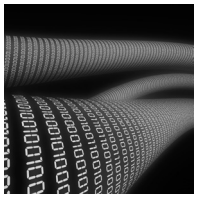

Archives of
Transport System
Telematics

Volume 3

Issue 4

November 2010

Possibilities of industrial Ethernet usage in safety critical applications

M. FRANEKOVÁ[a], T. ONDRAŠINA[a], J. ĽUPTÁK[a], P. VESTENICKÝ[a]

[a]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia

EMAIL:maria.franekova@fel.uniza.sk, tomas.ondrasina@fel.uniza.sk, juraj.luptak@fel.uniza.sk, peter.vestenicky@fel.uniza.sk

ABSTRACT

Authors describe the possibilities of the industrial Ethernet usage in safety-critical applications as a component of safety-related control systems. The main part of the paper summarizes the safety requirements of industrial Ethernet ProfiNet and Ethernet/IP based on ProfiSafe and CIPSafety safety profiles oriented towards identification of communication errors and recommendations of protective mechanisms which are applied in communication protocols. In the practical part the results of performed cryptanalytic attacks on the wireless communication protocol based on the IEEE 802.11 standard are mentioned.

KEYWORDS: industrial Ethernet, ProfiSafe, CIP Safety, Wi-Fi, Safety Integrity Level, cryptanalytic attacks

1. Introduction

In many cases the industrial communication subsystems are components of a system which participated in the safety critical process control. An undetected corruption of data transmission can cause considerable damages in the equipment, environment or human health and this is the reason why systems have to be designed so that guarantee the required Safety Integrity Level (SIL). For this reason the safety - related wired or wireless industrial equipment must have implemented a number of safety mechanisms located into special safety or security profiles [1].

Nowadays the number of industrial Ethernet type (wired or wireless) applications is increasing. At present many types of industrial Ethernet can be used in standard real-time applications. Several of them are additionally SIL3 safety profile certificated for the use in control of safety critical processes. Based on general principles, which are valid for safety related industrial communications defined in the standard IEC 61784-3 [2], the following safety profiles for CPF (Communication Profile Families) were certificated:

- CPF 1: Safety Foundation Fieldbus
- CPF 2: CIP Safety
- CPF 3: ProfiSafe
- CPF 6: Interbus Safety

After approval of the new standard ISA 100.11a [3] valid for wireless systems used in industrial automation the barrier to the use safety – related wireless machine – to – machine communications was broken. Wireless industrial Ethernet based on Wi-Fi, Bluetooth and ZigBee wireless technologies begins to be used in safety process control applications. An example of safety - related wireless communication with the master node is illustrated in Figure 1.

2. Solutions of safety industrial Ethernet

The unsuitability of standard IEEE 802.3 use in industrial applications in real time results from using a stochastic access method CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This disadvantage may be

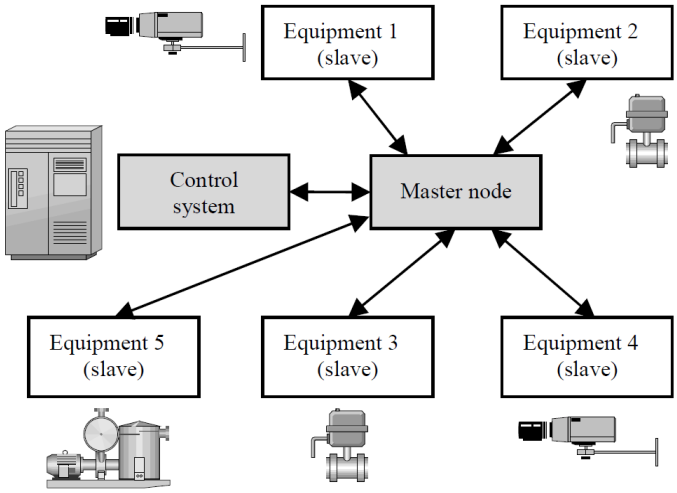

Fig. 1. Example of wireless communications with a master node
Source: [own work]

eliminated applying several principles and modifications to standard IEEE 802.3, which at the present leads to developing several variants of industrial Ethernet (see Table 1).

Nowadays on the technological level of control the industrial Ethernet replaces very popular fieldbus industrial networks and becomes the standard for large scale in the field of industrial control systems.

