ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ ТА СИСТЕМИ КЕРУВАННЯ

SAFETY ANALYSE OF CRYPTOGRAPHY PROTOCOL USED WITHIN SAFETY-RELATED CONTROL SYSTEMS IN INDUSTRY

Mária Franeková [1], Fedor Kállay [2], Igor Piotr Kurytnik [3]

[1]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Slovakia, maria.franekova@fel.uniza.sk

[2]Department of Mechatronics and Electronics, Faculty of Electrical Engineering, University of Zilina, Slovakia, fedor.kallay@fel.uniza.sk

[3]Department of Electrical Engineering and Automation, Faculty of Mechanical Engineering and Computer Science Universitay of Bielsko-Biala, Poland, ikurytnik@ath.bielsko.pl

In the paper the possibilities of solution safety communication within area of safety-related control industry system are summarised with using cryptography techniques. Requirements to safety are based on generic standard for functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) systems IEC 61508 and standards, which define safety and security profiles in industrial network used in measurement and control systems. In mainly part of paper the model of safety-related communication protocol is described and overview of recommendations for selection of cryptography mechanisms and methods for their safety evaluation.

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

As it is illustrated on the Figure 1 communications are increasingly occurring horizontally at the field level as well as vertically at the cell level.

At the sensor/actuator level signal of binary sensors and actuators are transmitted over a sensor bus (e. g. AS-Interface). At the level of devices (field level) distributed devices such as input/output modules, transducers, drive units, valves or operator terminals communicate with automation systems over device bus (fieldbus). On the present ten types of fieldbus technologies and its protocols are avaiable on the market, which are supported by vendors in the world. There are concerned to the following technologies: Foundation Fieldbus (FF), Control Net, Profibus, P-Net, FF Ethernet, SwiftNet, WorldFIP, Interbus - S, FF FMS and ProfiNet [1]. Between basic requirement to fieldbus networks is communication in real time. At the control level (cell level) programmable controllers (PLC) are used, which communicate with each other and with information technology (IT) systems of the office using standard on the base of Ethernet, TCP/IP, Intranet and Internet. At the top of cell level information flow required large data packets and range of powerful communication functions.

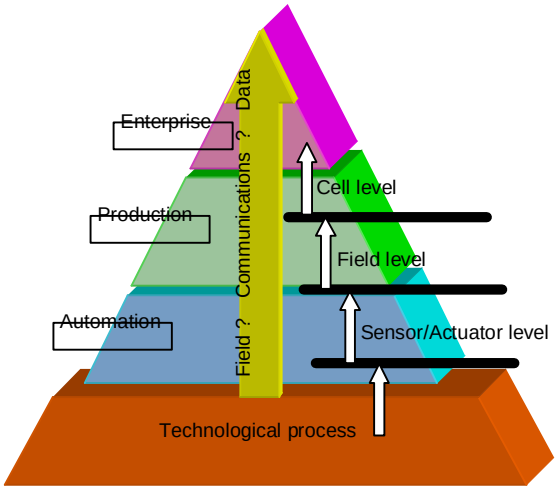

Figure 1 Hierarchical levels of communication in automation

In many cases communication system is a component part of system which participates in control of safety-critical processes. Undetected corruption of data transmission (e.g. control commands) can cause considerable substantially damages within equipments, environments or demands on human health and this is the reason why system has to be designed to guarantee required Safety Integrity Level (SIL) [2].

Secure communications is defined in COTS (Commercial Off-The-Shelf) standards achieving of confidentiality, integrity and availability [3]. For achievement of safety goal within communication it is recommended the safety functions to apply, which support safety and perform with using seemly selected safety mechanisms. Safety mechanisms can be implemented in SW (control access to system, using of passwords, mechanisms on base of cryptography...), in HW (cipher modules, authentication and identification cart...), by physical means (safe deposit box, interlocks,...) or by administration measures (norms, legislations, certification authority,...)

COTS communication technologies are essentially not available (without supplementary technical measures) for transmission safety-related data, although their transmission systems involve detection and correction methods for assurance of transmission, eventually other protective mechanisms. Concerning to safety of transmission, these systems are denoted as non-trusted. Which types of additional technical measures are necessary to apply depends on the risk analysis results (analysis of attacks and their effects) related with controlled process and on the acceptable risk.

