Journal of Cybernetics and Informatics

published by

Slovak Society for Cybernetics and Informatics

Volume 10, 2010

http://www.sski.sk/casopis/index.php (home page)

ISSN: 1336-4774

SECURITY AND SAFETY FEATURES OF INDUSTRIAL COMMUNICATIONS SYSTEM

Mária Franeková – Tomáš Ondrašina

University of Žilina, Faculty of Electrical Engineering
Univerzitná 1, 010 07 Žilina, Slovak Republic
Tel.: +421 41 513 3346
e-mail: maria.franekova@fel.uniza.sk

Abstract: The paper deals with problems of safety and security principles within industrial communication systems witch is used in safety critical applications. The summarisation of attacks to industrial automation systems and security issues and recommendations applicable to the industrial networks based on cryptographic techniques is mentioned. The mainly part is oriented to identification of risks and summarisation of defensive methods of wireless communication. Practical part the cryptoanalytic's attacks to standard wireless communications are mentioned.

Keywords: safety and security issues, industrial communication system, attack, safety integrity level, cryptographic techniques, wireless communications, cryptoanalysis

1 INTRODUCTION

Modern industrial communications networks are increasingly based on open protocols and platforms that are also used in IT (*Information and Telecommunications*) technologies. Industrial automation systems are used in wide variety of application, e. g. process manufacturing, electric power generation and distribution, gas and water supply, transportation and others. Communication networks and facilities are an important element within distributed control systems. In many cases communication systems is component part of system which partook in control of SRCP (*Safety-Related 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 reason why system have to be designed so that guarantee required SIL (*Safety Integrity Level*).

In the past automation systems were not linked to each other and were not connected to public networks like internet. Nowadays within distributed control system (DCS) the number of interconnection between different automation system, between automation systems and office systems is increasing. This is reason deals with safety and security problems within communication networks in all level of DCS. In the Figure 1 we can see the summarisation of the attacks (A) to industrial automation systems.

Cryptographic algorithms are used for secure data storage and for secure transmission. The algorithms within secure networks are implemented to cryptographic protocols and they are the important part of secure a safety standards (see Table 1). In praxes hybrid encryption is used which combines the advantages of both types of encryption (symmetric and asymmetric too). Symmetric cryptographic system is used for ciphering data of large lengths because it is faster and asymmetric cryptographic system is used for protection of shared keys.

Safety-related industrial communication systems are typically resisting against hazardous faults. Failure effects on the system can be determined directly by monitoring the original system installation, by simulation of the system operation using its model, or by computing or theoretical reasoning.

