INFORMATION SYSTEMS SAFETY IN A CONTEXT OF AUTMOTIVE APPLICATIONS

Michał Śmieja

University of Warmia and Mazury in Olsztyn
Faculty of Technical Sciences,
Słoneczna Street 46A, 10-710 Olsztyn,
tel.: 89 524 51 50, fax: 89 524 51 01
e-mail: smieja@uwm.edu.pl

Artur Rygiewicz

Bogart Sp. z o.o.
Nowa Wieś Mała 40, 11-040 Dobre Miasto
tel.: 89 616 15 77, fax: 89 615 17 18
e-mail: bogart@bogart.pro

Abstract

Strong expansion of IT tools in area of management and control of systems and devices of road transport is connected inseparably with a need of assurance of proper level of credibility and data safety. In paper one related to issues connected with threatens and ways of their reduction in a context of selected law regulation and analysis obtained during studies on modern motion sensor applied in system of digital tachograph in vehicles from delivery trucks and buses group. Departures from assumed scheme of information flow in vehicle can result from random interfering environmental factors as well as , action taken deliberately for specific purpose, as change of object's operation (e.g. tuning of power transmission system), or illicit modification of data subjected to revision by institutions obligated to control of vehicle. Presented in the paper example of threads and methods of information protection are part of the whole system of defined threats and securities necessary to obtain applied certificates granted by selected institutions such as BSI (Bundesamt für Sicherheit in der Informationstechnik) and development of so called PP-protection profile. In summary there are also pointed another ways to enhance a security level of described system such as e.g. redundancy in acquiring and transmission of data.

Keywords: *data safety, motion sensor, system of digital tachograph*

1. Introduction

Together with an increase of an amount of transport means present on roads, increases in relevant way a complexity of problems and issues connected with optimal use of possibilities, given by developed transport system with assurance of widely understood high level of security.

Rational and effective way of transport management among many other factors is based mainly on the credible information on state of road net, vehicles moving on it, and also people operating them.

The most commonly known system influencing on safety, requiring efficient information system, is a set of regulations known as OBD. This system regards to technical state of vehicle. Its undoubted advantage is a fact, that it concerns all currently produced vehicles. Security system of information used within the OBD, transferred by data bus is not formalized with official regulations, and on a branch between the DLC interface and tester it is officially published. In parts of information system data exchanges including OBD, unavailable (secured) is mostly information protecting intellectual properties of producers applying their individual solutions.

Difficulties in the access to IT systems including among the others OBD relate mainly to the set of codes typical for given producer, not published in official documents or to not reveal the format of data transfer in parts of data buses connecting subassemblies of a vehicle.

An example of the system requiring a high activity in the maintenance of proper level of data safety can be digital tachograph applied in vehicles which belong to group of delivery trucks and buses.

Due to the fact that road transport is realized in public space, there is no doubt for necessity of its control, dictated by safety of people and devices staying in it. Many years of experiments and results of studies on mutual interaction human-machine in relation driver-vehicle leaded to formulate defined law regulations concerning conditions and work time of active participants of road traffic.

2. System security of digital tachograph

During a design and then during the manufacturing and exploitation of a device its manufacturer predicts and designs defined way of generation, transfer, processing and utilization of information. This way is a result of producer's know-how, use of widespread and checked technical solutions, and also adjustment to standards, obeying of which is regulated in legal course.

Departures from this assumed scheme of information flow in an object can result from random interfering factors, such as damages of its elements during normal operation, or disturbances connected with interaction of external environment, and also action for specific purpose, as change of object's operation (*e.g.* tuning of power transmission system), or illicit modification of data subjected to revision by institutions obligated to control of vehicle.

