SAFETY MODELLING IN MOBILE SAFETY-RELATED SYSTEMS IN RAILWAYS

Denitsa Peteva Kireva, Christo Angelov Christov, Anelia Ivanova Doseva

Faculty of Communication Technics and Technologies, Technical University of Sofia, 8, Kliment Ohridski Str., 1797 Sofia, Bulgaria, phone:+359 2 932 27 49, e-mail: kireva@tu-sofia.bg

European railways interoperability requirements enjoin the introduction of the standardized train monitoring and control systems. Along these lines, the mobile communications are up-to-date foundation utilizable in vital information transfer. In this paper the possibility of safety-related information to be transferred via mobile communications in the train movement control systems is described and safety model of the vital process is presented. Based on the produced model, safety analysis of the train monitoring and control mobile systems is carried out. A set of possible basic message errors has been derived and the corresponding threats to the transmission system are analyzed (repetition, deletion, insertion, resequence, corruption, delay, masquerade).

On the basis of the elected model safety estimation of the mobile safety-related systems is worked out in accordance with the threads analyzed and specific conditions in the railway.

Keywords: safety, mobile communications, safety-related information, railways

1. INTRODUCTION

Historically safety was approached from a component reliability perspective in the belief that if each component of a system was safe that the system too would be safe. However, over time it was realized that many safety incidents were the results of complex interactions between components, each of which was reliable. This observation gave rise to the concept of system safety, where safety is considered in the context of not only the components that make up a system, but in the context of the interactions between the components, and between the system and its environment.

Safety-related (safety-critical) systems are defined as systems whose failure could potentially result in loss of human life, damage to property, or damage to the environment. Modern railways are comprised of a range of systems that can be considered safety-critical according to this definition. Safety results from a combination of system design and the operational environment in which that system is used. Changes in the operational environment of safety-related systems can result in dramatic changes to the safety of such systems. In our days, mechanical and electromechanical devices are being replaced by solid state and programmable electronics that are often controlled remotely via communications networks – fixed and mobile.

2. SPECIAL REQUIREMENTS OF MOBILE COMMUNICATIONS SYSTEMS FOR THE CONTROL OF HIGH SPEED TRAINS

Recently mobile communications rush into railways as train control systems and GSM is adopted as Europe standard. Nevertheless, GSM technology had to be

adapted to the special requirements of train communications and control, specially for high speed trains. For this reason GSM technology has been used and a new frequency band (GSM-R band) was allocated, Table 1 [1]:

Table 1

Parameter	GSM-R
Frequency (MHz) Mobile Station – Base Station Base Station – Mobile Station	 876 – 880 921 - 925
Duplex distance	45 MHz
Total bandwidth (MHz)	2+2
Radio channel bandwidth	200 (kHz)
Number of carriers	19

In this new band the requirements of coverage, availability, call establishment, lost calls, etc. are much higher than the requirements of commercial services.

Train control procedure has some specific features:

- The train maintains a data call during the entire track. This link is used to interchange data between the train and the traffic control operator. This is one of the most complex points of the mobile communications application - data communications are connection oriented so the lost of call has a great impairment in the system.
- All the GSM-R is redundant with two equal networks working in parallel in "hot stand-by". The result is that the probability of lost calls is very low.
- There are propagation problems due to the speed of the mobile station (MS) and the special environment of the train track. The maximum speed of high speed trains is specified to 500 km/h and for this reason GSM-R communications must be able to operate to this speed. Commercial GSM is limited to a maximum speed of 250 km/h due to the bit equalizer used in the base station (BTS) to mitigate multipath. The algorithm of the equalizer has been modified to permit it to be used up to 500 km/h.
- The high speed of the MS also complicates the process of handover between BTS. So, the areas of handover must be very well defined and the undesired handovers must be minimized.
- Another problem is the short cut that produces the handover process. During a handover there is a lost of communications that last around 500 ms. This short cut produces the lost of several message (4800 bits at 9600 bit/s) which suppose a degradation of the total BER of the system. As the handovers are very frequent during the entire track, the result is that quality of service is degraded. For this reason synchronized handovers between BTS or dual link between MS and BTS with uncorrected handover between the two links are proposed.

3. TRANSMISSION OF SAFETY–RELATED INFORMATION OVER MOBILE COMMUNICATIONS

If a safety-related system involves the transfer of information between different locations, the communication system then forms an integral part of the safety-related system and it must be shown that the end to end transmission is safe. The safety requirements for a data communication system depend on its characteristics which can be known or not.

