Verification and Supervision of Process Bus Communication

Andreas Klien, Matthias Wehinger, Fred Steinhauser, OMICRON electronics GmbH, Austria

Abstract

With the increasing usage of non-conventional instrument transformers applying IEC 61850-9-2 sampled values and GOOSE messaging being used also for process level communication, more critical information is transmitted on the communication network. Thus the proper functioning of the process bus communication infrastructure becomes mission-critical. Methods are needed to verify and supervise correct operation of process bus communication.

This already starts in the commissioning phase, where configuration errors and communication problems have to be ruled out and correct transmission of all signals has to be verified. Also after commissioning, during the operation phase of a digital substation, communication problems have to be detected immediately, so that the operational staff can react on it.

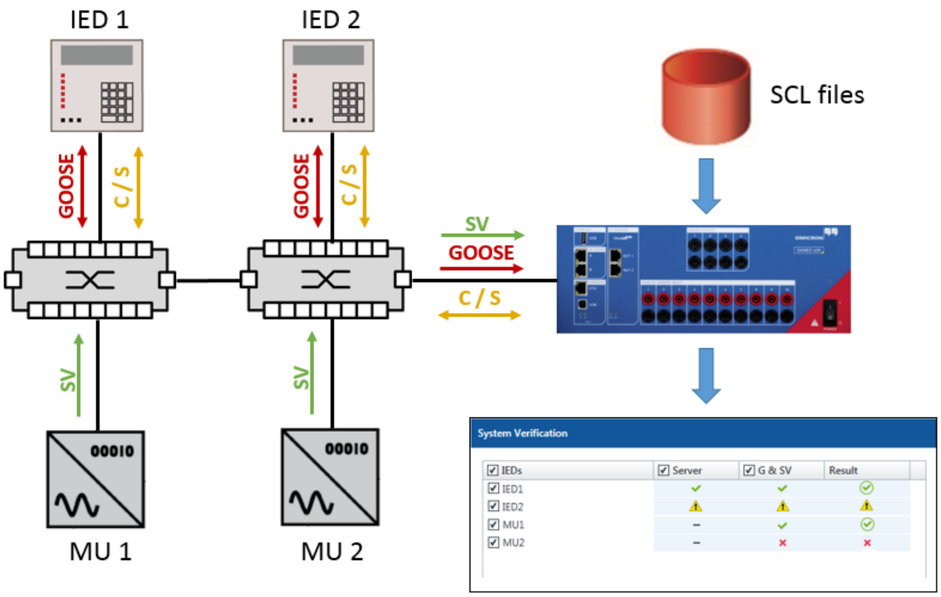
This paper starts by describing how the configuration for the IEC 61850 process bus communication can be verified against the Substation Configuration Description (SCD) during commissioning. This ensures correct sampled values and GOOSE configuration and also ensures that all IEDs are reachable via client/server communication according to their definition in the SCD. Subsequently, it is described how process bus communication can be supervised permanently. It is shown how sampled values and GOOSE communication can be permanently inspected for e.g., lost samples, GOOSE timing problems and PTP time synchronization issues. The paper concludes with example setups on how network supervision can be applied in redundant network structures using RSTP, HSR, or PRP redundancy protocols.

Verifying IEC 61850 Communication during Commissioning

For IEC 61850 substations the communication system and the IEDs present in the communication system can be described in the standardized substation configuration language (SCL) [1]. SCL can be used already in the specification phase to specify the requirements for the project, known as substation specification description (SSD) files. After the project was realized, the substation configuration description (SCD) file describes the actually implemented system. In the factory- and site acceptance test the SCD file can be used to verify that all IEDs are communicating correctly. This verification can be done by comparing the actual communication occurring on the wire against the information in the SCD file.

When commissioning the IEC 61850 system, often communication and interoperability problems occur because certain communication parameters in the publishing device are different than in the subscribing device. This can happen e.g., if the configuration of the publisher was changed after the subscribing device was already commissioned. To find the cause of such an error, all configuration parameters of publisher and subscriber would have to be compared in order to find the differences. With the system verification setup described in the following such differences can be found with less effort.

