FUNCTIONAL SAFETY SPECIFICATION OF COMMUNICATION PROFILE PROFISAFE

J. Rofár, M. Franeková

Department of Control and Imformation Systems, Faculty of Electrical Engineering,
University of Žilina, Univerzitná 1, 010 26 Žilina
e-mail:jan.rofar@fel.utc.sk, maria.franekova@fel.utc.sk

Summary Paper maps the trends in area of safety-related communication within PROFIBUS and PROFINET industry networks. There are analyses safety measures and Fail-safe parameters of PROFIsafe profile in version V2 and their localisation in Safety Communication Layer SCL, which guarantees Safety Integrity Level SIL according to standard IEC 61508. The last chapter analyses the reaction in the event of fault during transmission of messages.

1. INTRODUCTION

Standard automation has in the past decades been dramatically influenced by the introduction of new types of microcontrollers, software, communication networks, thus leading to cost reduction, higher flexibility, availability and requirements of safety (often marked with attribute Fail-safe). The number of applications increases, and special care and special safety automation technology in accordance with standard IEC 61508 is required. General principles, valid for implementation of safety rules for functional safety of electrical, electronic and programmable electronic safety–related systems are described in [1]. In this group belong applications in which run active industrial processes (e. g presses, saws, chemical factory, transport...). These include the risk to injure people, to damage investments or destroy nature and system has to guarantee required Safety Integrity Level SIL.

Nowadays, in the area of industrial networks fieldbus technology is acceptable standard, which is now widely used for transmission of non-safety related and safety related control data [2]. The specific utilization of the common function within fieldbus communication by the specific groups of participants is called a profile. For the fieldbus industrial networks are defined (according to [3]) seven communication profiles families CPF and (according to [4]) ten types of communication protocols. Relation between them is shown in Tab. 1.

Communications protocols of PROFIBUS and PROFINET (types 3 and 10) [5] are belonging to communication profile family CPF3.

Tab. 1 Relation between CPF and types of protocols

CPF	**Types of communication protocols**		
CPF1	FF **type 1**	FF HSE **type 5**	FF FMS **type 9**
CPF2	Control Net	**type 2**	
CPF3	Profibus/Profinet	**type 3/type 10**	
CPF4	P-Net	**type 4**	
CPF5	WorldFIP	**type 7**	
CPF6	Interbus-S	**type 8**	
CPF7	SwiftNet	**type 6**	

Note: FF Fieldbus Foundation
HSE High Speed Ethernet
FMS Fieldbus Message Specification

These protocols are created as open solution, based on reference model ISO/OSI. From seventh-layer architecture, PROFIBUS uses physical, link and applications layer. PROFINET uses physical, link, network, transport and applications layer. There are several specific profiles of PROFIBUS and PROFINET networks:

- PROFIBUS DP (Decentralised Periphery) and its range of transmission technologies, such as RS 485 (mainly in area of production), Manchester Coded – Bus Powered and Intrinsically Safe MBP - S (mainly in area of process) and optical fibre,
- PROFIBUS PA (Process Automation) in intrinsically safe area,
- PROFIBUS FMS (Fieldbus Message Specification); this version in the future does not have practical imports because of PROFINET development,
- PROFINET IO (Input/Output) for distributed field devices,
- PROFINET CBA (Component Base Automation) for intelligent devices with programmable functionality [6].

For fail-safe applications within PROFIBUS technology was developed profile **PROFIsafe**, which is merging standards of Fail-safe automation and standard automation in one technology, running on the same bus and using the same communications mechanisms. General principles of PROFisafe are described in [1]. Safety measures are implemented as extension up application layer to so called safety communication layer SCL. At present software realisation of PROFIsafe by TÜV (Association for Technical Inspection) and BIA (National Institution on-the job- safety) is being accepted. PROFIsafe is actually standardised in norm IEC 61784-3 [7]. This norm defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 for functional safety. Standard was discussed for the second time in national committee and passed on at the section of work group IEC SC65C//WG12.

2. BASIC FEATURES OF PROFISAFE

PROFIsafe profile describes the communications between Fail-safe peripherals and Fail-safe controllers. PROFIsafe provides two operational modes:

- V1 – is sufficient for the safe data transmission using PROFIBUS DP (versin CPF 3/1),
- V2 – is used for PROFINET IO (CPF 3/2), PROFINET CBA (CPF3/3) and/or PROFIBUS DP.

