Journal of Cybernetics and Informatics

published by

Slovak Society for
Cybernetics and Informatics

Volume 14, 2014

http://www.kasr.elf.stuba.sk/sski/casopis/

ISSN: 1336-4774

SECURITY CONSTRUCTIONS USED WITHIN CONTROL AND INFORMATION SYSTEMS INTEGRATION IN MANUFACTURING PLANTS CONDITIONS

Mária Franeková, Peter Peniak and Alžbeta Kanáliková

University of Žilina, Faculty of Electrical Engineering
Univerzitná 1, 010 26 Žilina, Slovak Republic
Tel.: +421 41 513 3346
e-mail:maria.franekova@fel.uniza.sk;peter.peniak@fel.uniza.sk;alzbeta.kanalikova@fel.uniza.sk

Abstract

Issue of the article represents the actual problem of security constructions applying which are an important part of control and information systems integration in conditions of industrial plants. A special section is dedicated to the issue of the use the cryptographic mechanisms in industrial communications system especially for applications of safety-relevant (SR) processes control with a higher integrity level SIL (Safety Integrity Level) and the possibilities of their evaluation based on mathematical approaches.

Keywords:

control system, information system, SCADA, MES, ERP, virtualization, information security, cryptographic mechanisms, safety assessment

1 INTRODUCTION AND PRELIMINARIES

Integration of information systems together with control systems is a natural consequence of need for advanced management of enterprise resources, capacities and it as well, contributes to overall optimization of development process in perspective of productivity and production effectiveness. To typical requirements of integration includes the support of the main information streams ongoing between information and control systems. Control systems often use the control centers with visualization of manufacturing process - SCADA systems (*Supervisory Control and Data Acquisition*). Connections between control and information systems ERP/MES (*Enterprise Resource Planning*)/(*Manufacturing Execution Systems*) are realized through LAN (*Local Area Network*) [1].

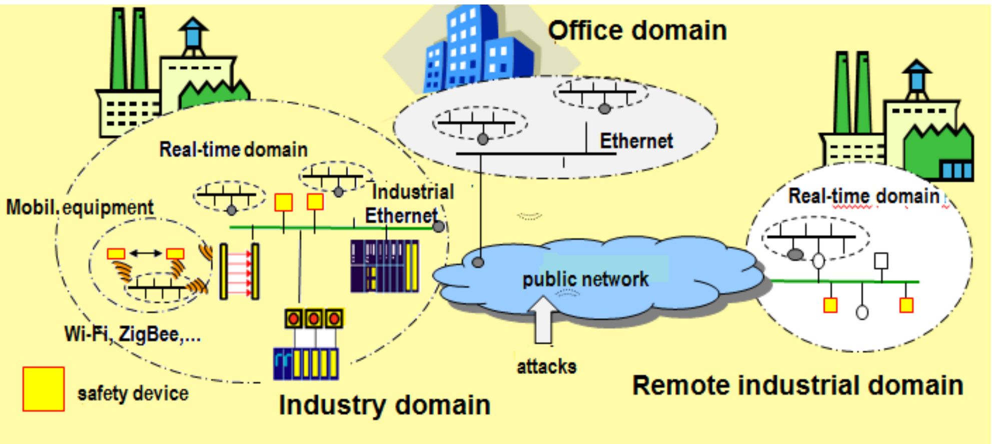

Figure 1: Inter-connection of security a safety elements within industrial and office domains

Increasingly of "security" elements (information and communication security area) and "safety" elements (safety in connection to safety-related devices) could be seen in industry [2]. Industrial domains are linked together with office domains and remote workplaces of manufacturing plants (see Figure 1). Within industrial domain (representing real time domain) could occur standard or SR devices in applications which communicated together for example via industrial Ethernet or wireless technologies. Functional safety of SR applications is realised by additional "safety" profiles, which are implemented in SW manner to SR devices (in industrial applications usually with SIL3).

The security policy of office information systems and networks is realized by well-established "security" principles used in information communication technology (ensure of confidence, integrity, authentication and availability), similarly as it is in communication via public network with remote industrial workplaces.

