ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING
Tome X (Year 2012) – FASCICULE 3 (ISSN 1584 – 2673)

[1.] Ján KOLESÁR, [2.] Martin PETRUF

RISK MANAGEMENT IN THE SPHERE OF CIVIL AIRPORT PROTECTION AGAINTS OF UNLAWFULL INTERFERENCE

[1-2.] TECHNICAL UNIVERSITY, FACULTY OF AERONAUTICS, DEPARTMENT OF AVIATION ENGINEERING, RAMPOVÁ 7, 041 21 KOŠICE, SLOVAKIA

ABSTRACT: *The current civilian airport protection against acts of unlawful interference is secured through mechanical and technical protection devices, complex regime measures and physical protection systems, which operate in integration in the circuit, spatial and object protection. Ensuring the required airport protection against illegal acts is currently solved by building a multilevel security system, the role of which is to eliminate potential security threats as far as possible. This paper deals with the methodology useable in the risk assessment of civil airport protection against acts of unlawful interference. Attention is focused on analyzing the current state of the airport perimeter and an analysis of risk assessment procedures in the safety management of civil airports.*

KEYWORDS: *safety management system, risk management, safety, acceptable risk, level of risk, security analysis, act of unlawful interference in aviation*

INTRODUCTION

The current civilian airport protection against acts of unlawful interference is secured through mechanical and technical protection devices, complex regime measures and physical protection systems, which operate in integration in the circuit, spatial and object protection. Ensuring the required airport protection against illegal acts is currently solved by building a multilevel security system, the role of which is to eliminate potential security threats as far as possible.

Extensive security measures in aviation have been mainly taken after September 11, 2001. Even now, there are real security threats from terrorist groups, criminal elements, and other potentially "disruptive elements" that represent a certain threat level of aviation safety.

The present strategy for increasing prevention and ensuring reliable protection of civil aviation against acts of unlawful interference is based not only on the installation of modern security equipment and harmonization of inspection procedures but also on risk management through a safety analysis in risk management and assessment in logistics and service processes in aviation transport.

SAFETY MANAGEMENT SYSTEM

The International aviation organization ICAO (International Civil Aviation Organization) and EASA (European Aviation Safety Agency) recommended that all national aviation authorities adopt a uniform approach for regulation and management of aviation safety. For that purpose, the legislative conditions have been normally defined and safety programs have been processed putting the rules of risk management, evaluation and control of security into practice for airports and airline operators, called Safety Management System (SMS). SMS in air traffic is a systematic, explicit and comprehensive tool to ensure, as required, a high level of aviation safety using the methodology of assessment and evaluation of security risks. As with all management systems of safety risks, SMS defines the objectives, procedures and ways of measuring the performance of the security system. For the implementation of SMS, three fundamental management imperatives of security in civil aviation have been adopted; they are ethical, legal and financial.

It is the responsibility of airport and aircraft operators to ensure implicitly that the individual operating segments and working activities comply with all rules of workplace safety, legislative requirements are clearly defined and that a system of risk management and security is reliable and efficient. In order to ensure the efficiency of SMS in the process of air traffic, particular attention should be paid to the sphere of risk management, risk identification, evaluation and control activities. The base of the SMS functionality when implementing it in aerodrome practice is also the effective communication which should be at all levels of aviation infrastructure with the aim of a continuous improvement process to ensure airport security. The spheres of interest and fulfillment of the SMS objectives at civil airports also include the area of civil aviation protection against acts of unlawful interference.

Safety measures for the prevention and elimination of unlawful acts in aviation have the aim to reduce the security risk as far as possible. For this purpose, in current airports, lots of control processes have been implemented, new detection equipment is introduced to screen passengers and cargo, the identification systems are modernized and control procedures are standardized.

