Electrical Power and Energy Systems 104 (2019) 515–523

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Safety related functions with IEC 61850 GOOSE messaging

Micaela Caserza Magro, Paolo Pinceti*, Luca Rocca, Giorgio Rossi

Department DITEN, University of Genova, Genova, Italy

ARTICLE INFO

Keywords:
Communication protocols
Fieldbus
Functional safety
IEC 61508
IEC 61850

ABSTRACT

The international standard IEC 61508 introduces the concept of "safety related function" to achieve a satisfactory level of safety in processes that show unacceptable risks. A safety function is actuated by a safety system made up of one or more "sensors" that detect the abnormal condition, a "logic solver" that acquires the data from the sensor(s) and commands one or more "actuators" to drive the plant in safe condition. In many applications, the actuator is an electrical device, i.e. a circuit breaker that may be controlled through an IEC 61850 network. A typical architecture for industrial applications sees a PLC/DCS for controlling the process and an IEC 61850 network for controlling the electrical system. Safety related systems (SIS) are to be certified, and the availability of the system must be calculated using the procedure described in IEC 61508. Today, electrical devices with IEC 61850 are not yet certified for safety applications, so a formal issue arises.

In this paper we compare the technical specifications of IEC 61850 with the requirements for safety fieldbus specified by IEC 61784-3. A complete series of tests was carried out to verify the robustness of IEC 61850 to the communication errors that may affect a network, and results are reported.

1. Introduction

Every risk associated to an industrial process must be lower than the so-called "acceptable risk". A process or a machinery has an intrinsic level of risk. If the risk deriving from a certain fault or malfunction is above the acceptable risk, it is necessary to introduce a safety function to reduce it. A safety 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 risk is the probability of occurrence of a fault multiplied by the consequences of the fault, in terms of damages to people or to the environment. It is mandatory that any safety related system has an adequate integrity level, i.e. it properly works 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 [1,2].

According to IEC 61508, a safety function is composed of:

- Sensor(s), responsible for measuring or detecting abnormal operation,
- Logic Solver, e.g. a Programmable Logic Controller (PLC), that implements the safety logic,
- Actuator(s), that acts on the process to drive the system into a safe condition.

Traditionally, the connection between the field devices and the logic solver uses copper cables for transmitting ON/OFF or 4/20 mA signals. As shown in [3], digital communication is today replacing analog signals for exchanging data from/to the field devices. In process automation, the most used fieldbus are Profibus/Profinet and Foundation Fieldbus, while for electrical systems it is common the use of IEC 61850 [4].

The use of digital networks for implementing safety related functions is possible only if the communication protocol supports a set of methods for detecting the expected transmission errors. The specifications of these methods are in IEC 61784 [5]. Fieldbus for process control support safety profiles that make them applicable in safety functions. Safety profiles are tested and certified by recognized bodies.

In most modern industrial installations we have a Process Control System (PCS) that uses a safety profile for implementing the safety functions, and an IEC 61850 for monitoring and controlling the electrical distribution system. It is likely that a safety function acts on an electrical device (e.g. contactor or circuit breaker).

As the example in Fig. 1 shows, a push button generates an emergency signal. The safety PLC acquires this signal that is transmitted

* Corresponding author.
E-mail address: paolo.pinceti@unige.it (P. Pinceti).

https://doi.org/10.1016/j.ijepes.2018.07.033
Received 6 November 2017; Received in revised form 16 March 2018; Accepted 16 July 2018

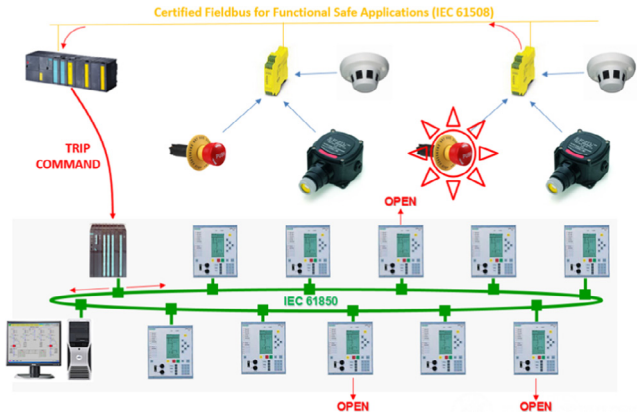

Fig. 1. Example of safety system interaction with IEC 61850.

through the certified safe fieldbus. The processor of the PLC elaborates the signal and decides, for example, to open a circuit breaker to de-energize the plant. The trip command is sent to a PLC or an Intelligent Electronic Device (IED, e.g. a protection relay) that transmits it as a GOOSE message though the IEC 61850 network to the IED that controls the breaker to open. It is apparent that the positive actuation of the emergency function requires a safe transmission of the signals/commands both in the PCS fieldbus, and in the IEC 61850.