The advantages of using industrial Ethernet in distributed control system (DCS) are the following:

- Uniform structure of network on all levels of DCS.
- Compatibility with network of higher level of control in the DCS based on TCP/IP.
- Simplified configuration.
- Remote configuration.
- The possibility to use the existing network elements.
- The possibilities to use the existing information technology for remote access and www services in process automation.
- The possibilities to connect and address a large number of equipment.

According to the standard IEC 61784-4 [4] the safety solutions for open safety industrial Ethernet can be summarized in the following points:

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

These solutions can be generally implemented with the use of:

Safety solution of VPN (Virtual Private Networks) based on tunnelling communications protocols:

- L2TP (Layer 2 Tunnel Protocol).
- GRE (Generic Routing Encapsulation).
- PPTP (Point to Point Tunnelling Protocol).
- IPsec (IP Security Protocol) and its part: AH (Authentication Header), ESP (Encapsulating Security Payload) and IKMP (Internet Key Management Protocol).

Safety solution of Wi-Fi networks based on:

- SSID (Service Set Identification).
- MAC (Media Access Control).
- WEP (Wired Equivalent Privacy).
- WPA (Wi-Fi Protected Access).
- WPA2 (Wi-Fi Protected Access 2).
- AES – CCMP (Advanced Encryption Standard – Counter Mode Cipher Block Chaining Message Authentication Protocol).

2.1. Solution of safety measures in safety industrial network Ethernet/IP

Safety industrial Ethernet/IP (Industrial Process) is based on the communication protocol CIP (Common Industrial Protocol) which supports many vendors and companies from the area of industrial automation. The vendors are concentrated within international organisation ODVA (Open DeviceNet's Vendor Association). At present the protocol CIP contains the protocols from standard (SIL 0) industrial networks as DeviceNet, ControlNet, Ethernet/IP and communication profiles which expand the standard services of protocol. These profiles are the following:

- CIP Safety – used in the area of safety related communications (the idea is illustrated in Fig. 2).
- CIP Sync – used in the area of equipment synchronisation.
- CIP Motion – used in the area of distrusted control of motion.

Table 1. Variants of industrial Ethernet

Standard	Type
IEC/PAS 62030	MODBUS - RTPS
IEC/PAS 62405	Vnet/IP
IEC/PAS 62406	TCnet
IEC/PAS 62407	EtherCAT
IEC/PAS 62408	Ethernet Powerlink
IEC/PAS 62409	EPA
IEC/PAS 62410	SERCOS III
IEC/PAS 62411	ProfiNET
IEC/PAS 62412	P – NET on IP
IEC/PAS 62413	EtherNet/IP

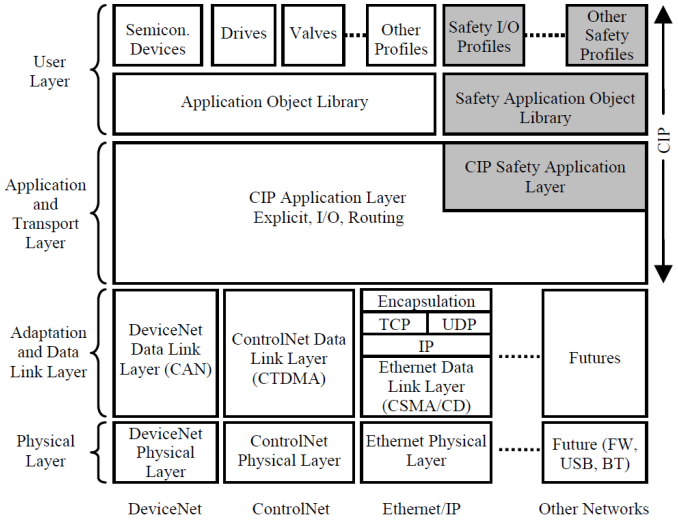

Fig. 2. Safety layers of CIP Safety protocol
Source: [own work]

The open idea of CIP Safety was certified by the organisation TÜV Rheinland Group with safety integrity level 3 (according to standard IEC 61508 [5]). In the first phase the CIP safety is implemented in safety DeviceNet network and the next extension is directed to networks ControlNet and Ethernet/IP. The CIP Safety assures simply the transmission of safety related and safety non related data across one medium and for the user allows to create a safety related connection between two (unicast) or several (multicast) applications [6].

Table 2 illustrates the safety measures, which can eliminate predicted communication errors during transmissions.