From a view of industrial communication system, preferred in distribution control system, it has been Fieldbus technology (IEC 61158 and IEC 61784-1) which used to be in demand for the last decades. It became the standard in relevant secure applications (IEC 61784-3, IEC 61784-4 [3]). Nowadays this communication technology is being replaced by industrial Ethernet, which has already become industrially stabile solution with its modifications in all levels of control. Support within safety solutions is for example in Ethernet Powerlink (EPL) in form of Open Safety profile, in ProfiNet in form of ProfiSafe profile or in Ethernet/IP in form of CIP Safety solution [4]. Those profiles are additional safety layer implemented over communication layers of office Ethernet protocol. For industrial applications this profiles are usually certified in safety integrity level SIL 3.

This trend of development and certification of additional security layers over standard communication protocols of industrial networks still continues even for applications with wireless SR devices communicated via wireless communication technologies (Wi-Fi, ZigBee etc.), where it is important to extend the assortment of rated security systems for cryptographic technics, implementing into security layer of access security, either to device or separately on access points from non- confidential to SR networks.

2 PROBLEM STATEMENT

Entry for cryptographic mechanisms in industry opens mainly increasing in use of wireless technologies or solutions in industrial communications with remote workplaces via public networks. Today it is sure that wireless communication systems have a great potential in automation as could be provided by (except already customised standards of Wi-Fi, Bluetooth, ZigBee, etc.) introduction of relatively new standards in practice, oriented to process automation as Wireless HART, WIA-PA and ISA 100.11a.

It is important to deal with solutions for security based on variable cryptographic schemes and protocols, not only on technological level of control, but as well on higher levels of DCS (*Distributed Control System*). For example together with SCADA systems, where it is important to verify information coming from different remote sensors (in order to prevent forgery) or it is needed to have mechanisms for signing command, that should be done, for example on remote actuator (schemes for verification of source credibility).

Problems of analysis and synthesis of safety-relevant communication systems intended to applications with increased safety integrity level SIL are detailed processed for railway control and communication systems, where general recommendations for use of an open and a close transmission system were published in standard EN STN 50159 [9]. Similar procedures are implemented in standards used in other, different resorts, where SR access is required, for example area of industrial automation.

It is important to register that safety requirements for safety-relevant communication systems could not be presented only by exams or results from practice (frequency in occurrence of dangerous events is unusually low and value of mean time between dangerous failures far exceeds the value of useful life duration of one safety- relevant system). Occurrence of random failures in SR communication system could be defined by mathematical formula for random variable using theory of relativity and mathematical statistics. Safety indicators of SR systems come from generally known indicators for non-failure operations, however it is important to relate them to incidence of important (critical) failure.

Most often it represents probability of dangerous failure $F_N(t_1,t_2)$ in defined time period, distribution law of dangerous failure $f_N(t)$, probability that system of needed functions in defined conditions and time period $R_N(t)$ realised without failures, intensity of dangerous failures $\lambda_N(t)$.

In order to evaluation of safety of SR data transmission with used close and/or open transfer systems, it is possible to use total or respectively local characteristics.

Total characteristics are theoretically are mutually equal expression of full description of a random variable possible distribution, while accepting the existence of clear relations (transmission relations) among them (1) to (4).

$$F_N(t_1,t_2) = \int_{t_1}^{t_2} f_N(t)dt, \tag{1}$$

$$f_N(t) = \frac{dF_N(t)}{dt}, \tag{2}$$

$$R_N(t) = 1 - F_N(t), \tag{3}$$

$$\lambda_N(t) = \frac{f_N(t)}{1 - F_N(t)}. \tag{4}$$

Often local characteristics are enough. Within SR data transmission via closed and/or open transmission system following characteristics could be used: mean time to dangerous failures $MTTF_N(t)$, probability of that the failure information would not be detected by decoder of security code $p_{ned,}$ mean probability of cryptographic code failure - relations (5) to (7):

$$MTTF_N(t) = \int_0^{\infty} R_N(t)dt, \tag{5}$$

$$p_{ned} = \sum_{\left\| i=\frac{d_{\min}+1}{2} \right\|}^{n} A_i \cdot p_b{}^i (1-p_b)^{n-i}, \tag{6}$$

$$\overline{p}_{CW} \approx \left(1-2^{-n}\right)^{-1}\left(1-2^{-k}\right) nP_b. \tag{7}$$

The meaning of symbols is the following:

n - length of code word (or message),

$d_{\min}$ - minimal Hamming distance on the safety code,
A_{i} - number of code words with weight i,
p_{b} - bit error rate of one element of communication channel,
k - block size of the cryptographic word (or message).