In this paper we show the results of a comprehensive set of tests we carried out to verify if the IEC 61850 can – technically – be considered "safe". Tests are based on the standard IEC 61784 that specifies the safety functions for communication fieldbus [6–8].

2. Basic concepts

2.1. IEC 61508 and functional safety

A safety related system must guarantee an integrity level adequate for reducing the risk to an acceptable value. IEC 61508 considers that the likelihood of a tolerable risk is equal to 10^{-5} dangerous events per year. If a process has a risk with a likelihood higher than 10^{-5}, for example 10^{-3}, a safety function is necessary to reduce the risk below the acceptable threshold. In this case, the Probability of Failure on Demand (PFD) of the safety function must be lower than 10^{-2} ($10^{-3} \cdot 10^{-2} = 10^{-5}$). The average probability of a dangerous failure on demand of a safety function is classified into four Safety Integrity Levels (SIL). SIL 1 means a PFD lower than 10^{-1}, while SIL 4 means PFD $< 10^{-4}$, for safety functions in Low Demand Mode (see [2], Table 2).

According to IEC 61508, we can model a safety function as in Fig. 2. One or more "sensors" detect the abnormal operating condition of the plant, and send the information to a PES (Programmable Electronics) that sends the commands to set the plant into safe conditions through

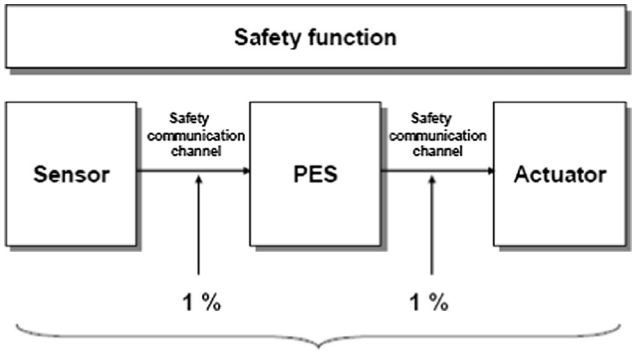

Fig. 2. Example of a safety function.

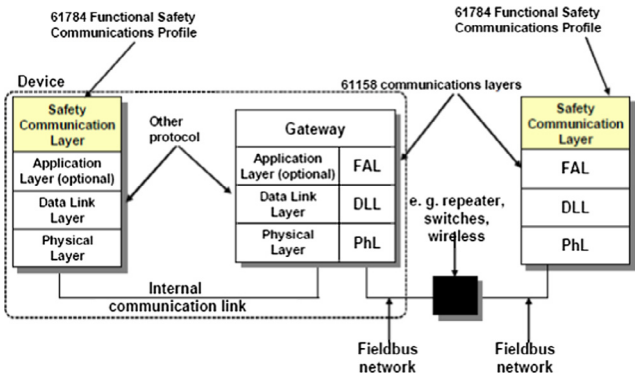

Fig. 3. The concept of "black channel".

the action of one or more "actuators".

The SIL applies to the overall safety function, so it includes both the communication network that connects sensors-logic solver-actuator, and the software (if digital devices are used).

IEC 61508 allows the use of digital communication protocols 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 uses no more than the 1% of the budget PFD for the safety function (see Fig. 2). For example, if the required SIL of the safety function is SIL 3, the PFD of the fieldbus must be $< 10^{-2} \cdot 10^{-7} = 10^{-9}$ [h^{-1}], since a fieldbus always works in High Demand Mode (see [2], Table 3).

2.2. Fieldbus for safety

Fieldbus used for safety functions must implement specific measures to detect communication errors and failures [12].

Today, all safety fieldbus implement the concept of the so-called "black channel" (see Fig. 2). A standard fieldbus becomes a safe fieldbus if a specific safety profile is added (see Fig. 3).

The safety profile detects the possible errors that may lead to the loss or the corruption of the packets. IEC 61784 specifies a set of errors that may happen in a digital communication channel. For every error a countermeasure is identified (see [3]). In addition to the error detection methods, the integrity of safety data is verified by suitable hash functions, such as parity bits, cyclic redundancy check (CRC), message repetition, etc. It may happen that both the standard fieldbus and the safety profile implement similar but independent data validation functions.

If a communication error is detected, the safety devices switch into safe mode (e.g. a digital output opens or an analog output moves to end-of-scale).

2.3. IEC 61850

IEC 61850 is an Ethernet based protocol specifically designed for the electrical systems [4]. The IEC 61850 series consists of ten parts that specify all the various aspects of communication. Section 7.2 defines the information models and the information exchange service models (ACSI Abstract communication service interface) [9,10].

IEC 61850 supports the exchange of two types of data:

- Control blocks for generic substation event (GSE) – used for exchanging 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),
- Logical Node (LN) – it contains the elementary data necessary for