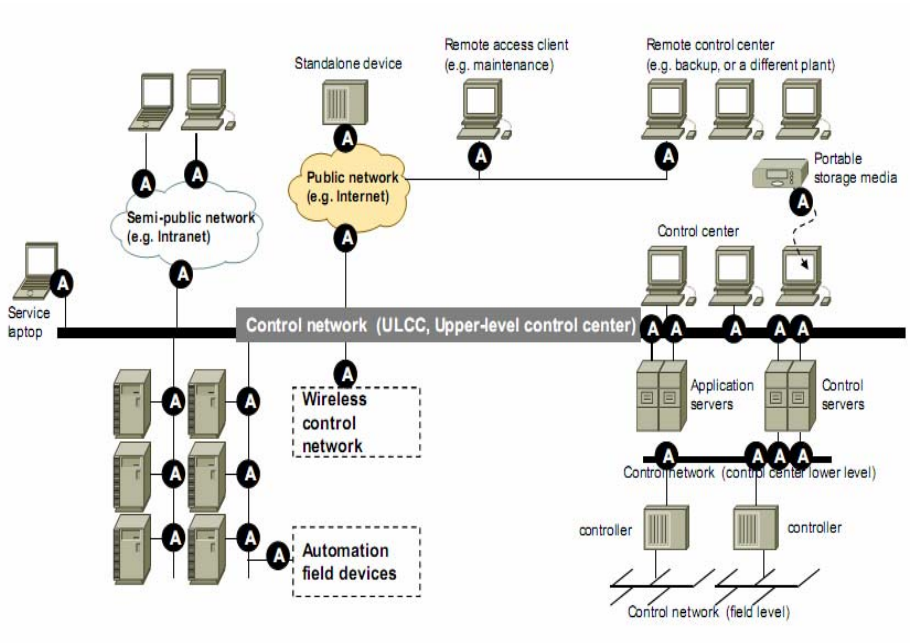

Figure 1: Attacks to industrial automation systems

Table 1: Security and safety standards for industrial communication system

Security standards	Title
ISO 27 001, 17799	Information Security Management
IEC 62443	Security for Industrial Process Measurement and Control – Network and System Security
IEC 62443	Security for Industrial Process Measurement and Control – Network and System Security
ISA SP99 **(TR1, TR2)**	Instrumentation, Systems and Automation, Manufacturing and Control System Security: TR1: Security Technologies for Manufacturing and Control Systems TR2: Integrating Electronic Security into the Manufacturing and Control System
NIST – PCSRF **SPP-ICS**	Process Control Security Requirements Forum, System Protection Profile – Industrial Control Systems (from Common Criteria)
NIST SP800-53	Recommended security controls for federal information systems
IEC 61784- 4	Digital Data Communication for Measurement and Control. Part 4: Profiles for secure communications in industrial network
Safety standards	
IEC 61508	Functional safety of Electrical/Electronic/Programmable Electronic Systems
IEC 61784- 3	Digital Data Communication for Measurement and Control. Part 3: Profiles for functional safe communications in industrial network

In the case if unauthorised access to distributed system is not able to negate, communication protocols within particular hierarchical level (on the Figure 2) are necessary to use the tools of modern cryptography.

The paper descript mechanisms of safety and security profiles located in technological level only (see Figure 2) using within safety – related industrial applications. Undetected corruption of data transmissionin these applications (e.g. control commands) can cause considerable substantial damage within equipment, environment and demands on human health.

In detail the safety and security mechanisms used for elimination of risks occurs during the wireless transmissions descript. Also the recommendations for selection of computationally safety cryptographic techniques are mentioned.

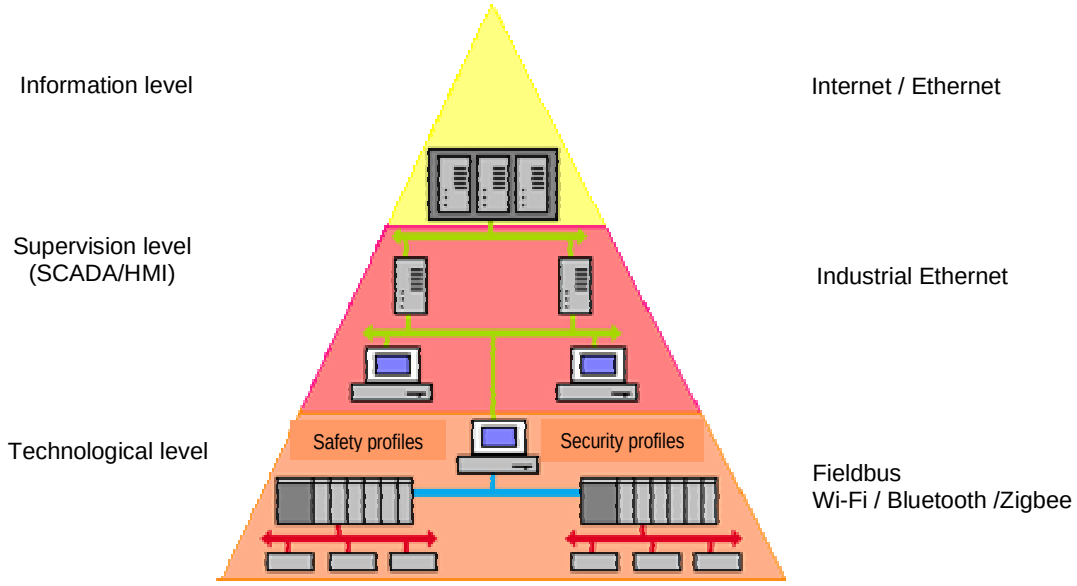

Figure 2: Hierarchical levels of communication in automation and location of safety and security profiles

2 BASIC PRINCIPLES OF SAFETY-RELATED COMMUNICATIONS

Safety and security functions of communication are implemented to additional safety communication layers and they are performed within safety - related communication protocol. Model of safety - related communication protocol for the area of industry networks according to [1] is illustrated in the Figure 3.

