SECURITY OF INFORMATION FLOWS IN TRANSPORT, AS AN IMPORTANT ITEM OF CRISIS MANAGEMENT WITHIN TRANSPORT SYSTEMS

J. Mikulski[1)], P. Dziula[2)]

[1)] *Chair of Transport Management and Logistic, Silesian School of Management,*
2 Krasinski Str., 40-952 Katowice, Poland, tel.: +48 602 226 799, e- mail: j.mikulski@swsz.pl
[2)] *Faculty of Navigation, Gdynia Maritime University,*
Al. Jana Pawla II 3, 81-345 Gdynia, Poland, tel.: +48 502 243 192, e-mail: przem.dz@wp.pl

Summary The article describes main aspects concerning security of information exchanged within transport systems. Definition of *critical infrastructure* and main matters coming out of fact transport systems are included in there, have been specified. The paper is also showing possibilities and limitations of wireless telecommunication systems, in case of their usage within crisis management in transport. Main directions of future research works, needed on information security within transport, have been pointed.

1. INTRODUCTION

Transport systems, due to performed tasks and processes, are generally functioning within wide areas. Wide functioning fields are resulting with necessity of using of different resources, capable of information exchange between particular system objects. Information flows in transport systems are usually performed within, broadly speaking, transport monitoring systems.

Base transport monitoring system components have been shown in Fig. 1.

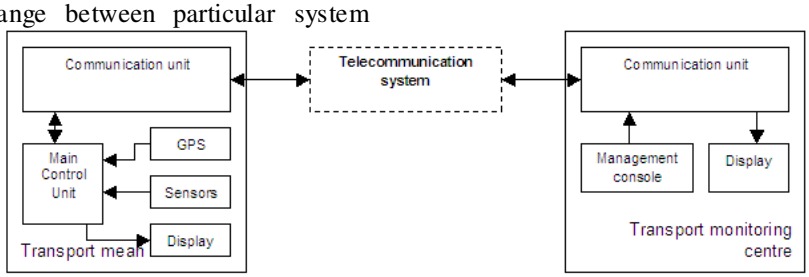

Fig. 1. System executing monitoring of transport means locations and both way information flow [1]

The fundamental items of transport monitoring systems, responsible for data flows between monitoring centres and transport means, are telecommunication systems. Transport systems, due to their special character, are mostly using wireless telecommunications. Last years we can observe very dynamic increase of usage of different kinds of means for wireless communication in transport. These systems are also constantly improved, thus, information amount able to be exchanged by means of them, is still expanding [3].

Increase of information amount flowing in the system, is resulting with higher effectiveness of transport processes performance on one side, but, on the other side, is causing appearance of many new menaces, connected to eventual access to the information, gained by non-authorised persons. Illegal access to information flows performed within transport systems can cause their decreased safety. I.e., it is easy to imagine potential results of access to dangerous cargo transportation detailed schedule, gained by terrorist attack's planners.

Higher level of information amount, exchanged within transport systems, is causing necessity of executing wide range of additional actions connected to ensure their proper security level. Improper security level of information flowing within transport systems, can lead to different crisis situations. Actions taken to secure data flows, are then very important element of crisis management in transport.

2. TRANSPORT AS A CRITICAL INFRASTRUCTURE

Activities connected to crisis management, are specifying the notion of ***critical infrastructure***, which can be defined as [4]: ***systems, including buildings, equipment, installations, services, specially important for state and its inhabitants safety; and serving for their administration, institutions and enterprises proper functioning.***

Critical infrastructure is including following systems [4]:

- energy, fuel and gas supplies,
- telecommunication and IT networks,
- financials,
- food and water supplies,
- health protection,
- **transport and communication,**
- rescue,
- ensuring functioning of state administration,

- production, storing and usage of chemical and radioactive substances.

Transport systems, carrying constantly increasing number of people and amount of cargo (including dangerous goods), are significantly exposed to crisis situations. Catastrophes of transport means carrying people and transporting dangerous cargo are especially severe. Very often accident in transport system carrying people is connected to human losses, sometimes very significant. Catastrophes of means performing transport of dangerous cargo are also usually causing huge environment destructions.

There are many different menaces classifications existing. Basing on their review, the following one has been specified [1]:

1. Catastrophe
2. Elemental disaster.
3. Fire.
4. Contamination.
5. Epidemics.
6. Public nuisance.
7. Terrorist attack.
8. Technical damage.

Each of above mentioned menaces kinds can appear in transport system, caused by loss of information flowing within this system, or illegal access to it, gained by non-authorised persons. That is why security and protection of information exchanged in transport system are extremely important.

Protection of information against illegal access, is very important especially because increasing level of terrorist attacks hazards. The attacks very often are directed to transport systems – it is enough to mention:

- 11th of September 2001 (NYC, Washington DC) – airplanes,
- 11th of March 2004 (Madrid) – commuter trains,
- 7th of July 2005 (London) – bus and subway.