In order to reduce the complexity of the approach to demonstrate the safety of the system the transmission system has been considered as open transmission system since its characteristics (subscribers) are unknown or partly unknown. The transmission system has in general no particular preconditions to satisfy. It is from the safety point of view not or not fully trusted and is considered as a "black box" [2].

A principle structure of the safety-related system using an open transmission system is illustrated in Figure 1 and the principle model of a safety-related message is shown in Figure 2.

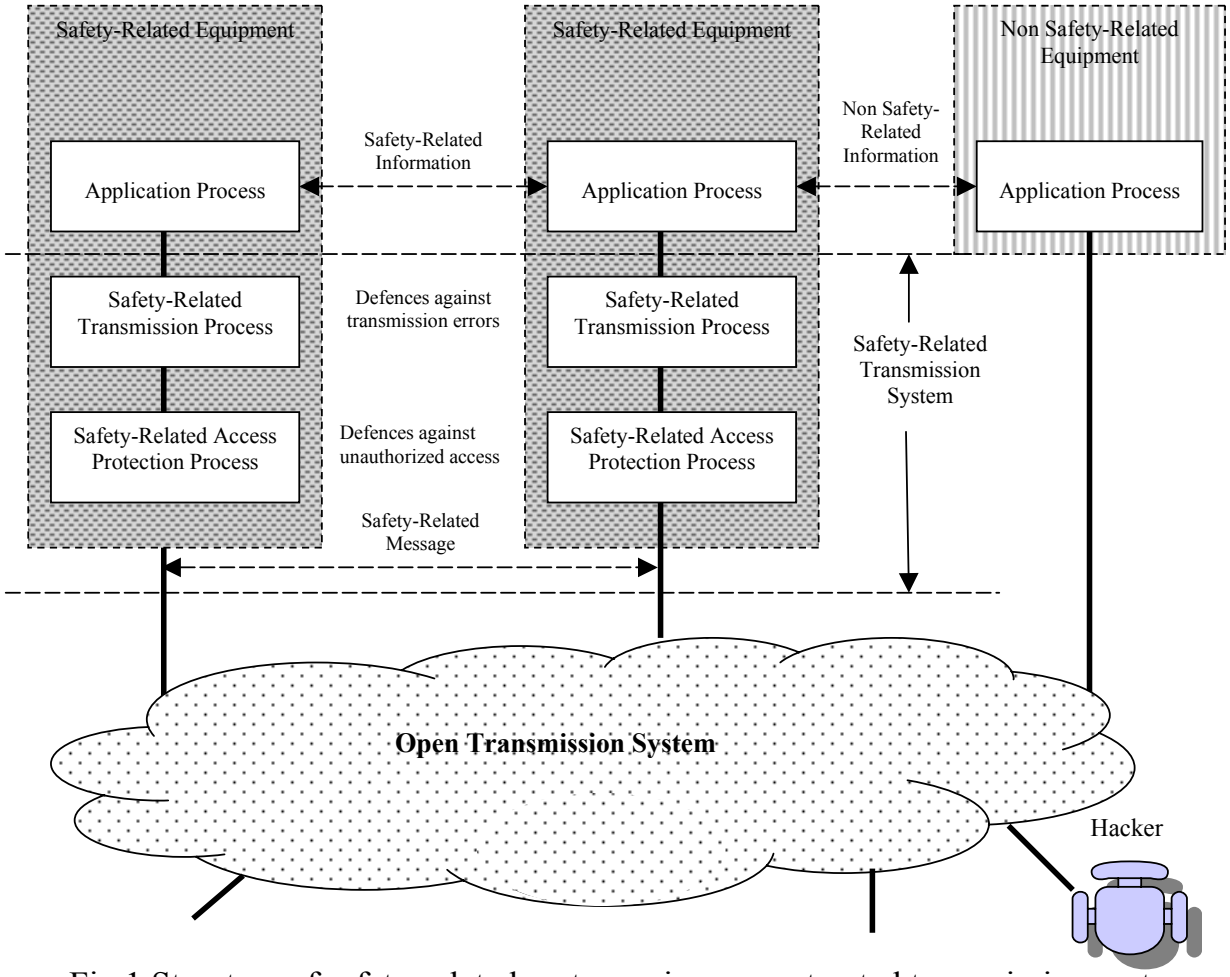

Fig.1 Structure of safety-related system using a non-trusted transmission system

Communications between trackside subsystems must obey all the requirements of an open communication system according to the CENELEC EN 50159-2 [2]

standard. This requires that such systems must be designed so to cope with the following threats:

