Interdisciplinary Description of Complex Systems 16(3-A) 342-349, 2018

PROBABILISTIC APPROACH AND FUZZY SYSTEM BASED SUPPORT OF THE RAILWAY STATIONS' SMART SECURITY SYSTEM

Gábor Liebmann*, László Hanka and György Schuster

Óbuda University, Doctoral School of Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.6
Regular article

Received: 5th February 2018.
Accepted: 31st August 2018.

ABSTRACT

One of the keystones of the smart city is the transportation. The railway is the crucial part in the main public- and also the goods-transportation today, and the significance will be constantly growing. Nowadays the increase in threats and decrease in the sense of security generates a high need for designing smart and multi-level integrated security systems on the railway stations. The security risk of these territories has risen in the last years, because the public transportation plays an important role in the lives of nowadays people and will grow in the future. That means a rise in incidences of robbery, vandalism and even terrorism. The integration of the conventional systems gives more possibility and reliability for the facility management and the end-users to prevent the aforementioned incidences. The power of the complex (human-electrical-mechanical) system can be usable if in the central monitoring station only qualified and well trained operators work. Because of the difficulty of the multi-level integrated security systems, without suitable and well-trained users and operators the efficiency of the security decrease. Furthermore, the efficiency of the complex system can be lower than the unintegrated conventional realizations, so that's why it is needed to integrate special smart functions.

Managing the smart complex security systems on the aforementioned railway stations are difficult due the human factor and the large number of connections and internal processes. However, the recently created and improved probabilistic approach- and fuzzy system can be a useful mathematical solution for the aforementioned cases. These methods can be used in the full scaled security system, if first – like the Fuzzy logic – an expert level analysis gives enough information about the crucial parts of the system. With them comes the possibility to give- and get data from the determined system, and continuously recalculate the factors and - in some cases – it can be done On-Line, too. It helps to generate and send prompt information to the facility management, and with it can maximize the fully functional operational efficiency and reduce the hazards.

This article gives a useful guideline for the facility management of the smart cities' railway stations. It declares the main connections with theirs hazards to find the key elements and the in-, and outbound parameters of the smart complex security system. The generated knowledge base will contain also more additional information about the efficient- and the improvement of the system, too.

KEY WORDS

smart security on railway stations, complex security system, FTA analysis, probabilistic approach

CLASSIFICATION

JEL: C60, O30

*Corresponding author, η: liebmann.gabor@gmail.com; +36 20 825 9954;
8th Népszínház utca, Budapest, H-1081, Hungary

INTRODUCTION

Nowadays the *smart city* is one of the most mentioned expression what can be found everywhere, but the real extent is un-, or poorly-defined. Everybody has only a feeling of it. One can find the broad, data-driven and the citizen-focused definitions depending on which sector is in the focus. There definitions rarely include liveability and sustainability [1].

The transportation is one of the keystones of the nowadays cities, where the railway is the crucial part in the main public and also the long distance goods transportation, and the significance will be constantly growing. The new smart cities also need these service, but with optimized function on a minimized territory is an essential condition, what concentrates the quantity of the travellers and the value of the goods, too. The security risk of these territories has risen in the last years, because the public transportation plays an important role in the lives of nowadays people and will grow in the future. That means a rise in incidences of robbery, vandalism and even terrorism, so to prevent these actions it is needed to design, and operate a *complex* security system on these areas. In this case the meaning of the *complex* expression is a hard connected human-, electrical (multi-level integrated security system), and mechanical protection. The integration of the conventional systems gives more possibility and reliability for the facility management and the end-users to prevent the aforementioned incidences. The power of the complex (human-electrical-mechanical) system can be usable if in the central monitoring station only qualified and well trained operators work. Because of the difficulty of the multi-level integrated security systems, without suitable and well-trained users and operators the efficiency of the security decrease. Furthermore, the efficiency of the complex system can be lower than the unintegrated conventional realizations, so that is why it is needed to integrate special smart functions.

Managing the smart complex security systems because of the aforementioned reasons is difficult due to the human factor and the large number of connections and internal processes. In this article we show and test more mathematical functions and methods that can be usable in the full scaled security system of the Facility Management.