Standard IEC 61508 [4] defines general principles valid for implementation of safety rules with the use E/E/PE systems. In standard notices general requirements for achieving functional safety of safety-related system include communication part.

On the present number of vendors of safety- related communications technologies is increased, which guarantee without standard communication, communication between safety- related equipments according to [4]. At the present time proposal of standard IEC 61784-3 [5] is prepared to vote, which deals in definition of functional safety for industry networks within digital communications using in area of measuring and control systems in industry.

Between first manufacturers, which begin to use safety principles in development their products belong vendors of CAN technologies and products developed within international organisation ODVA (Open DeviceNet's Vendor Association). New network standard CIP Safety [6], which was published ODVA make possible to consistence of standard and safety - related equipments across the same communication link. Vendors of Profibus and Profinet technology belong between the next important leaders in area of industry Fieldbus, which several years develop concept based on integration standard and safety - related techniques with use the same communications tools. This solution is signed as ProfiSafe and together with profile ProfiDrive was approved and is prepared for using in both types of industry networks Profibus and ProfiNet too [7]. In the present time buses with communication profiles CIP Safety and ProfiSafe are recommended for using in safety- related systems with Safety Integrity Level 3 according to EN 61508 [4] or category 3 according to EN 954-1 [8] .

For high levels of communication (shown on the Figure 1) works of preparation of standard IEC 61784-4 [9] was begun, which defined profile of secure communication in industrial network (mainly on the base of industrial Ethernet). Guarantees of strategies of development of secure for industrial control systems are ISA (Instrumentation, Systems and Automation Society) through committee SP 99 and NIST (National Institute of Standard Technology). ISA published two important technical reports TR1 [10] and TR2 [11], in which secure technologies are classified to five packets.

Common Criteria defined by NIST [12 ISO/IEC 15408] is transformed in document SPP-ICS (System Protection Profile for Industrial Control System) for using not only in government but in industry automation too.

On the high level of hierarchical model of communication safety is realised within safety Ethernet networks on the base of safety communication protocol, e. g. SNMP (Simple Network Management Protocol), SSL (Secure Socket Layer), TLS (Transport Layer Security) and VPN (Virtual Private Networks). For example vendors of Profibus/Profinet technologies developed secure solution (Scalance S) for ProfiNet on the base of VPN network through tunnel mode using IPsec protocol [13].

In the case if unauthorised access to distributed system is not able to negate, communication protocols within particular hierarchical level (on the Figure 1) are necessary to use the tools of modern cryptography.

2. Model of safety and security communication protocol. In the case if safety system is vulnerable to intentional attacks by an intelligent or automated agent, additional protocol or measurement elements for security are also required. Safety and security functions of communication are implemented to additional safety communication layers and they are performed within safety and secure communication protocol.

Types of safety and secure measures are selected in dependence of application and safety requirement to SIL. Basic principles of communication based on the standard and security layers or sublayers have tradition in secure protocols in Internet (e. g. IPsec, SSL, TLS).

Additional safety and secure layers (they are most often higher layers of RM OSI model or special profiles located up application layer) does not change protocols used in lower layers for communication between standard devices. Advantages of this solution are that all safety and secure mechanisms are centred in selected layers or profiles. This approach does not change conventional concept of communication and through one bus it is able to communicate between standard and safety-related equipment too. Model of safety and security communication protocol in area of industry network according to [5] is illustrated in the Figure 2. An equivalent model for a bus system is shown in Figure 3.

In the model shown in the Figure 2 mechanisms are implemented into three layers:

- Safety layer (layer, in which are implemented authentication algorithms and data integrity techniques).
- Security layer (layer, in which are implemented stronger safety mechanisms on the base of cryptography techniques, e. g. encryption).
- Transmission layer (layer, in which are implemented safety mechanisms of non-trusted transmission system).