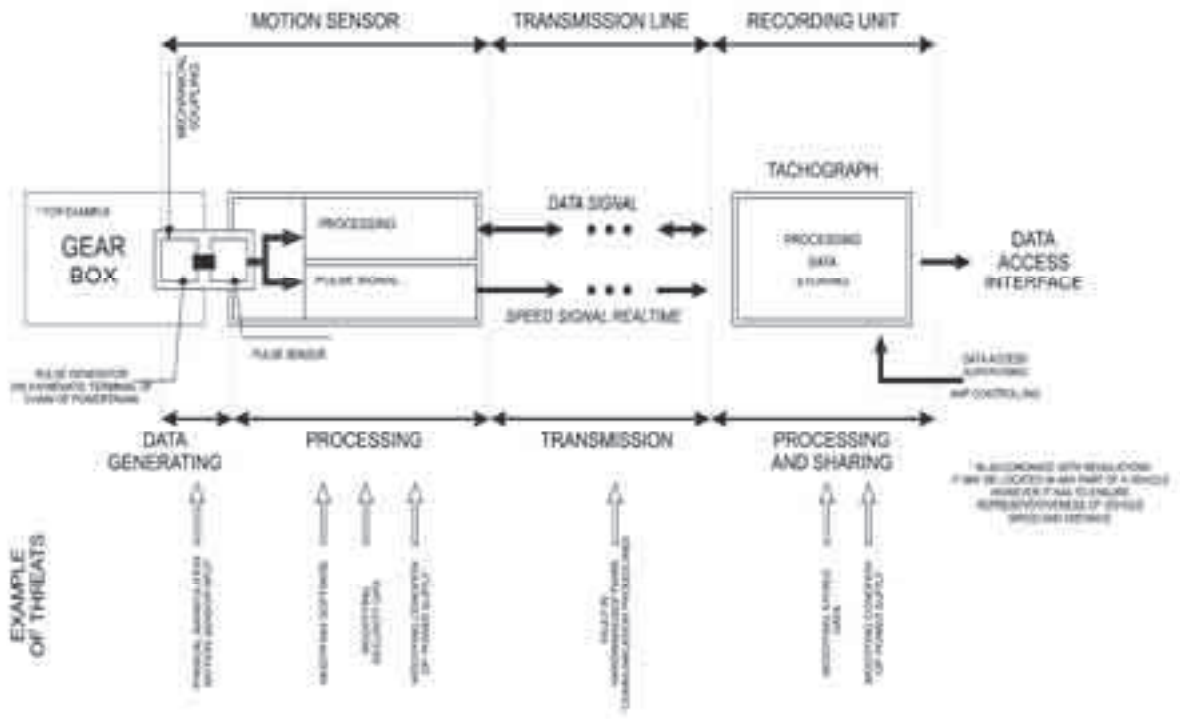

Fig. 1. Digital tachograph system

Presented in Fig. 1 digital tachograph system being classical example of a tool enabling supervision of defined group of traffic users consists of following elements:

– motion sensor connected mechanically with power transmission system, equipped in electronic unit which processes physical quantity in a form alternating magnetic field into electrical signal,

– communication line for transfer of obtained signal according to defined protocol,
– recorder enabling collection of obtained data and sharing them in a form readable for proper authorities responsible for their control.

Data safety in such complex system has to be considered in various perspectives. Presented in a Fig. 1 examples of threats were localized along the data processing chain on the way motion sensor–recorder, illustrates some ways of illicit intervention in a content of information designated, from assumption, for supervision of vehicle's operation. The only structure of system consists some mechanisms enhancing data safety, such as e.g. doubled information transmission channel in a form of speed signal real time and data signal, enabling a mutual verification of transmitted data.

As it can be seen in a figure, possibilities of threats' occurrence appear already at the stage of generation of information, what in practice means disturbances of conjugation between pulse generator and pulse, by interaction of external strong magnetic field with the use of neodymium magnets or physical disconnection of motion sensor from the power transmission system. Applied in such cases securities can limit in extreme cases to signaling an error. Detection of effects of such action from recording system point of view has to be treated as system inefficiency equal to low value of data. From external supervisor point of view, this means consciousness of lack of reliable information, what gives him a right to take defined restriction and prevention actions. As is can be seen, security of information system is not only a matter of security from direct access to data collected in records of device's memory or information transmitted via data line during vehicle operation. Moreover, such circumstances as illicit access to documentation *e.g.* at the design phase of a device or improper way of inspection of the system within the service works, also has to be treated as an element lowering security level of IT object.

Scheme of motion sensor in a context of its lifetime, being a basis of such solutions is shown in a Fig. 2.

Due to meaning which for traffic safety have mentioned issues, many of them were included in a formal way into official regulations. Fundamental document standardizing requirements related to security regarding to tachographs is the Council Regulation (EEC) No. 3821/85 [1] on recording equipment in road transport. In a result of technical development and evolution of technical systems, this regulation was repeatedly modified introducing new requirements, such as replacement of analogue tachographs with digital ones, minimum required content of motion sensor [2], or necessity of protection the motion sensors from mentioned earlier interactions of external strong magnetic fields [2], [3].In a scope of criteria of information system security assessment above documents refer to ITSEC (Information Technology Security Evaluation Criteria). Together with perfecting the IT techniques one departs gradually from this document for so called Common Criteria (included in PN/ISO IEC 15408-3).