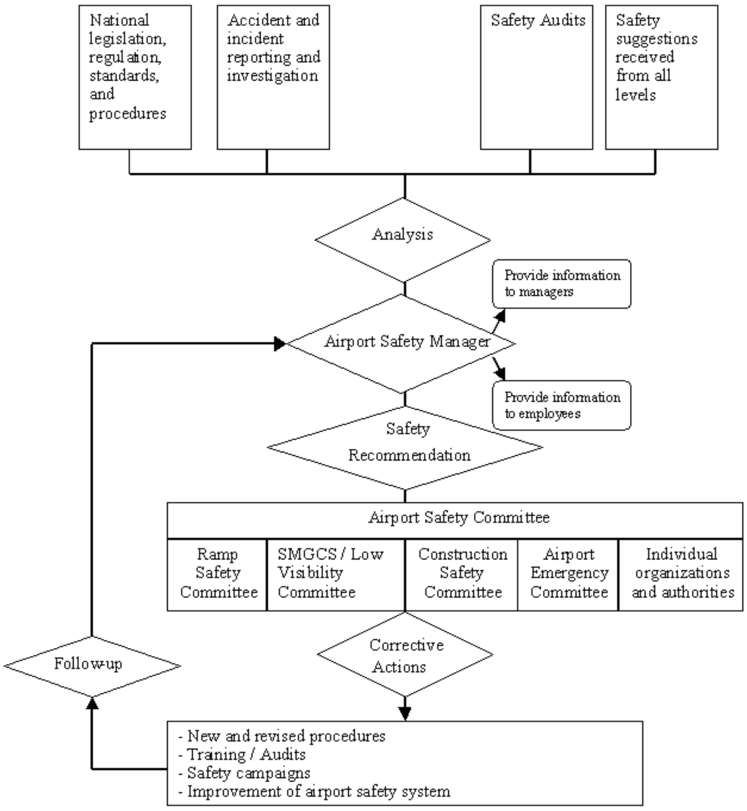
National legislation, regulation, standards, and procedures
Accident and incident reporting and investigation
Safety Audits
Safety suggestions received from all levels
Analysis
Provide information to managers
Airport Safety Manager
Provide information to employees
Safety Recommendation
Airport Safety Committee
Ramp Safety Committee
SMGCS / Low Visibility Committee
Construction Safety Committee
Airport Emergency Committee
Individual organizations and authorities
Follow-up
Corrective Actions
- New and revised procedures
- Training / Audits
- Safety campaigns
- Improvement of airport safety system

Fig. 1. Structural model of airport safety management system

The emphasis is put on mutual international cooperation in fighting against crime in aviation, against terrorism, standardization and harmonization of control processes. Ensuring the high safety in air transport is the service to the public and responsibility at the same time. It is a direct reflection of passenger satisfaction and feeling of safety in air transport, which is considered the safest means of transport.

COMPLEX AIRPORT SAFETY SYSTEM

The current protection of international civil airports against acts of unlawful interference is implemented through multi-layer protection, which aims to achieve the desired security level with security and control barriers (Fig. 2).

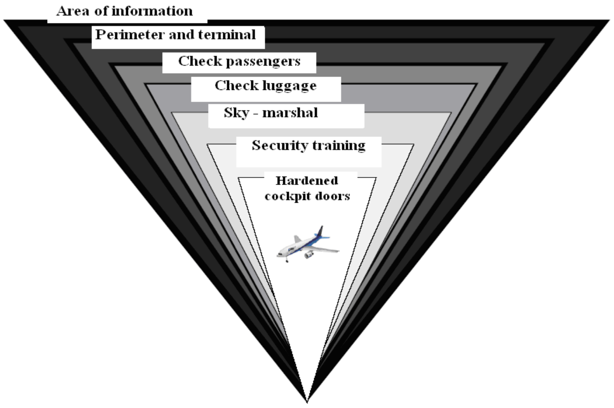

Fig.2. Scheme of multi-level protection of a civil airport against acts of unlawful interference

The primary safety element of a comprehensive security system is the airport perimeter (perimeter) protection. We see it as an integrated package of passive barrier means and active elements of protection. On the peripheral parts of the airport there are mainly mechanical barriers (fencing, gates and ramps), technical surveillance equipment and systems of access control to restricted parts of the airport.

Currently on the market with monitoring, detection and security technology, there are lots of modern means of object protection and entrance control facilities that can be used in securing the airport perimeter safety and access control (Fig.3).

These is mainly a network system of internal television circuit, entrance and access control systems to restricted areas of an airport, a set of detection devices, video detection equipment, thermal, radar systems and monitoring inputs. One of the conditions of efficiency and reliability of multi-level security system of the airport is timely and accurate transmission of relevant information from one control to another one.