Figure 1 describes the setup for verifying the communication of a small exemplary system consisting of merging units and protection IEDs, verified using a network analyzer with verification capabilities [7]. In this setup, all GOOSE [3] and IEC 61850-9-2 [4] sampled values communication can be verified in one step against the description in the SCD file. It



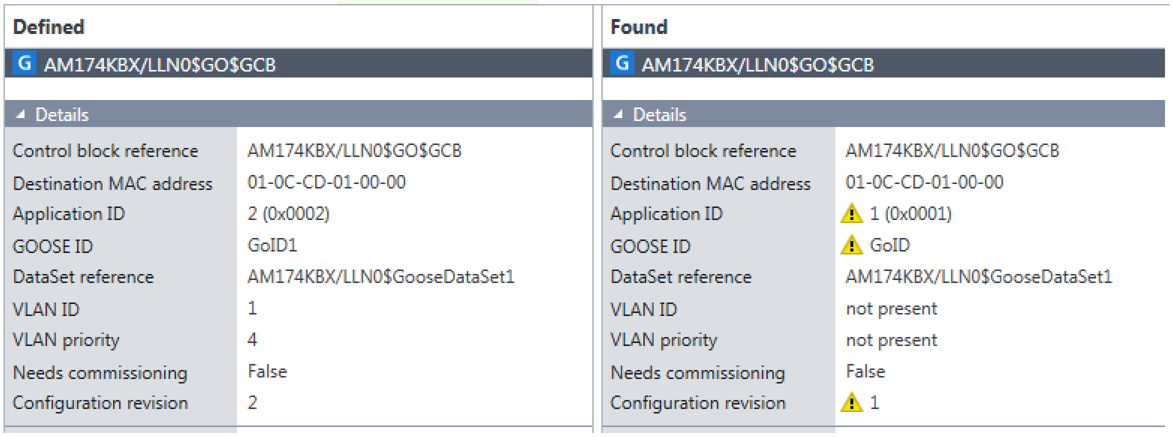
System Verification

☑ IEDs	☑ Server	☑ G & SV	Result
☑ IED1	✓	✓	✓
☑ IED2	⚠	⚠	⚠
☑ MU1	–	✓	✓
☑ MU2	–	✗	✗

Figure 1: Setup for verifying IEC 61850 communication

will be detected if communication parameters don't match the configuration and if GOOSE or sampled values (SV) messages described in the SCD are missing. If the IEDs also provide an IEC 61850 server [3] it is also verified that the server is available for client/server communication. To ensure that the correct server was reached the Logical Device names of the reached server are compared against the description in the SCD. The verification result shown in figure 1 indicates that all IEC 61850 communication aspects of IED 1 are correct, while the GOOSE and client/server communication of IED 2 was found different than expected. From MU 2 no SV communication was found at all. This can be either because MU2 was not commissioned yet, or because of network configuration errors.

Figure 2 shows the verification result of a GOOSE found different than expected. On the left, the GOOSE parameters specified in the SCD file are shown and on the right the GOOSE parameters found on the network are shown. The GOOSE had different values for Application ID, GOOSE ID, and Configuration revision. Because of the different GOOSE ID and Application ID, subscribing IEDs didn't receive this GOOSE. It can be recognized that the publishing device must have been configured with an older revision of the SCD, since its configuration revision is lower. The different configuration revision may cause that subscribers don't accept the GOOSE data, depending on the implementation of the IED. Therefore the configuration of the publishing device needs to be corrected so that it matches the SCD to enable communication.



Defined		Found	
G AM174KBX/LLN0$GO$GCB		G AM174KBX/LLN0$GO$GCB	
Details		Details	
Control block reference	AM174KBX/LLN0$GO$GCB	Control block reference	AM174KBX/LLN0$GO$GCB
Destination MAC address	01-0C-CD-01-00-00	Destination MAC address	01-0C-CD-01-00-00
Application ID	2 (0x0002)	Application ID	⚠ 1 (0x0001)
GOOSE ID	GoID1	GOOSE ID	⚠ GoID
DataSet reference	AM174KBX/LLN0$GooseDataSet1	DataSet reference	AM174KBX/LLN0$GooseDataSet1
VLAN ID	1	VLAN ID	not present
VLAN priority	4	VLAN priority	not present
Needs commissioning	False	Needs commissioning	False
Configuration revision	2	Configuration revision	⚠ 1

Figure 2: Differences between GOOSE definition in the SCD (left) and found on network (right)

Supervising Process Bus Communication during Operation

After commissioning, configuration errors are ruled out and all applications of the protection, automation, and control (PAC) system are tested. Also the underlying network infrastructure is verified. However, during operation of the PAC system, the PAC applications are relying on the proper functioning of the underlying network infrastructure. Protection functions rely on timely arrival of sampled values and also on the availability of time synchronization. Also the time synchronization service depends on the network infrastructure, if the IEEE 1588 precision time synchronization protocol [6] is used. How can malfunctions of the communication infrastructure, or of important services be detected 24/7 during operation? There are mainly two options: One option is to supervise each IED or PAC application separately. Vendors are increasingly adding such features to their IEDs recently. The other – or complementary – option is to supervise critical services directly on the process bus i.e., on the network, where all services are visible. In the remainder of this work it will be focused on network-based supervision.