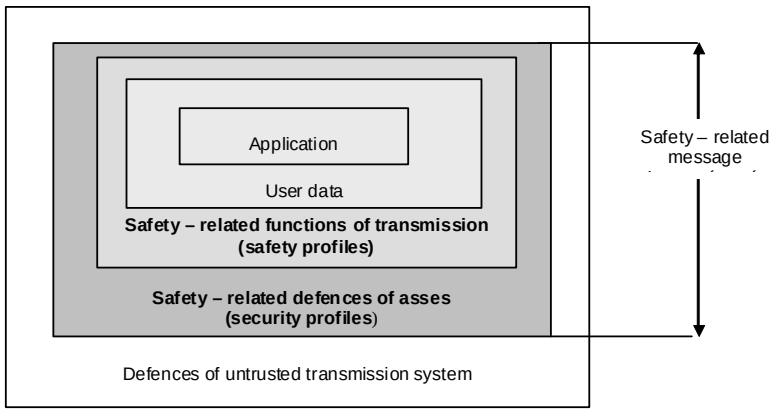

Figure 3: Model of safety - related communications in industrial applications

In the model shown in the Figure 3 mechanisms are implemented into three layers:

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

Additional security profile is necessary to implemented within open transmission system (e.g. Wi-Fi, Zigbee,...) in which is not reduced unauthorised access to system though intentional attack.

Development of safety and security profiles in industry was affected by the basic principles of safety- related communication between railway interlocking systems. Norms for area of control interlocking systems define communication safety within using the closed EN 50159-1 [2] and the open EN 50159-2 [3] transmission system. For railway applications the seven types of open transmission systems according to [3] are defined. In transmission system of types 5, 6, 7 we must assume an unauthorized access to system and predicted the masquerade of messages.

Norm IEC 61784-4 [4] the secure communications profiles (CP) for safety – related communications between participants within distributed networks describes. Norm 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.

In the present time safety a security profiles developed within industrial networks fulfil safety integrity level 3 according to EN 61508 [5].

Cryptography techniques are primarily used in security critical applications. Cryptography techniques in safety-related communication systems are necessary to use if intentional attacks within open transmission systems are not possible to handle [3]. 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 the 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. 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 quantify with the used several models. 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 cubic, …),
- O(2^n) exponential.

In the present algorithms with exponential complexity are regarded as computationally safety.

The other model which describes the security of cryptography algorithms used term equivalent security algorithms [6].

3 ANALYSIS OF THREATS AND THEIR CONSEQUENCES WITHIN INDUSTRIAL WIRELESS SAFETY – RELATED COMMUNICATIONS SYSTEM

The 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 widely used in the technological level of automation, too. The frequency is license free in most countries, which is the main reason for 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 safety and security related issues which can cause the new risks. Basic wireless communication threats and their consequences according to [7] are illustrated in the Table 3.

Table 3: Basic wireless communication threats and their consequences

Basic threats	Consequences
The transmission fades because the distance between sender and receiver increases.	Signal level is low. Bit error rate increases. Data is corrupted or lost.
The signal fades because of obstacles.	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signal fades because of environment conditions.	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances.	Signal level is low. Bit error rate increases. Data is corrupted or lost. Inserted new messages.
Two or more signals interfere with each other and cause proper signal for another receiver.	Bit error rate is high and therefore an acceptable transient signal can be initiated.
Receiver is too sensitive.	Signal is generated out from noise. Short message can appear.
Poor capability of a relaying station.	The signal can be delayed e.g. due to heavy traffic or extra signal processing in relaying stations.
The nodes understand the network state or configuration differently at the same time.	Consistency and stability problems especially when nodes are moving. Radio B can hear radio C and A, but radio A cannot hear radio C. This may cause confusion.
Nearby wireless network is using similar communication protocol.	One node is substituted intentionally or unintentionally with another node.
Security; intentional penetration to wireless network	New messages may be inserted.
Systematic failure, characteristics of wireless communication is not considered	Almost any of the above mentioned consequences may result.
Sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower power consumption i.e. longer battery life.	There is no communication through a sleeping node until the node awakes.

