TRANSPORT PROBLEMS 2008
PROBLEMY TRANSPORTU Tom 3 Volume 4 Part 1

Mária FRANEKOVÁ*
University of Zilina, Faculty of Electrical Engineering,
Univerzitná 1, 01026 Žilina, Slovakia,
* *Corresponding author*. E-mail: maria.franekova@fel.uniza.sk

SAFETY AND SECURITY PROFILES OF INDUSTRY NETWORKS USED IN SAFETY- CRITICAL APPLICATIONS

Summary. The author describes the mechanisms of safety and security profiles of industry and communication networks used within safety – related applications in technological and information levels of process control recommended according to standards IEC 61784-3,4. Nowadays the number of vendors of the safety – related communication technologies who guarantees besides the standard communication, the communication amongst the safety – related equipment according to IEC 61508 is increasing. Also the number of safety – related products is increasing, e. g. safety Fieldbus, safety PLC, safety curtains, safety laser scanners, safety buttons, safety relays and other. According to world survey the safety Fieldbus denoted the highest growth from all manufactured safety products.The main part of this paper is the description of the safety-related Fieldbus communication system, which has to guaranty Safety Integrity Level.

PROFILE BEZPIECZEŃSTWA I ZABEZPIECZEŃ SIECI PRZEMYSŁOWYCH WYKORZYSTYWANYCH W ZASTOSOWANIACH KRYTYCZNYCH DLA BEZPIECZEŃSTWA

Steszczenie. Autor przedstawia mechanizmy bezpieczeństwa i profili zabezpieczeń sieci przemysłowych i łączności używanych w aplikacjach związanych z bezpieczeństwem na poziomach technologicznym i informacyjnym sterowania procesami, rekomendowanych zgodnie z normami IEC 61784-3,4. Obecnie wzrasta liczba firm – dostawców technologii łączności związanymi z bezpieczeństwem, które gwarantują, poza standardową łącznością, łączność pomiędzy urządzeniami związanymi z bezpieczeństwem, zgodnie z IEC 61508. Zwiększa się także liczba wyrobów związanych z bezpieczeństwem, np. zabezpieczający Fieldbus, zabezpieczający PLC, osłony bezpieczeństwa, zabezpieczające skanery laserowe, przyciski bezpieczeństwa, przekaźniki zabezpieczające i inne. Zgodnie ze światowymi badaniami, zabezpieczający Fieldbus zarejestrował największy wzrost pośród wszystkich wytwarzanych wyrobów zabezpieczających. Główną częścią referatu jest opis związanego z bezpieczeństwem systemu łączności Fieldbus, który ma na celu zagwarantowanie Poziomu Integralności Bezpieczeństwa.

1. INTRODUCTION

In the last years the integration of automation and information technologies is increasingly observed, what allows significantly better communication between automation systems, extensive configuration and diagnostic possibilities and network-wide service functionality. The communication capability of devices, subsystems and consistent information methodology are indispensable components of future-oriented automation concepts.

In many cases communication system is a component part of the system which participates in control of safety-critical processes. Undetected corruption of data transmission (e.g. control commands) can cause considerable substantial damage within equipment, environment and demands on human health. This is the reason why the system has to be designed to guarantee the required safety integrity level (SIL).

As it is illustrated in Fig.1 communications are increasingly occurring horizontally at the information and supervision level as well as vertically at the technological level [1].

