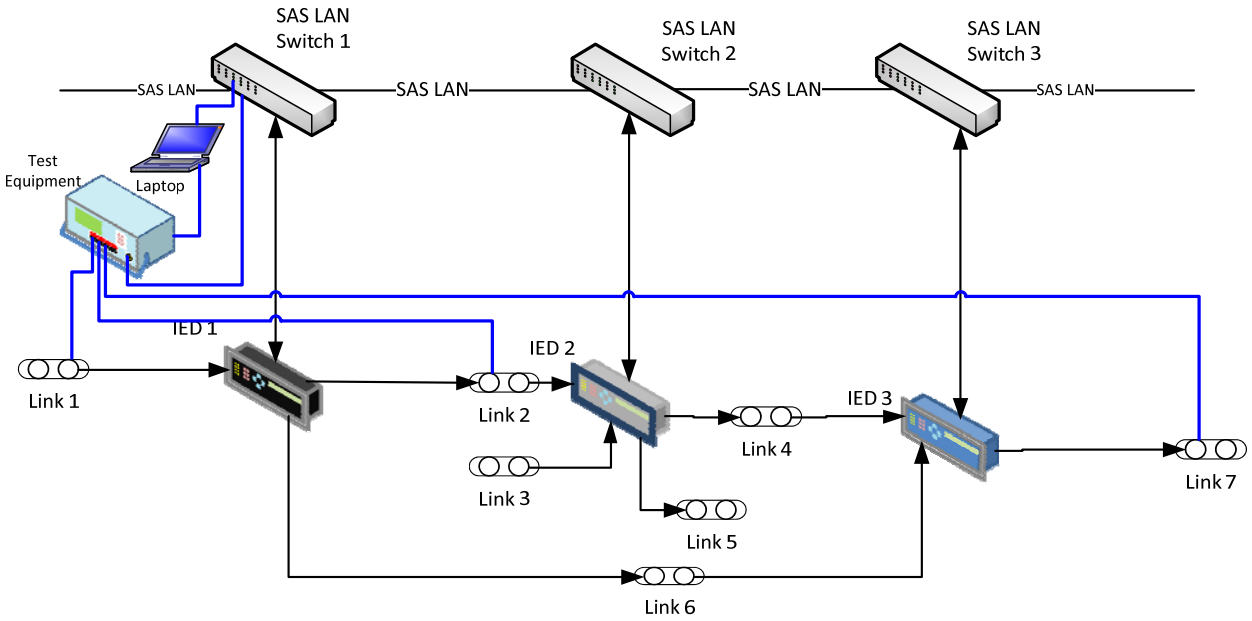


**Figure 2** – Test interfaces for hybrid Wire-LAN systems.

In order to maximize the ongoing utilization of non-IEC 61850 capable test sets, as shown in Fig 3, facilities are required to start/stop the sniffing process and start/stop the test set for

curve/timing accuracy tests. Verifying relay time curves of course demands minimum time delay of < 1 ms between GOOSE reception and registering that in the conventional test set and its timing analysis.

The test equipment operate connected to one LAN or connect to two different LANs such as Station Bus and Process Bus, Each port also needs to be used as either RJ45 cables or Fibre Optic to match the LAN switch connection.

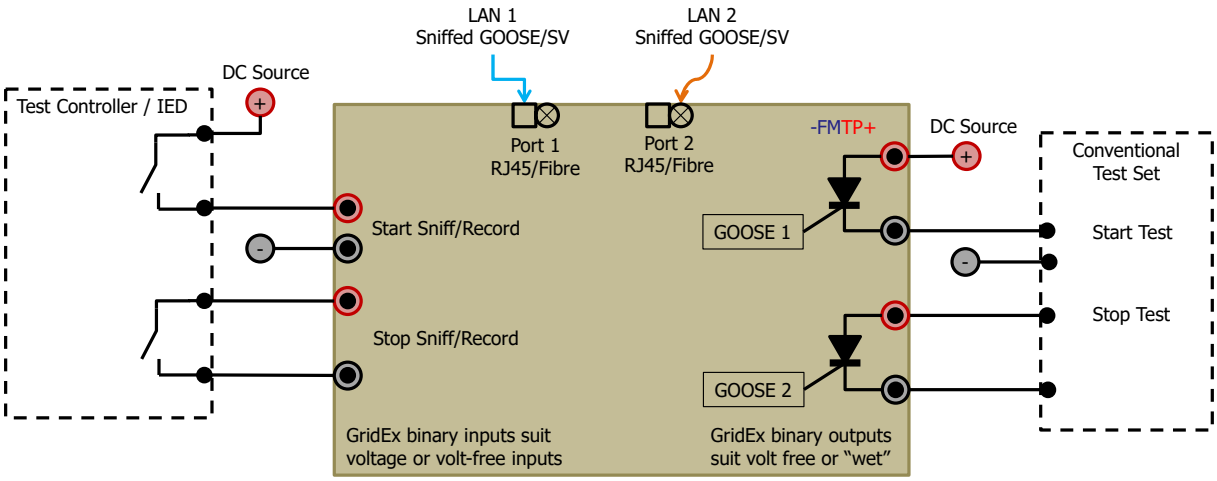


**Figure 3** – Interfacing IEC 61850 sniffing with wire-based test facilities.

### 2.5. Is it what is expected by design? Has it changed?

It is certainly helpful to capture a series of messages on the LAN. Amongst the key objectives of any testing is to verify the configuration as evidenced by what is actually appearing on the LAN, is as expected by design i.e. the right configuration has been loaded to the IEDs. This extends to verifying the message configurations have not changed since the system was last verified. It has also been necessary to identify when IEDs have been added, removed or swapped on the network which add/remove/change the GOOSE messages seen on the LAN. Identifying changes of physical IEDs has allowed identification of "rogue" hardware/firmware versions on the LAN and/or miscommunication and erroneous performance of the SAS.

