ON-BOARD UNIT AND ITS POSSIBILITIES OF COMMUNICATIONS ON SAFETY AND SECURITY PRINCIPLES

M. Vaculík[1], M. Franeková[2], P. Vestenický[3], M. Vestenický[4]

1) Department of Telecommunication and Multimedia, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia, tel.:+421 41 513 2228, e-mail: martin.vaculik@fel.uniza.sk

2) Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia, tel.:+421 41 513 3346, e-mail: maria.franekova@fel.uniza.sk

3) Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia, tel.:+421 41 513 3345,e- mail: peter.vestenicky@fel.uniza.sk

4) Department of Telecommunication and Multimedia, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia, tel.:+421 41 513 2239,e- mail: martin.vestenicky@fel.uniza.sk

Summary: The technical solution of on-board unit (OBU) for vehicles used for dangerous good transport and design of vehicle sensor network (based on CAN bus) for dangerous good monitoring will be discussed. In presentation the conception of GSM/GPRS networking subsystem for real time data transmission into monitoring centre will be described. Next themes of discussion will be focused on the possibilities of solution of safety-related communication channel for safety sensor network in accordance with standard for functional safety of Electrical / Electronic / Programmable Electronic (E/E/PE) systems IEC 61508 [4], recommended methods of risk analysis and possibilities of their modelling and proposal of secure communication channel over GSM/GPRS for secure data transmission into control centre on the base of IPsec protocol.

1. INTRODUCTION

The dangerous good transport by road network is everyday threat for population and environment close roads which are being used for these transports. Despite of respecting of all regulations there always exists possibility of technical failures, crashes and malfunctions. For elimination of these risks an information system for the monitoring of the dangerous good transport was developed [1]. This system uses standard communication technologies GPS (Global Position System), GSM/GPRS (Global System for Mobile Communications / General Packet Radio Service) and CAN (Controller Area Network). Non-detectable corruption of transferred data in vehicle sensor network or during transmission into monitoring centre can cause people’s health damage, material damage or environment damage. For these reasons the system must be designed to guarantee required safety integrity level (SIL).

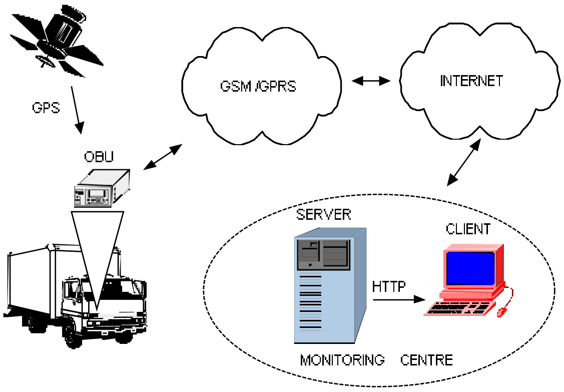

Fig. 1.Basic components of information system for monitoring of dangerous good transport

Therefore the control of dangerous good transport would be classified as safety-critical process control and the system would be designed in accordance with safety standards by which the safety requirements for elimination of risks must be classified. The safety index together with reliability, lifetime, readiness, no-failure operation, capability and feasibility of maintenance is a part of technical quality care which must be monitored in whole system life cycle.

2. SYSTEM CONCEPTION FOR MANAGING AND MONITORING OF DANGEROUS GOOD TRANSPORTS BASED ON STANDARD COMMUNICATION CHANNELS

Main part of system is mobile on-board unit with network of sensors which monitor status of dangerous good and monitoring centre which evaluates information from OBUs. In critical situation the monitoring centre sends actual data to rescue system (Fig. 1). Communication among individual components of system is based on well known communication standards GPS, GSM/GPRS and CAN. Basic requirements for this information system are:

- to provide information about dangerous good and manipulation rules with its,
- real time monitoring of dangerous good status,
- detection of non-authorized manipulation with dangerous good,
- voice and data connection with rescue system in case of damage or accident.

OBU consists of the control unit, the communication subsystem and the sensor network. Control and communication unit is based on the single board industrial PC of EPIC form (Embedded

Platform for Industrial Computing). Type of EPIC module is NANO-9452 and it is product of IEI Technology Corp., Taiwan. The CAN interface is interconnected with EPIC module by internal PC/104+ bus and it creates interface between OBU and sensor network (Fig. 2). The sensors for measuring / sensing of temperature, gas concentration, pressure, vehicle inclination and glass break have been developed [2, 3].