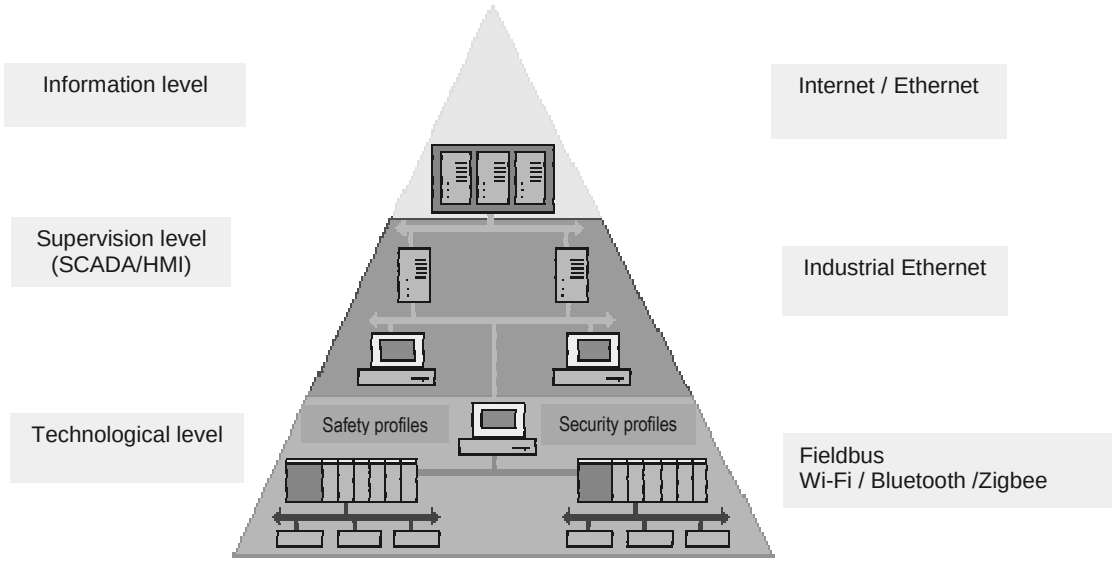

Fig. 1. Hierarchical levels of communication in automation and location of safety and security profiles
Rys. 1. Hierarchiczne poziomy komunikacji w automatyce i profilach lokalizacji bezpieczeństwa i zabezpieczeń

Nowadays, on the technological level the Fieldbus technology is an acceptable standard, which is now widely used for transmission of non-safety related and safety-related control data, too. The specific utilization of the common function by the specific groups of participants is called a profile. For industry communication, according to [2] seven communication protocol families (CPF) for ten types of communication protocols (Table 1) are defined.

Table 1

Communication protocol types for Fieldbus technology

CPF	Types of communications protocol		
CPF1	Foundation Fieldbus (Type 1)	FF High Speed Ethernet (Type 2)	FF FMS (Type 3)
CPF2	Control Net (Type 4)		
CPF3	Profibus/Profinet (Type 5/Type6)		
CPF4	P-Net (Type 7)		
CPF5	World FIP (Type 8)		
CPF6	INTERBUS (Type 9)		
CPF7	SwiftNet (Type 10)		

Nowadays the number of vendors of the safety-related communication technologies who guarantee besides standard communication, communication among safety- related equipment according to [3] is increasing. At present the standard proposal [4] was accepted, which deals with a definition of functional safety for industry networks within digital communications used in the measuring area and the control systems in industry. Among the first manufacturers who have begun to use safety principles in development of their products there are the vendors of CAN technologies and products developed within the international organisation ODVA (Open DeviceNet's Vendor Association). The new network standard CIP Safety [5], published by ODVA, makes it possible to join standard and safety-related equipment across the same communication link. The vendors of Profibus and Profinet technology belong to the next important leaders in the area of industry Fieldbus. They developed a concept based on the integration standard and safety-related techniques that have been using the same communication tools for several years. This solution is signed as ProfiSafe and together with ProfiDrive profile it was approved and prepared for using in both types of industry networks Profibus and ProfiNet. At the present time the buses with communication profiles CIP Safety and ProfiSafe are recommended for using in safety-related systems with the safety integrity level 3 according to EN 61508 or the category 3 according to EN 954-1 [6].

The work on standard IEC 61784-4 preparation [7] started which defined profiles of secure communication in industrial network using an open transmission system, e. g. wireless technologies. Wireless technologies are spreading also to safety – related applications. There are already several Fieldbuses, which are validated to be used in safety –related applications [8].

ISA (Instrumentation, Systems and Automation Society) guarantees development strategies of secure industrial control systems through committee SP 99 and NIST (National Institute of Standard Technology). ISA published two important technical reports TR1 [9] and TR2 [10], in which secure technologies are classified to five packets.

On the information level of hierarchical communication model the safety is realised within safety Ethernet networks on the basis of safety communication protocol, e. g. SNMP (Simple Network Management Protocol), SSL (Secure Socket Layer), TLS (Transport Layer Security) and virtual private networks. For example vendors of Profibus/Profinet technologies developed secure solution (Scalance S) for ProfiNet on the basis of VPN (Virtual Private Network) network through tunnel mode using IPsec protocol [11].

If unauthorised access to distributed system is not able to negate communication protocols within particular hierarchical level (in Fig.1), the tools of modern cryptography are necessary to use.