The threats to wireless communications systems cause the failures of the system. It is important to know where, when, and what types of failures occur in the wireless system, for

what reasons they occur and what their effects are on the system. Generally there are four ways in which errors can be divided:

- HW and SW systematic failures (e. g. underdimensionig, incorrect network definition).
- Random failures of the communications system HW (e. g. open/short circuit).
- Transcient and intermittent failures (e. g. echoes, environmental interferences, interferences by EMI).
- Failures caused by unauthorised modification of messages (e. g. node substitution, malicious attacks).

These basic failures can occurred the following communications errors during message transmission repetition, deletion, insertion, incorrect sequences, delay and masquerade.

The basic fault model of wireless communication is illustraed in the Figure 4.

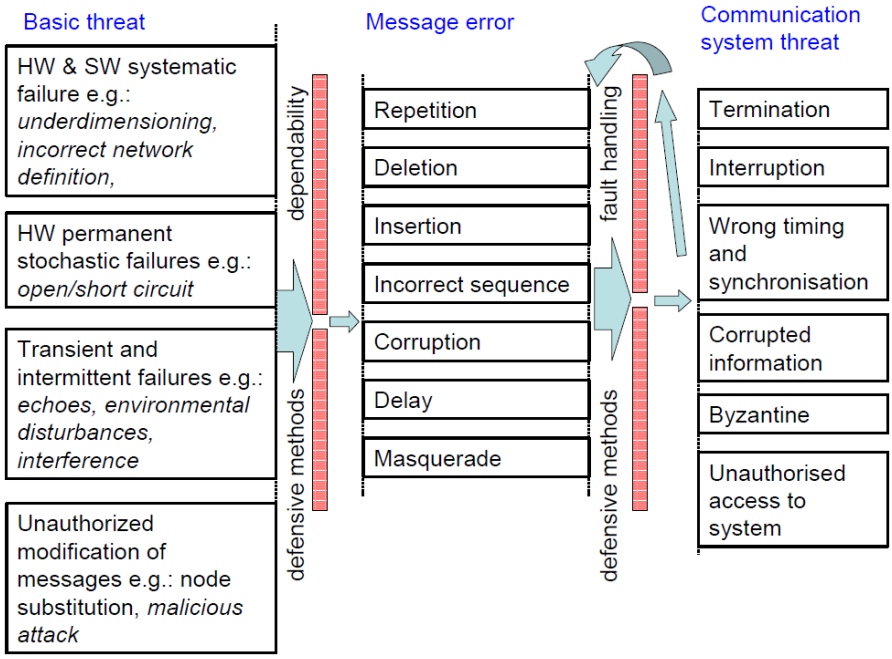

Figure 4: Fault model for wireless communications

4 ANALYSIS OF SECURITY PRINCIPLES WITHIN STANDARD WLAN TECHNOLOGIES

Basic specifications of communication Wi-Fi protocol defined according to standard IEEE 802.11 [8]. Nowadays series IEEE 802.11a to IEEE 802.11.n exist. Original cryptography standard IEEE 802.11 is based on the WEP (*Wired Equivalent* Privacy) protocol, which has implemented the stream Rivest Cipher RC4 (for data confidentiality) and check sum on the base of CRC (*Cyclic Redundancy Check*) CRC-32 (for data integrity). Standard length of the key is 40 bits, to which is added 24 bits of initial vector (IV). The key is represented by the hexadecimal number. Expanded length of the key in WEP protocol is 104 bits with 24 bits of IV. Less safe kind of ciphering, which supported WEP protocol is in the present time replaced by cryptography protocol WPA (*Wi-Fi Protected Access*), which uses stream cipher RC4 too, but the length of cipher key is 128 bits and the length of initial vector is 48 bits. Fundamental increasing of safety is obtained with using TKIP (*Temporary Key Integrity Protocol*), what is protocol for dynamic change of keys.

