World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:8, No:12, 2014

Safety of Industrial Networks

P. Vazan, P. Tanuska, M. Kebisek, S. Duchovicova

***Abstract*—**The paper deals with communication standards for control and production system. The authors formulate the requirements for communication security protection. The paper is focused on application protocols of the industrial networks and their basic classification. The typical attacks are analysed and the safety protection, based on requirements for specific industrial network is suggested and defined in this paper.

***Keywords*—**Application protocols, communication standards, industrial networks.

I. Introduction

AS we use the various forms of ordinary human communication (spoken word, written word, a personal interview, a letter, a phone call), in industrial communication we also use various media (metallic line, optical line, air) and similarly, as we recognise different languages (English, German, Spanish and many more), we can recognise different industrial communication protocols (ControlNET,: Profinet, CANOpen, PROFIBUS, AS-i, and others).

With industrial communication the question of securityis also linked. But it does not concern only the security of information transfer, but especially operational safety control systems. In the past and also today an electrical installation so-called safety relays provide and ensure the safety at work they are used for quick and safe shutdown of a control system, in the event of dangerous situations.

Industrial networks are now becoming part of comprehensive measurement and control systems. Communication paths within these systems represent one of the most important as well as vulnerable parts. Communication security/safety is in norms and standards defined by maintaining [1], [5]:

i. Confidentiality (only authorised institutions/ entities can have access to data),
ii. Integrity (data can be modified only by authorized entities and origin of information is verifiable).
iii. Availability (data are accessible within a specific time by authorised entities and therefore is there no denial of service).

P. Vazan is with the Slovak University of Technology in Bratislava, Faculty of Material Science and Technology in Trnava (phone: +421 906 068 723; e-mail: pavel.vazan@stuba.sk).

P. Tanuska is with the Slovak University of Technology in Bratislava, Faculty of Material Science and Technology in Trnava (phone: +421 906 068 720; e-mail: pavol.tanuska@stuba.sk).

M. Kebisek is with the Slovak University of Technology in Bratislava, Faculty of Material Science and Technology in Trnava (phone: +421 906 068 708; e-mail: michal.kebisek@stuba.sk).

S. Duchovicova is with the Slovak University of Technology in Bratislava, Faculty of Material Science and Technology in Trnava (phone: +421 906 068 742; e-mail: sona.duchovicova@stuba.sk).

It is recommended to apply security functions, which are carried out by means of appropriately selected security mechanisms in order to achieve security objective in communication. These mechanisms can be implemented in software, hardware, physical or administrative form.

The current industry aims toward integration into existing operational safety fieldbus.

These technologies will ultimately represent a reduction in costs of implementing control systems, as well as the safety process data use the same hardware resources. These technologies also bring an increase in operational safety and allow easy implementation in older control systems.

Just as in the classical industrial communication and communication in safety-relevant systems there are several communication protocols, e.g. PROFIsafe, openSAFETY and more [1], [2].

II. Communication Standards of Controlled Production Systems

Forcontrol of industrial systems, with regard on the transmission infrastructure, it is necessary to meet higher quality parameters than in normal communication in computer networks. Above all, it is a possibility to high-speed communication and deterministic transfers of time-critical input-output information for the control of processes and systems. Classic communication interfaces contained in the standard IEC 61158, or ISA S50.02 (Actual Sensor interface, CANbus, Controlnet, etc.) are designed directly for control needs. Their disadvantage is closed system. This disadvantage can be eliminated by implementing new protocols for communication of automation networks. By linking industrial networks and classical IT networks, it is possible to obtain following [3]:

i. Integration into generally available networks with the classification of internet/intranet, possibility of remote configuration
ii. Higher access speed, ability to transfer larger data packages
iii. Option for address and control multiple devices for the large distance
iv. Option to create homogeneous communications networks, thus automation and data network on a single protocol
v. Subsequent possibility of creation MES systems, online controlling, restoring firmware, error correction

III. Types of Attacks in Communication

Under attacks in communications, we understand a security incident, which uses vulnerable place communication system, thereby causing material damage or damage to human health. Attack can generally be classified as intentional, unintentional

or accidental. In general, the communication system may be to attack the hardware components of the system (natural disasters, attacks caused by fire, theft, etc.), system software (deletion software due to poor configuration, error filing system, operator error, etc.), or data. From the data we can these attacks to subdivide the loss of communication (active attack on availability), eavesdropping (passive attack on confidentiality), change (active attack on integrity.) and adding value (active attack on integrity and authenticity).

IV. Requirements on Security Protection

It is necessary that communication system includes safety protection and provides it to the extent required by the application to limit the risk associated with threats. During communication in particular the following requirements must be met to ensure communication [2]:

i. Authenticity of communication,
ii. Integrity of communications,
iii. Timeliness of service user data,
iv. Regularity of controlled reports.