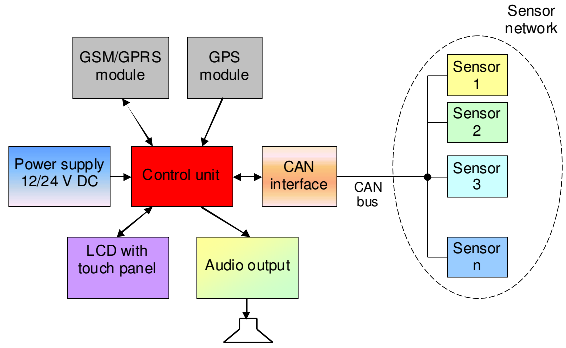

Fig. 2. Block diagram of OBU

3. POSSIBILITIES FOR SAFE AND SECURE COMMUNICATION

The standard communication buses and information networks without additional technical solutions are unusable for safety related critical data transfer, although they contain the basic methods for data integrity checking eventually other security mechanisms, too. From data transfer safety point of view such communication systems are marked as untrusted "black channels".

For analysis and synthesis of the safety related communication system in its lifecycle the modelling is being used. The results of the modelling are mostly used in pre-manufacturing phases of system lifecycle (specification of system requirements, design and construction) but also in the case of intervention into existing system, after repairs or at extension of safety functionality. The most significant method in automotive industry is analysis of the possible failures and their consequences (FMEA - Failure Mode and Effects Analysis). The results of this analysis are identification of all serious types of the fault states (failures, defects etc.) and their evaluation, sorting by importance and the proposals for possibilities of corrections.

4. SAFE COMMUNICATION CHANNEL FOR SENSOR NETWORK

The solution of the safety communication profile for sensor network based on CAN bus in vehicle OBU can be realized in two ways:

- design of new communication profile based on the safety fieldbus principles,
- improvement of existing technical solution by adding of the safety functions into communication system, whereby safety integrity level SIL will be increased from SIL 0 to the required value.

Note: Current highest required SIL level in majority of industrial application is SIL 3.

Authors incline to the second solution which does not violate original hardware design of OBU. The improvements are realized only in software of OBU by extending of communication protocol by safety related communication layer SCL (Safety Communication Layer). The placement of SCL in safety related communication protocol Fieldbus in accordance to standard IEC 61784-3 [5] is shown in the Fig. 3 over application layer. The physical, data link and application layers represent safety integrity level SIL 0 and SCL layer represents SIL 1 to SIL 4 following the number and force of implemented safety mechanisms.

This solution is compatible with existing and installed CAN bus network and is common for the standard and the safety related sensors [10, 11]. It allows safety relevant and safety irrelevant data transfer by the same bus with independent functions for the standard and the safety relevant end equipment.

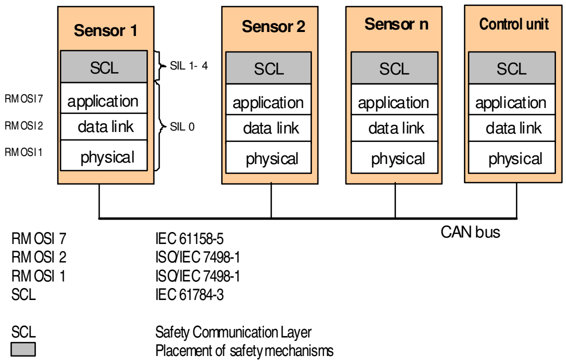

Fig. 3. Proposal of safety sensor network

CAN communication protocol used in OBU is equivalent to physical and data link layers of DeviceNet protocol. Therefore the suitable solution for the sensor network is CPF2 (Communication Profile Family) based on CIP Safety which is extension of CIP (Common Industrial Protocol) [9]. CIP Safety protocol is approved by TÜV Rheinland (Germany) for communication among safety relevant equipments which have to guarantee the SIL 3 level. Assortment of selected safety mechanisms would be selected in accordance with analysis of possible attacks on data transfer by untrusted bus. The full matrix of the communication errors and the associated safety mechanisms is given in Table 1.

Tab. 1. Recommended matrix of errors and protections for CIP Safety

COMMUNICATION ERRORS	SAFETY MECHANISMS				
	Time stamp	Identification of sender and recipient	Safety CRC code	Redundancy with cross check	Other
Repetition	X		X*		
Loss	X		X*		
Insertion	X	X	X*		
Change of order	X		X*		
Corruption			X	X	
Delay	X				
Combination of SR/SR data		X			
Combination of SR/SNR data	X	X	X	X	X
Errors of switches	X				

5. SECURE COMMUNICATION CHANNEL OF GSM/GPRS NETWORK

For transfer of traffic information into monitoring centre the GSM/GPRS network has been selected. This network can be classified in accordance with standard [4] as untrusted transmission system with safety integrity level SIL 0 and in accordance with [7] as class 6 or 7 of transmission system openness. This system without the modification is not suitable for transferring of the safety related data where traffic information appertains, too. The authors recommend to go out from the attack analysis and the secure services definitions in accordance with recommendation ITU-T X.800 “Security architecture for Open System Interconnection for CCITT applications” [8] when designing the secure mechanisms for transfer of traffic information into the monitoring centre. The typical attacks which must be taken into account in GSM/GPRS networks are the following:

- insertion of false information,
- insertion of older messages,
- change of information during transfer,
- delay of information,
- loss of information,
- attack on end station,
- attack with communication protocol.

