MASTER – EXTREME RISK MANAGEMENT TOOL IN AVIATION SECURITY SYSTEMS

Cătălin CIOACĂ

"Henri Coandă" Air Force Academy, Brasov, Romania

Abstract: *The research is focused on the conception, design and test of a decision-making tool necessary for going through the whole decision process which is specific for aviation security systems, integrating the results of risk assessments and providing the main action course through a graphical user interface. MASTER enables the collection, analysis and display of the level of risk and vulnerable areas based on a created mechanism linking Excel and Matlab components, both in the preventive phase (simulated scenarios decision) and in the response phase (which provides efficient investment solutions).*

Keywords: *risk index, aviation security, graphical user interface*

1. INTRODUCTION

The aviation industry is at the center of national and international transport system, with a significant role in the economic development globally. Aviation security has thus become a priority at the local - national and regional – global level.

Reducing the vulnerability of critical infrastructure of the aviation regarding security risks materializes through significant spending from the authorities. The last two decades have witnessed an increasing trend in the number of passengers and freight volumes. Security requirements have also increased, especially after the attacks of 9/11, and also the security costs (between 1.5 and 2.5 billion for aviation security community sector) (CSES, 2011).

The events of 11 September 2001 led to the identification of serious security problems in the critical infrastructure: limited capacity to discover the sources of risk, the existence of outdated and incomplete database, limited skills of security personnel, limited and inadequate action procedures, response coordination and control in situations of extreme events.

Existing blockages in current research in security risk management of extreme events area caused by extreme events refers to: the crisis approximation knowledge in organizations with different profiles, improving real-time access to information and knowledge in order to save lives, the lack of systems decision support at the strategic, tactical and operational level, the lack of consistent databases which can provide a comparison (generally held by the central authorities and the private and public beneficiaries, very difficult to transmit, not enough correlation between information and risk reduction measures); there are no dynamic set of relevant indicators (eg. risk maps that highlight the dynamic probability of extreme events) there are no security investment strategies based on cost-benefit, cost-risk or real options analysis.

Due to the analysis of the current state of knowledge in the field and the existing blockages, the need for a decision-making tool for the substantiation of extreme risk events in aviation security systems highlighted (SSA), an adaptable, flexible, modular, scalable decision tool, which can be applied both in the preventive phase (by simulated decision scenarios) and in the response (by improving security investments).

The complexity and dynamics of the problem requires urgent involvement of government and policy makers in order to find effective solutions to minimize the potential impact of extreme events on infrastructure associated aircraft systems. Proactive approach to understanding the threats, vulnerabilities and mitigating the consequences provides both prerequisites for effective decision making and direction for future standardization of extreme event risk analysis in both public and private critical infrastructure.

Treatment models of complex socio-technical systems such as aviation ones must take into account the following aspects: quick response by integrating all subsystems of intelligent network management, distributed knowledge organization in order to optimize resources, operation capacity in heterogeneous environments (specific systems knowledge management) interoperability (effective synergistic operation, translation or other communication solutions) open and dynamic structure, effective and rapid cooperation, human-machine integration, agility (adaptability to rapid and unexpected changes in the environment), the ability to quickly reconfigure and to interact with heterogeneous partners (the ability to use additional resources without disturbing the organizational interdependencies and established operating rules) acceptable error tolerance.

2. COMPOSITE INDEX OF SECURITY RISK

The risk of extreme events is regarded as an asymmetric function by the nature of the threat (A), vulnerabilities (V) of an attack and the consequences (C) associated to a possible attack scenario (Willis et al., 2005).

The threat can be defined as the intention to produce a negative change (loss, damage, failure) on the state of a system (Haimes and Horowitz, 2004). The study of the purpose of the threat must be done in specific terms (objectives, types of attack time), the probability can be used as a measure of the risk of an attack.

This threat could be measured as the probability of an attack on a particular target in a particular manner and in a fixed period of time. This probability refers only to the terrorist threat to one type of attack on a specific target, leading to the need for a full description of the typology of attacks combination (hijacking, bomb, cyber) with a limited number of possible targets in a geographic area. The threat is not an accidental or unpredictable phenomenon, however this manifestation is unpredictable and difficult to control. Threat assessment output is input for vulnerability assessment.

