R-GOOSE – Principles, Applications and Benefits

Alexander Apostolov
OMICRON electronics, USA

1 Introduction

IEC 61850 is being widely accepted around the world due to significant benefits that it provides compared with conventional hard wired solutions. However, there are still many specialists in the industry that are hesitating to make a decision and start using GOOSE messages for all the different protection and protection related functions. This is probably due mainly to the lack of understanding of the differences between hardwired and GOOSE based solutions. Taking advantage of the benefits is possible only when there is good understanding of the fundamentals and the applications.

That is why the paper first introduces the concepts of the IEC 61850 GOOSE (Generic Object Oriented Substation Event). It describes:

- Publisher and Subscriber functionality
- Multicasting
- Event reporting versus commands
- Repetition mechanism
- Data sets
- Simulation bit

The definition of R-GOOSE is later presented, followed by a discussion of a couple of use cases describing the application of this technology for reducing the fault clearing time

2 GOOSE Communications

Peer-to-peer is the characteristic communications type for the IEC 61850 based systems. It is one of the distinguishing features of the standard that makes it attractive to protection and control specialists. It describes the ability of arbitrary pairs of IEDs connected to the substation network to manage the exchange of information as necessary with all devices having equal rights, in contrast to the master/slave communication. High-speed peer-to-peer communications in IEC 61850 based protection and control systems use a specific method designed to meet a variety of requirements. It is very important that the concept of the Generic Substation Event (GSE) model is not based on commands, but on the sending indication by a function that a specific substation event has occurred. It is designed to support reliable high-speed communications between different devices or applications and allows the replacement of hard-wired signals between devices with communication messages exchange while improving the functionality of the protection, automation and control system. It uses a connectionless Publisher – Subscriber communications mechanism shown in Figure 1.

The model includes several features that can be used to improve the reliability and availability of the system. At the same time the proper use of these features in vendors' implementation will allow the reduction in maintenance and increase in the flexibility of the system. Initially GOOSE was developed for substation communications, but due the benefits that it provides there is a need to define how it can be used for substation-to-substation or wide area communications.

To understand the differences between the substation GOOSE and the wide area GOOSE, we need to look into some of the details of the Generic Substation Event model.

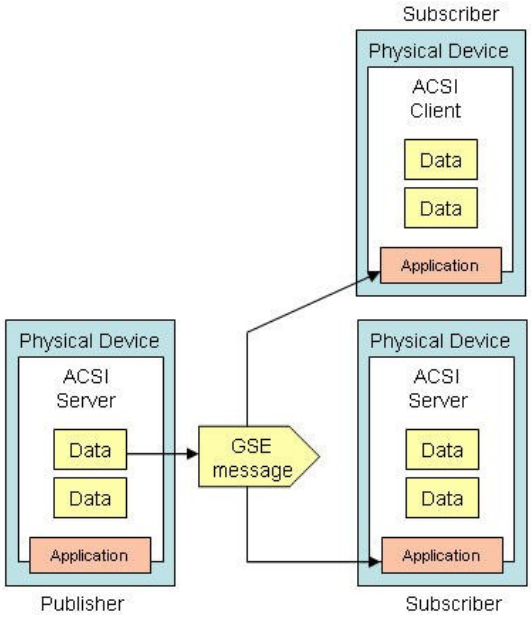


Figure 1: Publisher/Subscriber mechanism

The GSE method can be considered as a mechanism for reporting by a logical device. The achievement of speed performance, availability and reliability depends on the implementation in any specific device.

The generic substation event model is used to exchange the values of a collection of Data Attributes defined as a Data Set. GOOSE supports the exchange of a wide range data types organized in a data set.

