Enhancing Security of Critical Infrastructure in Sector Transport

Maria LUSKOVA*, Katarina BUGANOVA and Bohus LEITNER
University of Žilina, Ul. 1. mája 32, 01026 Žilina, Slovak Republic
*Corresponding author

Keywords: Risk, Threat, Security, Critical infrastructure, Transportation sector, FMEA.

Abstract. The issues of critical infrastructure protection are becoming one of increasing concern to national governments, infrastructure managers and local authorities. The paper is dealing with the effects of crisis situations in critical transport infrastructure. It highlights the importance of prevention and early identification of risk factors that could have an adverse effect on a system or process. It presents the Failure Mode and Effect Analysis as one of the most effective methods of risk analysis which is useful for the needs of increasing security of critical transport infrastructure.

Introduction

Critical infrastructure in the Slovak Republic (SR) is defined as that part of the national infrastructure (selected organizations and institutions, facilities, systems, equipment, services) whose destruction or disablement due to exposure to risk factors will result in danger or disruption of political and economic functioning of the state or threat to life and health of the inhabitants. The collapse of critical infrastructure can threaten food production, heating, industrial production and in principle to disrupt and subvert the whole society life. The attack upon any country may result in failure of infrastructures on a regional scale, or in a wider geographic area that is interconnected by different networks. In case the ensuring the basic functions of the state is failed it will be necessary to consider again their importance and know the reason of incurred situation and why the responsible institutions have not prevented this disaster.

Transportation—Significant Critical Infrastructure Sector

In the Slovak Republic transport infrastructure is included among eight identified significant critical infrastructure sectors that are strategically important for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in the state as a result of the failure to maintain those functions.

The transport sector in the Slovakia comprises road, railway, aviation and water transport. It is a vast, open interdependent networked system that moves millions of people and millions of tons of goods. Transport sector underlies economic growth, significantly contributes to functioning the Slovak economy and its regions and so create conditions for optimal use of economy and social potential. Transport, enabling free movement of persons, goods, capital and free delivering services underlies functioning simple internal EU market. Transport sector create about 4.2 % of working positions and 8.2 % of GDP. Ensuring its security is mission charged to government, private industry stakeholders and all sector partners [1, 2, 3, 4].

Critical infrastructure elements in transport sector represent mainly an engineering buildings, public services and information systems whose disruption or destruction should, according to the sectoral criteria and cross-cutting criteria, have adverse effect on the performance of economic and social functions of the state, and thus on the quality of life of residents in terms of the protection of their life, health, safety, property, as well as the environment [5, 6, 7].
Crisis Situations in Transport Infrastructure

The effects of crisis situations on the functionality and operational capability of critical infrastructure element depends on its type, characteristics, robustness, scope and on the other hand on the resilience of a particular element. In works [5, 8] states that specific types of crisis situations may affect the elements of critical infrastructure in two ways:

- Directly—they cause real crisis events and to solve them it is necessary to announce state of crisis,
- Indirectly—they can disturb management processes and are associated with addressing the consequences of crisis situations (e.g. in political sphere, economy, social sphere, etc.).

Crisis situations can through their effects overcome the resilience of critical infrastructure element. Resilience is a concept related to a system's ability to perform the critical functions required for its mission efficiently, even in the event of disruptive actions, e.g. natural, accidental or malevolent events. Resilient systems can maintain their performance through [9]:

- Prevention or absorption of a disruption impact.
- Reconfiguration and adaptation from normal operating procedures to a different set of operations.
- Restoration or recovery the system quickly and efficiently.

Crisis situation effects can thus disturb the basic functions of the transport system (e.g. ensuring the mobility of people and transfer of goods) by breaking the resilience of the element. The measure of disturbance of functionality and serviceability of the critical infrastructure element depends on the extent to which resilience is broken (disturbed).

Prevention of crisis situation occurrence is a great importance. For this reason continuous monitoring of the internal and external environment and early identification of risk factors that could have an adverse effect on a system or process in question are necessary. Timely and correct assessment of risk factors changes in the internal and external environment as well as the probability of their occurrence is a prerequisite for adoption of adequate measures to increase the level of resilience. The process of monitoring and evaluating changes of risk factors can be carried out together with a possible response to the expected but also random crisis events. Responsiveness is thus dependent on the level of preparedness of forces and means to deal with crisis events [10].

If we have applied the process view and assessed the risks of critical infrastructure in transport in relation to a certain process, 3 situations can be considered:

1. The risk arises just in the process.
2. The process affects risk factors, but the risk arises in other process or outside of the system under consideration.
3. The process has to respond to risk occurrence. Such processes which aim to respond to emerging risk, whether in terms of reducing the damage or preventing escalation of consequences, are called corrective actions.

Enhancing the security of critical infrastructure elements can be ensured with use of appropriate tools, methods and techniques. When analyzing the environment all possible risk situations that may occur in the system (process) as well as their consequences must be processed. It is important to capture the temporal, spatial and synergic linkages and share information even from possible negative events in the past. One of the most effective methods of risk analysis which is useful for the needs of increasing security of critical infrastructures is Failure Mode and Effect Analysis (FMEA). FMEA examines all possible causes of the failure of individual system elements or process.