Equally in reverse, it is critical to verify the system documentation does in fact reflect not just the "as built system" (a fabled concept for wire based systems, or at least not available instantly after energization), but more importantly the "as operating" configuration of the system. Practical completion of a project is usually associated with handing over the site to the asset owner for operational use … AND provision of the so-called "as built" diagrams. Wire based systems rarely have the "as builts" delivered at hand over, sometimes it is months later and even so may not be 100% accurate. There is a significant blackout event in Australia more than a year after the end of the warranty period of the project which subsequent investigations revealed that the CD Rom supposedly containing all the "as built" records and test sheets was in fact just blank forms! No-one checked the contents of the CD Rom.

Hence it is vital to be able to verify, and provide automated documentation of that accordingly, that the "as built" SCL files provided by the Systems Integrator do in fact represent the "as operating" configuration of the substation.

## 3. Main methodologies and tools for commissioning and maintenance

### 3.1. Extended use of supervision mechanisms.

The IEC 61850 standard expects IEC 61850 devices to perform self-supervision tasks; as example in the quality string of the data attributes there is one bit dedicated to “failure” (see Figure 4). This bit is intended to be raised when the device detects an internal failure, hence it is the result of the self-supervision in the device. Many more other similar examples can be found in the standard.

Table 2 – Quality

| Quality type definition | | | |
|---|---|---|---|
| Attribute name | Attribute type | Value/Value range | M/O/C |
| | PACKED LIST | | |
| validity | CODED ENUM | good \| invalid \| reserved \| questionable | M |
| detailQual | PACKED LIST | | M |
| overflow | BOOLEAN | DEFAULT FALSE | M |
| outOfRange | BOOLEAN | DEFAULT FALSE | M |
| badReference | BOOLEAN | DEFAULT FALSE | M |
| oscillatory | BOOLEAN | DEFAULT FALSE | M |
| failure | BOOLEAN | DEFAULT FALSE | M |
| oldData | BOOLEAN | DEFAULT FALSE | M |
| inconsistent | BOOLEAN | DEFAULT FALSE | M |
| inaccurate | BOOLEAN | DEFAULT FALSE | M |
| source | CODED ENUM | process \| substituted<br>DEFAULT process | M |
| test | BOOLEAN | DEFAULT FALSE | M |
| operatorBlocked | BOOLEAN | DEFAULT FALSE | M |

**Figure 4** - The “quality string” associated to a data attribute, IEC 61850-7-3 Ed2

The correct use of the quality during the substation design is a very important concept in order to simplify the commissioning and maintenance procedures, where it is important to be able to pinpoint in a short time which parts of the system may be affected by a failure.

At the Station HMI level, it is very important to clearly verify the desired processing of the data quality indication, which contains many more information that the one described in the above example. Also the time contains quality information and the SCADA system should be able to interpret it and give relevant messages to the operator.

The horizontal substation communication (GOOSE) can also be supervised at IED level and correct information can be sent to SCADA system (Station HMI) activating the investigations when they are really needed. The communication protocol for GOOSE messages allows the possibility of implementing supervision of the horizontal communication at the receiving IED. This means that the receiving IED is able to understand if the “sender is lost” for any reason (interruption of the communication path, failure in the sender).
This method is based on the supervision of the repetition GOOSE messages (see Figure 5).

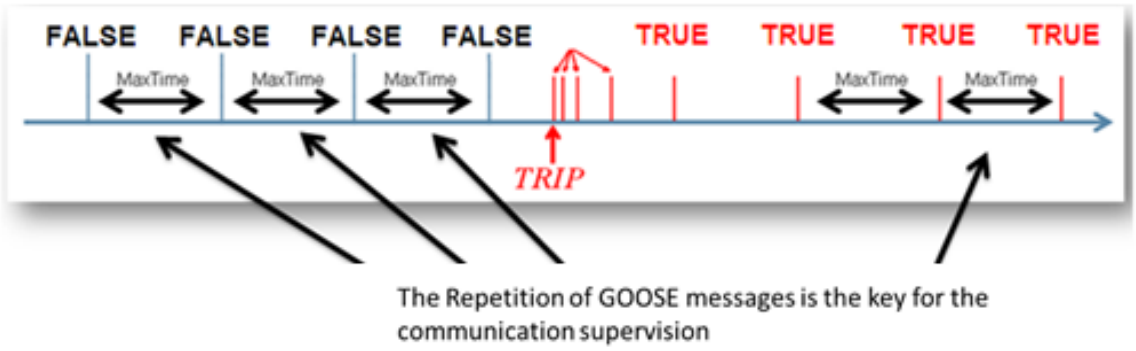


**Figure 5** - The “repetition mechanism” of GOOSE messages allows implementation of the

supervision of the communication path between the sender (publisher) and the receiver (subscriber). We here show the change from a FALSE to TRUE after a TRIP

The mechanism of the communication supervision can be explained in this way: when a GOOSE message is received, the receiver looks at the “timeAllowedtoLive” written in the message (this value is directly related to the SCL attribute “MaxTime” for the GOOSE message). Typical values of these times are of the order of seconds. Supposing the value to be 5 seconds (5000 ms), this means that the next GOOSE message must be received within 5000 ms. If a new GOOSE message is NOT received within this time, the communication with the sender is lost and a warning signal can be raised in the receiving IED, or test device.

