Making IEC 61850 GOOSE Communication More Reliable

C. Harispuru, N. Schuster, and D. C. Murray, *Member, IEEE*

Abstract--After achieving worldwide acceptance, IEC 61850 is convincing users of its many cost saving benefits, such as the reduction of substation wiring in automation projects. In protection applications, fast interbay communication via GOOSE messaging is necessary in order to satisfy the high expectations of customers. However, demanding applications, like interlocking and interoperable communication between devices from different vendors, require not just solutions on cost-saving and fast communications, but at the same time, they must achieve the highest reliability. This paper illustrates how to configure and test GOOSE communication to ensure that it provides the greatest reliability without sacrificing performance. The focus of this paper is on the tools and techniques to improve communication reliability at the IED level using GOOSE messaging. Reliability resulting from network topology considerations, such as network redundancy, is outside the scope of this paper.

Index Terms--Commissioning tool, communication aid, computer-aided testing, GOOSE messaging, IEC 61850, network sniffer, reliability, test mode.

I. INTRODUCTION

Several mechanisms inherent within GOOSE communication are intended to provide high reliability and must be considered during the engineering process in order to achieve the optimal results. As multicast messages, GOOSE messages are sent to all IEDs and are therefore not acknowledged; however, this is a powerful feature indeed. On the one hand, cyclical retransmission and short cycle times after a status change guarantee fast reception of the GOOSE message and continuous monitoring of the communication link. On the other hand, the use of quality bits allows the IED to evaluate the GOOSE message differently in case of communication interruption. A specific programmable logic, like bypass, can be implemented in IEDs for backup scenarios.

During device test, possibilities for setting and interpreting GOOSE test bits will be presented. Deactivating GOOSE transmission will also be discussed for interoperability purposes when receiving devices do not support the use of test

C. Harispuru is with Siemens AG, Nürnberg, Germany (e-mail: cedric.harispuru@siemens.com).

N. Schuster is with Siemens AG, Nürnberg, Germany (e-mail: norbert.schuster@siemens.com).

D. C. Murray is with Siemens Energy, Inc., Mountain View, CA 94043 USA (e-mail: dan.murray@siemens.com)

bits. This GOOSE test switch can be controlled by a substation automation unit.

Behind the configuration of supported GOOSE features, the commissioning process is the determining factor for ensuring working communications and a highly reliable system. New testing possibilities via software can be used to verify the correctness of "digital wiring". Based on the available GOOSE messages and connections engineered into the SCD file, commissioning tools can support, in real time, the verification of all transmitted attributes from sending devices and display user-friendly results without requiring extensive knowledge of the standard specification. Receiving devices can evaluate transmitted attributes or determine missing GOOSE messages. Status changes and GOOSE message anomalies can be logged in the IEDs. During commissioning, these GOOSE event logs can be analyzed and documented as proof of demonstrating high reliability and correct behavior, even in the case of communication interruption or when in test mode.

II. SAFE GOOSE MECHANISMS

Due to their physical presence, hard wired connections remain, in many people's minds, a symbol of high reliability. Since its publication, substation automation projects based on the IEC 61850 standard have become, worldwide, the "state of the art" solution due to its numerous advantages. However some customers still remain reluctant to take advantage of some IEC 61850 benefits, especially peer to peer communication between devices using GOOSE messaging, which nonetheless can provide both cost efficiency and a greater number of virtual inputs and outputs for protection and control schemes. The physical presence of a wire versus virtualization is, at first sight, not a battle clearly won in the minds of some as we see this technology progress.

However, several mechanisms inherent within GOOSE telegrams should convince users about its high safety and reliability, as well as high availability of the communications system as stated in IEC 61850-3 standard. Conversely, IED vendors could further improve their mechanisms at the application level.

A. Safe Mechanisms at the Sending Device

As multicast messages, GOOSE messages are transmitted on the substation bus from a publishing device to multiple

receiving devices (called subscribers). But the 61850 standard does not require receiving devices to acknowledge correct receipt of GOOSE messages. So to ensure that messages are received correctly, the same message is repeated several times. The use of GOOSE multicast messages result in a reduction of substation bus traffic because it is a point to multi-point connection approach that does not require acknowledgement from receiving devices.

The publisher device sends GOOSE telegrams containing standard attributes to be decoded at the subscriber side. In normal operation, GOOSE messages are transmitted cyclically after a state change. Transmission is immediate and repeated rapidly according to a repetition profile.

Fig. 1 shows the stream of a telegram on the network carrying a single point message containing quality and status value.