3. Communication between vehicle unit and motion sensor

An example of solution considering many aspects of information safety is an information exchange protocol between motion sensor and recording device defined in ISO 16844-3 (Road vehicles – Tachograph systems – Part 3: Motion sensor interface).

According with requirements described in above mentioned document, an information exchange between vehicle unit (VU) and motion sensor (MS) proceeds via 4-pin connector where:
– line 1 positive supply,
– line 2 speed signal (real time),
– line 3 data signal,
– line 4 battery minus.

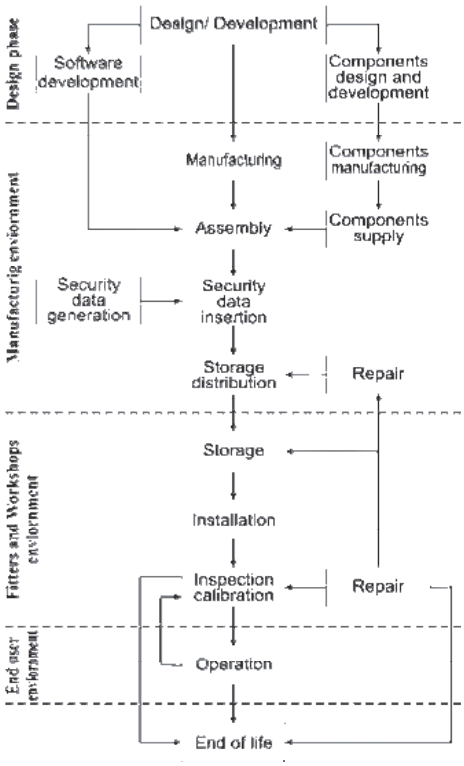

Fig. 2. Typical life cycle of motion sensor[2]

Tasks of particular lines are described as follows:

- via line 2 there is transmitted signal reflecting directly in an pulse form subsequent locations of rotating elements of power transmission system giving information on location and velocity of a vehicle,
- line 3 is used for link between motion sensor and recording device in order of:
  - initialization of communication between motion sensor and vehicle unit,
  - communication of motion sensor and vehicle unit in normal use,
  - read information,
- line 1 serves to supply the sensor fulfilling a function of transmission the information on motion direction (backward/forward) taking different current values.

Information exchange between VU (recording device–tachograph) and motion sensor is organized in a form of message exchange between VU and MS. Each Sequence (operation) of message exchange is initiated by VU in a form of request from vehicle unit to motion sensor. Confirmation of correct receiving of a request by MS should be sending by MS and acknowledge in a form of one byte containing instruction number. In a case of receiving by VU incorrect confirmation, VU can send so called Break Byte of optional value breaking sending an answer by MS, and setting it in an awaiting state for next request. In a case of correct continuing data exchange, MS sends so called replay with data requested by VU. Data transfer between VU and MS is realized as asynchronous transmission of bytes preceded by start bit (low) and finished 1 parity bit (even) and 1 stop bit (high). Maximum allowed periods between messages defined by a standard amount from 10 to 30 ms.

Numbers of instructions included in messages sent by VU, informing on type of information feedback transmitted by MS fulfill the function described for line 3, *i.e.*:

- 1 initialization communication,
- 2 communication in normal use,
- 3 read information.

Example of sequence of information exchange between VU and MS for a case 2 presented in a Fig. 4.

Formal requirements included in [4] impose application of algorithms of data encryption for information exchange between VU and MS.

Shadowed fields of frames in scheme presented in a Fig. 4 contain data encrypted according to algorithm TDES (triple data encryption algorithm) included in ANSI X 3.92 specification. To encrypt the data two keys are used according to scheme of Fig. 3

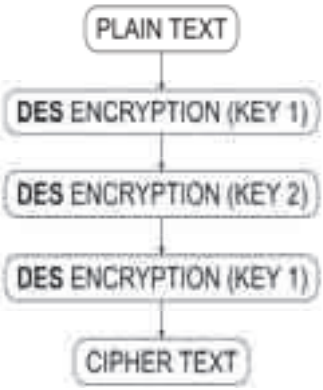

Fig. 3. Two key DES scheme

Presented above exemplary methods of information protection are only a fragment of the whole system of defined threats and securities necessary to obtain applied certificates granted by selected institutions such as BSI (Bundesamt für Sicherheit in der Informationstechnik) and development of so called PP-protection profile. Development of defined conditions of properly executed analysis of projects, functionality tests, or project and exploitation documentation, is reflected in achievement of evaluation assurance level defined by the standard [6].

