Wide Area GOOSE and Its Applications to System Integrity Protection Schemes

Alexander APOSTOLOV
OMICRON electronics – USA
alex.apostolov@omicronenergy.com

ABSTRACT

The expansion of IEC 61850 outside of the substation is the next step in the evolution of the standard that improves its functionality in order to better serve the Smart Grid. The paper discusses the definition of a routable GOOSE message, the differences with the conventional GOOSE and its applications for System Integrity Protection Schemes.

INTRODUCTION

IEC 61850 has been identified for more than ten years as a cornerstone technology for the Smart Grid. One of the key components that gives it this role is the Generic Object Oriented Substation Event (GOOSE) message that supports peer-to-peer communications between multifunctional Intelligent Electronic Devices (IEDs) which meet the high speed performance requirements of protection and automation applications. It was originally designed as a non-routable message used within the substation over the local area network. The success of using GOOSE messages for substation protection applications makes it attractive for use between IEDs in wide area protection systems. These are applications that impose different requirements on the peer-to-peer communications. The paper first introduces the concept of the routable GOOSE (R-GOOSE) and then discusses its applications in wide area protection and control.

Even that GOOSE messages have already been used in protection and automation applications outside of the substation, the fact that they are transmitted over wide area networks makes them vulnerable to cyber-attacks.

In order to address such concerns IEC TC 57 Working Group 10 developed the technical report IEC 61850 90-5, [2] which defined the communications of synchrophasors and GOOSE over wide area networks. The communications are based on the full seven layer OSI stack and use TCP/UDP multicast. The document also describes the use of end-to-end cyber security based on the definitions in the IEC 62351 standard.

The availability of secure peer-to-peer communications allows the use of R-GOOSE messages in distributed wide area protection systems. The bi-directional exchange of information between field IEDs and the wide area protection system controller for the monitoring of the power system, as well as for the execution of required actions to isolate faulted sections and maintain the stability of the electric power grid.

The benefits of using R-GOOSE for System Integrity Protection Schemes are presented at the end of the paper.

SYSTEM INTEGRITY PROTECTION SCHEMES

System Integrity Protection Schemes (SIPS) are distributed applications based on exchange of information and control signals between intelligent electronic devices located in different substations or feeders throughout the electric power system.

They play a very critical role in maintaining the reliability of the electric power system through different advanced protection and control functions, such as:

- system reconfiguration
- adaptive protection settings control
- distributed energy resources control
- load management
- load shedding

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

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 SIPS and execute locally the required action.

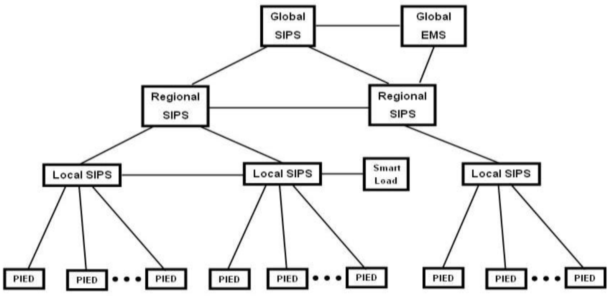


Fig. 1 Simplified block diagram of a hierarchical System Integrity Protection Scheme

SIPS can be simple and complex with different number of levels in the hierarchy depending on the complexity of the system. Figure 1 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 1, a wide area protection system 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 or other switching device in order to perform a specific action such as system reconfiguration or to reduce the load. They may also reduce the output of a distributed generator or completely shut it down.

GOOSE VERSUS 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.

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 2.

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.

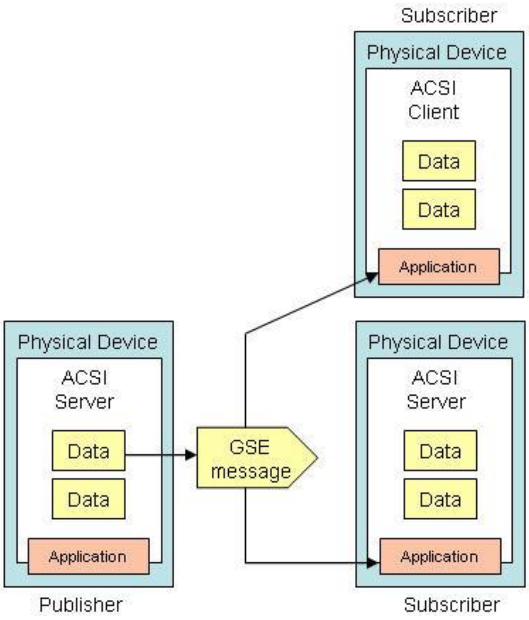


Fig. 2 Publisher/Subscriber mechanism

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.

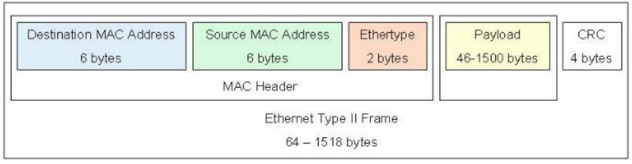
The generic substation event model is used to exchange the values of a collection of Data Attributes defined as a Data Set. GOOSE supports the exchange of a wide range data types organized in a data set.

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.