THE RAILWAY STATION'S ENVIRONMENTAL RISK

The stations comprise diverse outdoor and indoor facilities, many of them work 7/24. On the railway stations there is a crucial need to guard passengers, employees, goods, infrastructure, and assets against possible threats. These facilities in particular have become at least as vulnerable as airports. They must therefore meet very demanding criteria with regard to security, safety, communications, and building automation – also to uphold their reputation as providers of safe, well-organized services that travellers and freight forwarders can rely on [2].

The aforementioned enviromental risk generates security challanges of the complex system, such as preventing and responding vandalism, robberies, sabotage and terrorism. When the security challenges are succesfully met, it gives employees and passangers confidence in the safety of train stations [3].

DETERMINING AN OPERATIONAL MODEL OF THE STATION'S COMPLEX SECURITY SYSTEM

The designing-, installating-, and finalizing-term of the security system is only the begining, since the facility management has to operate it constantly 7/24. It cannot be done without specialized and expert employees at the economy and at the security part, too. To prevent the mailfunctions and get the highest efficiency of the system it is needed to generate a special pointer what can show the momentary state of the complex security system.

For the pointer generation the first step is to determine the inputs, the variables, the outputs and the functions of the security system on the station with their inner connections. With the aforementioned elements the operation diagram of the station's global security system is shown in Figure 1. The model is designed for the inner connections of the global security system. The arrows represent the connection and the direction, the bulk of the area represents the importance of the subsystem.