Figure 3 depicts a setup where a network analyzer is connected to a central communication link to permanently supervise GOOSE and SV communication. The supervisor accesses the network traffic by tapping passively into the Ethernet link without interfering communication on that link. Using this setup it is not necessary to configure any port mirroring on the Ethernet switches.

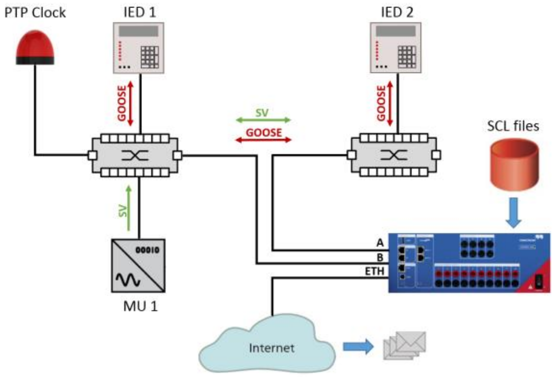


Figure 3: Setup for supervising process bus communication

The supervisor device can be configured with the SCL file of the substation. It detects abnormalities in GOOSE and SV traffic and logs all events with the corresponding detailed information (event details, captured network traffic) to its storage. Depending on the criticality of the event it can be necessary to just log the event to disk, or to notify the responsible operators. The setup described in the figure uses notifications sent via email to inform the operating staff about the occurrence of an event. Another option to signal a critical event is by operating a binary output contact on the network analyzer device which is then transmitted over SCADA to the remote control center.

For sampled values it is useful to detect when a single sample (message) is lost, which can be detected by the supervisor by inspecting the sample count in the SV messages. Such an event can be tolerated but it is highly unusual in modern Ethernet networks and requires further investigation. If no samples are received for more than 4 milliseconds, the sampled value stream is timed out, which is a critical event and requires immediate action. By evaluation the timestamps in the SV messages it can also be detected if the clock of the sampled values publisher drifts away too much. If the supervisor device is synchronized to a PTP time source, also a malfunction in the PTP time synchronization service can be notified.

GOOSE timeouts can be detected by inspecting the time allowed to live field of the GOOSE messages on the network. A GOOSE timeout can either be caused by communication loss e.g., faulty network cable, or because the publishing IED is malfunctioning. By supervising the sequence numbers (sqNum) of the messages, missing GOOSE retransmissions can be detected.

Another critical event is if two devices in the network send the same GOOSE. This can happen for example if somebody accidentally generates the same GOOSE with a testing tool but forgot to turn on the Simulation/Test flag for that GOOSE. This situation is also detected by the supervisor by inspecting status and sequence numbers. Figure 4 depicts this situation: The original GOOSE is sent with increasing sqNum by one for each packet, but when the duplicate GOOSE appears, the sqNum jumps back to 0. Therefore, if two identical GOOSEs are sent in the same network, the supervisor detects multiple GOOSE "out of sequence" events. Additionally, under normal circumstances not only the sqNum, but also the stNum is different at the duplicate GOOSE.

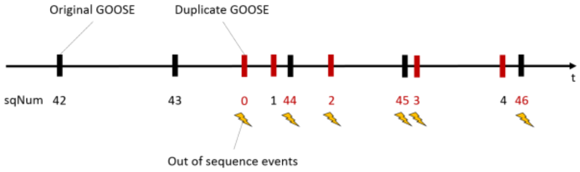
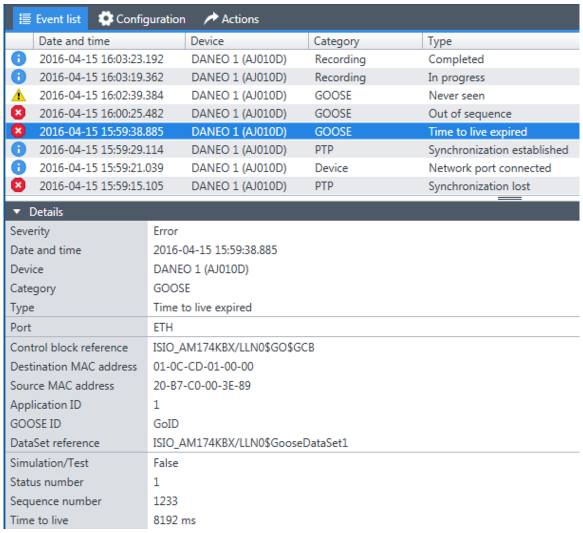