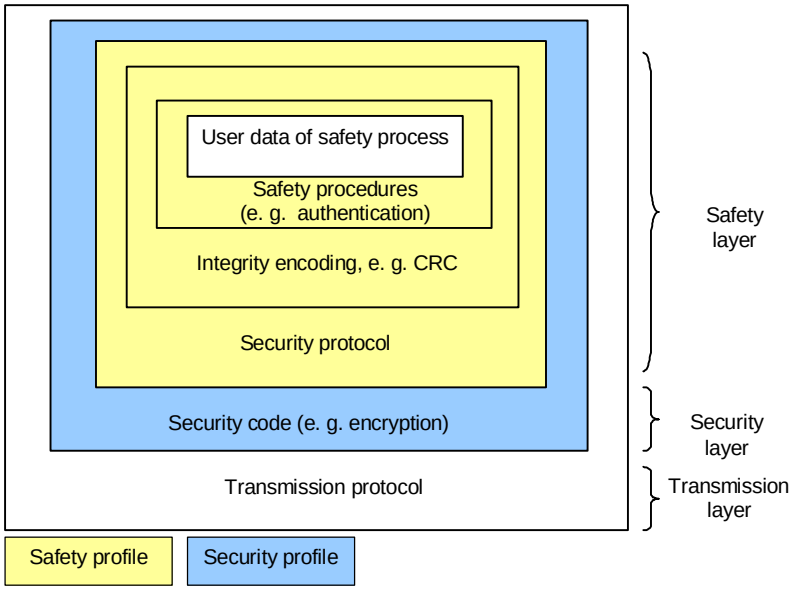

Figure 2 Model of safety and security protocol

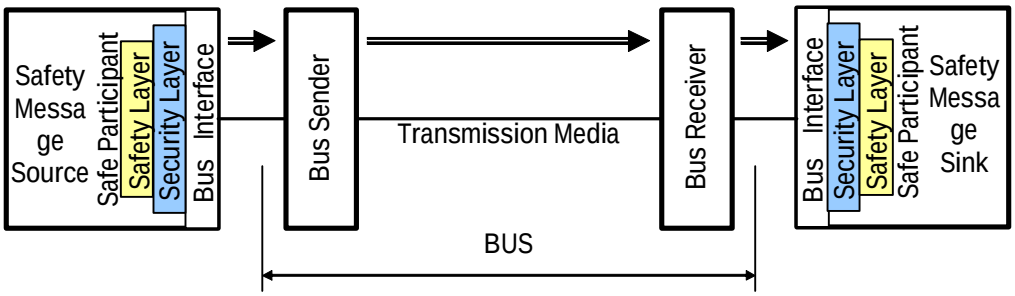

Figure 3 Model for bus system with safety and security layers

When we assume to use the closed transmission system (system without unauthorised access to system) model of communication protocol is reduced to use safety and transmission layer. Extra secure layer is necessary to implemented within open transmission system, in which is not reduced unauthorised access to system though intentional attack.

In the paper cryptography mechanisms locate in security layer are analysed, which selection depend on requirement to safety integrity level SIL to overall system.

3. Safety analyses of cryptography protocol's tools. Cryptography techniques in safety-related communication systems are necessary to use if intentional attacks within open transmission systems are not possible to handle [9]. It is necessary to reflect that in contrast with e. g. channel coding techniques cryptography techniques include not only algorithms, but methods for generating, transmission and archiving of keys. Development of cryptography is more dynamic as development of channel coding techniques. Enciphering standards are acceptable maximum for 5 -10 years and their strong have to be regularly revaluated. This fact it is necessary to take in the consideration and in the process of selection cryptography tools to fix to modern and recommended algorithms with experts.

In the present many types of cryptography techniques on the base of symmetric, asymmetric cryptography, accessory techniques and methods for key management exist [14], [15].

The most suitable the complex of safety services with the used of one cryptography module (in HW or SW version) is realised, which is located in input interface to open transmission system. In the process of selection of cryptography mechanisms it is necessary to take in consideration specification of transmission within control industry systems (mainly time validity of message and group communication process), what request the achievement of requirements to speed of algorithms, safety of algorithms and feasibility of algorithms in praxis.