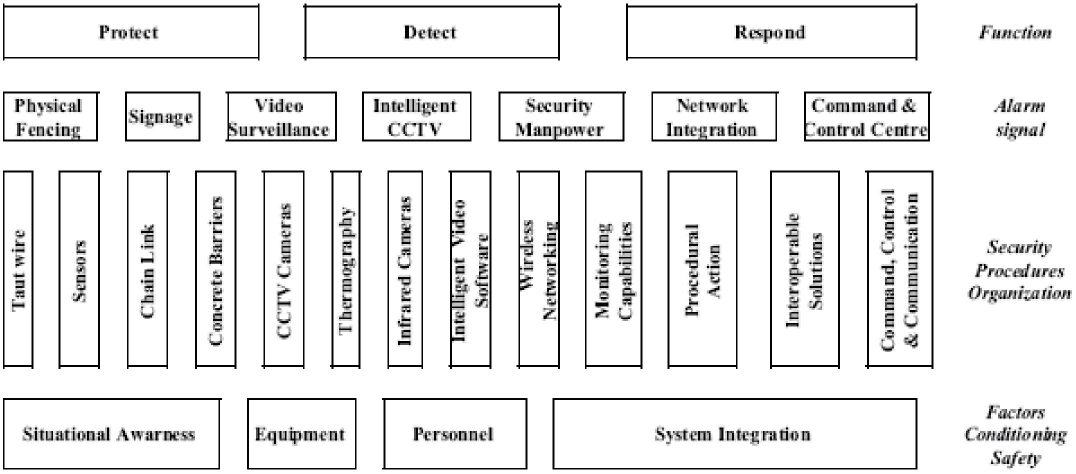

Fig. 3. The use of safety control means and civil airport protection

Immediately after the terrorist attacks in the USA in 2001, President George Bush signed a safety of aviation and air transportation act. The act was adopted with the same content in other countries of the world. Although the adoption and application in aviation practice caused the huge airport security technology development and airport security concept aimed to:

□ improve airport perimeter protection by installing intelligent security systems and control devices of input mode,

□ tighten of controls on persons from entering restricted areas of the airport security protection.

Under the Act, it was recommended to focus the attention to the implementation of management and risk assessment of the airport, particularly in the areas of:

□ risk assessment, with emphasis on political factors in the state and monitoring the activities of terrorist groups,

□ evaluation of airport infrastructure, with emphasis on sensitivity and throughput of the security system of airports,

□ assessment of the bottlenecks in airport infrastructure, organization of protection and implementation of modern systems of the airport.

Sufficient requirements on the airport protection have been defined with an emphasis on individual security zones at airports and defined for particular "sensitive" areas and places of airports. These requirements have been defined for so-called SIDA zone (Security Identification Display Area), AOA (Air Operations Area) and SA (Sterile Area) (Fig. 4).

In 2004 the U.S. adopted a document GAO (General Accounting Office) with the title "Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls."

The report implies the organizational efforts aiming to increase activities focused on control and monitoring of access to security restricted areas, risk management and rapid introduction of new technical means of protection. Implementation of the provisions of this document was expedited by the terrorist attacks carried out in Madrid in 2004 and in London in 2005.

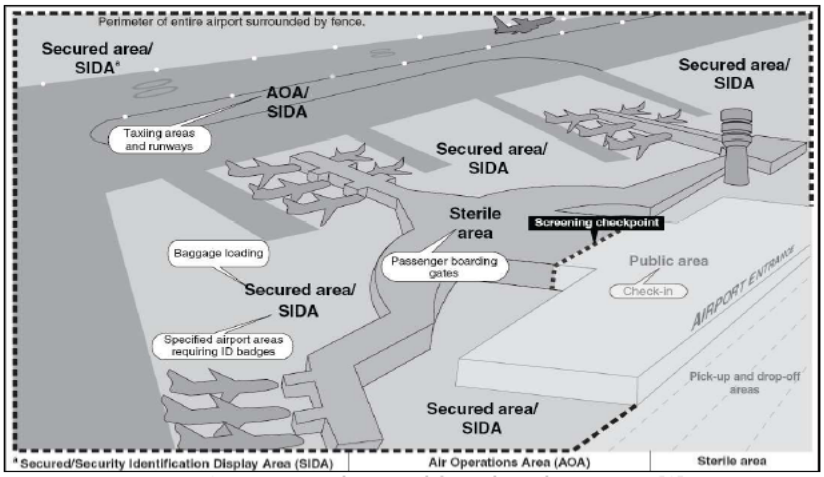
Perimeter of entire airport surrounded by fence.
Secured area/ SIDA*
AOA/ SIDA
Taxiing areas and runways
Secured area/ SIDA
Secured area/ SIDA
Sterile area
Screening checkpoint
Baggage loading
Passenger boarding gates
Public area
Check-in
AIRPORT ENTRANCE
Secured area/ SIDA
Specified airport areas requiring ID badges
Pick-up and drop-off areas
Secured area/ SIDA
* Secured/Security Identification Display Area (SIDA)
Air Operations Area (AOA)
Sterile area

Fig. 4. Zones of restricted areas of airport security protection

RISK MANAGEMENT IN THE AREA OF AIRPORT PERIMETER PROTECTION

Assessment of risks in the area of perimeter protection of the airport means to find vulnerabilities in a security system and to assess risks from the structural and procedural point of view.