Figure 4: Duplicate GOOSE triggers "out of sequence" events

Figure 5 shows a list of events collected by the supervisor. In the selected event in the figure the supervisor detected that the time allowed to live of a GOOSE message has expired due to communication loss. About a minute later, the GOOSE reappeared. Because there was a gap in the sequence numbers of the GOOSE, an "out of sequence" event was logged. In the detailed information of this event it was shown how many GOOSE retransmissions were missing. It was also logged if status changes (stNum changes) of the GOOSE message were missed during the period of communication loss. Another entry shows that a GOOSE that was specified in the SCD file was actually "never seen" on the network during supervision. This is sometimes caused by GOOSE that were only used during commissioning which should have been removed from the SCD after commissioning was finished.



	Date and time	Device	Category	Type
ⓘ	2016-04-15 16:03:23.192	DANEO 1 (AJ010D)	Recording	Completed
ⓘ	2016-04-15 16:03:19.362	DANEO 1 (AJ010D)	Recording	In progress
⚠	2016-04-15 16:02:39.384	DANEO 1 (AJ010D)	GOOSE	Never seen
✖	2016-04-15 16:00:25.482	DANEO 1 (AJ010D)	GOOSE	Out of sequence
✖	2016-04-15 15:59:38.885	DANEO 1 (AJ010D)	GOOSE	Time to live expired
ⓘ	2016-04-15 15:59:29.114	DANEO 1 (AJ010D)	PTP	Synchronization established
ⓘ	2016-04-15 15:59:21.039	DANEO 1 (AJ010D)	Device	Network port connected
✖	2016-04-15 15:59:15.105	DANEO 1 (AJ010D)	PTP	Synchronization lost

Details

Severity	Error
Date and time	2016-04-15 15:59:38.885
Device	DANEO 1 (AJ010D)
Category	GOOSE
Type	Time to live expired
Port	ETH
Control block reference	ISIO_AM174KBX/LLN0$GO$GCB
Destination MAC address	01-0C-CD-01-00-00
Source MAC address	20-B7-C0-00-3E-89
Application ID	1
GOOSE ID	GoID
DataSet reference	ISIO_AM174KBX/LLN0$GooseDataSet1
Simulation/Test	False
Status number	1
Sequence number	1233
Time to live	8192 ms

Figure 5: Supervisor event list with details for GOOSE timeout

Supervision in RSTP Networks

For station-level network structures, often ring structures using the Rapid Spanning Tree Protocol (RSTP) are used. Here the network switches are connected to form a ring structure so that each switch can be reached from two directions. Several protection relays and bay controllers contain integrated Ethernet switches with two external ports, so they can be directly linked into such a ring. This reduces the number of dedicated Ethernet switches needed for building such a network. The RSTP ensures that there is no circular path for packets, i.e. the ring is always opened by disabling redundant links. In the setup depicted in figure 6, one of the links L1, L2, or L3 will be seen as a redundant link and will be deactivated by RSTP.

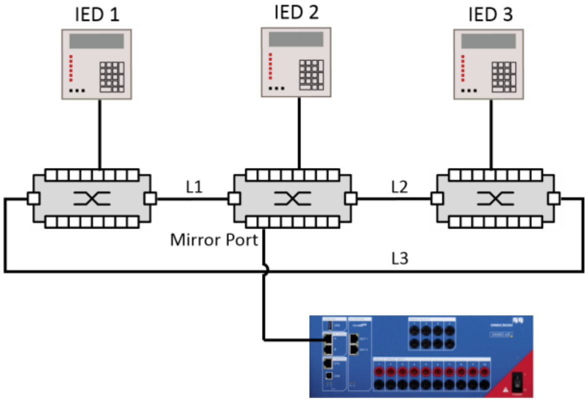


Figure 6: Setup for supervision in an RSTP network

If one of the connections fails, the RSTP-Protocol reconfigures the switching paths and re-enables one of the deactivated links to restore communication. However, during the reconfiguration phase communication is interrupted and packets which can't reach their destination are dropped. Depending on the circumstances, this reconfiguration phase can even take seconds with RSTP. For process bus communication like SV and GOOSE such long periods of communication loss are usually not tolerable. Therefore the redundancy mechanisms High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP), defined in IEC 62439-3 [2] are recommended for process bus networks [5]. These protocols will be covered in the following section.

