Identification and assessment of security risks of airport operation in context of a multi-layered security system

KOLESÁR Ján[1], BEGERA Vladimír[2], LIPTÁKOVÁ Dorota[3]

[1,2,3]Department of Air Transport Management, Faculty of Aeronautics, Technical University of Košice, Rampová 7, 041 21 Košice, Slovakia,
email: jan.kolesar@tuke.sk, vladimir.begera@tuke.sk, dorota.liptakova@tuke.sk

Abstract:
This article deals with the identification and evaluation of safety hazards with the highlight of the complexity of multi-layered airport security systems. The concept of multi-layered security system is explained in more detail with examples of current research conducted in this field. The paper also describes common methods for risk assessment and points out demerits of this approach in a multi-layered security system. On the other hand possibilities are outlined, how a thorough risk assessment analysis supplemented by cost and benefit analysis can lead to optimization of costs for security measures in the system as such.

Keywords:
acceptable risk, act of unlawful interference, risk identification, security analysis, security system

INTRODUCTION

Since early days of commercial aviation airplanes have been used for a different variety of unlawful activities such as smuggling of goods, weapons, people. Later it became a focus of terrorist groups. Any breach of the luxurious and high standard aviation travel immediately draw a lot of attention, which was the prime goal of these groups (Szabo S. el al., 2015). While at the beginning airplanes were their main target, when faced with increased security, terrorists did

not abandon commercial aviation as a venue for their violence. They started to attack airports instead. Attacks on airports give terrorists the symbolic value they seek and guarantee the attention of the international news media. They also create alarm locally.

Over the years every attempt to attack a plane or an airport were closely scrutinized and important lessons were learned. This article focuses on the current trend of building a multi-layered security system at airports. The concept of such system will be described more closely, as well as the identification and assessment of security risks at airports.

The current strategy to increase security and to ensure prevention and reliable protection of civil aviation against acts of unlawful interference is based on security analysis in the context of the management and monitoring of aviation security risks. Ensuring sufficient defence of aviation against unlawful conducts is currently addressed by building a multi-layered security system.

The goal of this paper is to present this approach to ensuring secure airport operations to be further implemented on airports globally or at other facilities threatened by various risk factors. The need for research in this field can be seen in various papers covering thematically close topics. The approach to use an integrated airport safety audit was described by Kozlowski, 2017. The development of a more risk-sensitive and flexible airport safety area strategy is the main focus of Wong et al., 2008. Pacheco, Fernandes and Domingos, 2014 studied the problematics of airport airside safety index.

1. MULTI-LAYERED AIRPORT SECURITY SYSTEM

The multi-layer security system is a set of security and control measures, technical means and activities of security forces that aim to ensure a high level of protection under the integrated security system and to possibly eliminate the potential threats and hazards in the field of unlawful activities in civil aviation.

1.1 Current security situation

Despite widespread security measures recently adopted in aviation, there is still a current threat from terrorist groups, criminals and other potentially "intrusive" passengers trying to overcome the airport security system for various reasons. And even in the near future these threats can not be completely eliminated.

A security strategy for preventing and eliminating acts of unlawful interference in aviation aims to reduce security risk to the minimum. To achieve this a number of security measures are currently being implemented at airports, new passenger and air cargo detection devices are introduced, identification systems are modernised and security control procedures are standardized. The principle of mutual cooperation in the fight against air crime and terrorism is used to ensure a high standard of aviation security. However, the role of aviation security management is also to take measures to mitigate the severity of the consequences in cases of overcoming the security system. The protection of civil aviation against acts of unlawful interference is therefore achieved through multi-layer protection, which aims to increase overall safety and improve the airport control process.

1.2 Corner stones of multi-layered security system

The efficiency and reliability of multi-layered control in the air transport process (Fig.1) is supported by the flow of information and security procedures that have to ensure that only a person or object that does not pose a threat to air transport can get on board.

One of the conditions of effectiveness and reliability of a multi-layered security system is the timely and accurate transmission of relevant information from one control point to another.

Through effective management, adherence to established procedures, monitoring of sources of risk and good equipment of airports by modern detection devices, security threats and their consequences can be mitigated to an acceptable level. The question is what can be considered an acceptable level.

Addressing this issue is the subject of extensive discussions among aviation security policy creators, national security, human resources development, financial resources, socio-psychological analyses, and other areas that directly or indirectly affect the process of securing a sufficient level of security and civil aviation protection.

Despite the varying constraints, financial difficulty, political decisions, interference with the personal freedoms of individuals and other factors that enter the problematics of protection of civil aviation from acts of unlawful interference, it is necessary to keep in mind the basic objective. And that objective is to ensure reliable and effective protection and safety of air traffic, with regard to the priorities and the prevention of acts of unlawful interference in the air.