A method used to solve risk management of entries and accesses to buildings and airport areas seems to be the method of safety system failure and its impact on airport and air traffic operation. It is the method in which we can use statistical evidence of safety analyzes of previous entry mode failures of an investigated airport, but also from other airports. Using this method with using the parameters of the risk level we can evaluate the various elements of the security system, the probability of the risk and severity of the consequences. It is a way of managing risk through modelling and simulation of a fictitious airport with the help of probability theory. Within the risk management we can use, for example, a graphical form of risk assessment (the Lorenz curve), which provides an overview of the seriousness of the risk assessment according to the same degree of tolerance. Herein, we define a numerical value in the interval, for example (1-100). For the final calculation, the so called Pareto principle 80/20 can be used, where the risks with a tolerance level up to 80% are viewed as unacceptable risks, and risks to the level of tolerance up to 20% as acceptable risks.

A methodological tool for a risk analysis in the perimeter protection of the airport can be represented by a method of cause and effect, in which we use so-called Ishikawa diagram (so called Fishbone diagram). Using the diagram we create a deeper analysis of the viewed phenomenon or action, with emphasis on the possible consequences. The main objective of the graphic expression with the Fishbone diagram is to identify the causes and to assess threat consequences after the existing airport perimeter protection has been overcome. The method is also suitable for identifying intended protection of the airport, endangered buildings and areas of interest, including failures of technical and technological processes.

Assessing the security risk and its consequences in cases of overcoming the airport perimeter protection is, in most cases, a very complex process in which we apply a deductive approach. We do not only review the technical equipment and readiness of airports, the type of aviation transport, human factors in aviation, the ability to react immediately but we also have to take into account the hard predictable factors and real facts such as terrorism, crime, political situation in the country, economic issues, standardization and harmonization of safety procedures and others. The deductive approach to the issue of risk assessment in the field of civil airport against acts of unlawful interference can be applied using analyzes of unlawful acts in aviation already committed, clarifying their reasons or assumptions that led to the expression of different possible scenarios of overcoming airport security. For this purpose, it is appropriate to exploit the method of simulation modeling, often using even abstract models.

In the sphere of risk evaluation and assessment of the security system of civil aviation, we can, however, use the inductive approach. Different scenarios of potential threats of protected objects or interests we shall assess using methods of safety management, probability theory and estimate the extent of damage. The analytical approach of risk assessment and the degree of threat, in cases where the inductive methods are used, is based on risk modeling with measurable statistical parameters (e.g. the extent of damage, the length of the assessed period, the number of passengers, amount of transported cargo, etc.).

Risk assessment is quite demanding because the safety analysis of the expected event, phenomenon is often in the realm of the subjective assessment in the sphere of civil aviation assessment against acts of unlawful interference. We assess phenomena (events) that have not yet happened, with hard defined consequences. When analyzing the risks and consequences of threats to civil aviation we often meet with inductive-empirical evaluation of qualitative and quantitative parameters of risk. Using qualitative expert methods we can evaluate the risk and size of threat with a scale of the acceptability (or unacceptability). The scale may have some levels. In most cases, three to five levels are sufficient in the range from acceptable to intolerable risk. In evaluating the level of risk with a quantitative expression it is very difficult to assess the impact of a human error which is significant in protection of civil airports. It is also quite difficult to examine the logical links between the factors influencing the formation of risks (e.g. we cannot primary define a motive of intruders overcoming the airport perimeter protection, similarly we cannot evaluate the consequences of misusing of the object when detected in passenger's hand luggage).

Airport security risk management is a systematic and analytical process, whose role is to assess the likelihood of threat, to define measures to reduce risk, to take effective means to mitigate its potential consequences and to support key decisions in order to protect property and persons in air transport. We follow the basic principle of risk management which concludes that we cannot completely eliminate risk but we can increase protection and so eliminate the potential threat. Through effective management, compliance with established procedures, a good airport with modern technical equipment and detection equipment monitoring risk sources it is possible to reduce a potential security threats and their consequences to acceptable levels. The question is: What is possible to consider acceptable level? Answer to this question is trying to give a lot of safety analysts, is the subject of extensive discussions in the field of national security policy, development of human resources, financial resources, social - psychological analysis and other analyses that directly or indirectly enter the process of provisioning adequate safety and protection of civil aviation.