Fig. 1. Stream of a GOOSE telegram on the Ethernet obtained with a network sniffer.

Short retransmission times increase the performance possibilities to monitor the communication link or in case of missed telegrams. However, retransmission times that are too short generate processor load and traffic without benefits for the receiving device. Based on experience, a repetition profile with T0=1s for cyclical transmission and T1=4ms for repetition after a stage change with an exponential decreasing time (e.g. 4-8-16-32-64-128-512-1000-1000) showed good results (Fig. 2).
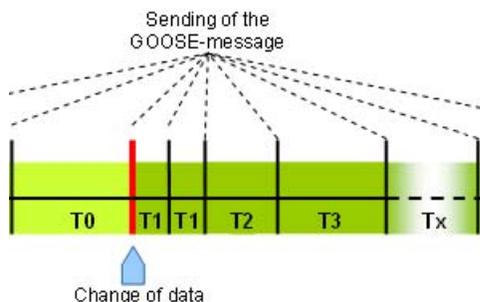

Fig. 2. Spontaneous transmission of GOOSE messages following status change of data objects in the telegram.

Attributes related to the repetitions like the state change number and the sequence number (attribute 85 and 86 in the telegram) prevent the introduction or the re-sequence of telegrams (See Fig. 1 for a list of attributes).

The attribute TimeAllowedToLive (attribute 81 in the telegram) could be set to 1.5 times the time until the next repetition planned, with a minimum of at least 50ms to take network reconfigurations into consideration.

GOOSE signals should be sent with their quality. This can be done by sending two FCDAs (e.g. stVal and q) or the complete Functional Constraint. Note: Depending on the IED, the complex structure of a Functional constraint is not necessarily supported by the receiving device. This should be clarified during the engineering process.

Furthermore, GOOSE messages contain a Frame Check Sequence to guarantee correct transmission of the message on the network.

B. Safe Mechanisms at the Receiving Device

To ensure safety, the receiving devices should filter the messages on the network. Only subscribed multicast telegrams should be transmitted to the application. In addition to GOOSE Ethertype, multicast addresses defined in the SCD file during configuration should be filtered by the hardware in order to be faster and avoid useless processor loading which may limit the performance of the receiving device.

Static attributes in the GOOSE telegram (e.g. attributes 61, 80, 82, 83, 88) should be checked then - when transmitted to the application software – to discard messages. Next, plausibility checks with dynamic attributes (e.g. 85, 86, 89, 8a) should be performed. Also, syntactically incorrect or corrupt telegrams should be declared as invalid.

Based on GOOSE repetition attributes (stNum, sqNum and timeAllowedToLive), the communication link can be monitored which is a major benefit in comparison to hardwired connections. If messages are duplicated or out-of-order, they should be invalidated by the subscriber. In case of missing telegrams, they should be invalidated in order to be noticed by the protection functionality.

The published quality attributes should be evaluated by the receiving IED in order to avoid trips in the substation if the GOOSE signal is invalid. This can be realized by a basic integrated solution in the communication module of the device, or with flexible and advanced logic plans. The flexible alternative offers the possibility of defining backup scenarios, e.g. for interlocking conditions by authorizing a bypass on the local HMI when signals are invalid and would block commands.

III. SAFE GOOSE MECHANISMS DURING TESTING

In addition to default mechanisms during normal operation, some advanced possibilities exist to facilitate live testing on site without tripping the substation.

A. GOOSE Test Mode Bit

During commissioning, some parts of the substation may already be in normal operation. Extensions with additional IEDs still need to be tested, without impacting the connected process. For that purpose, GOOSE telegrams contain a test bit (see attribute 87 in Figure 1) so that all data of the GOOSE telegram can be treated in a special way.

IED subscribers should ignore telegrams where the Test Mode flag is set. The test mode flag may be activated in a device via a binary input, or via the configuration tool. By activating the test mode flag, all data objects contained in GOOSE telegrams are spontaneously assigned the quality "Test." This leads to a change in the state of the objects as well as to spontaneous transmission of GOOSE telegrams, so that the receiving devices immediately receive the objects with the quality "Test." It is however not compulsory to include the quality for each transmitted object. This may be configured by the user or is set in a fixed manner within IEDs by the configuration tool.

Accordingly, different vendor-specific solutions exist for the transmission of the Test bit. It is recommended to check the behavior of each vendor IED and their response possibilities with the integrated logic. The engineering process should then take this into consideration as some alternatives may exist for a correct interpretation of the subscribing IED, e.g. configuring the quality for each Data Object, or adding a Data Object corresponding to the test mode of the IED. Integrated logic with an evaluation of invalid signals have the advantage to being flexible for the user to choose the behavior depending on if the sending and receiving device are in test mode or not.