Use of the FMEA Method for Risk Assessment of Potential Critical Infrastructure Elements in the Transportation Sector

The FMEA method belongs to the group of basic analytical methods used in the management, security, reliability and the quality control process. It is one of the basic methods used in the
semi-quantitative risk analysis and is applied not only for production processes and products but also for services, financial, social and other processes. Its origin dates back to the 40s of the 20th century, when it was formulated in the context of the USA military standards (MIL-P-1629). In the ‘60s, NASA formally developed this method and applied it in the context of the Apollo program in order to improve and verify the hardware of cosmic programme. The FMEA application includes two main phases [11]:

1. Identification phase, when experts focus on identification:
   - All potential failures that can occur in both normal and extreme operating conditions, regardless of their severity or likelihood of occurrence.
   - All possible consequences of failures.
   - All possible causes of the failure occurrence whereby one failure can have several consequences and similarly one consequence may have several causes.
   
   This phase may take place in the form of brainstorming or correspondence.

2. Numerical phase which focuses on calculating the risk level in the form of Risk Priority Number (RPN), which may arise in case of any possible cause of the failure. Typically, the risk level is calculated according to the formula [12]:

\[
RPN = \text{Severity} \times \text{Occurrence} \times \text{Detection}
\]

where: Severity is severity of each effect of failure, Occurrence is likelihood of potential failure occurrence and Detection is a likelihood of failure detection.

The rates of the severity, occurrence and detection are determined by experts on the basis of the scales which are optionally formed and may be suitably modified for each specific situation. However it is important to use a uniform scale for the assessment of the whole assessed system (subject, process). The scale is usually from 1 to 10, wherein the best evaluation value is corresponding to the 1.

Calculated values of RPN allow comparison of individual failures in terms of their causes and consequences in accordance with uniform gauge. Depending on the RPN value priorities for corrective and preventive measures specifically aimed at preventing the occurrence of potential failures can be set. After performing corrective and preventive actions experts again assess the value of the severity, occurrence and detection and the new value of RPN is calculated. In this way, several rounds may run until an optimal value of RPN is achieved.

In connection with the value of the RPN it is important to pay special attention to the severity of the effect of failure. Such situation can occur that the value of RPN will be low because the occurrence and detection are equal to one and only severity is high. This applies especially to very serious nearly crisis phenomena which are usually very unlikely. In connection with the wide range of FMEA applications in different types of systems and fields, there are many variants of the FMEA method.

The basic types of FMEA are considered [11]:

- Design FMEA applied within analysing structure (design) of a product.
- Process FMEA which is based on the individual steps of the process of production and assembly.
- Product FMEA applied for analysing design and manufacturing process of a product or a system completely from the viewpoint of the customer.

Classical FMEA method does not address the fact that the assessment of a number of experts can vary widely, but it is assumed that the RPN input values are determined based on their consensus.

This shortage eliminates the SAFMEA method, based on the statistical evaluation of the expert group answers file. The SAFMEA method supposes the participation of at least three experts ($n_e > 3$). For each line of the form $n_e$ number of expert values of RPN is found and the mean value and standard deviation of dispersion of RPN are calculated. If the number of experts is more than five, quantile of RPN distribution is calculated, too. In this way it is possible to determine the maximum deviations in the experts’ evaluations and analyse them again.
FMEA variant which analyses the human aspects of systems failure is a method known as HF-PFMEA. The method, used in NASA, analyses the tasks within the process for the purpose to identify human errors that can lead to system failure or the worst effects on the system. HF-PFMEA is based on the philosophy that human error can be controlled by managing the factors affecting the performance of a man, creating obstacles to prevent human error, adding controls to detect and correct human errors before they lead to undesirable impacts. In protection of critical infrastructure in transport primarily the system FMEU is appropriate for application. With the system FMEA application in addition to the existing design or process FMEA the following steps are carried out:

- Structuring of reviewed system on the elements and depiction of mutual functional connection of these elements.
- Identification of possible failures of a system resulting from the system functions.
- Consequential logical chains of related malfunctions of various system elements for determining analysed possible failures consequences, failures and failure causes.

The aim of the system FMEA is to prevent possible system failures already at its projection. It uses a comparison of systems and serves for objectively justified deciding on the design or selection of a system.

Conclusion

The main goal in securing the required level of critical infrastructure security in the transport sector is to reduce the risk of injury and loss of human lives, damage of critical infrastructure elements (system, processes) or environmental disturbance. Therefore it is necessary to use tools for preventing dangerous failures and their control [13, 14]. It is possible to use a number of methods for risk assessment and management and one of them is the FMEA method.

Within the system FMEA method application in the critical transport infrastructure as well as the process FMEA, it is necessary to pay special attention to the safety and reliability of the planned system and compliance with legal requirements. Great emphasis in the application of the FMEA on processes or systems, where the human lives are endangered, should be placed on the severity of failure, i.e. considering the severity of danger. In this case, the severity of failure has to be evaluated separately, because if the experts determined a low probability of occurrence or high probability of detection of failure then the value of RPN is low. This could result in improper risk level of critical transport infrastructure determination and consequently inadequacies in the processing of preventive and corrective measures.

Summary

In Slovakia transport sector belongs to the critical infrastructure sectors whose assets, systems, and networks are considered so vital to the country that their incapacitation or destruction would have a debilitating effect on security, economy, national public health, or any combination thereof. The main goal in securing the required level of critical infrastructure security in the transport sector is to reduce the risk of injury and loss of human lives, damage of critical infrastructure elements (system, processes) or environmental disturbance. In protection of critical infrastructure in transport primarily the system FMEA, focused on prevention of possible system failures already at its projection, is appropriate for application.

Acknowledgement

This work has been supported by VEGA grant No. 1/0240/15 named „Process model of critical infrastructure safety and protection in the transport sector“.
References