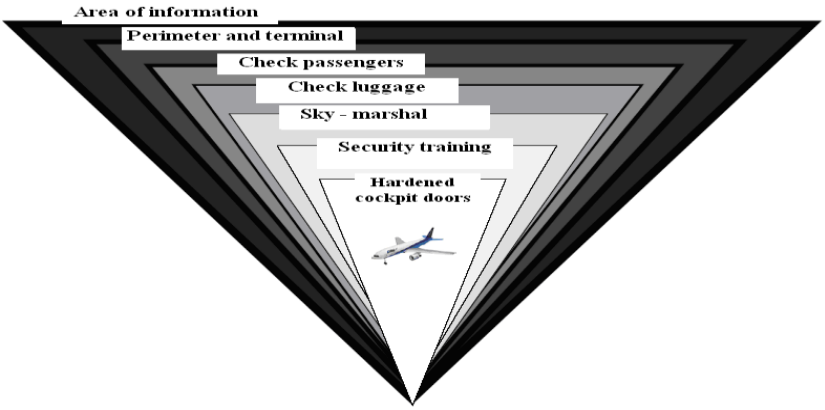

Fig.1 Multi-layered security system of air transport

2. SECURITY RISK PARAMETERS

Security risk is generally considered to be a function of the nature of the hazard, the degree of vulnerability of the security system, and the consequences associated with overcoming the security system.

$$\text{Risk} = f(\text{hazard, vulnerability, consequence}) \qquad (1)$$

It means that risk is a function of three risk parameters – hazard, vulnerability and the consequences. The hazard to the system, like the vulnerability of the system, can be defined by the likelihood of occurrence of risks and possible hazards. As a result of a thorough analytical process, we are able to identify the severity and consequences of risks and even the possible scope of consequences.

By using an economic analysis, we can evaluate the amount of investment needed and operating costs of a functional and efficient airport security system, as well as the costs of eliminating possible consequences. By mathematical expression we are able to generate potential operating losses, including losses on material values and human lives, in the event of a potential act of unlawful interference.

When assessing the relationship (1) with the estimated costs of building a sufficient security system and possible scenarios of its overcoming, three basic risk factors can be expressed as equation (2).

$$\text{Risk} = \text{threat} \times \text{vulnerability} \times \text{consequence} \quad (2)$$

The nature and degree of risk is directly proportional to the hazard, system vulnerabilities, and the consequences emerging by overcoming of the security system.

A number of well-known methods and process approaches can be used to develop a security analysis and risk identification in the structured airport security system to determine the nature of the risks and their possible consequences on air transport. By using these methods, we can determine the level of acceptable risk that we are able and willing to accept while ensuring sufficient and reliable protection.

A key problem in the security risk analysis of acts of unlawful interference is to determine the level of acceptable risk. It is very difficult to anticipate the consequences and the further development of an unlawful act in civil aviation. This is possible only on the basis of statistical data and analysis of such acts already committed, a thorough knowledge of the real geo-political situation and an analytical assessment of the likelihood of the possible occurrence of such interference. Identification of acceptable boundary when evaluating the risk is only possible in real time, under specific conditions, and depending on the possibilities of overcoming airport security and control barriers as potential intruders.

It is appropriate to apply optimization to the comprehensive analytical process of risk identification and subsequent risk assessment. Using mathematical simulation models, we can design and select the most effective way to address the civil aviation safety and security system problems and to protect the system against acts of unlawful interference.

In order to perform risk analysis in the context of security management, many existing methods of risk identification and potential threat are used in practice. We know the methods of both mathematical and graphic modelling of risks. The primary criterion for selecting the method should be the possibility of assessing and determining the most likely cause of the existence of a risk in the safety system. This concerns in particular the assessment of the weakest security feature in the organization of airport security, but also in the process of assessing the functionality of individual elements in the Man-Machine interference system. According to Popreda and Pappová, 2012, at the airport the Man-Machine interference can be represented for example by the airport security officer and the control and detection device.

As part of the risk analysis, a list of possible causes of the risks and their consequences has to be created. We process the catalogue in the form of defining

threats to structural elements in the designation of objects such as airport, airplane, airline, aircraft crew, etc.; or process threats to a range of processes from passenger handling process, air cargo transport, to airport perimeter protection, etc.

As stated by Balaščík et al., 2017, an important part of the analysis is the identification of hazards and the causes of their occurrence as sources of risk, taking into account both the external and internal conditions of the airport security system. Only this way we can determine the number of potential hazards, estimate the likelihood of their occurrence and define the possible consequences.