The detection of a failure in the horizontal communication has several benefits for the behavior of the substation: for maintenance purposes it is possible to have information about failures in the communication between two particular IEDs; for the protection and control application this detection can be used to increase the security of the protection scheme whenever the GOOSE messages are used for the implementation for schemes like direct intertrip, reverse blocking etc. avoiding for instance unwanted trips due to lack of functionality in the communication scheme (a very common situation in the conventional technology, unfortunately).

There are already instruments on the market that detect the loss of communication based on the above mechanism. Figure 6 shows some warning icons (“Ghosts”) informing that the particular GOOSE messages have been lost, so they did not reach the test instrument within the expected time.

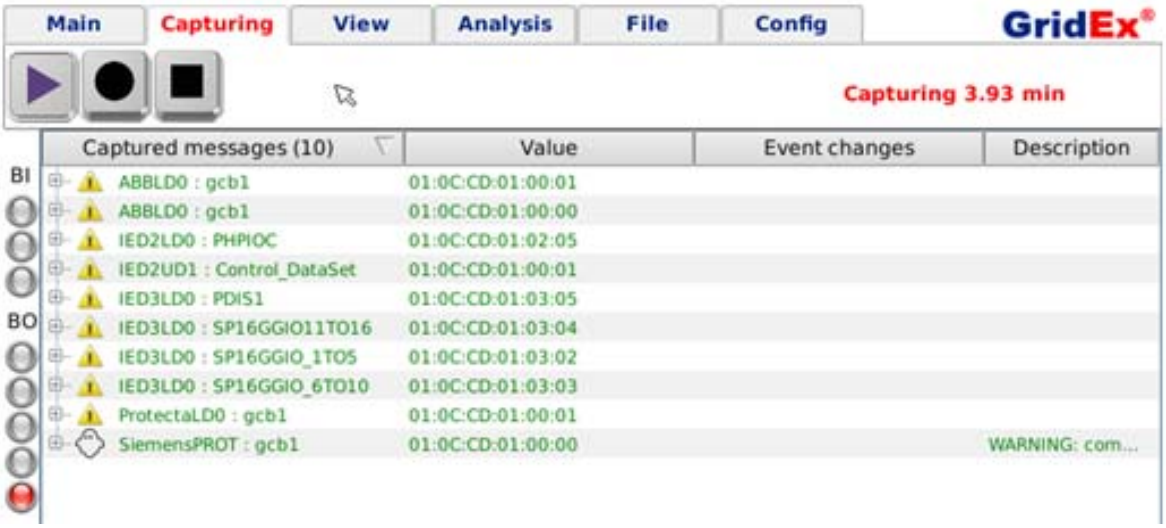


**Figure 6** – Example of detection of loss of reception of a particular GOOSE message, indicated with the “Ghost” icon. (FMTP GridEx)

Figure 7 shows a graphical representation of an analog signal (frequency measurement) sent through a GOOSE message together with its quality attribute. The quality is represented in the line below the value of the signal. It can be seen that the frequency was almost 50 Hz for a while, and the quality is good (black color). Something then happened and the delivered frequency was negative. The publishing IED was informing that the published value was not trustable (quality invalid, red color), so the receiving IED was supposed to not report that negative vale of the frequency on its local HMI (which it did instead). The publishing IED was removed from the network (pink area) and later on reconnected to the network in test mode (yellow quality). At the end it was put in normal service again. Without entering in the details of the troubleshooting of this situation, it appears clear that a simple visualization of information and the reporting of it allows to pinpoint the possible source of the problem and efficiently address the technical resources to its solution.

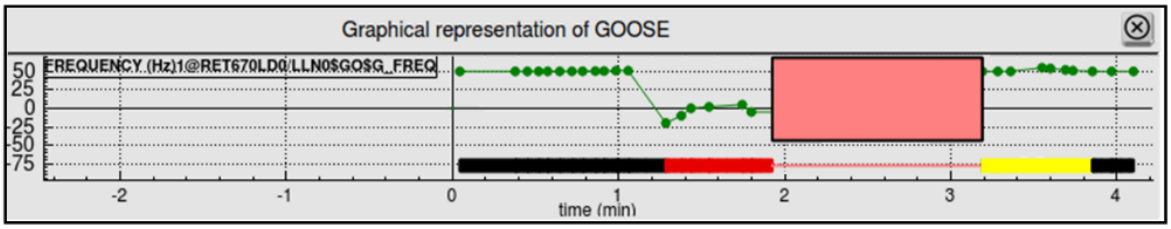


**Figure 7** – Graphical behavior of an “analog GOOSE” carrying the power frequency value and its quality (FMTP GridEx).

The successful implementation of the horizontal communication supervision requires a correct specification of it, it needs dedication during the design phase as well as it needs to be tested during commissioning.