Requirements for a security protection must be included in the specification requirements on the system and its safety. A set of protections may be in particular applications with small modifications to change in view of the types of attacks. Each selected protection to ensure safety communication must be analysed and sufficiently described.

V. Application Protocols of Industrial Networks

Layer model of communication according to the ISO/OSI is used in industrial network, like network in information systems. Superfluous layer ISO/OSI model of OSI protocol stack had to be deleted to increase performance and eliminating delays. Network, transport and relational layers were deleted as they are not directly required at industrial network level. Controlling connections in this case link layer takes over. Deleted layers reduce overhead controlling connections, redundant data and packet transmission, which will reduce delay to a minimum. The following table contains a classification of protocols of industrial networks.

TABLE I
Classification Protocols Industrial Networks

Layers ISO/OSI	Profiles
Application	Application Protocols
Presentation	(MMS, CAL, CIP, FMS/DP, ...)
Session Transport Network	Above/highet protocols (ISO, TCP/IP, etc.)
Link	Physical and Data Link layer protocols
Physical	(Fieldbus, industrial Ethernet, TokenBus, ...)

At physical and link layer, in addition to the standard local area networks (LAN), in particular, specific business buses and industrial networks, known as Fieldbus network are applied. These types of networks are used as in the standard fixed, as well as in wireless networks.

VI. Analysis Network Protocols

A. Fieldbus

Fieldbus is the name family of industrial network protocols used for managing in real time. Since 1999 it is standardised in the standard IEC 61158. Name Fieldbus indicates digital communication bus between control systems and devices attached to them. Fieldbus is working with several types and technologies to them existing protocols, and is one of the most widely used standards in the area of industrial networks [1].

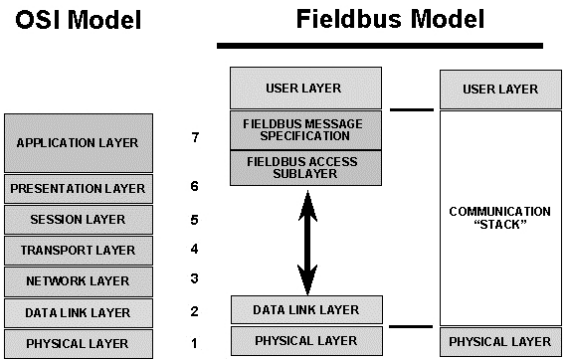

Fig. 1 The OSI Model and Fieldbus Model [4], [1]

In industrial Fieldbus networks, are according to the international standard IEC 61784-3 several types of attacks on transmitted messages are defined. With regard to these types of attacks and to ensure basic communication requirements are within industrial networks Fieldbus type set types of security protections. An overview of the types of attacks and individual protections is trapped in the table below.

TABLE II
An Overview of the Types of Attacks and Security Protections

Typesof attacks	Securityprotections
disturbance report	Serial number
unintended message repeat	Time stamp
change the order sequence	Acceptance time
unacceptable delay in the report	Connection authentication
loss report	Return message
Insert report	Security code
mask reports	Redundancy with cross-checking
faulty addressing a message	

It should be noted that the table does not reflect relations between kinds of attacks and corresponding protection.

B. CIP Safety

The CIP is one of the most widespread application protocols of industrial networks, in particular thanks to progressive architecture and independence from specific products specific producers. CIP presents an open object protocol that supports a broad range of communication services, not only for traditional Fieldbus network but also for Ethernet in industrial networks. It can be integrated into various products of individual producers in the single environment. Protocol CIP may be characterised as [3]:

i. Object designed, each communicating node is formed by means of a mutually linked objects,
ii. Provides a broad range of communication services and supports specific requirements industrial equipment and controlled applications,
iii. To transfer all reports it use a uniform format,
iv. Integrated line profiles for typical knots industrial networks.

Standard services protocol CIP can be secured by communication profile CIP safety. Thanks to this extension allows you to stream multiple data types with different levels required security to one medium.

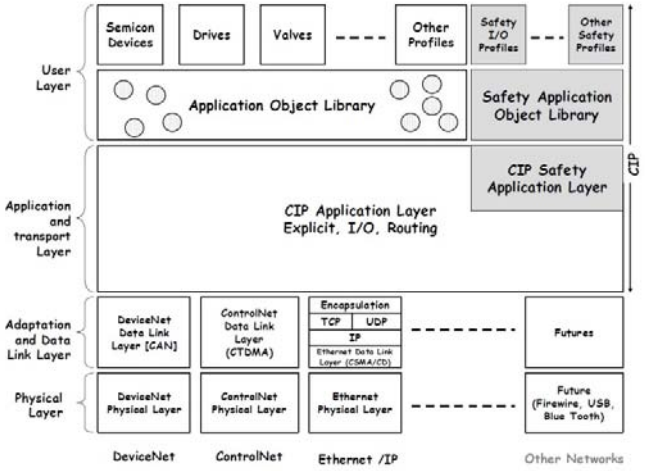

Fig. 2 CIP communications layers

CIP safety protocol is CIP, which has an extended model application layer and user profiles equipment by safety features. Adding CIP safety services into these layers, is increased the security compared to standard applications.