More detailed description of safety indicators for SR communication systems could be found e. g. in [5], [6].

Authors in the paper describe just safety analyses of cryptographic mechanisms, where in case of safety-relevant application, in relationship to required SIL and characteristics of safety-relevant process needed is to provide adequacy of: technical selection of cryptographic technics (promote technics of block ciphers with secret key) and processes of management of keys (the generation, testing keys, transmission, archiving and variation).

3 SOLUTIONS OF APPLYING CRYPTOGRAPHY CONSTRUCTIONS

It is known that implemented cryptographic principles protect against most of cybernetic threats, however their use in industrial safety-relevant communication system should be individually reviewed by case to case on the base of threats analysis for selected application.

Basic principle of open industrial SR communication system (from view of cryptographic mechanism use) is to build it up to have ability to, with a certain probability, withstand attacks, illegal or harmful events that impair the availability, authenticity, integrity and confidentiality of stored or transmitted data and related services that this system offers.

Approaches within application of cryptography in communication between SR devices in industrial communication system could be divided to two solutions: cryptographic technique is a part of safety protections of individual safety- relevant device, or it is a part of safety protection of several SR devices (nodes), communicated via internal industrial network, implemented into divided level of access protection. It is more frequently promoted approach, where advanced is use of for example firewall, but which should be included into safety politics of SR application. Firewall beside access protection could provide some other security services, too (for example confidentiality). Its main task is to block non - authorised network operation between internal (protected) and external network, for example by way that it do not permit to create direct connection between node in the Internet and node in industrial network.

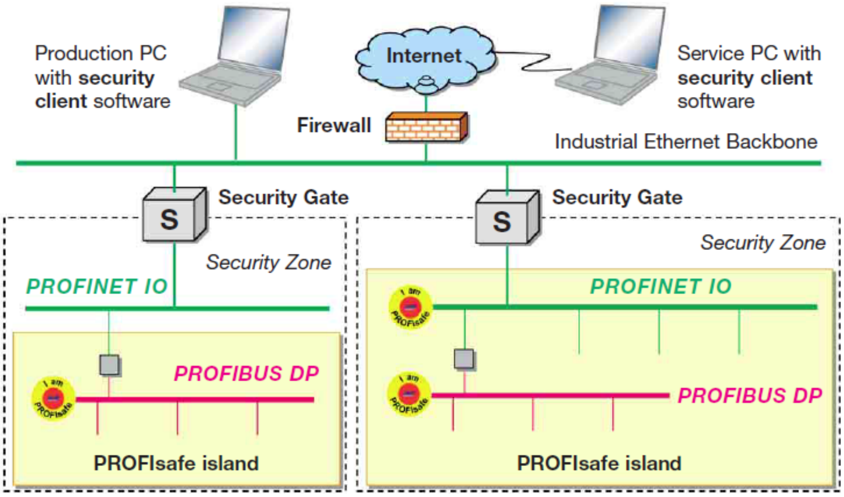

Figure 2: Example of secure solution within Profibus and ProfiNet technology [7]

Firewall could be configured that way, it would permit communication just according to some protocols. Some example of ProfiNet network protocol is described in Figure 2.

4 RECOMMENDATIONS FOR SELECTIONS OF CRYPTOGRAPHY CONSTRUCTIONS

Cryptographic techniques are recommended to apply within safety- relavant application (e. g. safety- relevant control system used in industrial communications systems) if malicious attacks within the open transmission network cannot be ruled out. This is usually the case when safety-relevant communication uses a public network, a radio transmission system and a transmission system with connections to public networks. Cryptographic techniques can eliminate masqueraded of message. Cryptographic techniques can be combined with the safety encoding mechanism or provided separately.

Cryptographic algorithm in the form of block cipher or hash function respectively in digital signature is in many applications used for protection of user data, although it could be as well used for some additional data that are not transmitted, but are well-known by sender and transmitter (implicit data). While using cryptographic techniques and methods of keys management, recommended is to follow up standardised techniques and regimes (for example standard ISO/IEC 10116). For SR applications with connection to block cipher is not recommended use the ECB (*Electronic Code Book*) mode. To provide better safety, regime CBC (*Cipher Block Chaining*) mode is recommended. Cryptographic algorithms could be registered in accordance with international standard ISO/IEC 9979, but registration itself does not provide force of algorithms.