3.1 Safety models of cryptography mechanisms. Cryptography mechanisms provide different level of safety in compliance with type of cryptography algorithm and length of its key. Level of safety in area of cryptography is possible to quantified with the used several model of safety. The most used model in the praxis is based on the theory of complexity and defines term „computationally safety". Cryptography algorithm is regarded as computationally safety, if it is broken with realisation of unavailable number of operations in time. On the base of term computationally safety cryptography techniques it is possible to compare and determine their safety. Complexity of algorithm O (order) is assigned by computationally 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 range of input data.

The following types of complexity of algorithms are defined in the cryptography praxis:

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

In the present algorithms with exponential complexity are regarded as computationally safety. With growing of n the time complexity of algorithm can affect markedly it is applied in praxis.

If basic attack (brute force attacks) is predicted only, quantitative safety of cryptography algorithm can be expressed by number of key bits of algorithm. It is necessary to take in consideration parameter, which formulates the effects of known attack to safety and marked as equivalent safety (in bits). For example cryptography algorithm 2-DES should have complexity 2x56 bits = 112 bits. Known attack against algorithm 2-DES (midle-in-the-midle) decrees its safety to equivalent safety of 80 bits.

3.2. Recommendations for selection of cryptography mechanisms. Problems of selection suitable cryptography tools for communication protocol used in safety – related applications are possible to summarise to the following steps:

3.2.1 Selection of cryptography systems (symmetric, asymmetric or hybrid)

In this step it is necessary to go out from well established hybrid model used in safety information networks, which employs positive attributes of symmetric and asymmetric cryptography systems. Fast symmetric system can be used for enciphering of large range of data and asymmetric systems for creating secret channel for

Table 1

Dimension of symmetric and asymmetric modules with similar resistance

Dimension of symmetric module	Dimension of asymmetric module
56 bits	384 bits
60 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2034 bits

transmission of key of symmetric algorithm. It is necessary to take in consideration, that safety of hybrid model can be decreased, if combinations of length of keys of symmetric and asymmetric module are chosen incorrect. In Table 1 is shown list of the most used pairs of cryptography modules with approximately identical resistance against brute force attack [16].

3.2.2 Selection of cipher (block/stream)

Not only block ciphers but stream ciphers too are considered as fast enciphering algorithms. However stream ciphers are not recommended for transmissions of safety-related data because of their low safety (used short length of key) but also for the reason the possibility of attacks realisation with using mathematical operation XOR (addition of modulo 2), if integrity check of message is based on CRC (Cyclic Redundancy Check) over Galois field GF(2). If for integrity check in protocol some type of hash algorithm is used realised over GF(q) for q >2, than this type of attacks can be excluded and stream ciphers using is possible to consider for system with lower requirements to SIL.

In the present as computationally safety enciphering algorithms are considered block ciher AES (Advanced Encryption Standard)-Rijndael with variable length of key [NIST PUB FIP 197] or block cipher 3-DES [NIST PUB FIP 46]. It is assumed that 3-DES algorithm will be changed in the future to AES/Rijndael, too. In area of asymmetric cryptography RSA (Rivest, Shamir Adelman) algorithm is recommended with minimal length of module N = 1024 and DSA (Digital Signature Algorithm) and DH (Diffie Hellman) algorithm with minimal length of PK=1024 (publik key) and SK=160 (secret key). In the Table 1 is shown the prediction of equivalent safety for widely-used symmetric and asymmetric algorithms for period of years 2010 – 2030.

Table 2

Prediction of equivalent safety of cryptography algorithms

Period/minimal equivalent safety	Symmetric algorithms	Asymmetric algorithms	
		DSA DH	RSA
by the year 2010 (80 bits)	3-DES AES-128 AES-92 AES-256	minimal PK = 1024 SK = 160	minimal N = 1024
2011 -2030 (112 bits)	3-DES AES-128 AES-92 AES-256	minimal PK = 2048 SK = 224	minimal N = 2048
after year 2030 (128 bits)	AES-128 AES-92 AES-256	minimal PK = 3072 SK = 256	minimal N = 3072

3.2.3 Selection of cipher modes of operations (ECB, CBC, CFB, OFB)

Chosen cryptography system can expand about additional parameters between which usually belong possibility to mask repeated patterns in plain text, generating initial vector in input of enciphering process and message with the same key enciphering differently. From four basic modes of operations, which are defined for block ciphers [NIST PUB FIPS PU 81] ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback Block) and OFB (Output Feedback Block) is more recommended for safety-related transmission CBC mode, which eliminates block reply effect (one of disadvantages of ECB mode). Modes CFB and OFB are more used within bit-oriented transmissions across noise channel, e.g. satellite communication. As it

was indicated the stream ciphers and their modes of operation is not recommended in block-oriented transmissions with using CRC determined over GF(2).