PROFIsafe V2 is a uniform profile for both PROFIBUS and PROFINET platforms. It can be used in all markets including production automation, drive technology, motion control and process automation too. PROFIsafe with safety integrity level SIL 3 or Category 4 according to EN 954-1 [8] fulfils the highest safety requirements of the process and manufacturing industry. Safety-oriented and standard communication is possible via one and the same cable (see Fig. 1).

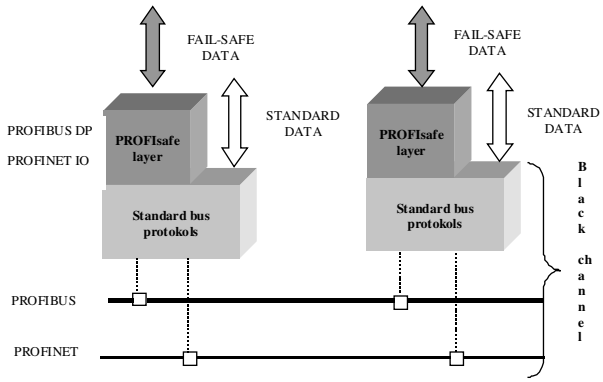

Fig. 1 PROFIsafe profile as extension of standard protocol

The safety layer is independent on the communication system, which includes the backplane buses of controllers and field devices. PROFIsafe in version V2 takes into account the special properties of Ethernet networks, such as the expanded address space and active network components, such as switches and repeaters.

PROFIsafe is based on the experience made in the railway signalling technique according to IEC 622280-1,2 [9]. In this area fail-safe communications is applied via standard transmission system, with reserved higher communication layers ISO/OSI for Fail-safe measures implementation. The safe transmission function comprises all measures to discover all possible faults or hazards that could be infiltrated by standard transmission system and keep the residual error probability under certain limit. Measures include:

- Random function (e.g. Electro-Magnetic Interference EMI),
- Failures of standard hardware,
- Systematic functions of components within standard hardware and software.

Fail-safe PROFIsafe components have established themselves in many safety technology applications (from the sensor systems through equipment up to safe machines). The standard transmission system includes the entire of HW of the transmission system and the related protocol function (for PROFIBUS OSI layers 1, 2, and 7). Safety application and standard applications are sharing the same standard PROFINET IO PROFIBUS DP communication system at the same time. This principle reduces the process of certification to safety layer only. As it is illustrated on the Fig. 2 within 1, 2 and 7 layers are located function of standard transmission system. We suppose black channel with the use of non safety relevant components (Application Specific Integrated Circuit ASIC, wires, switches …). Reserved layer (up application layer) is assigned for implementation of the following functions.

- Safety function of PROFIsafe – includes elements of safety related protocol (addressing, watch dog timing, sequencing, signatures …).
- Non safety related functions (e. g. diagnostic).
- The safe I/O devices and the safe logic controller functions (Note: These functions are not part of PROFIsafe).

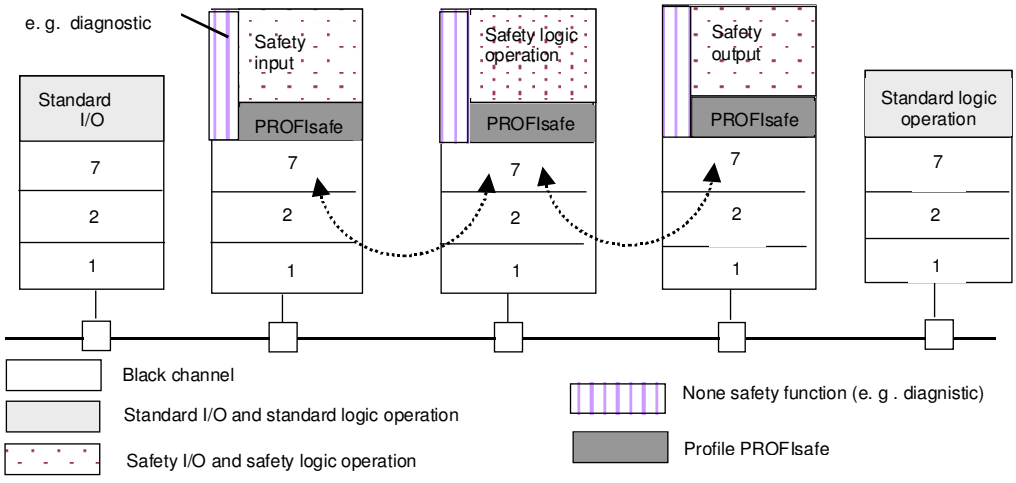

Fig. 2 Safety layer architecture

3. ANALYSIS OF SAFETY MEASURES

Within PROFIsafe profile the following safety measures are required (see in Tab. 2):
a) consecutive numbering,
b) watchdog timer with receipt,
c) codename for authenticity,
d) data consistency check.