Based on these identifiers, we use an appropriate method to calculate the acceptable risk coefficient as the basic identifier by which we are able to assess the functionality and nature of the security system, its operating elements (detection, alarm, reliability, system vulnerability, response, etc.), and technical elements (prohibited items on board, bomb attack, aircraft abduction, fire, theft, unauthorized entry, etc.).

3. IDENTIFICATION AND ASSESSMENT OF SECURITY RISKS

One of the ways that security analysts often use to conduct a security risk analysis and risk assessment is a rating assessment system. Its outputs are relatively reliable parameters, with which we can evaluate the degree of thread, vulnerability of the system and possible consequences. The individual evaluation elements are ranked in a scale in the form of a matrix and represent separate categories ranging from the "minimum risk" to an "unacceptable risk" category.

The generally applicable method of safety analysis and risk assessment in the field of civil aviation protection against acts of unlawful interference is the method of point assessment of risk parameters through the so called "Threat assessment cards". Cards need to be developed for each type of threat, including the possible consequences of this threat.

The values of the assessed risks are compared using a constant – the coefficient of acceptable risk within the defined scale. E.g. if we establish a four-point risk assessment scale, we will consider the likelihood of its occurrence twice as high as the risk itself, because according to (2) the vulnerability analysis will enter into the process. If risk analysis is included in the risk calculation, the risk is multiplied and the resulting risk coefficient rises. In practice, however, this method of risk assessment is of an ordinal nature, because the method of risk assessment is to a large extent subjective.

We can extend this approach to aviation protection against acts of unlawful interference into several dimensions. However, the basic element remains a security risk, the resulting value of which can be calculated using multiple variables. If we use three variables of the basic risk matrix, we can graphically express it in a three-dimensional space as shown in Fig.2.

In this risk matrix the individual vulnerability categories and the vulnerability of the security system in the field of civil aviation security are assessed at a scale from known (or frequent) to only potential risks (highly unlikely) (Petruf, et al., 2015).

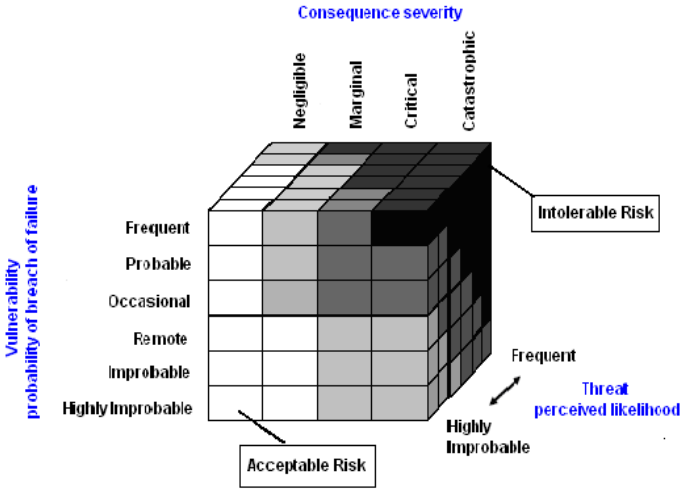

Fig.2 Scheme of multi-level protection of a civil airport against acts of unlawful interference

The scale interval in the risk matrix evaluation can be extended and described with an appropriate mathematical algorithm. As for the vulnerability of the system, we can evaluate the probable occurrence of a breach, thus the failure of the security system, on a scale with six categories from very probable (frequent) to highly unlikely. The categories will include ratings highly improbable (1), improbable (2), remote (3), occasional (4), probable (5) and frequent (6). A six-step assessment in the risk evaluation process can also be used to categorize the perceived security hazard in assessing the likelihood of occurrence of the thread. We assess the severity of the consequences of threats by assigning one of four

levels from negligible to catastrophic in order of severity: negligible (1), marginal (2), critical (3), and catastrophic (4).

This evaluation method illustrates a process that provides for a specific combination of threat assessment, vulnerability, severity, and consequences of security risk in view of specific risk assessment needs and priorities.

Using a risk matrix, we can quantify threat and vulnerability as a parameter formulated for probability and risk occurrence ranging from zero to one, or ranging from 0% to 100%, or another rating scale.

4. RISK ASSESSMENT IN A MULTI-LAYERED SECURITY SYSTEM

When conducting a risk assessment analysis in the context with a multi-layered security system, the main focus has to be turned to the creation of catalogue of possible hazards. As mentioned above, there can be many factors that need to be taken into account. We need to consider both the internal as well as the external factors affecting the security system. Than we have to identify different hazards that can occur in each of the levels of the security system, starting at the international level up to a simple process at the airport. A hazard on an international level could be a failure to identify and intercept a terrorist. A hazard in the airport security check is failure to confiscate some dangerous item or weapon, such as knife or gun. It is important to remember, that many hazards when not retained at one level could propagate into the next level. The failure to identify a terrorist could result in an attempt to enter the cockpit with a weapon and kidnap the whole airplane.On each level of the multi-layered security system a propagated hazard could receive another risk assessment score. Tobisová and Seňová, 2014 supplement a thorough risk assessment analysis with an optimization and cost and benefit analysis. This can eventually lead to recognition of weak links, which could be strengthened with relatively low costs in order to minimize a possible thread later in the chain, when lowering the probability of the latter thread would be connected with higher direct costs.