3. WIRELESS TELECOMMUNICATION SYSTEMS PERFORMING DATA FLOWS IN TRANSPORT

Radio systems

Equipping of transport object with radio transmitter/ receiver, is giving possibility of two-ways information exchange between the object and other elements of transport system it is belonging to. The communication can base either on voice transmission, or data transfer. Data transfer is possible, if radio transmitter/ receiver obtains radio-modem functionality. Usually radio-modem, by connecting to some kind of central unit, collecting information on current transport mean's status, can be a source of wide data spectrum, concerning actual status of transport processes performed (Fig. 2). By use of radio-modems also two ways: transport mean – transport monitoring centre, and transport mean – other transport means, communication can be obtained.

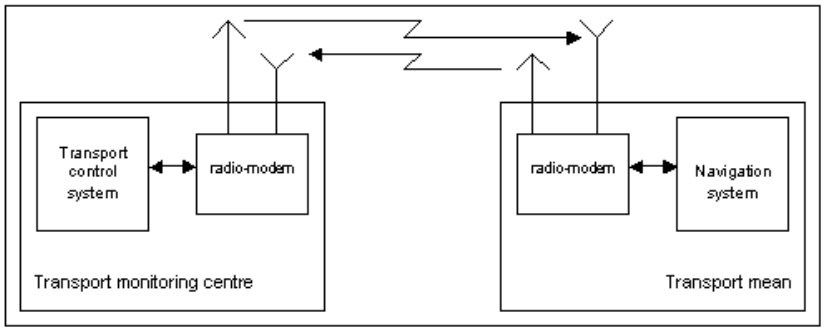

Fig. 2. Transport monitoring system exchanging data by means of radio [2]

Radio communication systems are showing following features:

- low transmission costs – only relatively low, yearly charges for the radio license
- they are not proof of bad weather conditions, heavy rain or storm, can interfere with their performance,
- radio systems are restricted about range – exact range, able to be reached, depends on transmitter's power, and frequency used,
- low amount of information is able to be transferred by means of radio.

Earth mobile communication systems (GSM)

Equipping of transport object with standard GSM phone, or GSM modem, gives possibility of very simple data exchange, between the transport monitoring centre and this object. GSM phone or modem is usually connected to central unit, collecting from sensors information, illustrating transport mean's progress (structure very similar to radio monitoring systems – GSM phone or modem replaces the radio-modem).

Monitoring systems working via GSM, are exchanging data usually by sending SMS messages, or through GPRS data link – these two services are giving possibility of relatively big amount of data transfer, within reasonable large areas, but still not global. There are also possibilities of using new GSM technologies – EDGE (speed up to hundreds of kbps), and UMTS (speed up to Mbps) within certain areas of GSM coverage. Rapid expansion of these technologies will soon give opportunities of very fast and effective GSM data exchange, to be performed within transport monitoring systems

Features of GSM telecommunication systems, when comparing them to radio ones, are:

- high costs of information transmission, in addition - rapidly increasing, when operating outside home-country (roaming costs),
- GSM transmission is practically proof of weather conditions, and land obstructions; there are only problems in areas not accessible by GSM signal, like tunnels, garages,
- very wide operational range, not demanding building of any additional infrastructure,
- bigger amount of information able to be transferred, and its high quality.

Satellite mobile communication systems

Satellite telecommunication systems are built to ensure communication possibilities for wide areas. First of commercial satellite systems – INMARSAT (*International Maritime Satellite Organisation*) – commissioned in 1982, was designated to give communication possibilities for ships at sea, covering simultaneously most of land-masses. Because of operational range, and high system performance, it has been used for many years already also by land users. During more than 20 years of operation, many successive standards, and 4 following generations of satellites were launched. Since December 2005, the 4th generation of satellites is under operation, used by the newest system – Inmarsat BGAN (*Broadband Global Area Network*). Inmarsat BGAN terminals give mobile users possibility of voice communication and data transfer of up to 500 kbps. Inmarsat was for the long time the only one mobile satellite commercial system. Nowadays we have three more under operation: Iridium (fully global), Globalstar (covering mainly lands), and Thuraya (regional system covering Europe, West and Central Asia, and North and Central Africa).

Satellite communication has similar features to ones indicated for GSM systems:

- transmission proof of bad weather conditions, and land obstructions; there are only problems in areas hardly accessible by satellite signals, like tunnels, garages, high forests, and spaces among high buildings,
- big amount of information able to be transferred, and its high quality, with following differences:
- wider operational range, in most cases truly global,
- high costs of information transmission, in most cases even higher than GSM.

4. SECURITY OF DATA FLOW SYSTEMS USED IN TRANSPORT

Security of information exchange systems, as an item of crisis management in transport, must be considered according to following features:

Integrity – protection against modification of flowing data,

entirety – protection against losses of transmitted data,

confidentiality – protection against illegal access to data,

accessibility – prompt access to information distributed within the system.