Safety measures are processed and monitored within one Fail-safe unit and are able to eliminate communication errors, which can occur during transmission of messages (repetition, deletion, insertion, resequencing, data corruption, delay, masquerade, revolving memory failures within switches). Relation between safety measures and communication errors is illustrated in Tab.2.

Tab. 2 Safety measures and errors

Errors	**Safety measures**			
	a)	b)	c)	d)
Repetition	*			
Deletion	*	*		
Insertion	*	*	*	
Resequencing	*			
Data corruption		*		*
Delay		*		
Masquerade				*
Revolving memory failures within switches	*		*	

Seeing that within factory or process automation different data lengths are transmitted two operational modes can be chosen for safety process data unit PDU: short mode or long mode.
PROFIsafe container includes (Fig. 3):

- F I/O data up to 12 bytes - short mode or up to 123 bytes - long mode).
- Status or control byte.
- Cyclic redundancy check CRC (3 bytes for 12 bytes F I/O data or 4 bytes for 123 bytes F I/O data).

Consecutive number is used for monitoring the propagation times between sender and recipient. Value "0" is reserved for the first run and for communication error reaction. Version V2 uses 24 bit counters for the consecutive numbering. Within V2 version is not transmitting the consecutive number in every safety PDU (in the Fig. 3 part of white colour), but only virtual consecutive number, which is reduced to a Toogle Bit within a status byte (see Fig. 3) or control byte. Counters are located within F-host and F-Device and a Toogle Bit (change from 0↔1, 1↔0) increases theirs appropriate counters.

Data consistency check is calculated with the use mechanisms of Cyclic Redundancy Check CRC. CRC is processed across F data, F parameters and consecutive number (include bytes in reverse order). F parameters are transferred to the F-Device during configuration. F parameters are for example source destination or codename, safety integrity level SIL and watchdog (time monitor).

Time monitor is monitoring the arrival of a new correct safety PDU at the F-Device within the watchdog time. This verification can be performed as often as necessary, but at least once at the end of the monitoring time interval. Every corrupted message is counted during a configurable SIL monitor time period. The SIL monitor shall be implemented within the F-Host only, one per safety function (safety control loop). The SIL monitor time period is a constant value with the dimension hour that result from the requested SIL and the configured CRC length.

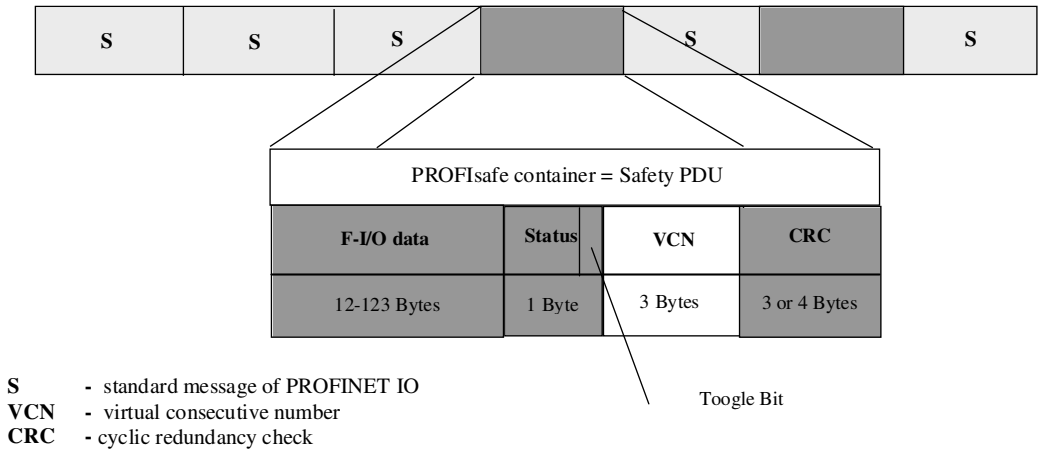

Fig. 3 PROFIsafe container of PROFINET IO

4. REACTION IN THE EVENT OF FAIL

- **Repetition, loss, insertion and incorrect sequence of message**

The data are transferred cyclically. If some safety message is repeated, order of message within consecutive numbering is wrong and receiver overwrites this message by a correct message. Possible delay of an emergency request can be one watchdog time. If some safety message is deleted (during transmission information was lost), inserted or was modified the safety message sequence receiver discovers this events by stringently incrementing and examining the consecutive number.