The paper deals with mechanisms of safety and security profiles located in technological level only (see Fig.1), which are recommended to use within safety – related industrial applications. Safety and security mechanisms used for elimination of risks, which occur during data transmission, are described in detail. Recommendations for selection of computationally safety cryptographic techniques are also described.

2. MODEL OF SAFETY AND SECURITY COMMUNICATIONS

Safety and security functions of communication are implemented in additional safety communication layers and they are performed within a safety - related communication protocol.

A model of safety - related communication protocol in the area of industry network according to [4] is illustrated in Fig.2. An equivalent model for a bus system is shown in Fig.3.

In the model shown in Fig.2 mechanisms are implemented in three layers: integrity

- safety layer (layer, in which authentication algorithms and data, techniques, e. g. safety code, are implemented),
- security layer (layer, in which stronger safety mechanisms based on cryptographic techniques, e. g. cryptographic or hash code, are implemented),
- transmission layer (layer, in which safety mechanisms of non-trusted transmission system, e. g. transmission code, are implemented).

When we assume to use a closed transmission system (system without unauthorised access to the system) the model of communication protocol is reduced to the use of safety profile and transmission layer only. Additional security profile should be implemented within an open transmission system, in which unauthorised access to the system through intentional attack is not restricted.

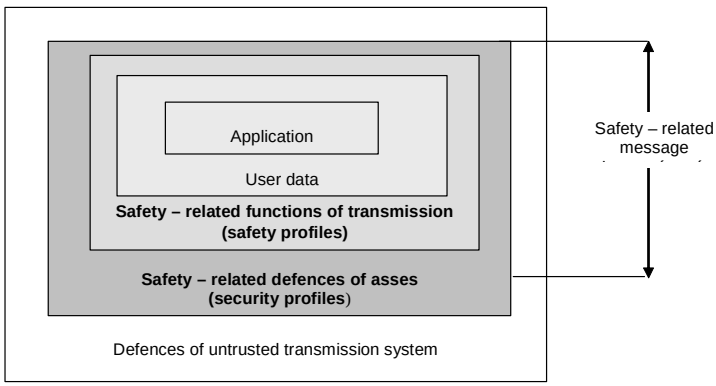

Fig. 2. Model of safety - related communications in industrial applications
Rys. 2. Model bezpieczeństwa - powiązania komunikacji w zastosowaniach przemysłowych

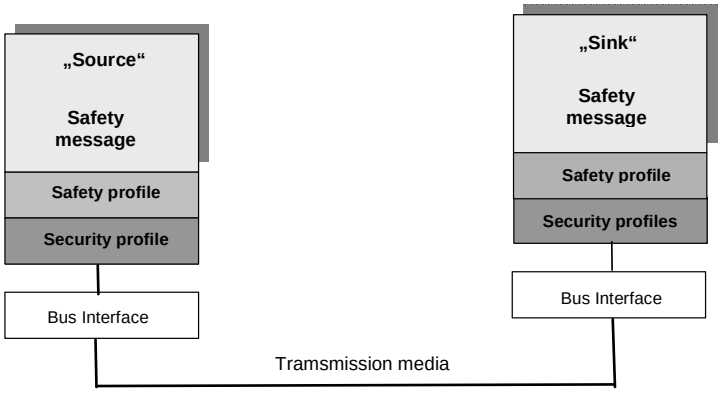

Fig. 3. Model of bus system with safety and security profiles
Rys. 3. Model systemu przesyłu z profilem bezpieczeństwa i ochrony

3. RECOMMENDED MECHANISMS FOR SAFETY PROFILES

Basic principles of safety - related Fieldbus system and the definition of additional services and safety – related communication protocols families are defined in the standard IEC 61784-3 [4].

The requirements for safety – related Fieldbus networks can be characterised with the following points:

- coexistence with standard networks, transmission of safety – related and safety not related data,
- special mechanisms to maintain safety integrity level are located in additional safety layer,
- the network contains redundant elements, actual data are usually transmitted twice (actual and inverse), control systems use techniques of two channel or three channel structure,
- in the case of dangerous events occurrence the system must finish communication and obtain defined safety state.