The Vertical Communication (communication between Station HMI and Station devices) can be also be supervised with relatively simple client / server TCP/IP based “ping” mechanisms. Once this is implemented it is very easy to understand, when the substation is in service, which parts of the system are not communicating anymore. Even in this case it is never enough to stress the fact that this implementation, technically possible, must be specified, engineered and tested.

### 3.2. Compare the GOOSE traffic with the substation master SCD file (consistency check).

The “as built”, even “as operating” configuration of the communication within an IEC 61850 substation is represented by the Substation SCD file, although many projects have not demanded this single source of truth from the system integrator and will suffer accordingly.

As maintenance activity, a network scanning of the network traffic and the comparison with the network traffic described in the SCD file is a good indication if the result shows “no differences”. We can therefore conclude that the design files have been correctly loaded to the IEDs, and in turn that the design files still reflect the current configuration of the IEDs i.e. the “as operating” configuration. In case of differences, it is very important that the tool responsible for the comparison gives focused information on where it has to be investigated.

This activity is already in use for FAT / SAT, where there is the need to validate the SCD file provided by the system integrator to the customer. If the comparison shows that there are some missing GOOSE messages or too many GOOSE messages or some messages are slightly different to what described on the Substation SCL file, the file cannot validated. Figure 8 shows an example of comparison between the GOOSE traffic in the substation network and the SCL file describing the substation (SCD file). Green result means that there are no differences between the GOOSE message detected on the network bus and the GOOSE message described on the SCL file, Red and Yellow results mean that several differences have been found, so in these cases that differences need to be explained. The yellow cases try to help the user in understanding what the difference could be and why. These detailed information are also shown in the final report.

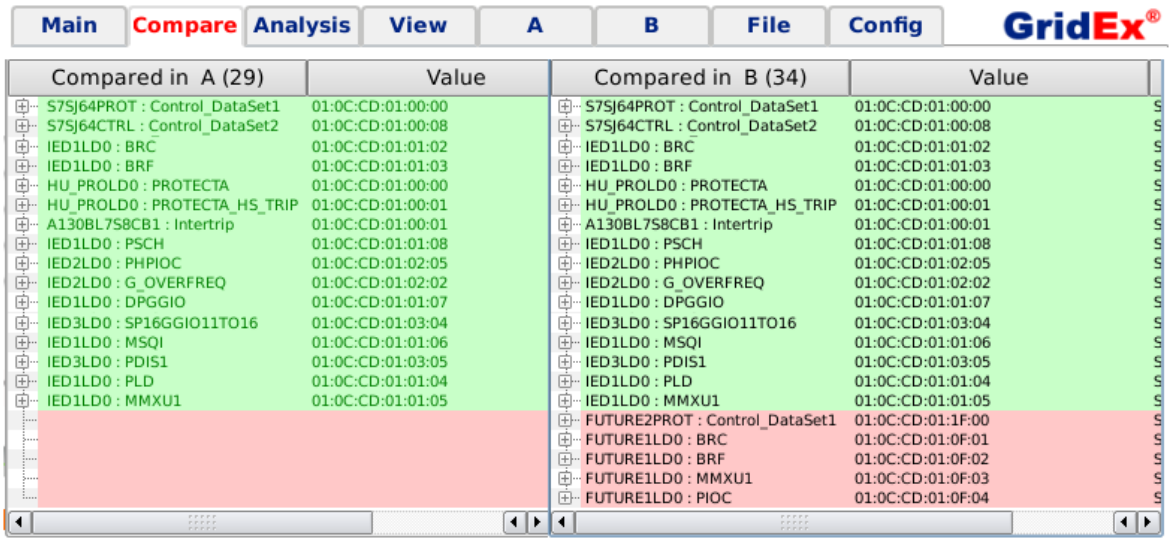


**Figure 8** – Example of comparison between network GOOSE scan (left column) and SCL description of the GOOSE traffic (right column). (FMTP GridEx)

### 3.3. Compare the GOOSE traffic scan with previous network scan

The horizontal communication traffic (GOOSE traffic) can be compared, from the functionality point of view, to the “binary input / binary output traffic” of conventional substations, where the binary outputs of several devices and apparatuses are connected to binary inputs of other devices or apparatuses, as well as SCADA/RTU equipment. This is done for signaling purposes, interlocking schemes as well as for protection schemes.

Some important parts of this “traffic” are usually monitored in the conventional technology, typical example is the so called trip circuit supervision. It is not common –however- to monitor all the binary inputs and outputs of the relays and compare the result of this monitoring with the result of a previous monitoring. It would be too expensive, too complicated and also probably not feasible.

The GOOSE traffic can be monitored in a relatively easy way (network sniffing), and the comparison with a previous network scan is -in principle- not complex. Also with this activity, if everything is the same, it’s a good sign. If some differences are found, investigations are needed and again it is very important that the tool gives good and significant information on where the differences are.