- **Corruption of safety data**

Perturbation of data integrity, which was changed during data transmission from sender to receiver indicates CRC signature. CRC signature is generated across the F-parameters (including code name), the F I/O data, the virtual consecutive number and the control/status byte. Messages in which data integrity corruption were detected are not acceptable in the receiver side for further processing.

- **Delay of message**

When the operational data exchange exceeds the capacity of communication link the messages can be delayed. We can detect this type of communication error with the following safety measures: consecutive number in the sender data and in the acknowledgement data and with the use mechanism of watchdog time for F-communication. The watchdog time is a part of a whole safety time of the safety control loop. The total time guaranteed by the safety control system t_{TOT} is the sum of the following segments (1):

- Input delay of the F- Input device (operation time) $t_{F/I}$,
- Watchdog time of F-communication (between F-Input and F-Host) $t_{F/I \leftrightarrow F/H}$,
- Execution time in the F-Host $t_{F/H}$,
- Watchdog time of F-communication (between F-Host and F-Output) $t_{F/H \leftrightarrow F/O}$,
- Output delay of the F-Output Device (operation time) $t_{F/O}$.

$$t_{TOT} = t_{F/I} + t_{F/I \leftrightarrow F/H} + t_{F/H} + t_{F/H \leftrightarrow F/O} + t_{F/O} \quad (1)$$

- **Masquarade**

If unauthorised access into communication system is not struck out, we must guarantee authenticity of senders and receivers. It means that data are coming from the correct sender and are going to the correct recipient. This authenticity is guaranteed with the use of F-Parameters as F-Address, determining F source and recipient destination relations. With the use of F-addressing the changes of safety-related messages and non-safety related messages and the data from a different sender or recipient must be detected.

- **Failures caused with network elements (switches, routers)**

Central elements of networks are switches and routers (PROFINET only), which belong to the active network components. They can have different faults. Messages may be sent to the wrong destination or their data content can be perturbed.

The routers connect two or more subnets over 3 levels. Every F-Host and F- Devices can be configured to use router together with an appropriate address. Possible switch and routers faults and reaction after detection are recommended in [7].

5. CONCLUSION

The paper has presented the specifications of PROFIsafe profile. It was developed for PROFIBUS and PROFINET industrial networks to guarantee safety-related communications according to norm IEC 61508. In the previous parts were analysed PROFIsafe profile and its ability to keep safety integrity level SIL 3. That's the reason why is it used in applications with the highest safety requirements of the process and manufacturing industry.

Acknowledgement

The work has been supported by the Agency for science and technical support by financial support No. APVP-20-P00705.

REFERENCES

[1] IEC 61508: Functional safety of electrical, electronic, programmable electronic safety- related systems. 1998

[2] MAHALIK, N. P.: Fieldbus technology, Industrial network standard for Real-Time Distributed Control, Springer. 2003

[3] IEC 61784-1: Digital data communications for measurement and control. Part 1: Profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems. 2003

[4] IEC 61158: Digital data communications for measurement and control – Fieldbus for use in industrial control systems. 2005

[5] IEC 61784-2: Digital data communications for measurement and control. Part 2: Additional profiles for ISO/IEC 8820-3 based communication networks in real time applications. Draft

[6] BALOG, R.-BÉLAI, I.-DORNER, J.-DRAHOŠ, P.: Priemyselné komunikácie, STU Bratislava. 2001

[7] IEC 61784-3 Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. Draft

[8] EN 954-1 Safety of machinery. Safety related parts of control systems. General principles for design. 1997

[9] IEC 62280-1, 2: Railway applications. Communication, signalling and processing systems Part 1: Safety-related communication in closed transmission systems. Part 2: Safety-related communication in open transmission systems. 2002