- Repetition of an old message performed by a hacker or due to an hardware-failure;
- Deletion: a hacker/hardware-failure deletes a message, e.g. emergency, stop messages;
- Insertion: a hacker/authorized third part inserts a message;
- Resequence: a hacker/hardware-failure changes the message sequence;
- Corruption: a hacker changes the message content;
- Delay: the transmission system is overloaded due to normal traffic or a hacker generates false messages such that the provided service suffers delays;
- Masquerade: a hacker/hardware-failure masquerades the true source of messages.

According to the specific conditions in the railways the safety model of the transmission process could be derived reflecting the threats mentioned above.

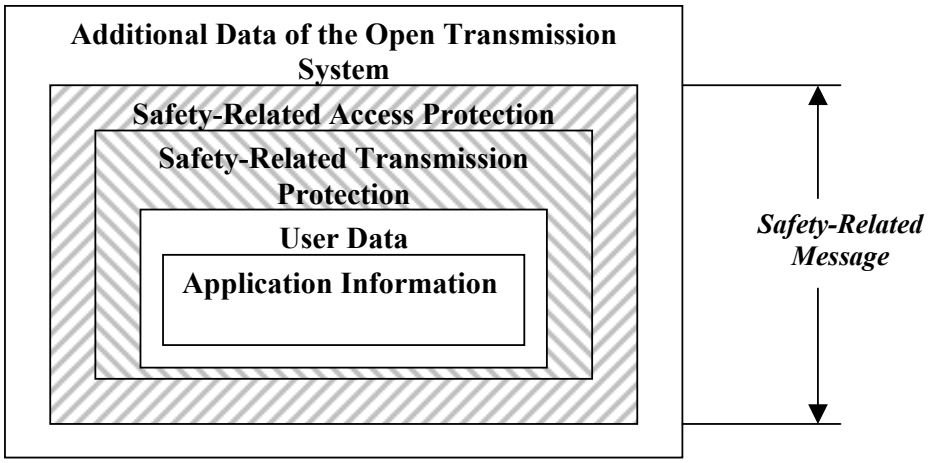

Fig. 2 Model of safety-related message

4. SAFETY MODEL OF THE SAFETY-RELATED TRANSMISSION PROCESS

In order to describe the safety of the vital transmission process the basic model shown on Fig. 3 is used.

There are four ways in which a hazard may be created:

1. The transmission hardware fails, so the messages are corrupted.
2. Bit errors arise due to electromagnetic interference (EMI) and are not detected by the transmission coding.
3. Danger comes of repetition, deletion, insertion, resequence, corruption, delay, masquerade performed by a hacker.
4. Faults occur in the transmission code checker, such that every corrupted message could be passed from the non-trusted commercial medium to the safety-related equipment.