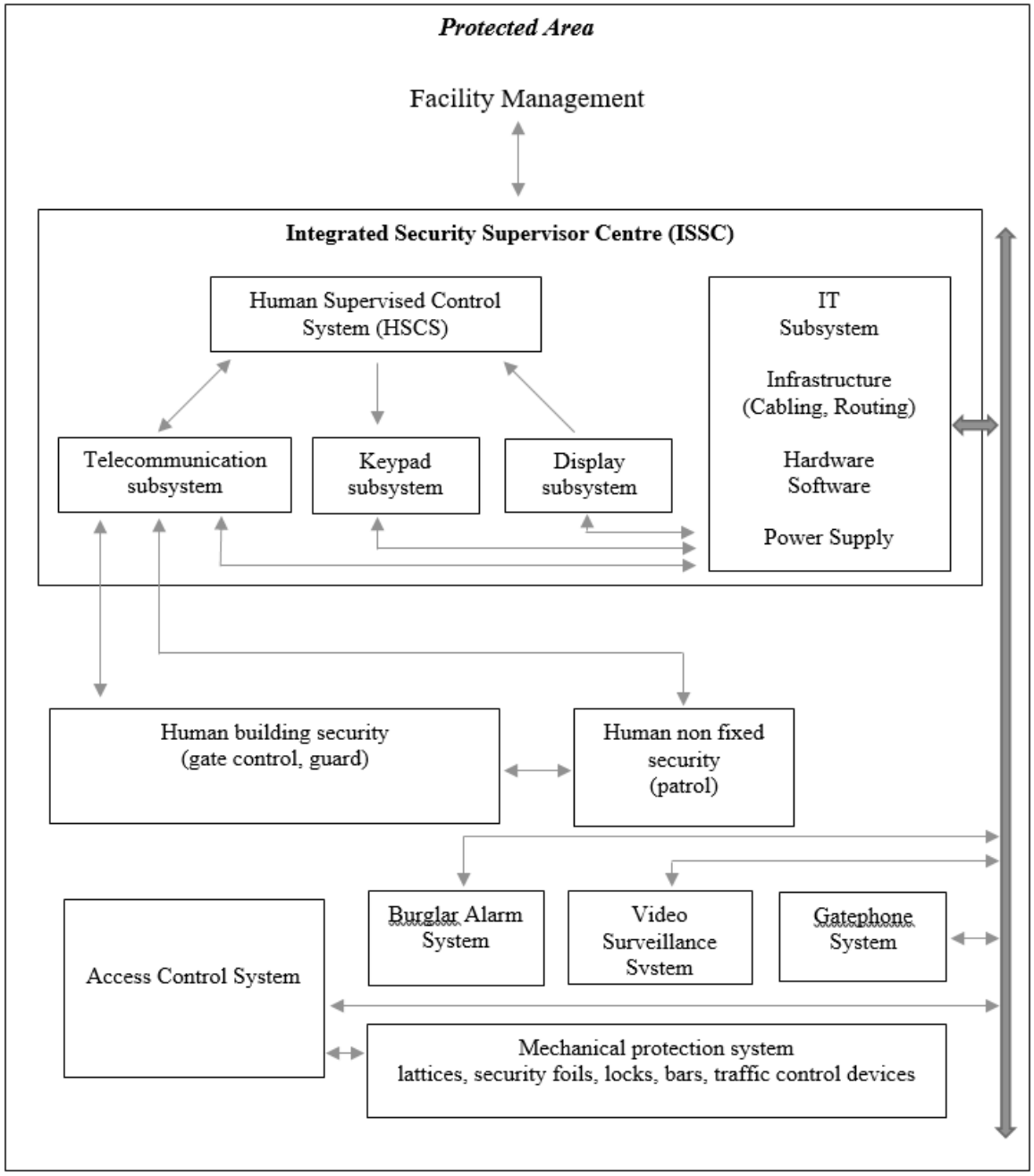

Figure 1. The model of the complex security system on a railway station.

Wthin a station, five independent security parts can be found: the mechanical protection, the access control system, the electrical protection system, the human security system and the integrated security supervisor centre (ISSC). In the system architecture an undetermined protection subsystem the Information Technology area can be found. It is not part of the protection but it has connected to all protection subsystems and it is also connected to the outer area, that means it is one of the most significante part of the complex protection system. The following security subsystems will determine the efficiency of the complex system.

The mechanical protection subsystem

To prevent the unauthorized entrance to a secured area it is needed to install special mechanical elements lattices, security foils to the windows and doors, bars and traffic control devices to the vehicle entrances, and locks for all places where higher risk is possible. These devices are the background of the complex protection.

The access control subsystem

The access control system is the bridge between the mechanical and the electrical protection system. It is neither mechanical, nor electrical part, but both. The main function is preventing the unauthorized entrance to the restricted area, but it also generates alarm signals to the ISSC. It is not only for controlling the traffic but it also stores all information with time-stamps in non-volatile memory at the controlled area and also send them into the supervisor system.

The electrical protection subsystem

The electrical protection subsystem contains the video surveillance, the burglar alarm, the gate-phone systems. These systems are working together and some inputs and outputs of the access control is integrated here through the ISSC, too. It means a burglar alarm signal can occur a video event, so the connected camera will display on the alarm monitor and also can generate an access control event where all connected electric locks are disabled, only the security guards are allowed to pass through these gates.

The *human* security guard and patrol subsystem

The *human* security of the complex system is the most important sector, because without any physical force there can't be an efficient security system. There are two independent part of it, the first part is for the building security, they stand on a pre-defined place (eg. on the passenger and the industrial entrances of the railway stations) of the area and check the traffic and operate the mechanical-, the electrical-, and the access control-systems. The other part of the human security is the patrol. They are well trained guards divided into small teams. They patrol the area, to prevent the hazards of unattended baggage, unauthorized entrance. Theirs official uniform and the physical demonstrative presence gives the opportunity of the secure feeling in the area what can reduce the hazards possibility. In an unexpected event the ISSC can send these teams immediately and directly to the risk to prevent or to solve problems. For the efficient managing of this system we need a hierarchical structure with well-defined information and command routes.

The integrated security supervisor centre's subsystem

The ISSC is for the efficient operation of the protection, what collects all information connected to the protection in the inner and outer area and converts them into the same protocol. With the converted and pre-analysed signals can coordinate with the subsystems.

It can be seen that the subsystems can work together without ISSC, but in this case because of the low level integration the efficiency of them is poor. To prevent any security hazard or bomb attack, it needs an efficient multilevel (low and high) integrated protection system with well-educated and well-trained operators, patrols and security guards. Without the suited trainings it can occur that the efficiency of the complex system is lower than the separated and low level integrated systems, in a disaster because of the latent of the secure feeling the response can be slow or wrong.

PROBABILITY TREE AND FAULT TREE ANALYSIS

To determine all functions with the risk factors in the smart complex security systems on the aforementioned railway stations are very difficult due to the human factor and the large

number of connections and internal processes. However, the recently created and improved probabilistic approach with fuzzy system expert analysis is a useful mathematical solution for the aforementioned cases. These methods can be used in the full scaled security system, if first – like the Fuzzy logic – an expert level analysis gives enough information about the crucial parts of the system. With them comes the possibility to give and get data from the determined system, and continuously recalculate the factors and – in some cases – it can be done On-Line, too. The best method for modelling the aforementioned multi-level integrated system is the fault tree diagram. It is used to conduct fault tree analysis (or FTA).