To simplify the design of integrated logic, rules are defined with Edition 2 of IEC 61850. Objects in test mode will not be passed onto the application if the recipient is in the normal mode. If however the recipient is also in test mode, the objects will be processed by the application. This ensures a degree of interoperability when devices are tested in a network in which GOOSE communication takes place and not all devices are from the same manufacturer. Signals transmitted for test purposes will not cause unwanted actions at the receivers. The necessity to interrupt the communication link during tests is not desired. Control of the test equipment, the protection configuration software and the device response must be tested while connected to the network.

B. GOOSE Deactivation

For devices not supporting the test bit, an alternate approach during testing is to deactivate the GOOSE Control

Block using the IEC 61850 standard attribute "GoEna" (see Fig. 3). If this variable is changed from 1 to 0 the device stops transmitting GOOSE messages.

Name	Type(Len[arr])	Value
Name		Control_DataSet1
Type		Data Object
Path		IEDSJ64gCTRL/LLN0GOControl_DataS
TypeID		3
	{ (0[11])	
GoEna	Bool (1[1])	0
GoID	VisString (66[-65	0
DatSet	VisString (69[-65	IEDSJ64gCTRL/LLN0$DataSet1
ConfRev	UInteger (4[4])	2
NdsCom	Bool (2[1])	0
DstAddress	{ (0[4])	
DstAddress$Addr	OctetStr (6[6])	010ccd010004
DstAddress$PRIORITY	UInteger (2[1])	4
DstAddress$VID	UInteger (2[2])	0
DstAddress$APPID	UInteger (2[2])	0
DstAddress	} (2[4])	
	} (0[11])	

Fig. 3. Termination of a GOOSE message transmission using an IEC 61850 Client (called the IEC Browser).

This allows testing the logic that detects an interruption of the link at the receiver without actually having to break the connection.

In practice, switching off a GOOSE message at the transmitting end in a device can be done via an IEC 61850 Test Client (e.g. IEC – Browser for IEC 61850 Stations [3]).

IV. COMPUTER-AIDED GOOSE MONITORING

While it is relatively simple to test a hardwired connection, a special PC supported test tool is required for GOOSE connections, which however can complete the test of the links in a few seconds. These test programs make use of the GOOSE parameters from the SCD file and compare these with the actual data traffic in the network. As GOOSE messages are transmitted repetitively, continuous monitoring can also be implemented.

A. Network Sniffer

Analysis software records the data traffic in a Ethernet network. Of particular interest are the GOOSE messages and the IEC 61850 data traffic between client and Server. However there are also other protocols e.g. SNMP for monitoring the network or IP telegrams of the IED configuration software, present in the network. Therefore, filters are required for selective recording of the data.

As hundreds of GOOSE telegrams may exist in applications for large projects that utilize GOOSE messages, the programs used for testing need to be very powerful to provide significantly more functionality than conventional network sniffers (refer to Fig. 1). These can display the GOOSE message bit stream exactly, but require detailed knowledge by the user for evaluation and are not suitable for large volumes of data.

GOOSE messages can be uniquely identified as data packages on the network and can then be filtered out. This can be executed by software running on a PC connected to the network. With hundreds of GOOSE messages travelling on the network, the network drivers must listen to the network in real time then quickly process and display the data for the user in an easily readable manner.

A PC program called ´GOOSE – Inspector´ [4] is used as an example to illustrate a computer-aided tool in this paper. Such a tool should display all GOOSE messages in a network in an easily readable tabular format. Within a few seconds the telegrams are identified and listed. Detailed information on the contents of GOOSE messages are provided by selecting a particular row.
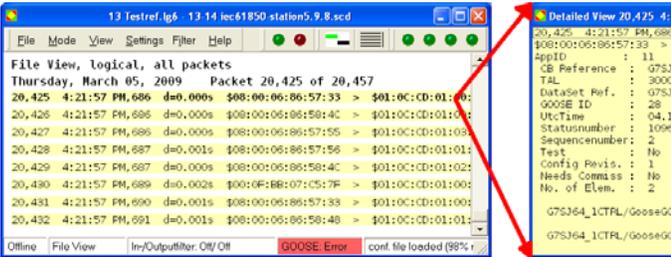
Fig. 4. Tabular overview of GOOSE messages with detailed view.