Despite various constraints, e.g. ethical dimensions, financial performance, political decisions, interference with personal freedoms and other factors, the basic objective must be kept in mind. It ensures reliable protection and aviation transport security against acts of unlawful interference. This process should involve airports, air carriers as well as other components of the air traffic control.

SECURITY RISK ANALYSIS OF IN THE AIRPORT PRACTICE

Security risk is a function of the threat nature, the degree of vulnerability of the security system and the consequences associated with overcoming the consequences of the security system.

$$Risk = f(threat, vulnerability, consequence) \quad (1)$$

The risk is therefore a function of three risk parameters - threats, vulnerabilities and consequences. The threat to a airport security system, like the vulnerability of the system can be defined as the likelihood of the risks and potential threats. The results of this process are the variables with which we can, in the safety analysis, identify the seriousness of the risks or consequences or the extent of consequences in overcoming the airport security system.

Using an economic analysis, we can evaluate the investment and operating costs for a functional and effective airport security system as well as the cost of disposal of possible consequences. With a mathematical expression we can also generate possible operating losses, including losses in material terms but also human lives in case of a potential illegal act in aviation.

In considering the relationship (1) with the estimated cost to build an adequate security system and the possible scenarios of its overcoming, the three main risk factors can be expressed by the equation as

$$\text{risk} = \text{threat} \times \text{vulnerability} \times \text{consequence} \qquad (2)$$

The character and degree of risk is directly proportional to the threats, system vulnerability and consequences that result from overcoming the security system.

In preparing the safety analysis and risk identification in structural airport security systems it is possible to use several known methods and procedural approaches that determine the nature of the risks and their possible consequences for air transport. Using these methods we can determine the level of acceptable risk which we are able and willing to take within adequate and at the same time reliable protection.

The fundamental problem in the safety analysis of the risks in the sphere of illegal acts in aviation transport is determining the extent of acceptable risk. To assume the further development and consequences of unlawful acts against civil aviation is very difficult. The reliable assessment of risk to an acceptable limit is possible only in real time, in specific circumstances, and depending on the penetration ability of airport security and control barriers for potential intruders. This is particularly relevant for assessing the weakest elements in the establishment of security and airport security regimes, but also e.g. in the process of evaluating the functionality of individual components in the system man - machine (or the airport security worker - control and detection equipment).

Methodological approach to risk identification, risk calculation, verification of results and process optimization in safety and control processes at airports is shown in the flow chart of safety analysis and risk assessment in accordance with Figure 5.

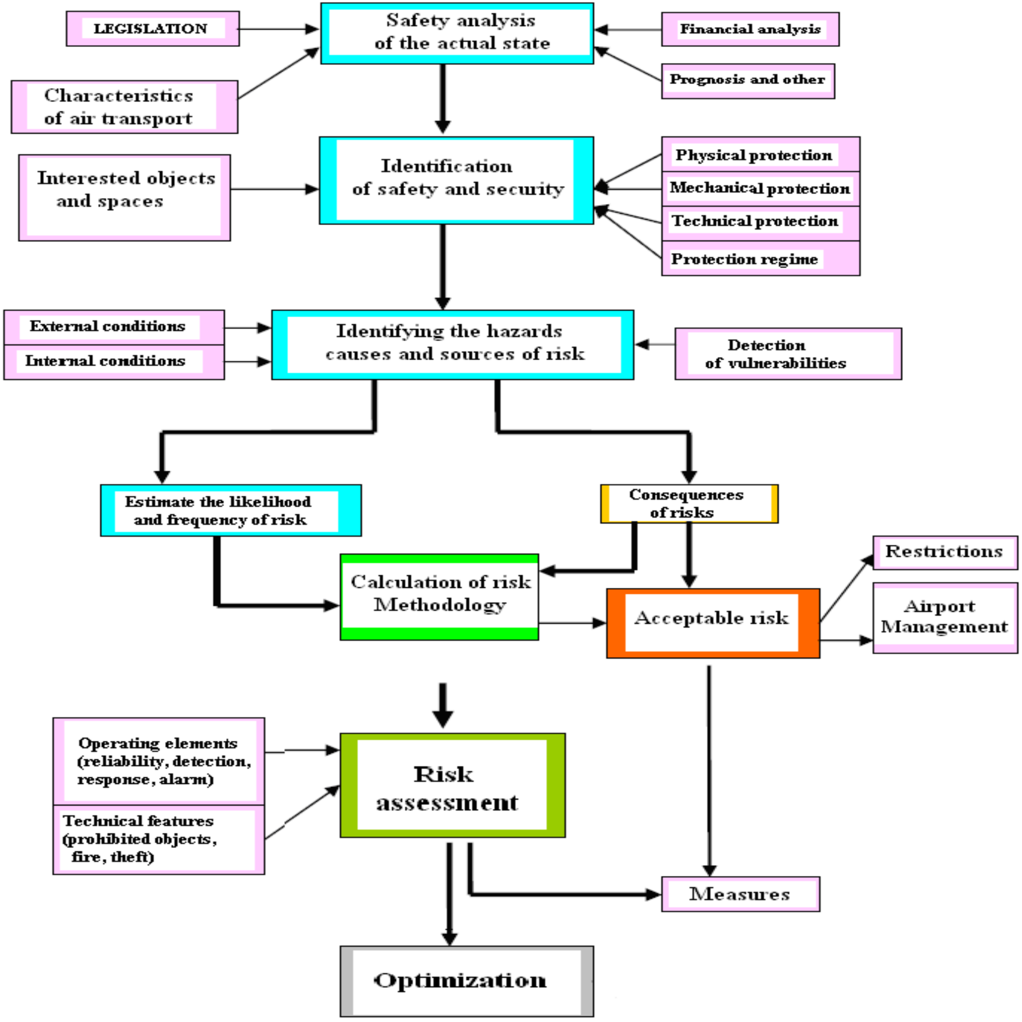
LEGISLATION
Safety analysis of the actual state
Financial analysis
Characteristics of air transport
Prognosis and other
Interested objects and spaces
Identification of safety and security
Physical protection
Mechanical protection
Technical protection
Protection regime
External conditions
Internal conditions
Identifying the hazards causes and sources of risk
Detection of vulnerabilities
Estimate the likelihood and frequency of risk
Consequences of risks
Restrictions
Calculation of risk Methodology
Acceptable risk
Airport Management
Operating elements (reliability, detection, response, alarm)
Technical features (prohibited objects, fire, theft)
Risk assessment
Measures
Optimization