When analyzing or supervising network traffic in an RSTP-Network it has to be considered that one of the links is deactivated. If the network analyzer is connected as previously described in figure 3 (tapped into a communication link), it can happen that this link is not used by RSTP and no traffic will be visible for the network analyzer. If the analyzer is connected using a mirror port on the switch, as depicted in figure 6, all SV and GOOSE traffic is visible even though one of the links L1, L2, or L3 is deactivated. This is because SV and GOOSE are multicast traffic which is sent out on all ports of the switch. Point-to-point traffic, such as IEC 61850 client/server, is not always visible for the analyzer in figure 6, depending on which communication partners are involved. Assume that link L1 is deactivated and IED 1 tries to communicate with IED 2 using client/server communication. The point-to-point communication will go over link L3 and the traffic will not be visible for the network analyzer.

Supervision in HSR Networks

HSR [2] networks are used for protection and substation automation networks which require redundancy and zero recovery time in failure cases. HSR uses a ring structure for the network. Each node in the ring is attached by two Ethernet ports and sends the same frame on both ports. The frame thus travels in both directions of the ring. The receiver gets the two identical frames from both directions and uses the first frame for its application and discards the second frame. Multicast messages are forwarded to each node in the ring until both frames arrive back at the publisher. Unicast messages are discarded at the destination.

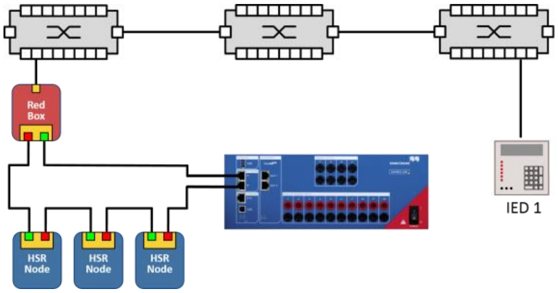


Figure 7: Setup for supervision in an HSR network

Figure 7 shows an exemplary setup with an HSR ring which is connected with a normal Ethernet network. A “Red Box” (redundancy box) integrates the normal network into the HSR network. The network analyzer is tapped into the HSR ring. In this setup, all traffic within the HSR ring is visible to the supervisor. Since SV and GOOSE messages are multicast, the supervisor will receive all messages from both directions. The SV and GOOSE messages can then be supervised separately for both directions. It is thus possible to detect a failed link in the HSR ring because SV and GOOSE will be timed out. Also the SV and GOOSE messages from IED 1 will be received by the analyzer because the multicast messages are forwarded into the HSR network.

Supervision in PRP Networks

The Parallel Redundancy Protocol (PRP) [2] uses two independent Ethernet networks and redundancy is achieved by connecting the devices to both networks. Each packet is sent over both paths and will be received twice at the destination. The network packets in PRP networks are tagged at the end of the frame with the redundancy control trailer. The receiver has to drop the duplicated packet, which can be done in a Red Box. Unlike HSR, PRP doesn’t require special hardware for accessing the network, the Red Box functionality of PRP could therefore be realized in software, integrated into IEDs with two Ethernet ports.

A possible setup for supervising communication in a PRP network is depicted in figure 8. In this setup the network analyzer receives all traffic because the identical traffic is available on both network paths. Alternatively, also both redundant paths can be supervised with one supervising device using a mirror port in both networks, or with two supervising devices tapped into communication links in both paths. This enables to detect timeouts of SV and GOOSE independently for both network paths. As described before in the HSR setup, this can be used to detect failed links because GOOSE and SV will be timed out in one of the redundant networks.