The FTA is a technique for reliability and safety analysis. The Bell Telephone Laboratories developed the concept in 1962 for the US Air Force for use with the Minuteman system. It was later adopted and extensively applied by the Boeing Company. The fault tree analysis is a symbolic *analytical logic technique* found in operations research and in system reliability. The FTA helps determine the cause of failure or test the reliability of a system by stepping through a series of events logically. The benefits of fault trees is that a fault tree creates a visual record of a system that shows the logical relationships between events and causes lead to that failure. The modularising of the FTA gives the opportunity to reduce the number of inputs and define them in blocks. The modularising has to be done before the analysis takes place [4]. It helps in computerising the FTA and helps also the facility management quickly understand the results of the analysis and pinpoint weaknesses in the design and identify errors. A fault tree diagram will help prioritize issues to fix what occur the failure. In many ways, the fault tree diagram creates the foundation for any further analysis and evaluation. For example, when changes or upgrades are made to the system, you already have a set of steps to evaluate for possible effects and changes. You can use a fault tree diagram to help you design quality tests and maintenance procedures. It is a good pointer that can show the state of the whole complex system.

TESTING THE COMPLEX SYSTEM'S FTA FOR EFFICIENCY METHOD

We made a complex system model of the railway station to test our efficiency computing method. We designed an event buffer on the test complex protection system, what have recorded all important events for a month, after it we have analysed all the events, with that data we could make three different groups that can be used for templates. We hope that these templates will give a fast method of the average efficiency measurement about the system. In the test month we recorded the following events in the event buffer: external buildings false alarms (infra beam detectors outside) occurred 10 times, external buildings false alarms (inside) 5 times, false fire alarms 5 times, stolen mobiles (office area) 3 times, while stolen official stamp and other devices and/or purse (no recorded data) occured 3 times. There was no recorded data for stolen purse, drug usage signs and for poisonous chemical stolen from a technical area.

The first event group contained data that is not directly connected to the complex system (events coming from outside only for redundant recording). The early recognition of these events will be important to reduce the mathematical analysing speed in the future, so they will not go through the FTA analyse method. They will not be dropped, because these items can be used for "no need for FTA analysing" template. These items were in our test system e.g. the false fire events, because these events also came into the *human* protection system but only for redundant recording.

The second event group contained data that is directly connected to the complex system and the occurrence was only one or maximum two times, so these data cannot be used for templates in the future but can significantly modify the efficiency of it (e.g. stolen chemicals, drug usage signs, etc.).

The third event group contained data that is directly connected to the complex system and the occurrence was more than two times, so these data can be used for templates in the future (e.g. external building false alarms inside and outside).

We generated blocks from the complex system elements to reduce the FTA diagrams size, without generating false information in the system, because the aforementioned – fuzzy logic style – expert level analysis gives enough information about the crucial parts of the system.

We could define the fault probability average rate for each subsystem's device of the test system, because of more than 10 years' operational experience in these mechanical and electrical protection systems and more than 4 years' operational experience in these *human* systems.

We made all FTA diagrams for the aforementioned second and third event groups. We made the fault analysis and counted all probability of them, we followed step by step and we got that the probability of fault is between 0,26 and 0,39 the efficiency of the system is between 0,61 and 0,74.

In our test system the following event occurred: From the technical area of the protected station a poisonous chemical was stolen. In that area there are access control system, but this room was not protected, there was a video-surveillance system, but in that room there weren't cameras, the nearest cameras were on the corridor and showed common view about the traffic. On the corridor an access control system can be found, and there was patrol, and at the building's entrance a security checkpoint, too.

The FTA diagram of the event can be seen in Figure 2. The core event can occur by only the Mechanical Protection System Fault – the doors lock fault, or the employee did not use it – but for the post analysing the other subsystems proper protection efficiency is needed. This is one side why we have used it for the FTA all the three other subsystems, and in the future with the FTA refining will give the possibility for the facility management to generate additional suggestions about the system's improvement. The defined access control subsystem fault probabilities were the following: Reader 0,03, Control Panel 0,01 and Electric Lock 0,05. The Access Control Fault probability can be calculated by the following formula:

$$P_T = 1 - \prod_{i=1}^{n}(1 - P_i) = 1 - [(1 - P_1)\,(1 - P_2)\,\ldots\,(1 - P_i)] \qquad (1)$$