Table 2. The matrix of communication errors with relation to security measures implemented in CIP Safety

Safety measures to detect communication errors				
Types	Time stamp	ID of sender/ receiver	Redundancy with cross checking	Diverse measure
Message repetition	X		X	
Message loss	X		X	
Incorrect sequence	X	X	X	
Message corruption	X		X	
Message delay	X		X	X
Coupling of SR data		X		
Coupling of SR and SNR data	X	X	X	X
Error of network element	X			

2.2. Solution of safety measures in safety industrial network ProfiNet

The new concept of safety related communication of industrial Ethernet – ProfiNet is called ProfiSafe. An additional safety profile ProfiSafe was SIL3 certificated and it is valid for industrial Ethernet types ProfiNet [7]: ProfiNet CBA (Component Based Automation) so-called ProfiNet V1, ProfiNet IO (Input/Output, Profinet V2) and ProfiNet IRT (Isochronous Real Time, ProfiNet V3). Versions V1, V2 and V3 of ProfiNet use different types of communication channels.

The ProfiSafe profile is compatible with Profibus and ProfiNet networks. The profile was designed on the basis of knowledge from the interlocking techniques used in the railway transport according to standard IEC 62280 [8]. The defined safety related measures eliminated the communication errors from untrusted transmission systems and guarantee the required SIL.

The ProfiSafe profile can be used in the following operation mode:

- Version V1 (V1.0 to V.1.2) – for safety related communication of Profibus DP/PA.
- Version V2 - for safety related communication of ProfiNET I/O and/or Profibus DP/PA.

Communication profile ProfiSafe is based on polling principle so called master – slave communication. Safety PDU (Protocol Data Unit) and its safety measures in the context of safety related (Fail safe - F) and combined with standard (S) communication is illustrated in Figure 3.

For elimination of communication errors (repetition, deleting, insertion, delaying, change of order, corruption, masquerade of messages and messages caused by network elements) in the ProfiSafe profile the following safety measures are recommended:

- Identification of source and destination addresses.
- Sequence number (virtual).
- Data integrity check.
- Time monitoring.

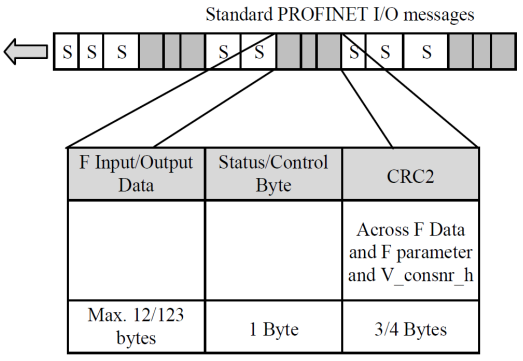

Fig. 3. Safety PDU of ProfiSafe profile
Source: [own work]

2.3. Solution of safety measures in safety industrial wireless Ethernet

When we compare wired fieldbus systems with wireless communication systems many similar risks occurring during the transmission are relevant also in wireless communication systems, but the wireless systems introduce also some new risks and the probability of failures is often higher than in the wired systems.

We can summarise basic threats to wireless communication in the following points:

- The transmission fades because the distance between the sender and receiver increases.
- The signal fades because of obstacles and environment conditions.
- Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances.
- Two or more signals interfere with each other and cause proper signal for another receiver.
- Receiver is too sensitive.
- The nodes understand the network state or configuration differently at the same time.
- Security; intentional penetration to wireless network.
- Systematic failure, characteristics of wireless communication are not considered.
- Sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower the power consumption i.e. longer battery life.

These communication threats can have the following consequences: the signal level is low, the bit error rate increases, the data is corrupted or lost, the signal can be delayed, and new messages may be inserted. There is no communication through a sleeping node until the node awakes and others.

In the communication between safety-related wireless machines all the risks or threats must be considered, safety requirements determined, adequate measures are applied to minimise the risks and the system is validated, the wireless communication can be a relevant possibility in safety-related machinery applications. Technical report [9] describes basic principles valid for safety and security profiles implemented in a wireless communication system.

The basic requirements for all cryptosystems are such as to make cryptographic mechanisms implemented in communication protocols resistant against known cryptanalytic attacks during all life time of system. To consider safety and effectiveness of cryptographic algorithm used the method to express the computational complexity of algorithms can be used, which is based on the principle of complexity theory. The operational demand of algorithm is determined by the asymptotic complexity, which is described by the behaviour of algorithm which will be changed according to input data of length n. The operational demand is generally marked by notation O (called Landau's notation or Bachmann - Landau's notation) and is a function f of input data $O(f(n))$. The computational complexity determines generally three parameters: S (Space), T (Time) and D (Data).