Radio communication systems seem to support low level of integrity and entirety, as they are not proof of bad weather conditions. Radio transmission can also be easily jammed by (intended or non-intended) interferences with other electromagnetic fields.

Voice and data transmissions performed by means of radio can be easily "listened in", until coded. This is important to underline however – radio users, if deciding to use special algorithms for voice and data sessions ciphering – are free to choose any solution they wish. As they are managing their telecommunication infrastructure themselves, their chose is not depending on any other parties. Important fact about radio communication systems also is – the user is supervising whole items responsible for transfer, there are no elements he can not control – that is resulting radio system proof of illegal access into its elements.

GSM and satellite systems are showing better resistance to bad weather conditions and electromagnetic interferences. It is not so easy to jam GSM or satellite transmission, however, at higher funds, still possible. It is also difficult, and demanding sophisticated equipment, to take the transmission over. GSM and satellite users, intending to use additional ciphering tools, are however limited with their choices to systems' limitations, and system supervisors' policy. As the users have no influence on telecommunication infrastructure at all, they have to follow regulations and limitations specified by system owners.

Users have also no possibility to control telecommunication system's elements against "leakage" or modifications of their data flows. As an example, Fig. 3 shows typical links' layout, that can be established by means of satellite equipment.

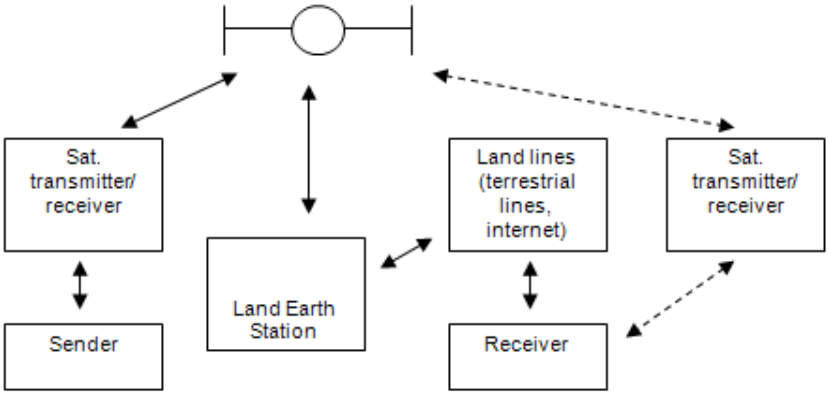

Fig. 3. Typical links able to be obtained by means of satellite telecommunication systems

The only one possibility to avoid "the week chains" users have, is to implement satellite equipment on both sides – then data flow is "bypassing" land lines (optional data flow is marked with dashed line in fig. 3). This option is not possible for GSM users – they have no any chance to choose channel their data is transmitted by.

Prompt access to information distributed within the system is one of very important aspects of crisis management. Increased amount of information obtained with the use of telematic applications, with lack of its proper management and processing, can lead to "overload" of information, consequently disturbances in its processing and whole system performance. There is then a high necessity, especially for the crisis management, for proper information flow modelling within transport systems. Increased amount of information must be properly "used", instead of causing improper system's functionality. Quick access to data processed within the system is not depending on telecommunication system used, but only on flow modelling tools and techniques.

5. CONCLUSIONS

Transport is one of sectors, where very fast development of telematics applications, observed last years, appears very significantly. The telematics mainly ensures flows and access to data describing system's, and processes' performed, actual state.

As previously mentioned, extreme attention must be paid to the fact that increased amount of information in the system means not only its higher effectiveness, but also higher emergency level of different kinds of crisis situations appearance.

Issues described in the paper let to form following elements of transport crisis management, within the range of security of data flows in transport systems:

- identification of transport systems, that should be specially protected (identification of transport systems belonging to critical infrastructure),
- identification of information processed by transport telematics systems, that should be specially protected,
- work on transport systems' data flows techniques – minimizing risk of information modification and loss – avoiding of "weak chains"
- work on algorithms of proper data transfers' ciphering and ensuring of proper security of IT systems against illegal access,
- development of information flow models within transport systems, for the purpose of crisis management,
- shortening of information resources access time.

REFERENCES

[1] DZIULA, P., MIKULSKI, J.: *Telematics in crisis management within transport systems*; 7th International Conference "Transport Systems Telematics TST'07", Katowice – Ustroń 2007.

[2] DZIULA, P.: *Telecommunication in transport monitoring systems*, 6th International Conference "Transport Systems Telematics TST'06", Katowice – Ustroń 2006.

[3] MIKULSKI, J.: *Contemporary situation in transport systems telematics*; 7th International Conference "Transport Systems Telematics TST'07", Katowice – Ustroń 2007.

[4] Polish low acts concerning crisis management, dated 26.04.2007.