The use of this type of protocol is based on the server RADIUS, this is way this solution is for assuring of company. For private sector simpler implementation exists via PSK (*Pre-Shared Key*), in which the keys in all equipment are set forwards. Protocol WPA MIC

(*Message Integrity Code*) has implemented (for integrity check) so called MICHAEL. This method uses the check of the frames counter, what eliminates against replaying attacks. Nowadays in recommendation IEEE 802.11i advanced cryptography protocol WPA2 is defined, which replaced protocols WEP and WPA.

In this protocol the stream cipher RC4 is replaced by cipher AES (*Advanced Encryption Standard*) [9], which is in the present time computationally safety cryptography standard, which symmetric cipher DES (*Data Encryption Standard*) replaced. Assuring by protocol WPA2 contents authentication according to IEEE 802.1x and definition of new protocol CCMP (*Counter Mode Cipher Block Chaining MIC Protocol*).The main characteristics of the cryptography protocols used in wireless networks are illustrated in Table 4 [10].

Table 4: The main characteristics of the cryptography protocols used in the witeless networks

Protocol	WEP	WPA	WPA2
Encryption	Rivest Cipher 4	Rivest Cipher 4	Advanced Encryption Standard (AES)
Key length	104 bits 40 bits	128 bits (encryption) 64 bits (authentication)	128 bits
Length of IV	24 bits	48 bits	48 bits
Data integrity	CRC-32	Michael	Counter with CBC-MAC (Cipher Block Chaining of Message Authentication Code)
Header integrity	None	Michael	Counter with CBC-MAC (Cipher Block Chaining of Message Authentication Code)
Key control	None	Extensible Authentication Protocol (EAP)	Extensible Authentication Protocol (EAP)

5 RESULTS OF CRYPTOANALYTICS ATTACKS REALISATION TO WEP PROTOCOL

WEP protocol is based on the RC4 encryption algorithm, with the secret key of 40 bits or 104 bits being combined with a 24 bits of IV (*Initialisation Vector*). The encryption of message *C* is determined using the following formula:

$$C = [M \,||\, \mathrm{ICV(M)} + [\mathrm{RC4(K} \,||\, \mathrm{IV)}],$$

where || is a concatenation operator, ICV is integrity check value and + is a XOR operator. Clearly, the initialisation vector is the key to WEP security, so to maintain a decent level of security and minimise disclosure the IV should be incremented for each packet so that subsequent packets are encrypted with the different keys. Unfortunately for WEP security, the IV is transmitted in plain text and the 802.11 standard does not mandate IV incrementation, leaving this security measure at the option of particular wireless terminal (access point or wireless card) implementations.

Security weaknesses of WEP can be summarised as follows:

- the weaknesses of RC4 algorithm due to key construction,

- the use of static key (maximum of 4 keys), change only IV,
- IVs are too short (24 bits) and IV reuse is allowed (no protection against message replay, cycle only 224), ICV encryption with data,
- the use the same algorithm for encryption and authentication,
- no proper integrity check (CRC32 is used for error detection and isn't cryptographically secure due to its linearity),
- no built-in method of updating keys.

These weaknesses are used within the active and the passive attacks against WEP protocol. The main attracts are the following: brute-force attack (distributed and dictionary attacks), FMS attack, KoreK, Klein's attack, Man-in-the-middle attack and others (in detail see in [11]).

The attacks can be realised via different SW tools as AirCrack, Airbase, AirSnort, Chopchop, Sorwep, WepAttack, WEPcrack, WepLab and others, which are generally supported by Linux. In the paper FMS attack is descript in detail.

FMS attack (the name according to authors Scott Fluhrer, Itsik Mantin, Adi Shamir) is based on the three basic principles:

1. Some IVs form the cipher RC4 in the manner in which information about the key in input bytes can be disclosed.
2. The weak invariant allows the use the output bits for choosing the most probably bits of key.
3. The first output bits of key we can discover always, because they include the head - lineof SNAP (*SubNetwork Access Protocol*).