Nowadays, the algorithms with exponential combinational complexity, which can be broken up in real time for small value of n input data only, are considered computational safety algorithms.

Basic specifications of communication Wi-Fi protocol are defined according to standard IEEE 802.11. Nowadays series IEEE 802.11a to IEEE 802.11n 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 checksum on the base of CRC (Cyclic Redundancy Check) CRC-32 (for data integrity). A standard length of the key is 40 bits, to which 24 bits of initialization vector (IV) are added. The key is represented by a hexadecimal number. An expanded key length in the WEP protocol is 104 bits with 24 bits of IV. Less safe kind of ciphering, which supported WEP protocol is now time replaced by cryptographic 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 increase in safety is obtained using the TKIP (Temporary Key Integrity Protocol), which is the protocol for dynamic change of keys.

The use of this type of protocol is based on the server RADIUS, this solution is suitable for companies. For the private sector a simpler implementation exists via the PSK (Pre-Shared Key), in which the keys in all equipment are set forward. Protocol WPA MIC (Message Integrity Code) has been implemented (for integrity check) by so called MICHAEL. This method uses the check of the frames counter, what eliminates replaying attacks. Nowadays recommendation IEEE 802.11i defines advanced cryptography protocol WPA2, which replaced the protocols WEP and WPA.

In this protocol the stream cipher RC4 is replaced by cipher AES (Advanced Encryption Standard) [10], which is at the present the computational safety cryptographic standard, which replaced the symmetric cipher DES (Data Encryption Standard). Protocol WPA2 assures contents of authentication according to IEEE 802.1x and defines a new protocol CCMP (Counter Mode Cipher Block Chaining MIC Protocol).

3. Results of cryptanalytic attacks on wireless protocol

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

$$C = [M \,||\, \mathrm{ICV(M)} \oplus [\mathrm{RC4(K} \,||\, \mathrm{IV)}] \qquad (1)$$

where || is a concatenation operator, ICV is the 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 incrementing, leaving this security measure as the option for 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), changes only IV.
- IVs are too short (24 bits) and IV reuse is allowed (no protection against message replay, cycle only 2^{24}).
- The use of the same algorithm for encryption and authentication.
- No proper integrity check (CRC-32 is used for error detection and it is not cryptographically secure due to its linearity).
- ICV encryption with data.
- No built-in method of updating the keys.

These weaknesses are used in active and the passive attacks against the WEP protocol. The main attacks are as follows: brute - force attack (distributed and dictionary attacks), FMS attack, KoreK, Klein's attack, attack PRGA, 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. The paper describes in detail the FMS attack.

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

- Some IVs form the cipher RC4 in the manner in which the information about the key in input bytes can be revealed.
- The weak invariant allows the use of the output bits to choose the most probable bits of the key.
- We can always discover the first output bits of the key, because they include the headline of SNAP (SubNetwork Access Protocol).

On the basis of capturing the couple (weak IV, the first byte of RC4 stream) it is possible to determine the secret key.

The Aircrack-ng application was used in the paper to implement the FMS attacks. The Aircrack is a WEP and WPA-PSK cracker, which is based on the passwords attack after summarisation of the sufficient number of packets. The Aircrack application 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.

The testing was carried out in the monitoring mode of attacker wireless card. The attack can be specified as a passive attack, because it cannot observe the authorised network operation side. The attack was realised in the following steps:

- The use of tool airodump-ng from the package of programme aircrack-ng:
  root@bt:~# airodump-ng -c 11 mon0
- Determination of file for writing of captured data:
  root@bt:~# airodump-ng -c 11 -w subor mon0
- A scan of wireless network via application airodump-ng – result (see Figure 5).

For testing purposes the network has been realised, which is illustrated in Figure 4.