Fig. 5. Development diagram of risk identification and process optimization of ensuring security and protection of civil aviation

The optimization process, where the use of mathematical - simulation models can determine and select the most effective way of dealing with the protection and ensuring the safety of civil aviation against acts of unlawful interference is appropriate to apply to the comprehensive analytical process of risk identification and subsequent evaluation of risk information.

The basic elements of risk analysis of airport securities are:

- □ *The assessment of potential threats, their identification based on factors which are the airport equipment, its readiness, intentions and past actions. This assessment is a systematic approach to identifying potential threats, and is based on information obtained from e.g. an intelligence service. This information should be evaluated and updated frequently in order to detect new threats. These data also represent a critical point in the evaluation process difficult to identify.*
- □ *The assessment of vulnerability of the airport building is possible only on the basis of extensive analytical work with a team of skilled professionals with tools of intelligent systems, advanced security equipment, information resources, financial and other sources. Vulnerability assessment of civilian airports is another basis for determining the procedures and management processes that are necessary to ensure the security of operational procedures at airports. The analytical approach to risk management can be represented graphically with the set intersection of risk assessment (Fig. 6).*

The attention in the process of risk management should focus on the highest priority. For example, an airport, which is likely to occur, in terms of risk, more vulnerable to risk and probably more threatened, should be given special attention to its protection. Such are the major fungal airports, transfer airport, airports in the countries with the occurrence of terrorist acts, airports in the territories of ethnic and social riots, and others. The risk analysis is a constructive tool representing a certain parameter of threat assessment, risk and vulnerability. Priorities, in this case, are also necessary to establish in terms of financial, technical, organizational security and personnel staffing.

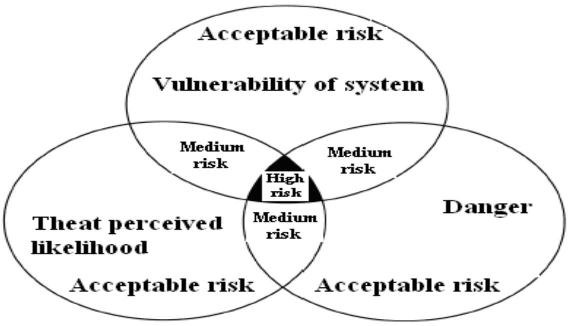

Fig. 6. Set intersection of risk assessment

The risk analysis of aerodrome safety management should be developed in e.g. a catalogue of possible causes of risks and their consequences. Its aim is to define the threats of structural elements in determination of objects (an airport, airplane, air passengers, crew and aircraft, etc.), operating elements (detection, response, operating room, a level of vulnerability, reliability) or in terms of threats, in the processes (check-in process of passengers, air cargo transport, aircraft technical handling, etc.).