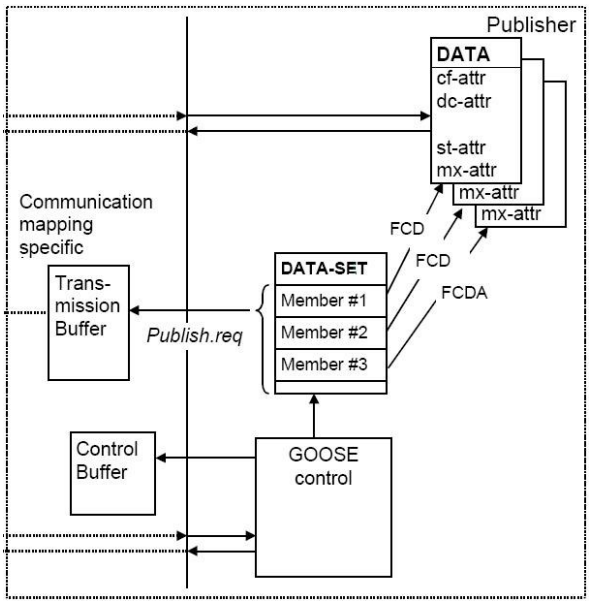


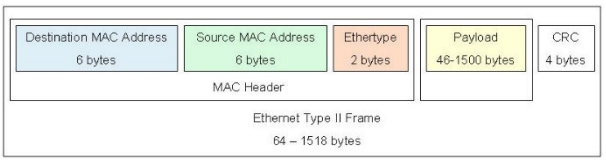
Figure 2: Publisher functionality

The publisher writes the values in a transmission buffer at the sending side and multicasts them over the substation local area network to the different subscribers – clients or servers.

The data in the published GOOSE messages is a collection of values of data attributes defined as members of a data set. The receiver reads the values from a local buffer at the receiving side. A GSE control class in the publisher is used to control the process. If the value of at least one of the DataAttributes has changed, the transmission buffer of the Publisher is updated with the local service “publish” and the values are transmitted with a GOOSE message.

The publisher/subscriber mechanism allows the source IED to reach multiple receiving IEDs thus significantly improving the efficiency of the communications interface. In substation communication networks this is based on the use of a MAC multicast destination address in the Ethernet frame shown in Table 1.

Table 1 Ethernet Type II frame



Where:

Destination address (6 bytes) identifies which station(s) should receive the frame

Source addresses (6 bytes) identifies the sending station

Length is 6 Octets and contains the value of the destination Media Access Control (MAC) address to which the GOOSE message is to be sent. The address shall be an Ethernet address that has the multicast bit set TRUE.

If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches.

Specific communication services in the subscribers update the content of their reception buffers and new values received are indicated to the related applications.

Since the GOOSE messages replace hard-wired signals used for protection and control applications IEC 61850 introduces mechanisms that ensure the delivery of the required information.

Once a new value of a date attributed has resulted in the multicasting of a new GOOSE message, the repetition mechanism ensures that the message is sent with a changing time interval between the repeated messages until a new change event occurs.

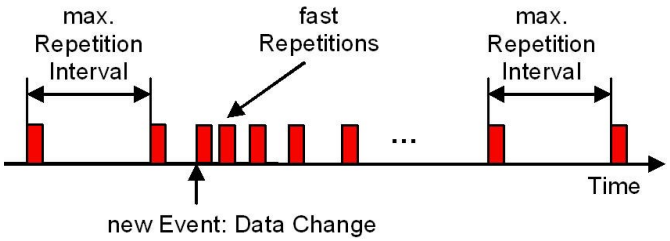


Figure 3: GOOSE repetition mechanism

As shown in Figure 3, at the beginning after a change the interval is very short – a few milliseconds, which later increases until it reaches a value of a few seconds. This method achieves several important tasks:

- Ensures that a loss of a single message is not going to affect the functionality of the system
- Allows any new device to inform all subscribing devices about its state
- Allows any new device to learn the state of all publishing devices it subscribes to

The GOOSE messages contain information that allows the receiving devices to know not only that a status has changed, but also the time of the last status change. This allows a receiving device to set local timers relating to a given event.

At the same time the repetition mechanism can be used as a heartbeat that allows the continuous monitoring of the communications interface – something that is not possible in conventional hard wired systems.

The state number and the sequence number can be used to detect intrusion, thus allowing significant improvement in the cyber security of the system without the need for encryption or other cyber security methods.

The GOOSE Control Block class defined in Edition 1 of IEC 61850 (Figure 4) includes attributes that define the behavior of the peer-to-peer communications and is related to a logical device, and more specifically to its LLN0.

GoCBName (GOOSE control name) identifies a GoCB within the scope of a GoCBRef (GOOSE control reference) - a unique path-name of a GoCB within LLN0:

LDName/LLN0.GoCBName

GoEna (GOOSE enable) indicates that the GoCB is Enabled (if set to TRUE) to send GOOSE messages. If set to FALSE it shall stop sending GOOSE messages.

AppID is an application identification represented by a visible string that represents a logical device in which the GoCB is located.