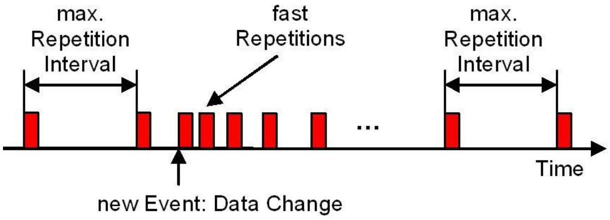


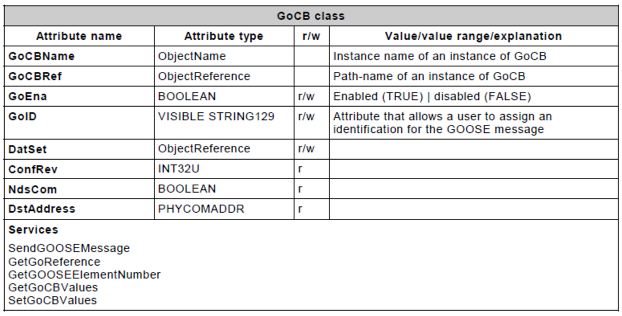
Fig. 3 GOOSE repetition mechanism

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.



GoCB class			
Attribute name	**Attribute type**	**r/w**	**Value/value range/explanation**
GoCBName	ObjectName		Instance name of an instance of GoCB
GoCBRef	ObjectReference		Path-name of an instance of GoCB
GoEna	BOOLEAN	r/w	Enabled (TRUE) | disabled (FALSE)
GoID	VISIBLE STRING129	r/w	Attribute that allows a user to assign an identification for the GOOSE message
DatSet	ObjectReference	r/w	
ConfRev	INT32U	r	
NdsCom	BOOLEAN	r	
DstAddress	PHYCOMADDR	r	
Services SendGOOSEMessage GetGoReference GetGOOSEElementNumber GetGoCBValues SetGoCBValues			

Fig. 4 GOOSE Control Block class

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 2 [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.
GoID is a user definable identification of the GOOSE message.
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.
DstAddress is the SCSM specific addressing information like media access address, priority, and other information

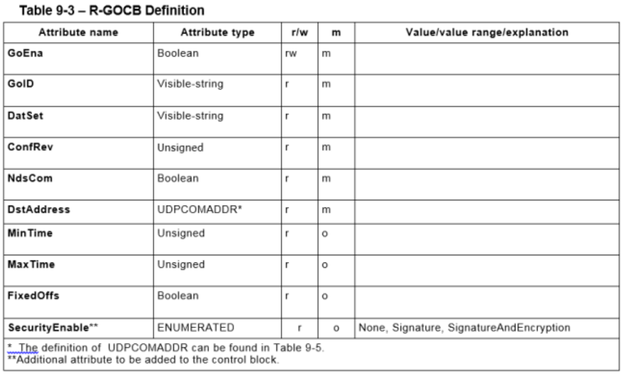


Table 9-3 – R-GOCB Definition

Attribute name	Attribute type	r/w	m	Value/value range/explanation
GoEna	Boolean	rw	m	
GoID	Visible-string	r	m	
DatSet	Visible-string	r	m	
ConfRev	Unsigned	r	m	
NdsCom	Boolean	r	m	
DstAddress	UDPCOMADDR*	r	m	
MinTime	Unsigned	r	o	
MaxTime	Unsigned	r	o	
FixedOffs	Boolean	r	o	
SecurityEnable**	ENUMERATED	r	o	None, Signature, SignatureAndEncryption
* The definition of UDPCOMADDR can be found in Table 9-5. **Additional attribute to be added to the control block.				

Fig. 5 R-GOOSE Control Block class

The R-GOOSE control block defined in IEC 61850 90-5 has the DstAddress as UDPCOMMADR. Its structure includes attributes that support the use of both IPv4 and IPv6 addresses.

As already mentioned, the content of the GOOSE message 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 –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 ―real‖ message depending on the setting of the receiving IED.

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:

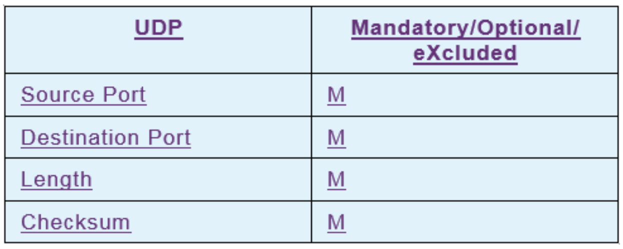
- source port number
- destination port number
- datagram size
- checksum

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.

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

Table II UDP Implementation requirements



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

R-GOOSE APPLICATIONS IN 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 wireless 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.

R-GOOSE can be used for both vertical and horizontal communications in hierarchical 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

CONCLUSIONS

R-GOOSE is an important addition to the arsenal of tools provided to protection and control engineers involved in the development of SIPS for smart grids.

It allows the development and implementation of high-speed peer-to-peer communications based system integrity protection schemes that result in the improved reliability of the electric power grid.

REFERENCES

[1] IEC TR 61850 7-2:2010 Communication networks and systems in substations –Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)

[2] IEC TR 61850 90-5:2012 Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

[3] IEC TS 62351-6:2007 Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850