Figure 9 shows an example of comparison of two different scanned GOOSE messages in the network. Green result means that no differences have been found, Red and Yellow results mean that several differences have been found, so in both cases the differences need to be explained. The yellow cases try to help the user in understanding what the difference could be and why. These detailed information are shown in the report.

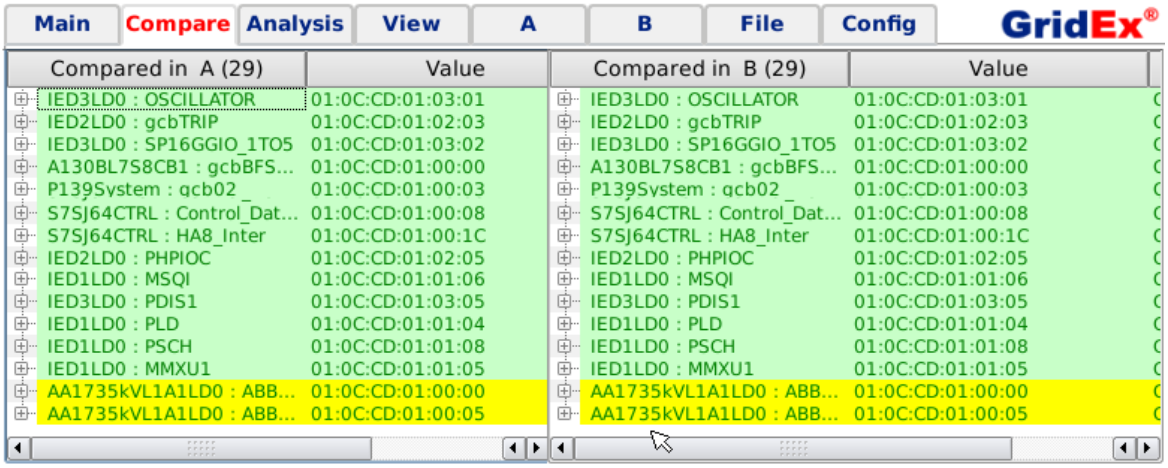


**Figure 9** – Example of comparison between two different GOOSE scans of the same substation. (FMTP GridEx)

### 3.4. Protection Relay setting comparison.

Also this concept described is based on “comparison”. The protection relay master settings are stored in a central database. These are the finally approved settings that are also stored in the protection and control devices (protection relays, bay controllers, switches, substation clocks etc).

The activity maintenance is based on comparing those settings with the setting values that are read directly from the protection devices. A warning flag is raised by the maintenance activity in case this comparison should give some differences, and of course investigations are started to understand the cause of the difference.

The role if IEC 61850 standard in the above procedure is to provide the technical community with a standardized way to store the relay protection settings in the SCL files. This would allow easier methodology for storing the relay protection settings in what is already accepted by IEC 61850 community that SCL files are the key of the engineering and documentation processes.

Apart for IEC 61850 standard, implementing this concept requires Utility strategy, database tools and vendor tools for the protection and control IEDs that allow this comparison to be done. These tools exist already and are used by several utilities in the world, but not all protection devices have tools with such comparison capability, and this of course restricts the choice of the devices to be used in the substation.

### 3.5. Extended use of post-event analysis for preventive maintenance.

Disturbance Fault Recorder (DFR) files contain important power system information like the waveforms of currents and voltages after and before the ”perturbance” or the event and the Sequence Of Events (SOE) like relay operation (trip) with open command, autorecloser start, autorecloser close command, blocking signals sent to other relays, important internal relay device signals, position of primary apparatuses.

The combination of all this information, together with the information from disturbance recorder files from other devices (in the same bay, in different bays or in a different substation), allows to perform a post-analysis to verify the correct/wrong behavior of the protection system and decide actions to improve the system performance or pinpoint deficiencies/defects in equipment and apparatuses. It is important that the events from different devices can be time-correlated, i.e. that the devices in the substations and possibly in different substations are time synchronized.

Through the post-fault or post-event analysis activity it is possible to:

- detect incorrect relay settings and give facts supporting their improvement
- verify relay coordination
- verify relay and primary objects performances
- determine the position of the fault (fault location)
- perform asset condition monitoring (preventive maintenance)

Retrieving the disturbance files has been a complex task in the past: proprietary vendor software was necessary to retrieve the information, proprietary communication protocol, lack of fast and reliable communication structure to transmit the disturbance files to a central location. The IEC 61850 standard provides all the elements to facilitate this process by providing these standardized elements for all vendors:

- the definition of Logical Nodes associated to disturbance recorder (RDRE, RADR, RBDR)
- the communication protocol for file transfer (FTP or MMS)
- the communication media (Ethernet, 100 Mbit/s or 1Gbit/s)
- the file format to store the recorded waveforms and binary signals (COMTRADE)
- the location where the files are stored in the IED (root, folder COMTRADE)
- the time synchronisation method for IEDs accurate enough to perform this activity (SNTP, practical order of accuracy +/-1 ms)

It can be said that the IEC 61850 standard has made it difficult to justify the absence of this type of data collection. The rest that needs to be done is to slowly change the attitude towards preventive maintenance based on post-event analysis by understanding that in the long term this activity heavily contributes in reducing the costs associated to maintenance by reducing the activities during periodic maintenance and also by prolonging the time interval between the activities.