GoCB class	
Attribute name	**Value/value range/explanation**
GoCBName	Instance name of an instance of GoCB
GoCBRef	Path-name of an instance of GoCB
GoEna	Enabled (TRUE) | disabled (FALSE)
AppID	Attribute that allows a user to assign a system unique identification for the application that is issuing the GOOSE. DEFAULT GoCBRef
DatSet	
ConfRev	
NdsCom	
Services	
SendGOOSEMessage GetGoReference GetGOOSEElementNumber GetGoCBValues SetGoCBValues	

Figure 4: GOOSE Control Block class

DatSet is the reference of the data set whose values of members shall be transmitted.

ConfRev is the configuration revision indicating the number of times that the configuration of the data set referenced by DatSet has been changed. The counter is incremented every time when the configuration changes.

NdsCom (needs commissioning) is TRUE if the attribute DatSet has a value of NULL and is used to indicate that the GoCB requires configuration.

GOOSE message		
Parameter name	**Parameter type**	**Value/value range/explanation**
DatSet	ObjectReference	Value from the instance of GoCB
GoID	VISIBLE STRING129	Value from the instance of GoCB
GoCBRef	ObjectReference	Value from the instance of GoCB
T	TimeStamp	
StNum	INT32U	
SqNum	INT32U	
Simulation	BOOLEAN	(TRUE) simulation | (FALSE) real values
ConfRev	INT32U	Value from the instance of GoCB
NdsCom	BOOLEAN	Value from the instance of GoCB
GOOSEData [1..n]		
Value	(*)	(*) type depends on the appropriate common data classes (CDC).

Figure 5: GOOSE message

As already mentioned, the content of the GOOSE message (shown in Figure 5) allows the receiving devices to perform processing of the data in order to execute required actions. Some of the attributes in the GOOSE message that help perform the functions described earlier are:

T – the time stamp representing the time at which the attribute StNum was incremented.

StNum indicates the current state number - a counter that increments every time a GOOSE message (including a changed value) has been sent for the first time. The initial value is 1.

SqNum is the sequence number – the value of a counter that increments each time a GOOSE message with the same values has been sent. The initial value is 1.

Simulation is a parameter that indicates that the GOOSE message is used for test purposes (if the value is TRUE) and that the values of the message have been issued by a simulation unit and shall not be used for operational purposes. The GOOSE subscriber will report the value of the simulated message to its application instead of the —reall‖ message depending on the setting of the receiving IED.

The basic concept described above applies also to the GSSE model is similar to the GOOSE model. However, there are a couple of major differences:

- GOOSE provides flexibility in the definition of a data set with different data types, while GSSE provides only a simple list of status information.
- While the mapping of GOOSE to IEC 61850 8-1 supports VLAN and priority tagging

2.1 R-GOOSE

The GOOSE message was designed for peer-to-peer substation communications and because of that it uses a three layer stack and MAC multicast.

This is not suitable for messages that need to be sent over a wide area network. For that reason the technical report IEC 61850 90-5 Use of IEC 61850 to transmit synchrophasor information according to

IEEE C37.118 selected UDP/IP as the option to transmit data over arbitrary large distances.

The Internet Protocol (IP) is a Layer 3 protocol. The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examine to determine if the data has reached its final destination. If that is true, this Layer 3 formats the data into packets delivered up to the Transport layer. The IP allows the routing of data packets (IP packets) between different networks over any distance.

The User Datagram Protocol (UDP) is a Transport Layer 4 network protocol. While TCP (Transmission Control Protocol) is a connection oriented protocol that requires first to establish communications between a client and a server, UDP is connectionless, which makes it more suitable for GOOSE communications.

UDP network traffic is organized in the form of datagrams. A datagram comprises one message unit. The first eight (8) bytes of a datagram contain header information and the remaining bytes contain message data.

A UDP datagram header consists of four (4) fields of two bytes each:

- source port number
- destination port number
- datagram size
- checksum

The UDP checksum protects the message data from tampering. The checksum value represents an encoding of the datagram data calculated first by the sender and later by the receiver. If the checksum does not match indicating a tampered or corrupted data during transmission, the UDP protocol detects it. In UDP the check sum is optional as opposed to TCP where it is mandatory.

The many working applications of the IEEE C37.118 protocol confirm that the use of UDP for the streaming of the synchrophasor data is a proven method that can also be used for the routable GOOSE.

Considering the importance of the check sum as a cyber security tool, IEC 61850 8-1 Edition 2.1 defines

It as mandatory for the IEC 61850 implementations.

The table below shows the UDP field implementation requirements defined in the standard.