An important part of the analysis is to identify hazards, their causes and sources of risk with respect to external conditions and also the internal security of the airport. Only then, we can define the possible consequences, establish the risk frequency and estimation of their occurrence probability. Based on these identifiers, a suitable method is used to calculate the coefficient of acceptable risk as a key identifier by which we are able to assess, within the overall analysis, the function and character of the security and efficiency of its operational elements within the different categories of hazards (a forbidden object on board of an aircraft, bomb attack, hijacking, sabotage, fire, theft, unlawful entry and others).

SECURITY ASSESSMENT OF AIRPORT VULNERABILITY

One of the ways which security analysts use in the safety analyses for risk identification and assessment is a point scoring system. Its outputs are quite reliable parameters by which the degree of a threat, vulnerability, and consequences can be evaluated. The assessment criteria are listed in a row scale in a form of an evaluation matrix and represent separate categories arranged in ranging from setting a minimum risk to the category of unacceptable risk.

The generally applicable method of a security analysis and risk assessment is a point evaluation method of risk parameters with processing of so called "cards for threat assessment." The cards can be developed for each type of risk, including possible consequences of this threat.

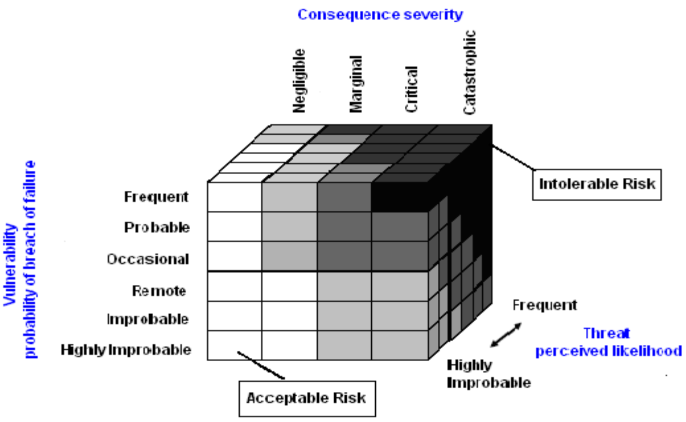

Fig. 7. Three dimension matrix with an evaluation scale of threats, vulnerability and consequences

The risk assessment values are compared with the constant - coefficient acceptable risk within the defined scale. In the airport security practice, however, this method of risk assessment has an ordinal character, because the method of risk assessment, especially in the field of civil aviation against acts of unlawful interference *is largely subjective. The reliability of output can be scaled up by using multiple parameters with multi-criteria functions. An essential element, however, remains security risk whose resulting value can be calculated using several variables. If we use three variables the underlying risk matrix can be expressed graphically in three dimensions according to Figure 7.*

In the risk matrix there are different categories of a threat and vulnerability of a security system rated from the known (or frequent) to the potential risk (highly unlikely).

The interval scale with evaluation in the risk matrix can be expanded and described in appropriate mathematical algorithms. The vulnerability of a system will be evaluated in e.g. a scale of probable occurrence and failure of a security system in six categories from very probable (frequent) to the stage of highly unlikely. The category will include evaluation of highly unlikely (1), unlikely (2), distant (3), occasional (4), probable (5), and frequent (6). The level of assessment in the six-speed process of identifying risk can also be used to categorize the perceived security threats in assessing the likelihood of risk. The severity and consequences of threats will be assessed by evaluation of one of four levels from negligible to catastrophic in order of seriousness: negligible (1), marginal (2), critical (3) and catastrophic (4).

This method of risk assessment is illustrated by a process which, due to the specific needs and priorities in the field of civil aviation against acts of unlawful interference, provides a combination of threat assessment, vulnerability, severity and consequences. Using the risk matrix, we can quantify the degree of a threat and vulnerability as a parameter formulated in terms of probability and risk in the range of values from zero to one, or between 0% to 100%, or another evaluation interface.

An example for calculating the acceptable risk coefficient represents the study of terrorism experts, who, based on political - security analyses, have evaluated that the likelihood of committing terrorist acts against civil aviation, depending on the density of air traffic worldwide over the last 10 years, is about 25%. If we use a range of values from 0 to 1 in the safety analysis for assessing the threat degree, we can determine the coefficient of the threat of a terrorist act in air transport by the coefficient of K_t = 0, 25. The coefficient K_t is the fundamental identifier of the likelihood of a terrorist act in air transport. In structural terms, a threat to the safety of persons and probability to commit a terrorist act in the airport terminal building, we analogically determine by the coefficient of $K_{tt.}$ The likelihood of the terrorist attack in the airport departure hall can be expressed as a numerical value K_{tt} = 0,50. This is due to the fact that airport terminals are usually designed as objects of public spaces generally accessible and as restricted sterile zones where complete detection screening precedes entering of people and transfer of objects.