It should understand that distributed control system consists in many cases of multiple nodes, where communications in real time is needed to be provided. Even minor disruption of such application could cause loss of ability to work in real time. Paradoxically SR applications require choice in parameters of cryptographic mechanisms in the highest safety level, which has a significant impact on the time demands of performing operations. Additional specifications needed to be considered in cryptographic techniques selection are:

- limited processing power equipment,
- implementation of cryptographic operations must be carried out in real time,
- to be followed in order that the required response time.

The most recommended cryptographic techniques in SR industrial communication system are cryptographic techniques (e.g. used for secret production recipes, procedures and general "know-how" of company, but also at the technological control level in conjunction with safety integrated circuits with fast processor) and techniques of digital signature (recommended for use wherever it is necessary to verify the veracity of information coming from remote nodes).

From the perspective of cryptographic standards today, for secure computational algorithm of symmetric ciphers are considered some modifications of DES (*Data Encryption Standard*) mainly 3-DES with three keys K_1, K_2, K_3 in which, given the existing cryptanalytic attacks, the effective key length is 112 bits.

However more enforced is encryption standard AES (*Advanced Encryption Standard*) in versions AES-128, AES-192 and AES-256, which nowadays is applied in all spheres of communication, respectively for data store in different programming languages and platforms and it is considered to be computationally secure cipher.

If we focus on algorithms of digital signatures, than currently the best known schemes of digital signatures using asymmetric cryptography:

- RSA (*Rivest Shamir Adleman*) digital signature scheme - security based on the difficulty of factoring large numbers),
- DSA (*Digital Signature Algorithm*) digital signature scheme - security based on the complexity of calculating discrete logarithms),
- ECDSA (*Elliptic Curve Digital Signature Algorithm*) digital signature scheme with security of the Elliptic Curve algorithm also based on the complexity of calculating the discrete logarithmic.

Every cryptography constructions are propended to generic cryptoanalytic's attacks which are independent to quality construction of cryptography algorithms. As example we can mentioned brute force attack. With the using integrated cryptography constructions it is necessary to choice the algorisms with the same equivalent security (the lengths of keys with approximately equal complexity of selected cryptography constructions). In the Table 1 we ca see the comparison of key lengths for representants of symmetric cryptography (2-DES, 3-DES and AES algorithms), asymmetric cryptography (RSA algorithms) and perspective ECDSA digital signature schemes as results of ENCRYPT II project [8].

Table 1: Comparison of equivalent lengths of keys in cryptography constructions [9]

Defence [in year]	**Length of symmetric algorithms keys [bits]**	**Length of hash code [bits]**	**Length of of asymmetric algorithm keys (RSA) [bits]**	**Length of EDSA keys for digital signature scheme [bits]**
4	80 (2-DES)	160	1248	160
20	112 (3-DES)	224	2432	224
30	128 (AES-1280	256	3248	256
more then 30	256 (AES -256)	512	15424	512

5 RESULTS OF ERROR PROBABILITY DETERMINATIONS WITH USING BLOCK CIPHER

Within communications and communication protocols used in safety-relevant applications cryptography code is very often combined with safety code.Let us assume that safety code used within SR industrial communication systems uses the detection cyclic linear block code works in the principle of CRC (*Cycling Redundancy Check*) - CRC-16. Further we assume that probability of undetected error of code word $P_w = 2^{-16}$ (according to norm [10], so called the worst case). The ensemble-average cryptographic word error probability $\bar{P}_{cw}$was realized according to relation (7). The results of $\bar{P}_{cw}$ for different length of code word in the input of ciphering encoder (k = 64, 128, 192, 256) and different length of input plaintext (n = 1.10^4, 5.10^4, 1.10^5, 5.10^5, 1.10^6, 5.10^6) are illustrated in The Table 2 and Table 3.

Graphical results of $\bar{P}_{cw}$ as function input bit stream of plaintext n for constant value of code words in input of cryptography decoder is illustrated in the Figure3.