B. Integrated SCD Intelligence

GOOSE messages are configured in the system configurator during the engineering process. For this purpose, messages that will be sent are configured in the sending devices, and linked to receiving objects in one or more devices. The result of this configuration, that replaces hardwired connections between the devices, is a station configuration file in XML format (SCD file) containing all interconnections. An extract of the SCD file is loaded into those devices that will eventually transmit GOOSE messages onto the network.

If the SCD file is loaded in the program, all the GOOSE messages are compared with the values stored in the file. In this manner, it is possible to check the cyclic repetition time or whether if all the configured telegrams are present. Deviations are graphically displayed by means of colored symbols. Further detailed analysis is possible and in some cases warnings or errors are displayed. Ideally the result should indicate full correspondence and that all the configured information could be detected in the network.

The program can also show the recorded GOOSE applications, the resulting telegrams and the individual signals in a source–target arrangement that corresponds to the view provided by the offline system configuration software. Furthermore, IEC 61850 descriptions of transmitted and received objects in the SCD file are supplemented with indication text and presented to the user on the device and in the operating program. This makes it much easier for the user

to read. GOOSE messages that are not listed in the configuration file, e.g. those that are transmitted for testing purposes or messages from other network segments, can also be detected to avoid possible interference at IED subscribers.
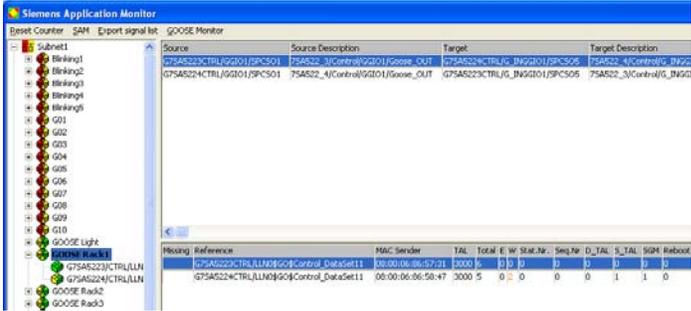

Fig. 5. Display of GOOSE connections with GOOSE – Inspector.

C. Simulation of GOOSE Messages

One application is the simulation of GOOSE messages from IEDs that will only be fitted in the substation at a later point in time. This could also be used for devices not able to simulate state changes. For this purpose, IEDs with GOOSE messages are configured offline in an IEC 61850 system configurator in order to provide a SCD file.
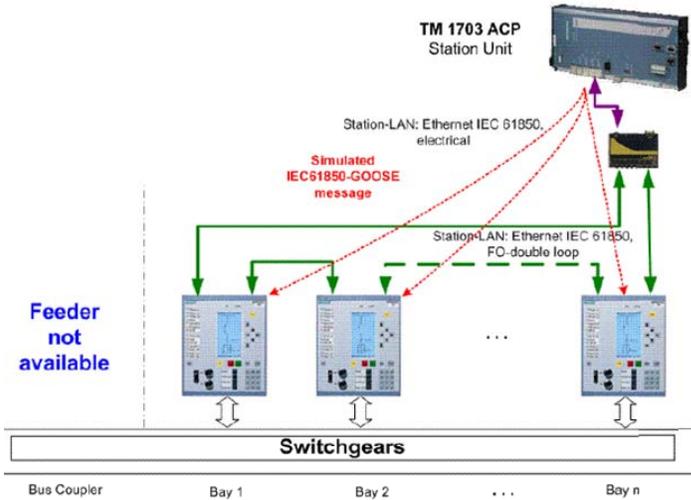

Fig. 6. Simulation of GOOSE messages in a test server.

The different states of the signals can also be defined and tested through use of a GOOSE Simulator that is configured accordingly (such as the TM 1703 ACP as shown in Fig. 6). The substation control device takes over the function of the devices that are not yet available in the substation with regard to the transmission of the GOOSE messages.

V. IED INTEGRATED TEST AID

Devices may provide integrated test aid for displaying and monitoring the transmitted and received GOOSE objects.

A. Test Aids for GOOSE Messages Integrated in the Device

The generation, testing or continuous monitoring of GOOSE messages can be additionally supported by the device by means of integrated functions.

For example, the test mode at the transmitting device can be activated using the configuration tool. Furthermore, objects can be set by the user so that these result in the spontaneous transmission of GOOSE messages without the need to simulate these events from the outside by means of secondary injection equipment. These are detected and recorded, by the GOOSE–Inspector or other analysis software, in the network. In the devices the changes are registered with millisecond accuracy and saved in the event log. If all the devices in the network are synchronized via SNTP, the time of sending and receiving can be determined exactly with a one millisecond resolution.