In the sterile zone an airport terminal there is a threat of terrorist bomb attacks unlikely and highly unlikely, when we determine the coefficient of the threat, depending on specific conditions within K_{st} = 0,01 - 0,25. In the public part of the terminal, on the contrary, the threat is relatively high, ranging K_{vt} = 0,5 - 0,75.

Based on the knowledge of these coefficients, the vulnerability in case of threats to the airport terminal caused by a bomb attack of terrorists is calculated as

$$Z_{LT} = K_{st} \times K_{vt} \tag{3}$$

Thus, the overall vulnerability of an airport terminal in a catastrophic scenario in case of a bomb attack is

$$Z_{LT} = 0{,}25 \times 0{,}75 = 0{,}1875 \text{ or } 18{,}75\ \% \tag{4}$$

The percentage reduction in the coefficient of vulnerability of an airport terminal can be achieved by taking additional security measures, e.g. construction of a modern monitoring system in public areas, organizational measures in separation and profiling of passengers in the check-in process, implementation of 100% control of people already at the entrances to the terminal (the terminal sterile zone) and others.

Evaluation scenarios of civil aviation security threats, based on highly unlikely occurrence of threats with minimal or no effects can be regarded as acceptable risk. On the other hand, in cases of impended failure of the security system and a result of the probable scenario is considered high risk to catastrophic risk, is considered unacceptable risk.

Between acceptable and unacceptable risk there is so called "a gray area" (see risk matrix Fig. 6), which is there for mostly reserves searched in airport security systems. Here, within the organizational and personnel changes, it is possible to mitigate the risks to acceptable levels by technological modernisation of an airport security system and after accepting the new regime measures. It is in this "gray area of risk" where a conflict of views on aviation security and significant controversies of experts have arisen. It is rather the area that does not solve safety and security of aviation comprehensively, but rather affects the security issues of sub-areas such as work organization in the control of passengers, checking of luggage and cargo, airport zoning, entrance regime to airport areas and aircraft boards and others. The solutions adopted in this area disproportionately increase financial costs of airports and *airlines, often extend beyond the sphere of personal freedom restriction and take unpopular measures (e.g. whole-body screening of passengers, regular security checks and airport staff training) that overcharge and in a special way restrain the air transport compared to other transport sectors. Despite the unpopularity of this phenomenon, at present this "gray area" provides more options and space to improve and ensure reliable protection of civil aviation against acts of unlawful interference.*

The "black area" in the risk matrix with the catastrophic consequences and unacceptable risk represents a particular threat from terrorist attacks, whose solution is rather in the political, ideological and social level. Eliminating of this threat is the comprehensive solution of national state security, intelligence activities, building information networks, standardized security procedures and other measures within the national and international security.

The spheres connected with insufficient work organization at airports, incompetence, inconsistency, breaking of safety rules or other deficiencies that do not have signs of threats to persons or endangering airport operations and air traffic can be considered the acceptable risk in the risk matrix "white space".

CONCLUSIONS

The analysis of security risk in aviation has been especially recently monitored area that significantly affects the process of adopting safety measures and procedures in civil aviation. The results are also the basis for financial analyses of investment and operating costs, assessing the level of airport security, evaluation of the level of services to the public, regional development, tourism and other areas of society.

ACKNOWLEDGMENT

This article was written with the support of the project VEGA No.1/1117/11 – "Integration of algorithms, automatic flight control and control air turbo compressor engines" and project VEGA No.1/0298/12 – "Digital control of complex systems with two degrees of freedom".

REFERENCES

[1.] 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

[2.] PACAIOVA, H., et.al.: Safety and Risks of Technological Systems. SF TU in Kosice, Vienala, L.t.d. ISBN 978-80-553-0180-8.

[3.] FLANAGAN, R., NORMAN, G.: Risk Management and Construction, Blackwell Science Oxford, 1993

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

[5.] KOLESAR, J.: The Protection of Civil Aviation against Acts of Unlawful Interference, LF TU, Kosice 2010, ISBN 978-80-553-0357-4.

[6.] SCUREK, R.: The Study Analyses the Risk of Unlawful Acts at the Airport, Technical University Ostrava, 2009.

ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING