Can we use IEC 61850 for safety related functions?

Micaela Caserza Magro, Paolo Pinceti, Luca Rocca
Department DITEN
University of Genova
Genova, Italy
paolo.pinceti@unige.it

***Abstract*—Safety is an essential issue for processes that present high risk for human beings and environment. An acceptable level of risk is obtained both with actions on the process itself (risk reduction) and with the use of special safety systems that switch the process into safe mode when a fault or an abnormal operation mode happens. These safety systems are today based on digital devices that communicate through digital networks. The IEC 61508 series specifies the safety requirements of all the devices that are involved in a safety function, including the communication network. Also electrical generation and distribution systems are processes that may have a significant level of risk, so the criteria stated by the IEC 61508 applies.**

Starting from this consideration, the paper analyzes the safety requirement for the communication network and compare them with the services of the communication protocol IEC 61850 that represents the most used protocol for automation of electrical plants. The goal of this job is to demonstrate that, from the technical point of view, IEC 61850 can be used for implementing safety-related functions, even if a formal safety certification is still missing.

***Keywords*—communication protocols, fieldbus, functional safety, IEC 61508, IEC 61850**

I. Introduction

The automation system of an electrical generation or distribution system is today based on intelligent electronic devices (IED) connected through a digital network. Each intelligent device controls, protects, supervises, measures a section of the plant. In medium voltage switchgears we normally have an intelligent device per cubicle, in high voltage substations one or more per bay.

All the status signals, interlocks, closing or tripping commands are transmitted through the communication network. Some general purpose protocols can be used for communicating with intelligent devices (e.g. Modbus RTU, Ethernet TCP/IP and others), but also specific protocols for electrical plants exist, like the series IEC 60870 and DNP3. All these protocols can be effectively used for the configuration and the interrogation of the IEDs, and support all the functions that are typical of a SCADA (Supervisory, Control, And Data Acquisition). On the other hand, none of these protocols supports real-time functions, so they cannot be used for commands or interlocks. The only protocol that supports all the functions required for the substation automation is the more recent IEC 61850. It has services both for SCADA and for real time functions. With the use of IEC 61850, protection logic, safety interlocks, commands from real time functions (e.g. load-shedding) are transmitted digitally. Fig. 1 shows a typical architecture of the automation system in a substation, with different protocols used for different functions:

- IEC 61850 for real-time control
- IEC 61870 for remote control
- TCP/IP for remote maintenance
- USB for local set-up and commissioning

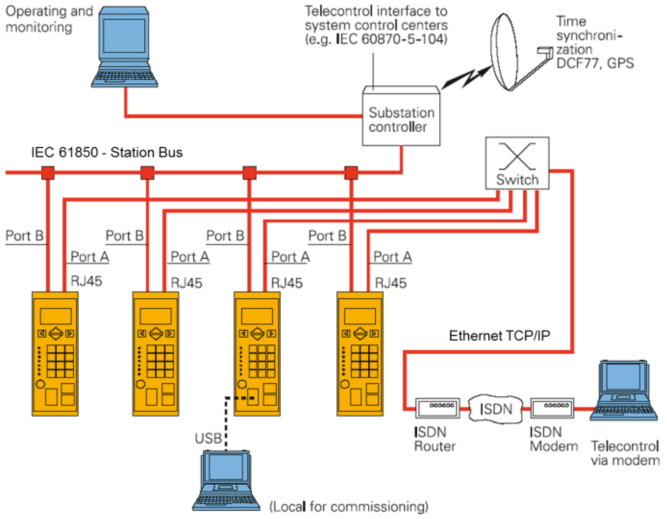


Fig. 1. Typical architecture for substation automation

With a full-digital architecture, also the commands related to safety functions are transmitted through the communication protocol. In electrical plants most safety commands lead to the de-energization of a circuit or a machinery (e.g. the emergency stop of a motor, fire alarm, etc.). In some cases, the safety electrical command is related to a risk of the process and requires the energization of a circuit (e.g. starting a ventilation fan in a tunnel, starting an emergency generator, switching from one source to another, etc.).

Fig. 2 shows an example of interaction between an emergency stop push button and the trip of one or more circuit breakers. When the button is pushed, the safety PLC receives the status through the safety fieldbus and sends a trip command to the station control unit on the IEC 61850 network. Then the trip command is sent on the IEC 61850 bus, normally via GOOSE message, to the IEDs that command the relevant circuit breakers.