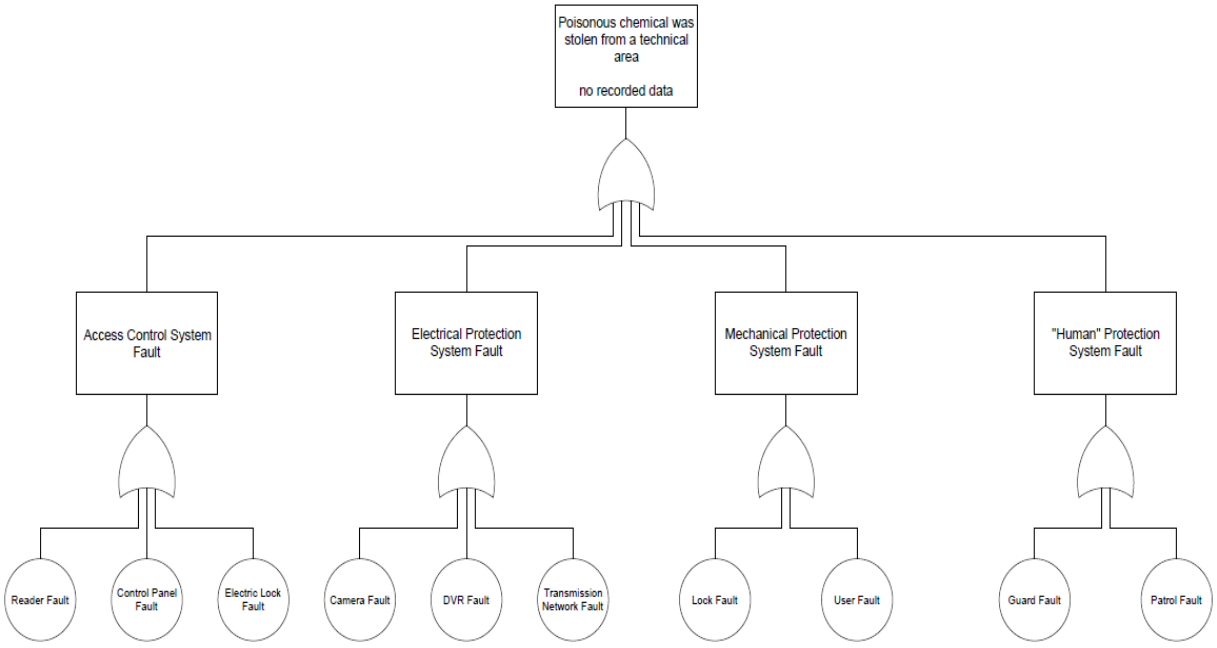

Figure 2. An example event FTA diagram.

The calculated probability of this subsystem was $P_T = 0{,}083$.

The defined electrical protection subsystem fault probabilities were the following: camera 0,1, DVR 0,05 and transmission network 0,05. The counted probability of this subsystem was $P_T = 0{,}18775$.

The defined mechanical protection subsystem fault probability were the following: lock 0,01, and user 0,1. The calculated probability of this subsystem was $P_T = 0{,}109$.

The defined *human* protection subsystem fault probability were as follows: guard 0,02 and patrol 0,01. The coalculated fault probability of this subsystem was $P_T = 0{,}0298$.

The accumulated fault probability indicator number was in this event $P_T = 0{,}356139$, so the efficiency indicator was $1 - P_T = 0{,}64386$.

The analysis showed that the stolen events fault probability rate was the same in the tested complex system, because of the connected subsystems and was not related to the fact that the owner left it unattended or not.

More than 50 events can be recorded in this period and most of them can be used as a template because of the frequently occurrence.