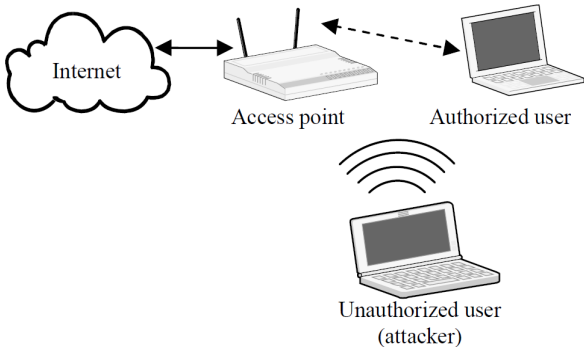

Fig. 4. Realized wireless network
Source: [own work]

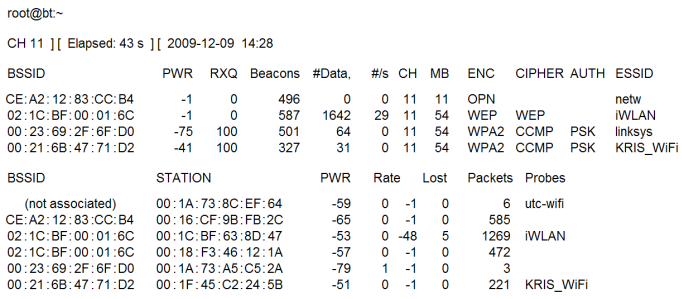

Fig. 5. The results of the network scan using the Aircrack-ng application
Source: [own work]

The name of tested network was iWLAN. The 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.

The breaking of WEP password is possible after capturing of sufficient number of frames with different IV only. In the realisation of FMS attack about hundred frames with weak IV was captured. For successful breaking of 64-bits WEP password (password: wi1fi) it was necessary to capture 20 011frames.

The practice of breaking 128-bits WEP password was similar. At first the number of captured frames was 20000 and the experiment was unsuccessful. The experiment was repeated and a successful breaking of the WEP password was realised with 78131 frames.

4. Conclusion

Nowadays the number of safety communication profiles valid for safety industrial Ethernet is increasing. The trend is to use one safety profile for all types of industrial networks implemented within the technological level of distributed control systems.

In safety-related wireless communication it is necessary to choose the safety mechanisms according to standards relevant for the open transmission systems. In security critical applications to reduce the masquerading of messages the cryptographic mechanisms are recommended to be used. Cryptographic mechanisms provide different levels of safety in compliance with the type of cryptographic algorithm and length of its key. Under the results of realisation of one of best known cryptanalytic attacks on a standard wireless communication we can observe that this system without implementation of additional security layer does not fulfil the requirements for safety-related communication. In this case the value of SIL 0 is necessary to be increased to SIL 1 – 4 (by implementation of security communication profile).

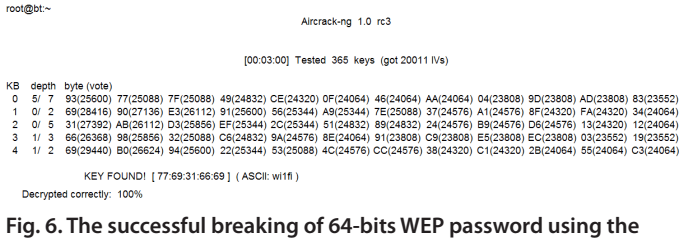

Fig. 6. The successful breaking of 64-bits WEP password using the Aircrack-ng application
Source: [own work]

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

Bibliography

[1] FRANEKOVÁ M., KÁLLAY F., PENIAK P., VESTENICKÝ P.: Communication safety of industrial networks. EDIS, ŽU Žilina, 2007. In Slovak. ISBN 978-80-8070-715-6
[2] IEC 61784-3: Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. 2007
[3] ISA SP 100.11a: Wireless Systems for Industrial Automation: Process Control and Related Applications
[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] NAIR, S. - VASKO, D.: DeviceNet Safety: Safety networking for the future. CAN conference, München, October 2003
[7] TÜV Automotive GmbH – TÜV SÜD Group Electronic Systems – TÜV Product Service GmbH, Evaluation Report, Profibus specifications, PROFIsafe – Profiles for Failsafe Technology, Report No .:PK55299T, Revisison 1.2 July of 26th 2005, Order No.:700 43831
[8] IEC 62280: Railway applications - Communication, signalling and processing systems - Part 2: Safety related communication in open transmission systems
[9] MALM, T.- HÉRARD, J.- BOEGH, J.- KIVIPURO, M.: Validation of safety – related wireless machine control systems. Technical report TR 605. 2007. ISSN 0283-7234
[10] http://www.fips-197.com
[11] http://www.hsc.fr/ressources/articles/hakin9_wifi/index.html.en