Table 2: Result of the average error probability with using cryptography code in accordance with parameter *n*

Length of input plaintext *n* [bits]	**Average error probability $\bar{P}_{cw}$ if *k*=64**	**Average error probability $\bar{P}_{cw}$ if *k*=128**	**Average error probability $\bar{P}_{cw}$ if *k*=256**
1.10^4	3,13E-14	1,56E-14	7,81E-15
5.10^4	1,56E-13	7,81E-14	3,91E-14
1.10^5	3,13E-13	1,56E-13	7,81E-14
5.10^5	1,56E-12	7,81E-13	3,91E-13
1.10^6	3,13E-12	1,56E-12	7,81E-13
5.10^6	1,56E-11	7,81E-12	3,91E-12

Table 3: Result of average error probability with using cryptography code in accordance with parameter *k*

Length of input block *k*	64	128	192	256
Average error probability $\bar{P}_{cw}$	3,13 E-14	1,56 E-14	1,04 E-14	7,81 E-15

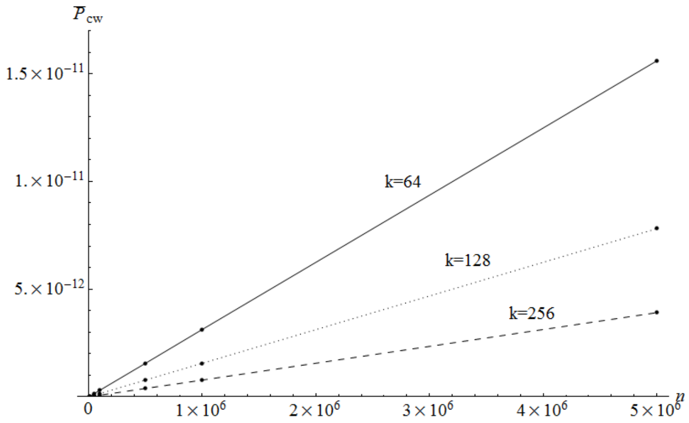

Figure 3: Average error probability of the cryptography code word in dependence on *n*

6 CONCLUSION

If we would summed the main reasons of cryptography beginning in industrial applications so it's maybe defined as follows:

- integration of information and control systems in area of manufacturing plants,

- applying price available transmission media with orientation to wireless technology with increasing number of attacks,
- increasing of applications with remote control and monitoring via internet protocols,
- connection of industrial and office domains within manufacturing plants.

The safety-relevant communication systems must be resistant against the random failures which can occur in HW elements of a transmission system or in a noise communication channel. Cryptography constructions are developed very dynamically and this is way is necessary to scope trends of cryptography parameters selection, connected them to concrete applications after realisation of risk analysis and via using mathematical apparatus to determine error probability of choice cryptography mechanism.

ACKNOWLEDGEMET

Paper was supported by project (KEGA) Nr: 024ŽU-4/2012: Modernisation of educational technologies and methods with focus on cryptography for safety relevant applications.

REFERENCES

[1] KÁLLAY, F.- PENIAK P.: Počítačové sítě LAN,MAN, WAN a jejich aplikace. Monografia, Grada Publishing 2003, ISBN 80-247-0545-1

[2] AKERBERG, J. at. al.: Efficient integration of secure and safety critical industrial wireless sensor networks. In: EURASIP Journal on Wireless Communications and Networking, 2011

[3] IEC 61784-4: Digital data communications for measurement and control.. Part 4: Profiles for secure communications in industrial network. 2005

[4] FRANEKOVA, M.- KÁLLAY, F.- PENIAK, P.- VESTENICKÝ, P.: Komunikačná bezpečnosť priemyselných sietí. Monografia, EDIS ŽU Žilina 2007, ISBN 978-80-8070-715-6

[5] FRANEKOVÁ, M.: Mathematical apparatus for safety evaluation of cryptography and safety codes used in safety related communication system. In: TST 2011, Katowice-Ustrón, Poland, October 2011, selected papers: Springer-Verlag. Berlin Heidelgerg CCIS 104. ISBN 978-3-642-24659-3, s. 126-135.

[6] RÁSTOČNÝ, K.- FRANEKOVÁ, M: Modelling of safety properties of communication Systems. In: Communications, ŽU v Žiline, r. 2008, 4. 1, s. 24-30, ISSN 1335-4205

[7] PI International: ProfiSafe. Open Solution for World Applications. In: http://www.profibus.com

[8] http://www.encrypt.eu.org

[9] STANEK M.: Kryptológia II. In: http//creativecommons.org/licences/by-nc-nd/3.0

[10] STN EN 50159: Dráhové zariadenia. Komunikačné a zabezpečovacie systémy a systémy spracovania dát. Komunikácia v uzatvorených a otvorených prenosových systémoch. SÚTN, Bratislava 2010