### 3.6. Upfront information to the user in Power System language

IEC 61850 is for a lot of protection and control engineers still a new technology. Tools that are able to translate the numerical information into the most relevant power system information in a simple way are of great benefit as they minimize the gap between the numerical communication technology and the power system competence, letting the power engineer able to handle with confidence the new technology by minimizing the risk of misunderstanding in the interpretation of the data.
Figure 10 and Figure 11 represent a tool that shows the protection and control signals to the engineer, hiding as much as possible the complexity of the communication protocol. It is possible to associate the relevant signal information available in the GOOSE message to a so called “Visualizer”, and the user can decide to work only with “Visualizers” abandoning any message or tree view of the GOOSE or Sampled Value messages.

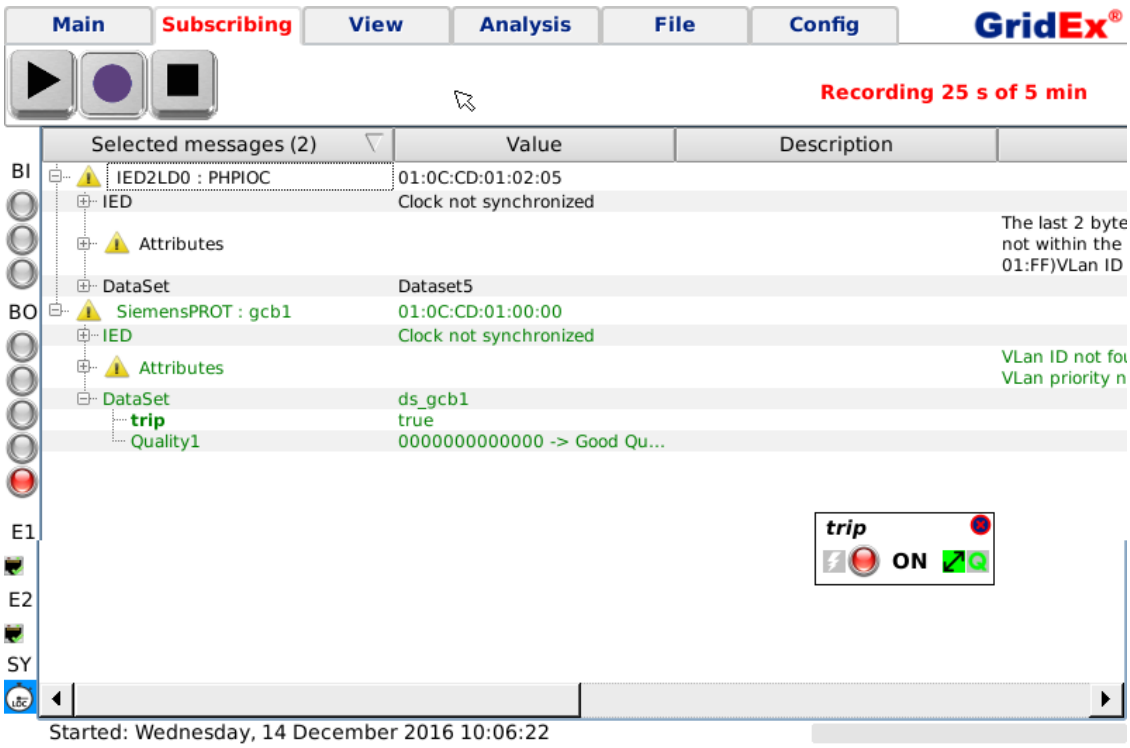


**Figure 10** – The “Visualizer” shows to the user the most important information available in the GOOSE message (FMTP GridEx: Tree view and Visualizers are both shown for better understanding).