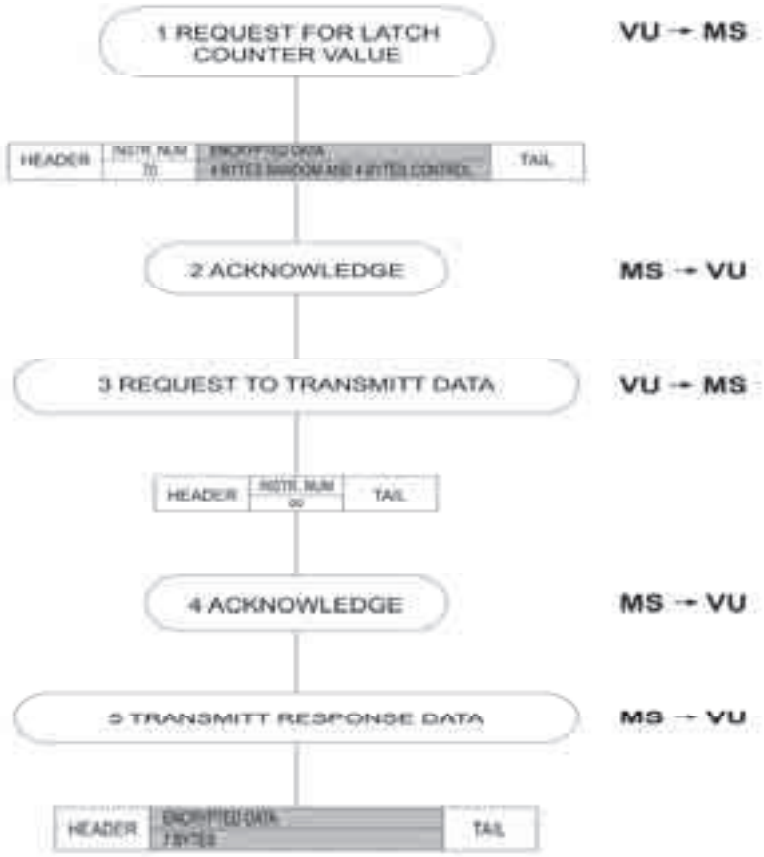

Fig. 4. Scheme of communication between VU and MS in normal use

4. Summary

Works on preparation of motion sensor for digital tachograph, carried out within the project BogArt company, concentrate on analysis of potential threats and methods of their signaling, and prevention by adjustment of final product to requirements defined by proper standards, including:

– obtaining conformity with level EAL 4+ according to Common Criteria standard,
– assurance of possibility of operation in environmental conditions in temperature range, foreseen by the standard [4].

In this order there are carried out works on application of encryption system and modern core of microcontroller on the one system FPGA, system protecting by magnetic attack, and set of appropriate procedures protecting from the attack at all phases of life of product, from design to the end of life.

In a case of digital tachograph system, data safety reflects in visible way on the safety of traffic users, independently from perfecting the methods of direct protection of particular elements of a system, in order to enhance level of data safety has to be considered the possibilities of additional authentication of registered data [3] by application of redundant systems. Redundancy can be realized on the level of source of data collecting *i.e.* data can be collected from the gear box and in parallel from independent system located on board *e.g.* GPS. Additionally location of vehicle can be confirmed from external source of information, such as toll collection system, what of course would require centralization of serviced data.

Because target receiver of information from assumption is external supervisor, such option seems to be feasible in future. Places of data collection can be related both with moving vehicle, and with database of transport company or road net administrator.

Acknowledgement

Artykuł finansowany ze środków w ramach projektu p.t. „Opracowanie technologii wytwarzania innowacyjnych czujników ruchu nowej generacji do tachografów cyfrowych zgodnie z kryteriami EAL4+”.Umowa o dofinansowanie Nr UDA-POIG.01.04.00-28-004/11-00 w ramach działania 1.4 Wsparcie projektów celowych osi priorytetowej1 Badania i rozwój nowoczesnych technologii, Programu Operacyjnego Innowacyjna Gospodarka 2007–2013.

References

[1] *Council Regulation (EEC) No. 3821/85* from December 20, 1985.
[2] *Comission Regulation (EC) No. 1360/2002* from June 13, 2002.
[3] *Comission Regulation (EC) No. 1266/2009* from December 16, 2009.
[4] ISO 16844-3 (Road vehicles-Tachograph systems Part 3: Motion sensor interface).
[5] PN-ISO/IEC 15408-1:2002 Information technology - Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
[6] PN-ISO/IEC 15408-3:2002 Information technology - Security techniques – Evaluation criteria for IT security – Part 3: Requirements for justification of trust for security.