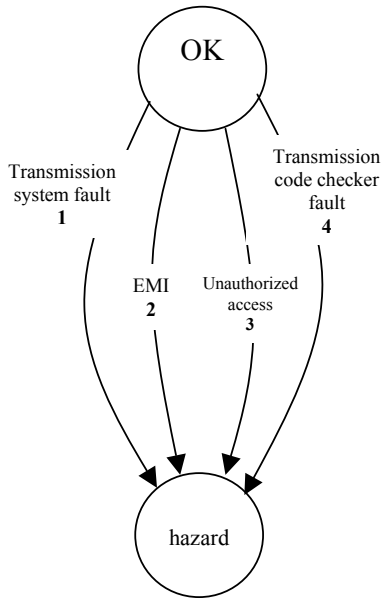

Fig.3 Basic safety model

The possible hazardous cases will be:
$P_{HW}.Q_{EMI}.Q_{COD}.Q_{UA}$ or
$Q_{HW}.P_{EMI}.Q_{COD}.Q_{UA}$ or
$Q_{HW}.Q_{EMI}.P_{COD}.Q_{UA}$ or
$Q_{HW}.Q_{EMI}.Q_{COD}.P_{UA}$ or
$P_{HW}.P_{EMI}.Q_{COD}.Q_{UA}$ or
$P_{HW}.Q_{EMI}.P_{COD}.Q_{UA}$ or
$Q_{HW}.P_{EMI}.P_{COD}.Q_{UA}$ or
$P_{HW}.Q_{EMI}.Q_{COD}.P_{UA}$ or
$Q_{HW}.P_{EMI}.Q_{COD}.P_{UA}$ or
$Q_{HW}.Q_{EMI}.P_{COD}.P_{UA}$ or
$P_{HW}.P_{EMI}.P_{COD}.Q_{UA}$ or
$P_{HW}.P_{EMI}.Q_{COD}.P_{UA}$ or
$P_{HW}.Q_{EMI}.P_{COD}.P_{UA}$ or
$Q_{HW}.P_{EMI}.P_{COD}.P_{UA}$ or
$P_{HW}.P_{EMI}.P_{COD}.P_{UA}$,

where:
P_{HW}.- Probability of the transmission hardware fails, so the messages are corrupted;
P_{EMI}.- Probability of bit errors arise due to the electromagnetic interference and are not detected by the transmission code;
P_{COD} – Probability of faults occur in the transmission code checker, such that every corrupted message could be passed from the non-trusted commercial medium to the safety-related equipment;
P_{UA}- Probability of an unauthorized access

The probability of a failure leading to a hazardous situation in the whole system will be:
Equation (1)

$$P = P_{HW}.Q_{EMI}.Q_{COD}\ Q_{UA} + Q_{HW}\ P_{EMI}\ Q_{COD}\ Q_{UA} + Q_{HW}\ Q_{EMI}\ P_{COD}\ Q_{UA} + Q_{HW}\ Q_{EMI}\ Q_{COD}\ P_{UA} + P_{HW}.P_{EMI}.Q_{COD}\ Q_{UA} + P_{HW}\ Q_{EMI}.P_{COD}\ Q_{UA} + Q_{HW}\ P_{EMI}\ P_{COD}.Q_{UA} + P_{HW}\ Q_{EMI}\ Q_{COD}.P_{UA} + Q_{HW}\ P_{EMI}\ Q_{COD}.P_{UA} + Q_{HW}.Q_{EMI}.P_{COD}\ P_{UA} + P_{HW}.P_{EMI}.P_{COD}\ Q_{UA} + P_{HW}.P_{EMI}.Q_{COD}\ P_{UA} + P_{HW}.Q_{EMI}.P_{COD}\ P_{UA} + Q_{HW}.P_{EMI}.P_{COD}\ P_{UA} + P_{HW}.P_{EMI}.P_{COD}\ P_{UA}$$

We can assume that:
$P_i.P_j \approx 0$, $P_i.P_j.P_k \approx 0$, $P_i.P_j.P_kP_n \approx 0$ as very neglected quantities and $Q_{i,j,k,n} \approx 1$ as $Q_{i,j,k,n}=P_{i,j,k,n}-1$.

So, finally the result for the probability of a hazardous failure of the whole system will be Equation (2).
Equation (2) $$\boldsymbol{P = P_{HW} + P_{EMI} + P_{COD} + P_{UA}}$$

5. CONCLUSIONS

As it could be seen from equation (2), the probability of a hazardous failure of an open transmission system depends on the hardware dependability, electromagnetic interference severity, transmission code power and cryptographic mechanism, which is used. In the railway applications hazardous failures in the hardware equipment could be minimized if dependability is increased and fail-safe principles are carried out in the design phase. The severity of an unauthorized access is difficult to be predicted since the number of the legal subscribers is small in contrast to the commercial mobile networks. Since the railways is specific application the electromagnetic interference component is higher due to the electrification tracks so extra measures should be taken to go down.

6. REFERENCES

[1] Briso C., C. Cortes, F. Arques, J. Alonso, *Requirements of GSM Technology for the Control of High Speed TRains*, IEEE 2002.

[2] CENELEC, EN 50159–2, *Railway applications–Communications, signaling and processing systems, Part 2: Safety-related communication in open transmission systems*

[3] CENELEC EN 50159–1, *Railway applications–Communications, signaling and processing systems, Part 1: Safety-related communication in closed transmission systems*

[4] Bondavalli A., E. De Giudici, S. Porcarelli, S. Sabina, F. Zanini, *A Freshness Detection Mechanism for Railway Applications*