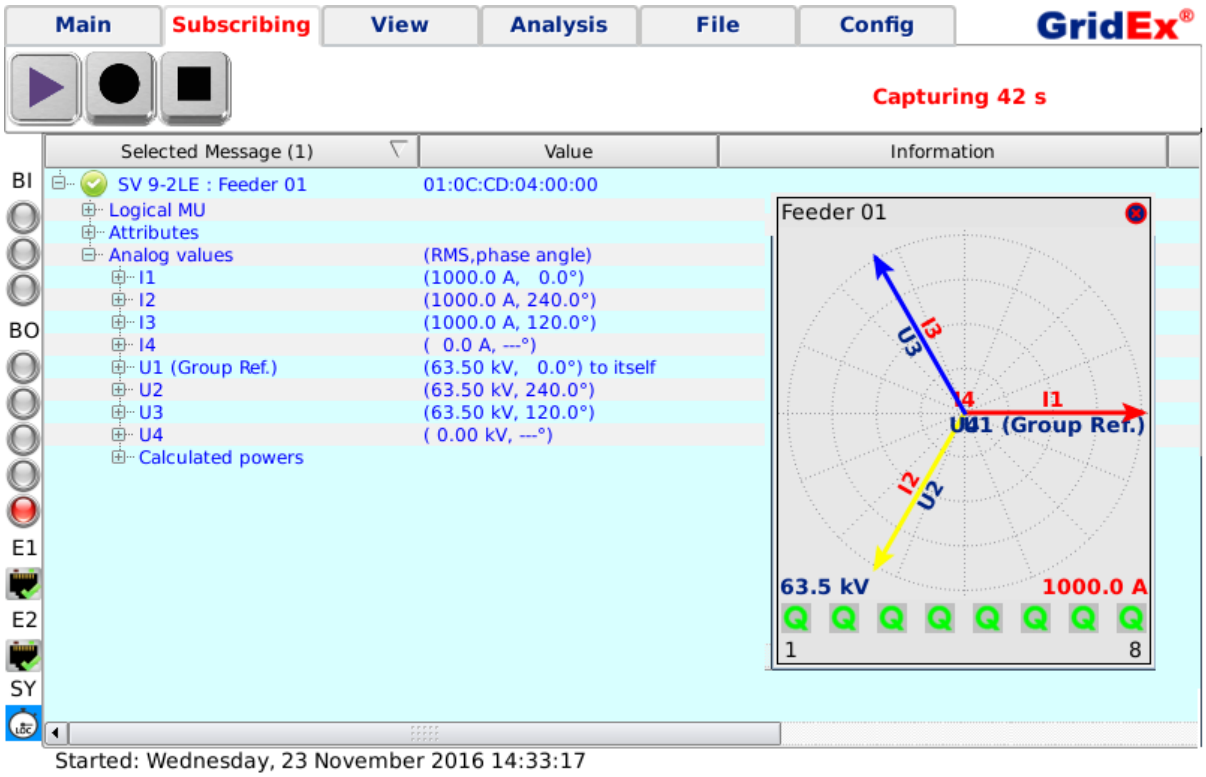


**Figure 11** – The “Visualizer” shows to the user the most important information available in the Sampled Value data stream (FMTP GridEx: Tree view and Visualizers are both shown for better understanding).

### 3.7. Equipment and tools for a secure connection to the substation buses

Cyber-Security is a very hot topic during maintenance of an IEC 61850 substation. In order to be able to perform the majority of the tests mentioned in this paper it is necessary somehow to connect test instrument to the LAN. Many Utilities simply do not allow anyone to connect PCs/laptops/tablets/smart phones to the substation network as they may have viruses, or may open a communications access path inside the firewalls which hackers and viruses could infiltrate. Sniffing a network is a common test diagnostic, but sniffers installed on PCs therefore should not be used. Connecting a device to the network which can do anything more than sniff is simply not permissible.

New stand-alone test equipment do not need any PC to run; the firmware cannot be upgraded “on line” which severely limits opportunities for viruses to be implanted.. The device (Figure 12) is also fully “passive”, which means it does not (per design) inject (send) any IEC 61850 signal in the network that it is “listening to”. This allows the maintenance engineer to comfortably connect the device to the substation network when the substation is energized, with the 100% certainty that if “something happens” after this connection, the cause of it shall not be searched in the device itself.


**Figure 12** – A stand-alone IEC 61850 test equipment. (FMTP GridEx)

## 4. Conclusions

All the activities described in this paper need instruments and tools to be allowed to be performed in an easy and efficient manner. They also require a clean strategy in the application of the IEC 61850 standard, which means a clear technical specification providing engineering workflow methodology (SCL Engineering, as built SCD file as part of the Substation delivery), direct engineering guidelines (use of the <<.q>> “quality” bit for instance, to remain within the themes discussed), provision of one “substation network access point” to allow maintenance activities to be performed or one dedicated service computer for the same purpose. Instruments and tools are available on the market, and more will come to further contribute to maintenance and any other activity.

Clear Utility strategies on the implementation of the standard are seen to grow in several parts of the world but they should probably grow more to allow a smooth engineering, commissioning and maintenance.

The IEC 61850 substation, in very few words, can be considered as a standardized numerical system. As numerical technology is the basic competence of the new generation of engineers, they are here to stay. The best is to contribute to make them to grow in the correct direction so that we all can get the best of their advantages.

Certainly new testing methods are part of that evolution – using more advanced tools to tell us more about what is happening, and importantly if it is what we expect to happen, with automated documentation evidence.

## 5. About the authors

Graduating from Sydney University in 1980, **Rod Hughes** has over 36 years' experience in the power industry across Australia and internationally specifically involved in protective relay, instrumentation and metering solutions. Rod's application experience is acknowledged world-wide and covers the earliest moves from electromechanical relays to electronic, microprocessor, communicating and numerical relays, and has been a champion of adoption of IEC 61850 in the region. He has served in senior management roles with a vendor (including living in France for three years), transmission utility and consulting firms. His own private consulting firm was established in 2009 focused on application of conventional and IEC 61850 systems and "technology change management" advisory services. Rod has provided many highly acclaimed protection application courses to hundreds of protection specialists across Australia and New Zealand. Over the last 8 years he has become one of the few industry recognised vendor-independent Australian trainers for IEC 61850. Keen to assist the industry at large, he is a prolific contributor to protection and IEC 61850 forums on LinkedIn. He is one of the longest serving members of the CIGRE Australia B5 Panel and was the previous Convener of the Australian Panel with two Merit Awards.