In both systems (closed and open) the message is one of major subjects of safety analysis. According to [12] is a message defined as useful information, which is generated from a source and must be transmitted in time Δt from beginning of transmission to the destination station. Attacks on messages, which are transmitted across communication links can result in failure in communication equipment. Communication channel affects transmission of messages by noise, interferences or can cause fading of useful signal. These effects are generally marked as disturbance caused by Electromagnetic Interference (EMI) and they have strong effect on the value of intensity of undetected (corrupted) messages. Effects of noise can have different forms, which depend mainly on physical characteristics of the channel.

Within Fieldbus networks we may predict the following types of attacks on messages: corruption of message, unintended repetition of message, resequencing, missing of message, and unacceptable delay of message and insertion of message.

For risk elimination it is necessary to use safety measures. The types and power of measures depend on concrete application and required SIL. The following requirements must be fulfilled in the communication: keeping of authentication, integrity, timeouts of sending messages and correct sequenced messages.

The following safety measures were defined within Fieldbus networks to assure these requirements: sequence number, time stamp, timeout, authentication of connection, feedback message and safety code.

Requirements for safety measures must be included in specifications of requirements for the system and its safety.

Example of safety profile for Profibus and Profinet technology called PROFIsafe is illustrated in Fig.4. Within PROFIsafe profile, the following safety measures are required: consecutive numbering,

watchdog timer with receipt, codename for authenticity and data consistency check. PROFIsafe with safety integrity level SIL 3 or Category 4 according to EN 954-1 [6] fulfils the highest safety requirements of the process and manufacturing industry. 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.

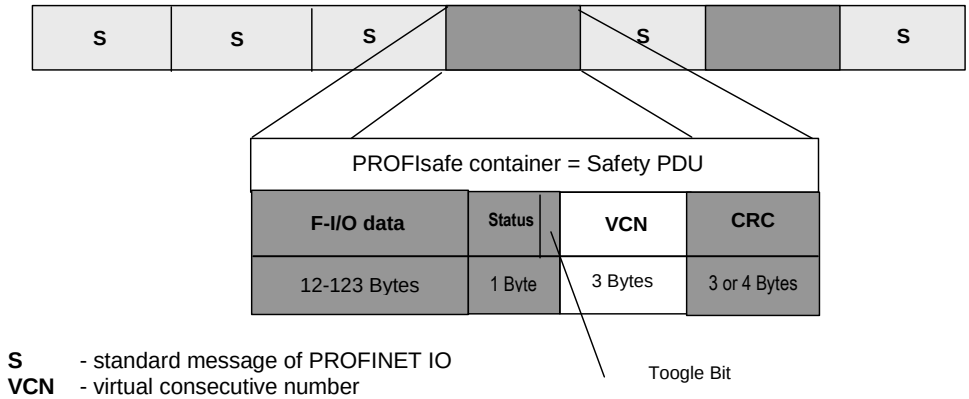

Fig. 4. PROFIsafe content of Profibus and Profinet
Rys. 4. Zawartość PROFIsafe w Profibus i Profinet

4. RECOMMENDED MECHANISMS FOR SECURITY PROFILES

Development of safety and security profiles in the industry was affected by the basic principles of safety-related communication between railway interlocking systems. Norms valid for the area of control interlocking systems define communication safety within the use of closed EN 50159-1 [12] and open EN 50159-2 [13] transmission systems. For railway applications seven types of open transmission systems according to [13] are defined. In transmission system of types 5, 6, 7 we must assume an unauthorized access to the system and predicted masquerade of messages.

Prepared standard IEC 61784-4 describes the security communications profiles (CP) for safety – related communications between participants within distributed networks based on Fieldbus technology. The standard defines the following types of secure profiles:

- CP- ECI External network interconnection to a control network,
- CP- IRA Interactive remote access to a control network,
- CP- ICC Inter control centre access to a shared control network.

An open transmission system based on the wireless technology (e. g. Bluetooth – up to 10 m, WLAN – up to 100 m and ZigBee – up to 300 m) is beginning to be widely used in the technological level of automation, too. The frequency is license free in most countries, which is the main reason for its popularity. A wireless system is characterized by physically disconnected and depending on radio communication between different parts of system, these characteristics have some obvious advantages but also disadvantages. Disadvantages are mainly related to new safety and security related issues where new risks are introduced. Cryptographic or hash codes are recommended to reduce masquerading of messages.