UDP	Mandatory/Optional/ eXcluded
Source Port	M
Destination Port	M
Length	M
Checksum	M

3 R-GOOSE Applications

The R-GOOSE may have many different applications.

It can be used for complex hierarchical System Integrity Protection Schemes (SIPS) at the transmission level of the system in order to communicate the change of state of system components that have an impact on the stability of the system. It also can be used by the SIPS to send GOOSE messages to the system components that are used to execute the required actions.

At the distribution level of the system the R-GOOSE can be used very successfully for Distribution Automation applications.

3.1 System Integrity Protection Schemes

System Integrity Protection Schemes are distributed applications based on exchange of information and control signals between substation intelligent electronic devices located in different substation throughout the system.

SIPS play a very critical role in maintaining the stability of the electric power system through load-shedding or shutting down generators. That is why it is very important to ensure that they are properly tested before being put in service.

SIPS can be considered as systems that have three main types of functional elements:

- System monitoring elements
- Protection elements
- Execution elements

The function of the system monitoring elements is to:

- Detect a change in the electric power system topology
- Detect a change in system load
- Detect a change in generation

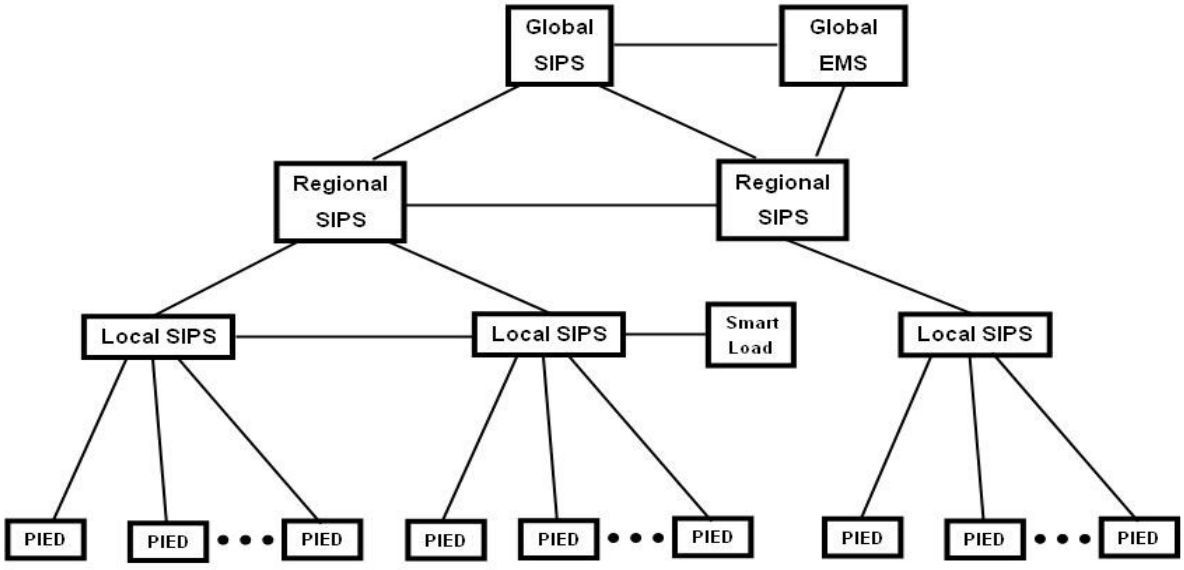


Figure 6: Simplified block diagram of a hierarchical System Integrity Protection Scheme

The function of the system integrity protection is to determine if any of the above changes or their combination represents a threat for the stability of the electric power system. If there is a possibility for a local or wide area disturbance, it needs to make a decision and send signals for some action required to prevent the disturbance or at least limit the effect from the event.

The function of the execution elements is to receive the signals from the protection system and execute locally the required action.

SIPS can be simple and complex with different number of levels in the hierarchy depending on the complexity of the system. Figure 6 shows a multilevel SIPS that uses multifunctional protection IEDs as the devices at the monitoring and execution levels of the system.

As can be seen from Figure 6, a System Integrity Protection Scheme requires different types of communications:

- Between multifunctional intelligent electronic devices (IEDs) at the bottom of the hierarchy and the substation level (Local SIPS)
- Between SIPS at the same levels
- Between the different levels of the SIPS
- Between SIPS and smart loads

All of the above communications interfaces may be based on different protocols and use different types of communications links. IEC 61850 is playing an increasingly important role due to the significant benefits that high-speed peer-to-peer messages play in the implementation of different functional elements of the scheme.