On the base of catching the couple (weak IV, the first byte of RC4 stream) is able to determinate the secret key.

In the paper the application Aircrack-ng was used for implementation of FMS attacks. AirCrack is WEP and WPA-PSK cracker, which is based on the passwords attack after summarisation of the sufficient number of packets.

The application Aircrack contains three main utilities, used in the three attack phases required to recover the key:

- airodump: wireless sniffing tool used to discover WEP-enabled networks,
- aireplay: injection tool to increase traffic,
- aircrack: WEP key cracker making use of collected unique IVs.

For testing purpose was realised the network which is illustrated in the Figure 5.

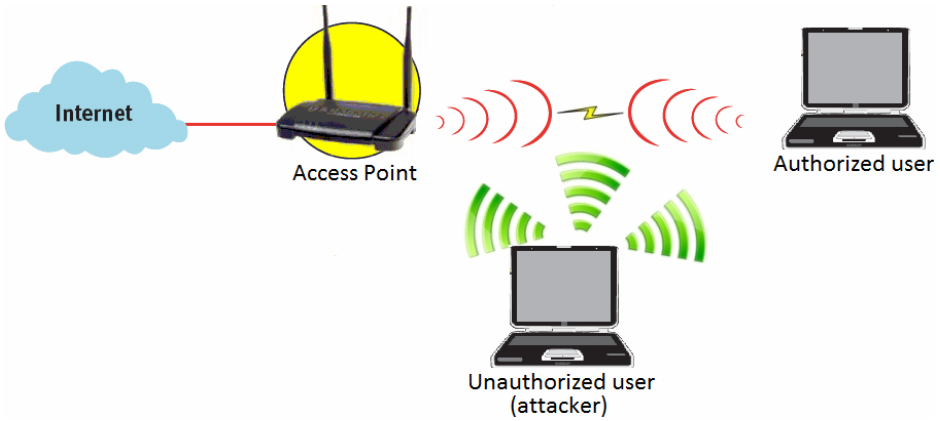

Figure 5: Realised wireless network

The testing was realised in the monitoring mode of attacker wireless card. The attack can be specified as passive attack, because it is no able to observe on the authorised network operation side. The attack was realised in the following steps:

1. The use of tool airodump-ng from package of programme aircrack-ng:
   root@bt:~# airodump-ng -c 11 mon0
2. Determination of file for writing of catching data:
   root@bt:~# airodump-ng -c 11 -w subor mon0
3. To scan of wireless network via application airodump-ng – result (see the Figure 6).

```
root@bt:~

CH 11 ][ Elapsed: 43 s ][ 2009-12-09 14:28

BSSID              PWR  RXQ  Beacons    #Data,  #/s  CH  MB  ENC  CIPHER  AUTH  ESSID

CE:A2:12:83:CC:B4   -1    0      496        0    0  11  11  OPN                    netw
02:1C:BF:00:01:6C   -1    0      587     1642   29  11  54  WEP  WEP               iWLAN
00:23:69:2F:6F:D0  -75  100      501       64    0  11  54  WPA2 CCMP  PSK    linksys
00:21:6B:47:71:D2  -41  100      327       31    0  11  54  WPA2 CCMP  PSK    KRIS_WiFi

BSSID              STATION            PWR   Rate    Lost    Packets  Probes

   (not associated) 00:1A:73:8C:EF:64  -59    0   -1  0        6  utc-wifi
CE:A2:12:83:CC:B4   00:16:CF:9B:FB:2C  -65    0   -1  0      585
02:1C:BF:00:01:6C   00:1C:BF:63:8D:47  -53    0  -48  5     1269  iWLAN
02:1C:BF:00:01:6C   00:18:F3:46:12:1A  -57    0   -1  0      472
00:23:69:2F:6F:D0   00:1A:73:A5:C5:2A  -79    1   -1  0        3
00:21:6B:47:71:D2   00:1F:45:C2:24:5B  -51    0   -1  0      221  KRIS_WiFi
```

Figure 6: The results of the network scan via application Airodump-ng

The name of tested network was iWLAN. Testing was realised for two examples:

- The use of 64-bits WEP assurance with 40-bits secret key.
- The use of 128-bits WEP assurance with 104-bits secret key.