TABLE III
SAFETY RULES

Communication errors	Safety Rules				
	Time stamp	Sender and recipient identification	Safety CRC code	Redundancy with cross-checking	Other
Repeat	X				
Loss	X				
Insert	X	X			
Reorder	X				
Distortion			X	X	
Time delay	X				
LinkingSC/SC data		X			
Linking SC/NSC data	X	X	X	X	X
Bridging errors	X				

When you design a security measures communication protocol, CIP safety was based on the general communication errors for Fieldbus technology. In the following table, safety measures eliminating effect anticipated communication errors are defined.

Despite the fact that the CRC code provides additional protection for communication errors in the report, it was not associated to the errors in the table.

C. ProfiSafe

TABLE IV
SAFETY RULES

communication errors	Safety Rules			
	Serial number	expiration time with confirmation	authentication transmitter and receiver	Data integrity check
Repeat	X			
Delete	X	X		
Insert	X	X	X	
Change of order	X			
Distortion				X
Delay		X		
Mask		X	X	X
Error switches	X			

Security profile for ProfiSafebus network Profibus (belonging to the group fieldbus protocols) is based on the universal requirements for secure communications. It has been designed for safe communication between multiple peripheries and the controllers. In the view of the fact that most equipment is designed based on computers, ProfiSafe profile is implemented in software form [4].

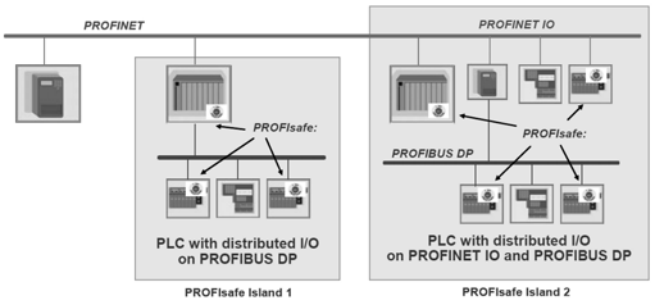

Fig. 3 ProfiSafe [3]

Security measures belong to the important parts ofProfiSafe profile. They eliminate errors arising in communication channel (communication channel) and other general communication errors based on Fieldbus technology. The individual security measures that have been assigned to communication errors are shown in the table.

In addition to these safety rulesare manufacturer: Profinet devices defined the so-called F parameters, which are not transmitted and are created during parameterisation and configuration of the equipment prior to the transfer of data. This includes, for example address source and destination, the time Watchdog monitoring and extension parameters for the report.

VII. CONCLUSION

A common feature of industrial networks is opening local means of communication technology devices toward publicly available networks, or compatibility communication protocols. It is necessary to be taken into account the possible

unauthorized access to the network, because online surveillance of devices and remote control of technological equipment has resulted in penetration of undesirable elements from the internet. That is why it is necessary in the communication and control networks to incorporate active agents to ensure access to individual components of technological process.

In the process of selection it is necessary to consider the limitations of individual solutions, and on the basis of the requirements of industrial networks, the appropriate solution is chosen.

ACKNOWLEDGMENT

This publication is the result of implementation of the project: "Research of monitoring and evaluation of non-standard conditions in the area of nuclear power plants" (ITMS: 26220220159) supported by the Research & Development Operational Programme funded by the ERDF.

We support research activities in Slovakia. The project is co-financed from EU resources.

REFERENCES

[1] M. Franekova, F. Kallay, P. Peniak, P. Vestenický, *Communication safety in the industrial network*. Zilina: University of Zilina,2007. ISBN 978-80-8070-715-6

[2] Ch. Brenton, C. Hunt,*Mastering - Network Security*,SYBEX Inc. CA, 2003. ISBN: 0-7821-4142-0

[3] I. Halenar, M. Kopcek, E. Nemlaha, *Computer networks*. Trnava: AlumniPress, 2013. ISBN 978-80-8096-191-6

[4] X. Shen, H. Yu, J. Buford, M. Akon, *Handbook of Peer-to-Peer Networking*. New York: Springer,2007. ISBN 0-387-09750-3.

[5] H. F. Tipton, M. Krause,*Information Security Management Handbook.* CRC Press LLC,2004.ISBN 0-8493-1997-8.