For received GOOSE messages, there are test aids in the device. For each received object (e.g. a pick-up signal) it is possible to monitor if GOOSE repetitions are missed in order to generate an alarm at the receiver or to influence the state of the object through integrated logic in such a manner that a secure state is obtained in the event of an interruption of the communication link. State changes of received objects can be retrieved from the event log of the device or as spontaneous alarms immediately upon reception. A received signal may also be used to trigger the oscillographic recording in which the binary traces of received objects are registered.
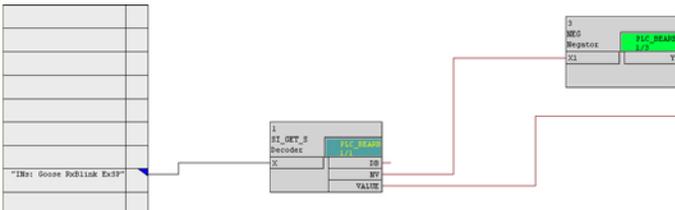
Fig. 7. Possible logic at IED subscriber for detection of an interruption of the communication link.

A Web server that transmits diagnostic variables to a browser can be included on the Ethernet module with its own communication processor. In the browser these values are displayed as HTML pages. Sent telegrams and received IEC 61850 objects are displayed. Furthermore, the number of sent and received GOOSE messages as well as the number of received faulty telegrams are continuously registered.

Fig. 8. Display of sent and received GOOSE messages in a device via an HTML page.

Fig. 9. MIB description file for a network monitoring system with GOOSE indication.

Using a network management system, it is possible to determine via the Simple Network Management Protocol (SNMP), at cyclic intervals, the number of sent and faulty GOOSE messages in a device. Fig. 9 shows a description file (MIB file) that is imported into the monitoring system. If the number of received GOOSE messages is no longer increasing, or if faulty telegrams are indicated, the system can alarm this.

VI. CONCLUSION

Various methods testing diagnosing GOOSE messages were described. By means of external test programs the data traffic in the network can be validated. The SCD file in which the GOOSE configuration is contained serves as a basis. These test programs can check whether the GOOSE messages are transmitted correctly on the network and if they correspond to the configured data. In case of errors, they make provision for further analysis. Furthermore, the reception of data contained in a GOOSE message must be checked at the receiving devices. This is done by means of integrated test aids and by monitoring the application that is influenced by the received information. Various states such as normal operation, test mode or interrupted communication must be considered in this context.

VII. REFERENCES

[1] Dawidczak, H., Dufaure, Th., Englert, H., "IEC 61850 GOOSE Communication: Performance of Transmission," presented at the International Scientific & Technical Conference – Actual Trends in Development of Power System Protection and Automation, Moscow, Russia, September 7-10, 2009.

[2] Dawidczak, H., Dufaure, Th., Englert, H., "Konfiguration und Diagnose der GOOSE – Kommunication der IEC 61850," presented at VDEW Energieverlag, Frankfurt/Main, Zeitschrift Netpraxis, Jg. 47 (2008), Heft 6.

[3] IEC Browser. Available: http://siemens.siprotec.de/download_neu/html_soft/soft_iec_browser_m.htm

[4] GOOSE-Inspector – Online Monitoring for IEC 61850 GOOSE telegrams. Available: http://siemens.siprotec.de/download_neu/html_soft/soft_goose_m.htm

VIII. AUTHORS

Cédric Harispuru (1983) was born in France and graduated from Supélec (Paris) and TU Darmstadt. His employment experience at Siemens AG in Nuremberg includes configuration and commissioning of the first IEC61850 substation projects in France, technical consulting for project delivery of IEC 61850 substations and now technical consulting for IEC 61850 systems worldwide. He is member of TC 57 WG10.

Norbert Schuster (1958) was born in Germany and graduated at the Technical University in Stuttgart (Germany). He has been working for Siemens AG in protection and communication since 1990. His current role is as product manager specializing in communication protocols and communication interfaces for protection relays.

Dan Murray (M'10) is a Marketing Manager for Siemens Energy specializing in Energy Automation products and systems. He has more than 30 years experience in the analysis, design, development and implementation of a wide variety of real-time data acquisition and control systems in a range of industries, and has been working in the electric utility industry since 1994. He received his bachelor of science degree in Information Systems Management from the University of San Francisco.