To break WEP password is possible after catching of sufficient number of frames with different IV only. Within realisation of FMS attack about an hundred frames with weak IV was catching.

For successful braking of 64-bits WEP password (password wi1fi) 20 011 frames was catching. In this reason was decryption realised with successful 100 %. The list from application Aircrack-ng is ilustrated in Figure 7.

```
root@bt:~
                                Aircrack-ng 1.0 rc3

                        [00:03:00] Tested 365 keys (got 20011 IVs)

KB    depth   byte (vote)
 0    5/ 7   93(25600) 77(25088) 7F(25088) 49(24832) CE(24320) 0F(24064) 46(24064) AA(24064) 04(23808) 9D(23808) AD(23808) 83(23552)
 1    0/ 2   69(28416) 90(27136) E3(26112) 91(25600) 56(25344) A9(25344) 7E(25088) 37(24576) A1(24576) 8F(24320) FA(24320) 34(24064)
 2    0/ 5   31(27392) AB(26112) D3(25856) EF(25344) 2C(25344) 51(24832) 89(24832) 24(24576) B9(24576) D6(24576) 13(24320) 12(24064)
 3    1/ 3   66(26368) 98(25856) 32(25088) C6(24832) 9A(24576) 8E(24064) 91(23808) C9(23808) E5(23808) EC(23808) 03(23552) 19(23552)
 4    1/ 2   69(29440) B0(26624) 94(25600) 22(25344) 53(25088) 4C(24576) CC(24576) 38(24320) C1(24320) 2B(24064) 55(24064) C3(24064)

                KEY FOUND! [ 77:69:31:66:69 ] ( ASCII: wi1fi )
    Decrypted correctly: 100%
```

Figure 7: The succssesfull braking of 64-bits WEP password via application Aircrack-ng

The practice of breaking 128-bits WEP password was the similar. In thr first the number of cathing frames was 20000 and the experiment was unsuccssesfull. The experiment was repeteted and the succssesfuly breaking of WEP password was realiseds with 78131 frames.

6 CONCLUSIONS

In safety – related wireless communications is necessary to choose the safety mechanisms according to norms relevant for open transmission systems. In security critical applications for reducing of masquering of messages are recommended used the cryptography mechanisms.

Cryptography mechanisms provide different level of safety in compliance with the type of cryptography algorithm and length of its key. Under the results of realisation of one of most well known cryptanalytic attack to standard wireless communication we can observe that this system without implementation of added safety layer does not fulfil the requirements to safety-related communications. In this case the value of SIL 0 is necessary to increas to value of SIL 1 – 4 (by implementation of safety communication layer).

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0023/08 "Theoretical apparatus for risk analysis and risk evaluation of transport telematic systems".

7 REFERENCES

[1] IEC 61784-3: *Digital data communications for measurement and control. Part 3*: *Profiles for functional safety communications in industrial networks*. CDV 2007

[2] EN 50159-1: *Railway applications – Communication, signalling and processing systems. Part 1: Safety-related communication in closed transmission systems*. 1998

[3] EN 50159-2: *Railway applications – Communication, signalling and processing systems. Part 2: Safety-related communication in open transmission systems*. 1998

[4] IEC 61784-4: *Digital data communications for measurement and control. Part 3: Profiles for* secure communications in industrial network. 2006

[5] IEC 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems*. 1989

[6] STALLINGS, W.: *Cryptography and Network Security*. PrenticeHall, New Jersey. 2003

[7] MALM, T.- HÉRARD, J.- BOEGH, J.- KIVIPURO, M.: *Validation of safety – related wireless maschine control systems.* Technical report TR 605. 2007. ISSN 0283-7234

[8] IEEE 802.11:*IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area network. Specific requirements.* Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2007

[9] http://www.fips-197.com

[10] SANKAR, K.- SUNDARALINGAM, S.- BALINSKY, A.- MILLER, D.: *Cisco Wireless LAN Security*. Cisco Press. 2004. ISBN : 1-58705-154-0

[11] http://www.hsc.fr/ressources/articles/hakin9_wifi/index.html.en