The monitoring functions are typically based on:

- Current, voltage, active and reactive power measurements
- Synchrophasor measurements
- Monitoring the status of breakers associated with transmission lines, transformers and generators

The execution elements usually operate a breaker to reduce the load. They may also reduce the output of a generator or completely shut it down.

3.2 R-GOOSE Applications to SIPS

The R-GOOSE described above has multiple applications in SIPS. It brings some significant benefits for wide area distributed applications, especially when they are based on cloud communications technologies. The cyber security features defined in IEC 61850 90-5 and IEC 62351 provide a high level of security, which is a key requirement for SIPS.

The following are some of the main applications of R-GOOSE communications in SIPS:

- Exchange of load and power flow information between the local monitoring elements of the SIPS and the higher levels of the SIPS hierarchy based on analog R-GOOSE
- Exchange of breakers and switches status information between the local monitoring elements of the SIPS and the higher levels of the SIPS hierarchy based on R-GOOSE
- Exchange of aggregated load, power flow and status information between the higher levels of the SIPS hierarchy based on R-GOOSE and analog R-GOOSE
- Exchange of tripping and control signals between the higher levels of the SIPS hierarchy and the local execution elements based on R-GOOSE

3.3 R-GOOSE Applications to Distribution Automation

The R-GOOSE described above has also multiple applications in Distribution Automation. It brings some significant benefits for such distributed applications, especially when they are based on wireless communications.

An example of such distribution automation application is fault location, isolation, and service restoration (FLISR) technologies and systems that can help accomplish fewer and shorter outages.

The implementation of FLISR can be accomplished using peer-to-peer communications between the IEDs at the reclosers. Since typically there are no fiber channels on the distribution circuits, using R-GOOSE messages over wireless communications is a solution.

3.4 R-GOOSE Applications to Transmission Line Protection

The R-GOOSE can also be used in case we need to reduce the fault clearing time for short circuit faults in Zone 2 of the distance protection. In this case if a Permissive Overreaching Transfer Trip (POTT)

scheme is used, R-GOOSE message is sent from the start of the Zone 2 distance element to the remote end, and the line is tripped without any additional time delay when the message is received by the distance protection IED.

4 Benefits of Using R-GOOSE

There are some significant benefits in using R-GOOSE:

It uses existing wide area communications which eliminates the need of dedicated communication channels typically used for protection and control applications.

It meets the requirements for cyber security when communicating using the routable communications services

Since it is based on the IEC 61850 standard, it supports communications interoperability between IEDs from different manufacturers

As a result, the reliability, security and efficiency of the electric power system can be significantly improved, moving us towards meeting the goals of a smarter grid.

5 Conclusions

R-GOOSE is a version of the popular IEC 61850 peer-to-peer communications method that can be used for wide area protection and control applications.

While the principles remain the same, the R-GOOSE uses UDP multicast as the transport mechanism.

R-GOOSE offers significant benefits for many different electric power system protection, automation and control applications, such as:

- System Integrity Protection Schemes at the transmission level
- Distribution automation systems
- Accelerated transmission line protection schemes
- Accelerated distribution protection schemes

Such applications will have a positive impact on the efficiency of the protection and control systems in smart grids.

Biography

Dr. Alexander Apostolov received MS degree in Electrical Engineering, MS in Applied Mathematics and Ph.D. from the Technical University in Sofia, Bulgaria. He has 42 years' experience in power systems protection, automation, control and communications.

He is presently Principal Engineer for OMICRON electronics in Los Angeles, CA.

He is IEEE Fellow and Member of the Power Systems Relaying Committee and Substations C0 Subcommittee. He is past Chairman of the Relay Communications Subcommittee, serves on many IEEE PES Working Groups and is Chairman of Working Groups C2 "Role of Protective Relaying in Smart Grid".

He is member of IEC TC57 working groups 10, 17, 18 and 19. He is Leader of the Task force "Functional testing of IEC 61850 based devices and systems".

He is Distinguished Member of CIGRE and Convenor of CIGRE WG B5.53 "Test Strategy for Protection, Automation and Control (PAC) functions in a full digital substation based on IEC 61850 applications" and member of several other CIGRE B5 working groups.

He holds four patents and has authored and presented more than 500 technical papers.

He is IEEE Distinguished Lecturer and Adjunct Professor at the Department of Electrical Engineering, Cape Peninsula University of Technology, Cape Town, South Africa.

He is Editor-in-Chief of PAC World.