The paper analyses the requirements of communication protocols when used for carrying out safety functions, with reference to the international standards series IEC 61508. The transmission mechanisms of IEC 61850 are then considered to check if it can be used for safety related functions.

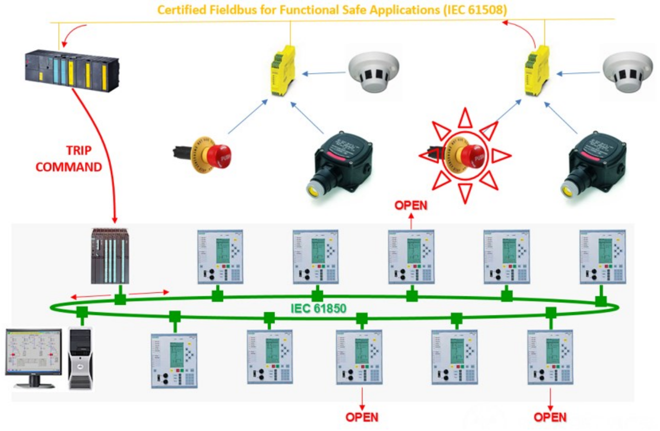

Certified Fieldbus for Functional Safe Applications (IEC 61508)
TRIP
COMMAND
OPEN
IEC 61850
OPEN
OPEN

Fig. 2. Example of safety system interaction with IEC 61850

II. FUNCTIONAL SAFETY CONCEPTS

Safety is a concept dealing with the reduction of the risk of physical injury or of the damage to the people/environment health. The overall risk must be below the so-called acceptable risk. There are several concepts of safety, and this paper focuses on the functional safety, which involves the operation of the industrial processes or machineries.

Functional safety [1] is a part of the overall safety, and it is based on the principle that a system or equipment operates correctly in response to its inputs. Functional safety cannot be determined without considering the system as a whole and the environment with which it interacts.

A process or a machinery has an intrinsic level of risk. The risk is the probability of happening of a fault multiplied by the consequences of the fault, in terms of damages to people or to the environment. If the risk of a certain fault or malfunction is above the acceptable risk, it is necessary to introduce a safety related function to reduce it. Such a function has the role to intervene for avoiding the fault or for reducing the consequences of the fault; in other words, for reducing the risk below the level of acceptable risk. The safety related systems can be implemented using any technology, but there is the constraint to respect some requirement of integrity. This means that it is mandatory that any safety related system has an adequate integrity level for assuring the proper operation. Integrity is here intended as the probability that a specific function/system is properly working when requested. The required safety integrity level (SIL) of a safety function must be adequate to the risk of the process/machine malfunctioning. The higher the risk of a fault the higher the required SIL.

Today, most safety related functions use electrical and/or electronic and/or programmable electronic (E/E/PE) technologies. E/E/PE safety functions are regulated by the IEC 61508 series [2].

One of the concept within the IEC 61508 is the definition of safety function as the coordinated operation of some basic elements, like in Fig. 3:

- Sensors, that are responsible for measuring or detecting the abnormal operation,
- Analogic/digital conversion, if needed,
- Logic solver, within one Programmable Logic Controller PLC, that may be programmable or not. It is responsible for implementing the safety logic according to the inputs coming from the sensors,
- Analogic/digital conversion, if needed,
- Actuators, that are responsible for acting on the process to drive the overall system in a safe condition.

The concept and performance of SIL applies to the overall safety function, thus the Probability of Failure on Demand (PFD) of each component should be compliant to the requirements identified to achieve the requested PFD of the complete safety function. The IEC 61508 defines four level of SIL: from 1 to 4. The higher the SIL the lower the PFD for the safety function and the higher the reduction of the risk. Note that PFD is a value that indicates the probability of a system failing to respond to a demand. The average probability of a system failing to respond to a demand in a specified time interval is referred as PFDavg.