The secure services according to X.800 [8] can be implemented into various layers of ISO/OSI model and can be divided into several groups:

- authentication services verify an identity of one or both communicating sides,
- access control services protect against non authorized access to resources of distributed system,
- confidentiality assurance services protect against non authorized revealing,
- integrity assurance services protect transferred information against non authorized modification,
- undeniable responsibility services assure possibility to prove of transmission / reception of message to other side i. e. to disable possibility of message transmission / reception disclaiming.

The selected safety functions could be preferentially applied in application layer of ISO/OSI model, or in network eventually in transport layer. Secure services are recommended to use with these security mechanisms: cryptographic protection of confidentiality and integrity, authentication, access control, digital signature, message transfer control, message encapsulation and notarial services.

In the case of the packet transmission (used in GSM/GPRS network) the simplest solution is utilization of secure versions of TCP/IP protocols (IPsec, SSL, TLS) and creation of secure VPN (Virtual Private Network) tunnel. Recommended configuration of VPN using IPsec protocol between vehicle and monitoring centre is shown in Fig. 4.

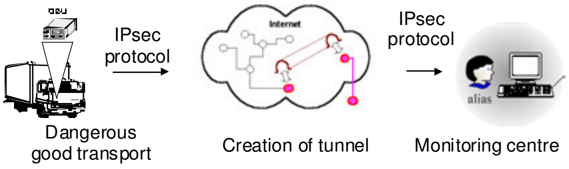

Fig. 4. Proposal of secure communication channel between vehicle and monitoring centre across VPN tunnel

6. CONCLUSION

The next possibilities of OBU development should have focused on the implementation of the new functions so that in the future the trucks can be operated with one multifunctional OBU only. The developed OBU after potential addition of the suitable modules (connected via sensor network) is able to perform more functions which are performed by the individual OBU nowadays, for example:

- navigation system,

- electronic toll collection,
- digital tachograph,
- logistic support.

In addition to the technical development of the information system for dangerous good transport monitoring the questions about standardization and legislative are interested, for example the standardization of sensors in vehicles, integration of the various functions into OBU, the international cooperation on dangerous good monitoring etc.

Acknowledgement

This paper was created as a part of solution of international project "Coordination and Stimulation of Innovative ITS Activities in Central and Eastern European Countries – CONNECT", TEN-T Programme EC. Project number: Addition no. 3 to Contract no. 472/ VÚD 2002.

REFERENCES

[1] DADO, M. et al.: *Coordination and Stimulation of Innovative ITS Activities in Central and Eastern European Countries - CONNECT*, TEN-T Programme EC, sub-domain 4.9. Research report, VÚD Žilina, April 2005 (in slovak).

[2] HRKÚT, P., KRŠÁK, E.: *Software Architecture of Vehicle On-board Unit and Monitoring Centre*. In: Proceedings of international conference ITS Bratislava '07, September 11th – 12th 2007, Bratislava. ISBN 978-80-254-0207-8 (in slovak).

[3] VACULÍK, M., VESTENICKÝ, P., VESTENICKÝ, M.: *Vehicle On-board Unit.* In: Proceedings of international conference ITS Bratislava '07, September 11th – 12th 2007, Bratislava. ISBN 978-80-254-0207-8 (in slovak)

[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*, 2007.

[6] IEC 61158: *Digital data communications for measurement and control - Fieldbus for use in industrial control systems*, 2003.

[7] CENELEC EN 50159-2: *Railway Applications - Communication, Signalling and Processing Systems - Part 2: Safety Related Communication in Open Transmission Systems*, 2002.

[8] ITU-T Recommendation X.800: *Security architecture for Open System Interconnection for CCITT applications*, 1991.

[9] FRANEKOVÁ, M., KÁLLAY, F., PENIAK, P., VESTENICKÝ, P.: *Communication security of industrial networks*. EDIS, University of Žilina, 2007. ISBN 978-80-8070-715-6 (in Slovak)

[10] SURMA, S.: *Issues of Monitoring Systems and Industrial TV.* In: Advances in Transport System Telematics, Katowice, Poland, 2006. ISBN 83-917156-4-7

[11] ŠKORPIL, V., ŠŤASTNÝ, J.: *The First Order Transmission System Modelling*. In: 5th Electronic Devices and Systems Conference Proceedings. Brno, June 11th-12th, 1998. ISBN 80-214-1198-8