3.2.4 Selection of hash algorithm

Within safety-related transmission of messages from variety of well-known hash functions it is necessary to chose functions, which fulfil the conditions of one-way functions and collision resistance functions (type „strong"). Computationally safety hash functions are recommended the following types: based on MD (Message Digest), e. g. Secure Hash Algorithm (SHA2/256, SHA2/384, SHA2/512) or RIPEMD 160, 256, 320, hash function based on modular arithmetic (MASH1, MASH2) eventually hash function based on block ciphers – type AES/Rijndael (Whirpool 512).

3.2.5 Selection of Message Authentication Code

Message Authentication Code (MAC) is very used authentication technique with control of data integrity. Both procedures are realised on the based on key hash function MAC [ISO 9797-1], which assumes that communicate parts share secret key. In the present several computationally safety modifications of MAC algorithms exist: type HMAC (based on hash functions), type TTMAC (To-Track MAC – based on RIMEMD 160) or type EMAC (Encryption MAC – based on block cipher used CBC mode of operation).

4. Conclusion. On the present security stands a key element within industrial control systems using in safety-related application. Industrial systems need to take advantage of networking technologies that can support greater efficiency reliability and security. Ethernet security standards can be implemented today in industrial environments on the base of standards valid in IT security networks.

Suggested computationally safety cryptography algorithms, which were remarked in the paper, it is necessary to implemented in safety protocol, which is suitable realised as set of authentication protocol (for data integrity check only) and enciphering protocol (for assurance of confidentiality of data). Cryptography protocol for safety-related data transmission should be having the following features: flexibility (solution with expansion in the future), variability (possibility to choice from several cryptographic algorithms) and modularity (simple exchange of protocol's subparts without corruption of all units). In dependence on applications cryptography mechanisms used in the protocol have to satisfy requirements to Safety Integrity Level.

1. Mahalik, N. P.: Fieldbus technology, Industrial network standard for Real-Time Distributed Control. Springer, 2003. 2. FRANEKOVÁ, M.- KÁLLAY, F.- PENIAK, P.- VESTENICKY, P.: Communication safety of industrial network. Monography, University of Zilina, 2007, ISBN 978-80-8070-715-6. 3. STALLINGS, W.: Cryptography and Network Security. PrenticeHall, New Jersey. 2003. 4. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 2005. 5. IEC 61784-3: Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. CDV 2007. 6. NAIR,S. – VASKO, D.: DeviceNet Safety: Safety Networing for the future. 9th international CAN conference, München, Oktober 2003. 7. ProfiSafe - Test Specification for Safety Related Profibus DP Slaves, draft version 0.82, January 2003, PNO Order No 2.242. 8. DIN EN 954-1: Safety of maschinery – Safety-related parts of control system. Part 1: General principles of design.1996. 9. ISA-TR99.00.01-2004 – Security Technologies for Manufacturing and Control Systems. 10. ISA-TR99.00.02-2004 – Integrating Electronic Security into Manufacturing and Control Environment. 11. SPP-ICS System Protection profile for Industrial Control System. 12. Simatic NET: Scalance S and SoftNET Security Client. Operating instructions, Siemens 2006. 13. LEVICKÝ, D.: Cryptography in information safety. Elfa, Košice, 2005, ISBN 80-8086-022-x. 14. KARPIŃSKI, M. KURITNYK, I., P. : Sieci komputerowe: bezpeczeństwo. ATH, Bielsko-Biala, 2006. ISBN: 83-89086-93-x. 15. PŘIBYL, J.: Information safety and secrecy of messages. ČVUT, Praha, 2004.