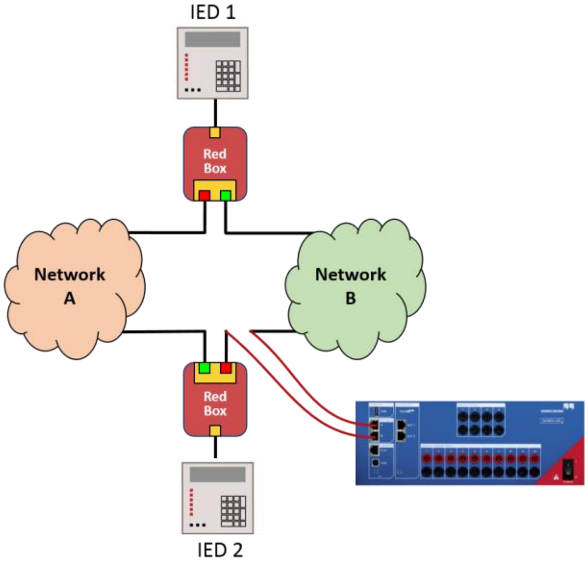


Figure 8: Setup for supervision in a PRP network with one supervisor

Conclusion

The application of IEC 61850 communication in PAC systems brings new challenges, but the new options and benefits have the potential to outweigh the difficulties by far.

The engineering concept and the resulting availability of configuration information in machine readable form (SCL files) greatly support the testability of the systems. The verification of the communication on the application layer as laid out in first section of this work is essentially facilitated by these features. This applies through the whole life cycle of a PAC system. A configuration and a test setup worked out for a FAT can then again be used during commissioning. Configuration changes that may have happened in between are immediately detected and can be cleaned up. If the configuration remained unchanged, this is verified and ticked off even faster. And the same configuration information serves its purpose for the supervision during operation or during maintenance work later on.

Considering the fact that the performance and reliability of the communication networks were often questioned by skeptics, it is surprising that only small effort was invested in verifying and supervising these important aspects until now. But commissioning the communication infrastructure on its own should become a dedicated task to ensure a solid base for the PAC system communication on top of it. Electrical power engineers with the focus on protection, automation, and control can perform such tasks easily with state-of-the-art tools.

References

[1] IEC. *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs (IEC Std. 61850-6 ed2.0)*. International Electrotechnical Commission, Dec. 2009.

[2] IEC. *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) (IEC Std. 62439-3),* Feb. 2010.

[3] IEC. *Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3 (IEC Std. 61850-8-1 ed2.0).* International Electrotechnical Commission, June 2011.

[4] IEC. *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3 (IEC Std. 61850-9-2 ed2.0).* International Electrotechnical Commission, Sept. 2011.

[5] IEC. *Communication Networks and Systems*

for Power Utility Automation. Part 90-4: Network Engineering Guidelines (IEC Technical Report 61850-90-4). International Electrotechnical Commission, 2012

[6] IEEE Power & Energy Society. *IEEE Standard Profile for use of IEEE 1588 Precision Time Protocol in Power System* Applications (IEEE Std. C37.238-2011). Institute of Electrical and Electronics Engineers, Inc., 2011.

[7] M. Wehinger and F. Steinhauser. *Verification and Supervision of Communication Networks for Utility Automation*. PAC World Magazine, June 2016 Issue, pages 54–59, 2016

Authors:

Andreas Klien was born in Austria in 1986. He studied Computer Engineering at the Technical University of Vienna and has been working at OMICRON since 2005. At OMICRON, he is currently managing a development team for products relating to IEC 61850. As a member of the Working Group 10 on the Technical Committee, TC 57, of the IEC, he contributes to the further development of the IEC 61850 standard series.

andreas.klien@omicronenergy.com

Matthias Wehinger studied Computer science at the Konstanz University of Applied Science in Germany and received an MSc degree of Integrated Product Development from the Vorarlberg University of Applied Sciences in Austria. He started working in product development of testing tools at OMICRON in 2003 and was involved in the introduction of new technologies for test object modelling.

Since 2014 he works as innovation manager for power utility communication products at OMICRON.

matthias.wehinger@omicronenergy.com

Dr. Fred Steinhauser studied electrical engineering at the Vienna University of Technology, where he received his diploma in 1986 and was promoted to Doctor of Technical Sciences in 1991. In 1998, he started at OMICRON and has been working on various topics for the protection testing of energy systems. From 2000 to 2014 he changed to product management with a focus on communication in switchgear. Since 2014, he is head of Power Utility Communication at OMICRON.

Fred Steinhauser represents OMICRON in the UCA International Users Group. As a member of the WG10 and WG17 in the TC57 of the IEC, he is involved in the IEC 61850 standard. He is also a member of the SC B5 of CIGRÉ.

fred.steinhauser@omicronenergy.com