In our test system an unneeded patrol usage event occurred 10 times. More building area have been protected by a burglar alarm system after working hours. This building has in-, and outside area with different sensors. In Figure **Error! Reference source not found.** can be seen the unneeded patrol usage *frequent* event's FTA diagram. In this situation the core event can occur only by the Electrical Protection System Fault (an opened window/door, a false PIR signal, a control panel hazard, or a *noise* in the communication circuit), but there is another subsystem what can occur as an unneeded operation, the Ctral Supervision System Fault. The defined electrical protection system fault probabilities were the following:

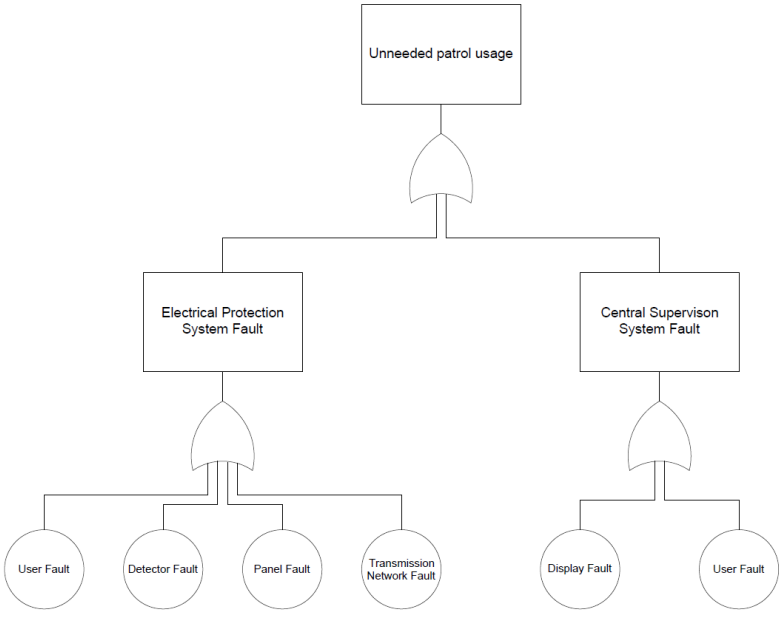

Figure 3. A frequent example event.

user 0,05, detector 0,15, control panel 0,03 and transmission 0,01. The Electric Protection System Fault probability can be calculated wth expression (1). The calculated probability of this subsystem was $P_T = 0{,}220561$.

The defined central supervision system fault probabilities were the following: display 0,05 and user 0,1 so the calculated probability of this subsystem was $P_T = 0{,}145$.

The accumulated fault probability indicator number was in this event P_T = 0,33358, while the efficiency indicator number was 1 – P_T = 0,66642.

In the test system the FTA showed that in this kind of fault group the probability rates are the same and independent of the fault's place, so they could be used as a template in future.

With the aforementioned FTA diagrams we could declare the weighted global indicator number of the complex system, what was P_T = 0,3483 and the global weighted average efficiency number was 1 – P_T = 0,6516.

SUMMARY AND CONCLUSION

The mentioned theoretical, logical and mathematical methods can give a useful information about the complex system's efficiency.

This article gives a useful guideline for the facility management of the smart cities' railway stations. It declares the main connections with their hazards to find the key elements and the inbound and outbound parameters of the smart complex security system. The pre-generated knowledge base and FTA templates gives the opportunity to get a main view of the global system's efficiency. If a special self-learning software algorithm will be used at the analysis and with a special maintenance and repairing contract, what contains also a system improvement agreement, it gives the possibility that the efficiency of the full scaled complex system will be continuously in the optimal state.

The facility management always gets on-line information about the state of the system with the needs of the improvement and also the cost, that means the management gets all important information for the proper budget planning for years and gets the ability to reduce the security risk of the smart cities' stations.

ACKNOWLEDGEMENT

The research on which the publication is based has been carried out within the framework of the project entitled "The Development of Integrated Intelligent Railway Information and Safety System" (application number: GINOP-2.2.1-15-2017-00098).

REFERENCES

[1] Ramaprasad, A.; Sánchez-Ortiz, A. and Syn, T.: *A Unified Definition of a Smart City*. Springer International Publishing AG, Cham, 2017,

[2] Bosch Security Systems: *Train station Solutions for Ensuring Security and Safety from Bosch Security Systems*. Bosch Security Systems, 2012,

[3] Ruffolo, F. and Cinquino, A.: *Smart security systems for the rail industry*. Alstom Industry, Montreal, 2006,

[4] Sinnamon, R.M. and Andrews, J.D.: *Fault Tree Analysis and Binary Decision Diagrams*. Proceedings of 1996 Annual Reliability and Maintainability Symposium. IEEE, Las Vegas, 1996, http://dx.doi.org/10.1109/RAMS.1996.500665,

[5] Systems and Reliability Research Office of Nuclear Regulatory Research: *Fault Tree Handbook.* U.S. Nuclear Regulatory Commission, Washington, 1981.