**Patrik Edström** received his Electronic Engineering degree from technical college in Östersund Sweden 1983. After military training in The air force as an airplane technician. Started to work for Vattenfall division BTM. 1985 - 1993 as a commissioning Engineer. Rebilling and upgrade hydropower stations and building new distribution and transformer stations. 1994 back to school and got my Certification on system voltage up to 420 kV, as electrical engineer in Westbergska skolan Västerås, Sweden. From 1995 to 2006 Patrik worked at BENIMA as consultant with commissioning and technical specialist for relay protection in Malaysia, K.L. USA, New York, Denmark, Copenhagen and Ålborg. For ABB, ADTRANS, BOMBARDER, AREVA. From 2006 - 2011, Vattenfall Services Nordic AB, Sundsvall, as technical specialist on relay protection and control equipment. From 2011 to 2015 Patrik worked for the consulting company AF (Ångpanne Föreningen) as senior expert in relay protection and commissioning with IEC 61850 implementations, where in parallel with the follow up of the projects he also started a relay protection and commissioning group in AF Sweden. From 2015, Patrik is employed at Vattenfall Services Nordic AB, Sundsvall as a technical project manager.

**Andrea Bonetti** was born in Bergamo, Italy, 1966. In 1993 he received his MSEE degree from Universitá La Sapienza of Rome, Italy. Between 1998 and 2008 Andrea worked as high voltage protection relay engineer for after sales customer support and training at ABB Substation Automation Products in Västerås, Sweden, with main focus to line protection relays and applications. From 2008 to 2012 Andrea worked at Programma/Megger in Stockholm, as product manager and technical specialist for relay test equipment where he worked on the development of IEC 61850 compatible test set and tools, test algorithms for distance protection and transformer differential protection relays.
After having worked 2012 and 2013 at STRI AB as technical manager for the Substation Automation Unit, Andrea works now at FMTP POWER AB as technical manager.
Andrea holds a patent in the area of IEC 61850 testing tools and algorithms for protection and control applications.
Andrea is member of the IEC TC95/MT4 since 2006; has been sub-group leader for the development of the IEC 60255–121 standard and has received the IEC 1906 Award for the contribution to the development of the IEC 60255–121 standard in 2013.

**Romain Douib** is General Manager at FMTP Power. He received his Master's degree in Electronic Engineering, from the CNAM Conservatoire National des Arts et Métiers, Paris in 1991. He started his carrier as manager for the Automation and Instrumentation Service team at SIEMENS France, Paris. Moved to Sweden in 1992 has been with Programma Electric AB, GE General Electric and Megger for 20 years. He worked at Programma Electric, Division Manager for HV Circuit Breaker, Manager for R&D Dept., Manager for

Product management, Customer service Dept. management. At GE he held the responsibility of EMEA Area Manager, for Automation, M&D and Test Products and Services. The company got bought by Megger, and he became Manager for Product Marketing, Product management and Customer service for the following application areas: Test equipment for Relay Protection, Circuit Breaker, Battery and Primary power equipment. Romain is currently Owner and General Manager for two companies in the energy sector: FMTP Power AB, Product & Services for Smart Grid IEC 61850 in the Power Industry and House of Specialists AB, a consulting company for long term projects, since 2013.

## 6. References


[1] “Considerations on maintenance strategies for data communication assets in power distribution utilities”, Mikael. Nordman; Lars Nordstrom, Power Engineering Society General Meeting, 2006. IEEE, Montreal, Quebec, Canada, June 2006,

[2] “Transfer time measurement for protection relay applications with the IEC 61850 standard”, Andrea Bonetti, R. Douib, 2010 IEEE International Symposium on Electrical Insulation, San Diego, CA, USA, June 2010

[3] “Implementerings & Nyttovärderingsmodell för IEC 61850”, Max Degerfält,, Elforsk Report, Sweden, February 2010.

[4] “Implementation of a standard integrated protective relays life time management structure in a newly established power utility”, Andreas Fräbel, Zeljko Schreiner, 21st International Conference on Electricity Distribution CIRED, Frankfurt, Germany, June 2011
“Using Hall-Effect Sensors to Add Digital Recording Capability to Electromechanical Relays”, Amir Makki, Sanjay Bose, Tony Giuliante, John Walsh; 2010 Georgia Tech Fault Disturbance and Analysis Conference Atlanta, Georgia, USA, May 3rd - 4th, 2010

[5] “A Universal Approach for Retrieving and Analyzing Event & Fault Records,” Jeffrey Pond, Amir Makki; Proceedings of the 2005 Distributec Conference, San Diego, California, USA, January 2005
“Using Event Recordings to Verify Protective Relay Operations”, A. T. Giuliante D. M. MacGregor A. & M. Makki A.P. Napikoski; Energy Council of the Northeast Spring Conference Portsmouth, NH, USA, March11, 2004

[6] “The IEC 60255-121 standard and its impact on performance specification, testing and evaluation of distance protection relays, Andrea Bonetti, Murty V.V.S. Yalla, Stig Holst; Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES, Dallas, Texas, USA, May 2016

[7] “GridEx® User’s Manual”, FMTP Power AB, Sweden 2016
“Wavewin™ User’s Manual”, Softstuf 2016, USA 2016
“IPS-RELEX™ User’s Manual”, IPS-Intelligent Process Solutions GmbH, Germany 2016

[8] “Time - what is it in IEC 61850? “ R Hughes https://ideology.atlassian.net/wiki/x/BIBUB