Cryptographic techniques are primarily used in security critical applications. Cryptographic techniques in safety-related communication systems are necessary to use if intentional attacks within open transmission systems cannot be handled [13]. It is necessary to reflect that in contrast with e.g.

channel coding techniques the cryptographic techniques include not only algorithms, but methods for keys generating, transmission and archiving. Development of cryptography is more dynamic than development of channel coding techniques. Enciphering standards are acceptable maximum for 5 – 10 years and their strengths have to be regularly revaluated. This fact should be taken into consideration and in the process of cryptographic tools selection to fix to modern and recommended algorithms with experts. Cryptographic mechanisms provide different levels of safety according to the type of cryptographic algorithm and its key length.

The level of safety in the area of cryptography may be quantified with the use of several models. The model used most in practice is based on the theory of complexity and defines the term „computational safety“. Cryptographic algorithm is regarded as computationally safe, if it is broken with realisation of unavailable number of operations in time. Based on computationally safe cryptographic techniques it is possible to compare and determine their safety. Complexity of algorithm O (order) is assigned to computational power, which is required to its realisation. Complexity is evaluated with three parameters: time demands T, space demands S and data demands D. Parameters T, S and D usually describe function n, what is the range of input data. The following types of algorithms complexity are defined in the cryptographic practise:

- O(1) constant,
- O(n) linear,
- O(nm) polynomial (for m = 2 quadratic, for m = 3 qubic, …),
- O(2n) exponential.

At present algorithms with exponential complexity are regarded as computationally safe.

The other model which describes the security of cryptographic algorithms used term equivalent security algorithms [14]. This parameter expresses the effect of known attacks on algorithms [bit]. Table 2 illustrates the most used cryptographic algorithms and their level of equivalent security. The grey collared cells in Table 2 may be marked as algorithms with sufficient equivalent security.

Table 2

Equivalent security of cryptographic algorithms

Equivalent security [b]	**Symmetric algorithms**	**Algorithms DSS DH**	**Algorithm RSA**	**Hash function SHA**
80	2DES	PK = 1024 SK = 160	N =1024	SHA -1/160
112	3DES	PK = 2048 SK = 224	N = 2048	SHA – 2/224
128	AES-128	PK = 3072 SK = 256	N = 3072	SHA – 2/256
192	AES- 192	PK = 7680 SK = 384	N = 7680	SHA – 2/384
256	AES - 256	PK = 15360 SK = 512	N = 15360	SHA – 2/512

Note:

DSS	Digital Signature Standard	PK	public key
DH	Diffie-Hellman’s algorithm	SK	secret (shared) key
RSA	Rivest, Shamir Adelman alg.	SHA	Secure Hash Algorithm

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 “Mathematic-graphical modelling of safety attributes of safety-critical control systems”.

Bibliography

1. Zolotová, I. – Landryová, L.: Knowledge model Integrated in SCADA/HMI System for Failure Process Prediction. WSEAS Transaction on Circuits and Systems. Issue 4, Volume 4, April 2005, P. 309-318.
2. IEC 61158: Digital data communications for measurement and control – Fieldbus for use in industrial control systems. 2003.
3. IEC 61508 (1998): Functional safety of electrical/electronic/programmable electronic safety-related systems.
4. IEC 61784-3: Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. 2007.
5. Franeková, M. – Kállay, F. – Peniak, P.- Vestenický, P.: Communication Safety of Industrial Network. Monography. EDIS, ŽU Žilina, 2007.
6. DIN EN 954-1: Safety of machinery - Safety-related parts of control system. Part 1: General principles of design.1996.
7. IEC 61784-4: Digital data communications for measurement and control. Part 3: Profiles for secure communications in industrial network, Draft.
8. Validation of safety – related wireless machine control systems. Technical report TR 605. 2007.
9. Instrumentation, Systems and Automation, Manufacturing and Control System Security: TR1: Security Technologies for Manufacturing and Control Systems.
10. Instrumentation, Systems and Automation, Manufacturing and Control System Security: TR2: Integrating Electronic Security into the Manufacturing and Control System.
11. Stallings, W.: Cryptography and Network Security. PrenticeHall, New Jersey. 2003.
12. EN 50159 – 1 (2002): Railway applications: Communication, signalling and processing systems - Part 1: Safety - related communication in closed transmission systems.
13. EN 50159 – 2 (2002): Railway applications: Communication, signalling and processing systems - Part 2: Safety - related communication in open transmission systems.
14. Levický, D.: Cryptography in information security. Elfa, Košice, 2005.

Received 25.02.2008; accepted in revised form 15.10.2008