CONCLUSION

Analysis of security risks in aviation is, in particular, recently the area under consideration, which significantly influences the process of engaging different security measures and practices in civil aviation. The risk assessment analysis

results are also based on financial analysis of investment and operating costs needed, assessing the safety level of airports, assessing the level of services provided to the public, development of regions, tourism and other areas of society.

The results of risk assessment are prone to subjective views. Thus it is important to highlight the need for expert evaluation, usage of available statistical data, and international cooperation and benchmarking or transfer of good practices among the aviation community as well as between different industries with demanding security levels.

REFERENCES

[1] BALAŠČIK, V. [et al.]: *Vývoj bezpečnosti leteckej dopravy v Slovenskej republike*. 2017. In: Bezpečnosť - Kvalita - Spoľahlivosť. Košice: TU. s. 14-19. ISBN 978-80-553-3115-7.

[2] KOZLOWSKI, M.: *Integated Airport Safety Audit*. 2017. In: LogForum: Scientific Journal of Logistics. 13 (1), p. 39-49. ISSN 1895-2038.

[3] PACHECO, R. R. - FERNANDES E. - DOMINGOS, E. M.: *Airport airside safety index*. 2014. In: Journal of Air Transport Management. Vol. 34 (2014), p. 86-92. ISSN: 0969-6997.

[4] PETRUF, M. [et al.]: *Risk elimination in air transport.* 2015. In: Acta Avionica. Roč. 17, č. 1 (2015), s. 62-67. ISSN 1335-9479.

[5] POPRENDA, J. - PAPPOVÁ, E.: *Human factor in aviation and consequences of its errors*. 2012. In: New Trends in Aviation Development: proceedings of the 10. International Conference : September 13-14, 2012, Hotel Teledom, Košice. Košice : LF TU, 2012 S. 1-6. ISBN 978-80-553-1083-1.

[6] SZABO, S. [et al.]: *Management bezpečnosti letiště* - 1. vyd. 2012 Brno : Akademické nakladatelství CERM. 172 p. ISBN 978-80-7204-933-2.

[7] TOBISOVÁ, A. - SEŇOVÁ, A.: *The economic-financial analysis of security risks of an airport.* 2014. In: Bezpečnosť a doprava : Teorie a praxe v bezpečnosti a krizovém řízení v dopravě : 10. konference s medzinárodní účastí : 14. února 2014, Letiště Hradec Králové. Pardubice : Institut Jana Pernera, o.p.s., 2014 P. 131-136. ISBN 978-80-86530-92-5.

[8] WONG, D.K.Y. [et al.]: *The development of a more risk-sensitive and flexible airport safety area strategy: Part II. Accident location analysis and airport risk assessment case studies*. 2009. In: Safety Science, Vol. 47 (2009), p. 913-924. ISSN 0925-7535.

[9] ELIAS,B.: *Airport and Aviation Security, U.S. policy and strategy in the age of global terrorism*, Auerbach Publications, © 2010 by Taylor and Francis Group, Boca Raton, Florida, USA, ISBN 978-1- 4200-7029-3

[10] PAČAIOVÁ, H., a kol.: *Bezpečnosť a riziká technických systémov*. SjF TU v Košiciach, Vienala, s.r.o. ISBN 978-80-553-0180-8.

[11] FLANAGAN, R. - NORMAN, G.: *Risk management and construction*, Blackwell Science Oxford, 1993

[12] GAO/AIMD-95-27 *FAA's Safety Performance Analysis System*, United States General Accounting Office,

[13] KOLESÁR, J.: *Ochrana civilného letectva pred činmi protiprávneho zasahovania*, Vysokoškolská učebnica, LF TU, Košice 2010, ISBN 978-80-553-0357-4.

[14] ŠČUREK, R.: *Studie analýzy rizika protiprávních činú na letišti*, Technická univerzita Ostrava, 2009.

[15] NEČAS,P. – SZABO, S. – BUČKA, P.: *Crisis management and security in simulation environment* , 2006. In: Science & Military. Roč. 1, č. 1 (2006), s. 33-37. - ISSN 1336-8885

[16] ROZENBERG, R. – SZABO, S.*: Základná letecká terminológia.* Košice : LF TU - 2009. - 116 s. - ISBN 978-80-553-0304-8.