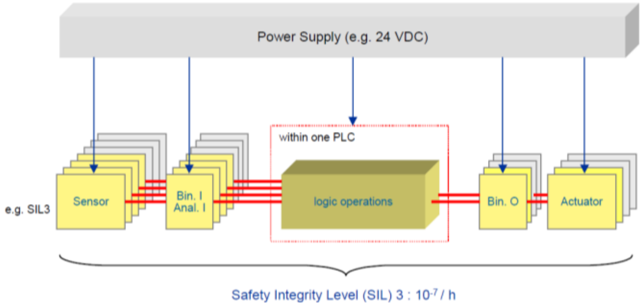

Power Supply (e.g. 24 VDC)
within one PLC
e.g. SIL3
Sensor
Bin. I
Anal. I
logic operations
Bin. O
Actuator
Safety Integrity Level (SIL) 3 : 10^{-7} / h

Fig. 3. Example of a safety function

TABLE I. VALUES OF PFD ACCORDING TO THE SIL VALUE

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Safety concepts are applied both to the hardware and to the software related to safety functions. This means that also the software should comply with the required PFD. The software is both the firmware and the specific application software. This is an important aspect also for the operation and the connections between the components of the safety function.

Traditionally, the connection between the field devices and the logic solver uses copper cables for transmitting ON/OFF or

4/20 mA signals. Today, with the wide use of digital communication networks there is the need of using digital communication protocols even for safety functions.

A communication system contains a hardware part (cables and communication chips) and a firmware part, responsible for the definition of the telegram, the technique for accessing the medium, the mechanism for transmitting, and so on. For safety applications, it is necessary that also the communication protocol comply with integrity requirements. IEC 61508 allows the use of digital communication protocol for safety functions, but it requires that methods are implemented to detect transmission errors. In a quantitative way, IEC 61508 requires that the communication system use no more than the 1% of the budget PFD for the safety function (see **Błąd! Nie można odnaleźć źródła odwołania.**).

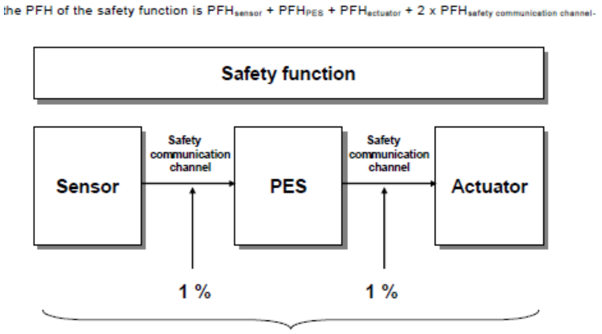

the PFH of the safety function is $PFH_{sensor} + PFH_{PES} + PFH_{actuator} + 2 \times PFH_{safety\ communication\ channel}$-
Safety function
Sensor
Safety communication channel
PES
Safety communication channel
Actuator
1 %
1 %

Fig. 4. Safety communication as a part of safety function

III. IEC 61850 BASICS

IEC 61850 is an Ethernet based protocol typical of electrical automation systems. Its main goal is to exploit the ability of IEDs from different manufacturers to exchange information used for protection, control and monitoring of an electrical substation. The standard defines this feature as interoperability [5].

The IEC 61850 series consists of ten parts that specify all the various aspects of communication into details. Section 7 is the core of the standard's innovative concepts. The standard defines all the devices and functions that exist in a substation, and it organizes them into a set of Logical Nodes. A LN has a four letters standardized name in which the first letter defines the class the LN belongs, i.e. protection, control or monitoring. LNs are the interface between the automation functions and the real world: the IED's manufacturer, following its own engineering practices, implements the function while the structure of data and data exchange are standardized.

Section 7.2 defines the information models and the information exchange service models (ACSI Abstract communication service interface). The information model consists on the definition of four elementary classes that can model any type of logic device [6]:

- **Server** – it represents the visible behavior of the device from the outside. A server's role is to manage communication with the client and send information to the other servers,
- **Logical Device (LD)** – it contains information managed and shared between different applications hosted in the same device. Homogeneous info are grouped into Logical Nodes,
- **Logical Node (LN)** – it contains the elementary data necessary for implementing the function the logical node refers to (i.e. overcurrent protection, measuring, breaker command, etc.),
- **Data** – it represents the value of interest with all the attributes that are used to describe it.

The ACSI comprises also the information exchange models needed to operate on data, which are:

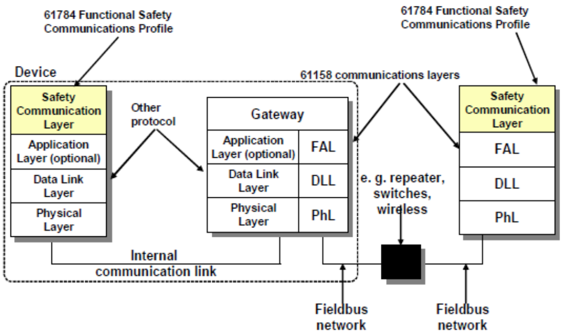
- **Data sets** – used to group data,
- **Substitution** – supports replacement of a process value by another value,
- **Setting group control block** - permits to switch from one set of setting values to another one,
- **Report control block** - describes the model used to exchange information between a LN and a client. Report generation can be triggered by a change of a process data value,
- **Control blocks for generic substation event (GSE)** - describes the exchange of hard real-time information. It is used for information changing sporadically and it provides simultaneous delivery of the same message to multiple devices using multicast/broadcast frames. The principal information exchange model for time critical information like tripping function or interlocking is called Generic Object Oriented Substation Event (GOOSE),
- **Control blocks for transmission of sampled values** - used by measuring devices to send fast and cyclically analog sampled values,
- **Control** - describes the services that a client use to control an IED,
- **Time and time synchronization** - provides the time base to the substation automation system,
- **File transfer** - provides the exchange of large data.

IV. REMEDIAL MEASURES TO DETECT ERRORS AND FAILURES OF A COMMUNICATION SYSTEM

If used in a safety function, the communication system must implement specific measures to detect communication errors and failures [3]. This is mandatory in order to avoid that any error or fault compromises the proper operation of the safety function.

While IEC 61508 does not restrict the use of communication technologies, IEC 61784-3 [3] focuses on the use of fieldbus based functional safety communication systems. When using IEC 61158 [4] based fieldbus structures without modifications in the definition of each communication layer, all the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 shall be supported by an additional "safety communication layer".

Fig. 5 describes the so-called “black channel” approach. The communication protocol of the selected fieldbus is not affected by any additional safety service. All the safety functions are in an additional layer, the safety layer, which is above the 7th layer (application) of the protocol. The safety messages are embedded within the standard protocol.



61784 Functional Safety Communications Profile
61784 Functional Safety Communications Profile
Device
61158 communications layers
Safety Communication Layer
Application Layer (optional)
Data Link Layer
Physical Layer
Other protocol
Gateway
Application Layer (optional)
FAL
Data Link Layer
DLL
Physical Layer
PhL
e. g. repeater, switches, wireless
Safety Communication Layer
FAL
DLL
PhL
Internal communication link
Fieldbus network
Fieldbus network

Fig. 5. Implementation of a safety layer over a standard fieldbus communication system

The role of the safety profile or layer is to detect all the possible errors that may lead to the loss or the corruption of the packets.

The safety data must satisfy the following requirements:

- Trusted data, the safety data must be correct,
- Correct receiver, the receiver of the data must be correct,
- Just in time, the data must receive the destination at a proper time.

The first step is to consider what are the possible errors in a digital communication system, as in IEC 61784:

- **Corruption**: Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference,
- **Unintended repetition**: Due to an error, fault or interference, old not updated messages are repeated at an incorrect point in time,
- **Incorrect sequence**: Due to an error, fault or interference, the predefined sequence (for example natural numbers, time references) associated with messages from a particular source is incorrect,
- **Loss**: Due to an error, fault or interference, a message is not received or not acknowledged,
- **Unacceptable delay**: Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied,
- **Insertion**: Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity,
- **Masquerade**: Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a safety relevant participant, which then treats it as safety relevant, may receive a non-safety relevant message,
- **Addressing**: Due to a fault or interference, a safety relevant message is sent to the wrong safety relevant participant, which then treats reception as correct.

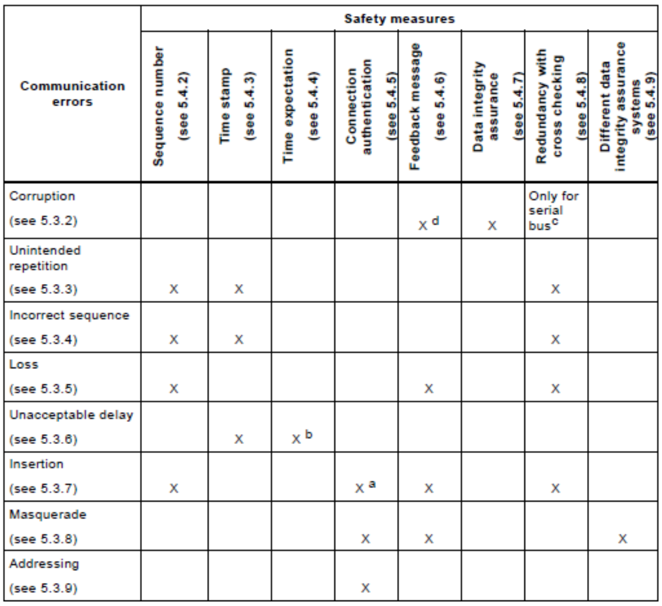
Starting from the list of the possible errors in the communication system, the IEC 61784 defines the measures that can be implemented in the communication stack in order to detect the errors and to set the system into a safe condition.

Proposed remedial measures are:

- **Sequence number**: A sequence number is integrated into messages exchanged between message source and message sink,
- **Time stamp**: In most cases the content of a message is only valid at a particular point in time. The time stamp may be a time, or time and date, included in a message by the sender,
- **Time expectation**: During the transmission of a message, the message sink checks whether the delay between two consecutively received messages exceeds a predetermined value. In this case, an error has to be assumed,
- **Connection authentication**: Messages may have a unique source and/or destination identifier that describes the logical address of the safety relevant participant,
- **Feedback message**: The message sink returns a feedback message to the source to confirm reception of the original message. This feedback message has to be processed by the safety communication layers,
- **Data integrity assurance**: The safety-related application process shall not trust the data integrity assurance methods if they are not designed from the point of view of functional safety. Therefore, redundant data is included in a message to permit data corruptions to be detected by redundancy checks,
- **Redundancy with cross checking**: In safety-related fieldbus applications, the safety data may be sent twice, within one or two separate messages, using identical or different integrity measures, independent from the underlying fieldbus. In addition to this, the transmitted safety data is cross-checked for validity over the fieldbus or over a separate connection source/sink unit. If a difference is detected, an error shall have taken place during the transmission, in the processing unit of the source or the processing unit of the sink.

In a safety communication profile errors must be detected and the methods for doing so are those described above. It is not mandatory to implement all the protection measures, since it is necessary to implement only the measures that can avoid all the possible errors.

IEC 61784-3 defines the correlation between the errors and the possible detection methods (Fig. 6).



Communication errors	Safety measures							
	Sequence number (see 5.4.2)	Time stamp (see 5.4.3)	Time expectation (see 5.4.4)	Connection authentication (see 5.4.5)	Feedback message (see 5.4.6)	Data integrity assurance (see 5.4.7)	Redundancy with cross checking (see 5.4.8)	Different data integrity assurance systems (see 5.4.9)
Corruption (see 5.3.2)					X [d]	X	Only for serial bus[c]	
Unintended repetition (see 5.3.3)	X	X					X	
Incorrect sequence (see 5.3.4)	X	X					X	
Loss (see 5.3.5)	X				X		X	
Unacceptable delay (see 5.3.6)		X	X [b]					
Insertion (see 5.3.7)	X			X [a]	X		X	
Masquerade (see 5.3.8)				X	X			X
Addressing (see 5.3.9)				X				

Fig. 6. Overview of the effectiveness of the various measures on the possible errors

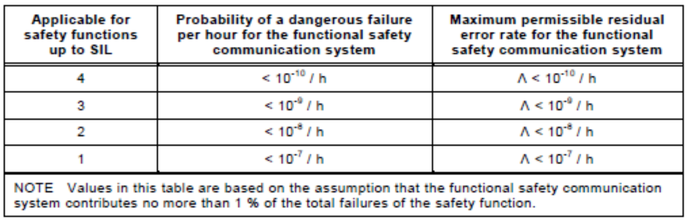
Even when the messages are arriving in a correct (deterministic) manner the safety data still may be corrupted. Thus data integrity assurance is a fundamental component of the safety communication layer to reach a required safety integrity level. Suitable hash functions like parity bits, cyclic redundancy check (CRC), message repetition, and similar forms of message redundancy shall be applied.

Generally, the communication channel shall not use the same hash function the superimposed safety communication layer uses. The safety code shall be functionally independent from the transmission code.

The residual error rate is calculated from the residual error probability of the superimposed (safety) data integrity assurance mechanism and the transmission rate of safety messages. The number of destination sinks has to be considered for this calculation.

The value of admissible residual error is related to the SIL level of the safety function, like TABLE II. shows.

TABLE II. RELATIONSHIP OF RESIDUAL ERROR RATE TO SIL LEVEL

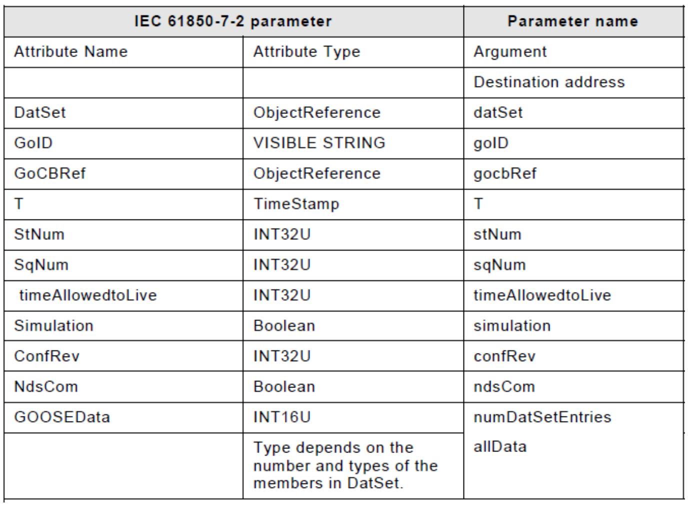


Applicable for safety functions up to SIL	Probability of a dangerous failure per hour for the functional safety communication system	Maximum permissible residual error rate for the functional safety communication system
4	$< 10^{-10}$ / h	$\Lambda < 10^{-10}$ / h
3	$< 10^{-9}$ / h	$\Lambda < 10^{-9}$ / h
2	$< 10^{-8}$ / h	$\Lambda < 10^{-8}$ / h
1	$< 10^{-7}$ / h	$\Lambda < 10^{-7}$ / h
NOTE Values in this table are based on the assumption that the functional safety communication system contributes no more than 1 % of the total failures of the safety function.		

V. SAFETY ANALYSIS OF IEC 61850'S COMMUNICATION SERVICES

Protection and interlocking functions are the main applications that may require a functional safe communication system. These functions use the GOOSE model to exchange information.

GOOSE is based on a publisher/subscriber mechanism, and it uses a multicast transmission of data. If the value of one or more data configured in the GOOSE application changes, one IED (the publisher) sends a message to a group of IEDs (the subscribers) simultaneously within a single GOOSE message. In addition to the data, a GOOSE frame contains a set of parameters that describe the message itself (see Fig. 7).



IEC 61850-7-2 parameter		Parameter name
Attribute Name	Attribute Type	Argument
		Destination address
DatSet	ObjectReference	datSet
GoID	VISIBLE STRING	goID
GoCBRef	ObjectReference	gocbRef
T	TimeStamp	T
StNum	INT32U	stNum
SqNum	INT32U	sqNum
timeAllowedtoLive	INT32U	timeAllowedtoLive
Simulation	Boolean	simulation
ConfRev	INT32U	confRev
NdsCom	Boolean	ndsCom
GOOSEData	INT16U	numDatSetEntries
	Type depends on the number and types of the members in DatSet.	allData

Fig. 7. GOOSE service parameter mapping

In particular, GOOSE messages implement a time stamp parameter that contains the time at which one value configured in the data set has changed. At the same time, the parameter "state number" is incremented. This parameter represents a counter that increments each time a value change is detected within the data set, and a GOOSE message has been sent. The frame contains also a sequence number that increment each time a GOOSE message is sent. Time stamp, state number and sequence number are remedial measures against unintended repetition, incorrect sequence, loss, unacceptable delay, insertion errors as defined in section IV.

GOOSE data exchange allows the use of VLANs and priority tagging as defined in IEEE 802.1 Q. The use of VLANs permits defining the set of IEDs that shall receive the GOOSE message. This feature prevents a safety relevant information to be delivered to the wrong device and to cause unintended events or errors: it is a remedial measure against masquerade and addressing errors defined in [3].

The GOOSE message frame is terminated with a Frame Check Sequence. FCS field contains a number calculated from the data in the frame. The receiver calculates autonomously this number, and compares it with the number in the FCS field. If the numbers are different, the receiver knows that an error in the communication is occurred and it discards the corrupted frame.

Furthermore, GOOSE messages use a specific scheme of re-transmission to achieve the appropriate level of reliability (Fig. 8). When an event occurs, the GOOSE server generates a SendGOOSEMessage request and the current data set values are encoded in a GOOSE message. The GOOSE message is transmitted immediately and then retransmitted with a variable time interval (T_1, T_2, T_3) not defined by the standard and gradually increasing the parameter “sequence number”. An effective scheme of retransmission is based on an exponential increment of the time between the frames. The time interval increments until it reaches the retransmission stable time T_0 defined in the configuration of the GOOSE application as T_{max}. T_0 can be shortened by the event ((T_0) in Fig. 8). Each message in the retransmission sequence contains a timeAllowedToLive parameter that represents the time the receiver waits before the next retransmission. If the timeAllowedToLive expires, the receiver reports a communication problem, and the system should be switched in a safe mode. The retransmission mechanism explained can be used as a time expectation measure defined in section IV.

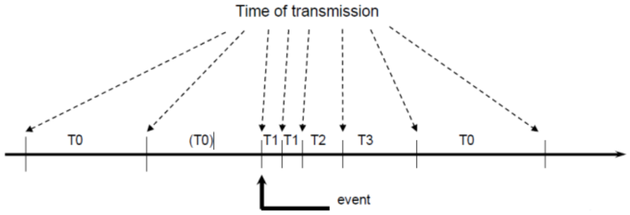


Fig. 8. Transmission time for events

VI. Conclusion

All the safety buses existing today use the “black channel” approach to detect communication errors. IEC 61850 does not implement any form of safety communication channel (black channel) as required by IEC 61784-3. However, the analysis made in section V reveals that the standard natively implements a bunch of remedial measures to detect all the communication errors defined by IEC 61784 [3]. The problem is that the standard does not define what must be done when a communication error is detected. If the communication between two IEDs fails, the system has to switch in a safe condition. It is reasonable to think that, for electrical plants, the safe state is considered a circuit de-energized. A possible solution is to implement in the 61850 stack the functions energize-to-trip and de-energize-to-trip. Another possible solution is to configure the IED to switch the system in safe mode when a communication error is detected using the IED’s configuration tool. The two solutions present a significant difference considering a hypothetical safe certification process. Implementing functions in the 61850 stack means that the stack should be certified compliant to the IEC 61508 standard; on the other hand, if a configuration software is used to program one or more safety function in a device, the software itself should be certified.

While this work focuses on IEC 61850 communication protocol, it is also important to remember that SIL’s concepts applies to all the hardware and the software that compose the safety system. This means that not only the communication protocol should be certified, but also all the IEDs and circuit breakers that compose the safety chain.

Further analysis will be made on a typical safety function that uses IEC 61850 as communication protocol. This will be useful to understand if IEC 61850 can satisfy the requirement of IEC 61508 about the maximum use of 1% of the budget PFD for a typical safety function and to estimate what is the maximum possible Safety Integrity Level of a safety system that uses a communication network based on IEC 61850.

References

[1] IEC 61508-0 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508”, 2010

[2] IEC 61508-1 “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements”, 2010

[3] IEC 61784 “Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions”

[4] IEC 61158 series “Industrial communication networks – Fieldbus specifications”, 2014

[5] IEC 61850-1 “Communication networks and systems for power utility automation – Part 1 Introduction and overview”, 2013

[6] IEC 61850-7-2 “Communication networks and systems for power utility automation – Part 7-2: Basic communication structure – Abstract communication service interface (ACSI)”, 2010

[7] IEC 61850-8-1 “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”

[8] K-P Brand, M.Ostertag, “Safety related, distributed functions in substations and the standard IEC 61850”, 2003 Bologna Power Tech Conference, June 23th-26th, Bologna, Italy

[9] J. Hoyos, M. Dehus and T. X. Brown, "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure", Proc. 2012 IEEE Globecom Workshops, pp. 1508-1513