Vulnerability defines the degree of (in) capacity of the system to respond at some point to a manifested threat (Smith et al, 2009). In risk analysis, vulnerability is assessed using known or perceived probability of the existence of a breach in the security or malfunctions which may occur in the analyzed target for a certain period of time, under an attack scenario. At some point of time, a system can present a high level of vulnerability to a specific threat, but also some potential for adaptation caused by dynamic ability to respond to new types of threats (Brooks, 2003).

Although belonging to different media organization (the threat - the external environment, the vulnerability - internal environment), there is a link between the two parameters of risk: vulnerability is highlighted against the background of the threat (initiating a successful attack).

The result is a variable defined in terms of severity of the potential impact. In the risk analysis, the result is represented on a scale of severity associated with an event or scenario. To measure the consequence of a successful terrorist attack it is necessary to quantify the expected damage (fatalities/injuries, property damage), without claiming to develop a comprehensive list.

The risk of terrorism can be considered as the expected result for an existing threat on a target based on the method of attack and the type of damage. Asymmetry complicates the understanding of the mechanisms and processes, especially in the context of "technological convergence" described above.

Risk score, expressed in terms of threat - vulnerability - consequences, becomes important for the evaluated organization/ aviation system in relation to the conditions of the level of risk tolerance. This level is then calculated to ensure a balance between costs and benefits.

Each cell of the risk matrix is a combination of the probability of the threat scores (p_a), the probability of vulnerability (p_v) and therefore (a_c), reflected by a single risk score determined as the weighted product of three factors Composite Indicator of Security Risk (ICRS):

$$ICRS = p_a \times p_v \times a_c \qquad (1)$$

Risk assessment involves comparing estimated risk levels with defined risk criteria in order to determine the significance of the risks and decide on future actions.

Extreme risk assessment methodology (ERAM) aims primarily to support the decision making, including at a political and economic level, to continuously improve the safety of the air transport system, under the accelerated development in recent decades and its backdrop of increased terrorist events of extreme nature (Cioacă and Boscoianu, 2013).

Consultation of human experts is essential in the study of the problems based on measurable data associated with complex socio-technical systems (eg. model selection analysis, interpretation of results). Quantification represents by no means certainty, but the adequate capture of the dynamics of processes that allows understanding of the highly asymmetric risk assessment in aviation.

Qualitative approach has the advantage of determining risks prioritization without requiring quantitative determination of the frequency and impact of threats to the organization.

If in utility theory, decision weights and the probabilities are the same, in the case of chances estimation theory, probability changes have less effect on decision weights. The similarity is that the weights depend only on the probability decision-making in both theories (Kahneman, 2012).

Because events with low probability of occurrence are overweight when they are described in terms of relative frequency than when formulated in terms of probability (Kahneman, 2012), threat assessment process should take into account this trend. In order to rank the consequences of risk and the association quantitative assessment of risk the following parameters are considered: the degree of destruction of infrastructure and the number of casualties (Dillon et al., 2009).

3. DESIGNING MASTER

MASTER application is a tool developed based on extreme risk assessment methodology, that can be successfully used in the foundation of decision making process by providing results in order to prevent the risks associated with extreme events. Any analysis of threats, vulnerabilities and consequences, with available resources, anticipation serves to anticipate extreme risk situations that may be faced at some point by an organization and to increase the resilience by identifying vulnerabilities and providing investment solutions to reduce thereof.

The main results that can be obtained with MASTER application are: the possibility of design risk scenarios, risk profiling, representation and update the risk map (Figure 1). The application is implemented in a graphical user interface (GUI) using Matlab (R2008b) and carried out on the basis of the methodology described in the risk assessment very (Cioacă and Boşcoianu, 2013).

The GUI design took into account the fact that in most cases the beneficiaries (decision makers) do not have advanced knowledge of computer use. Thus, to solve problems related to communication between the user and the system, but also for improving users ability to use and benefit from the support (Druzdel and Flynn, 2002), resulted in a intuitive and easy to use interface, with personalization and improvement possibilities.

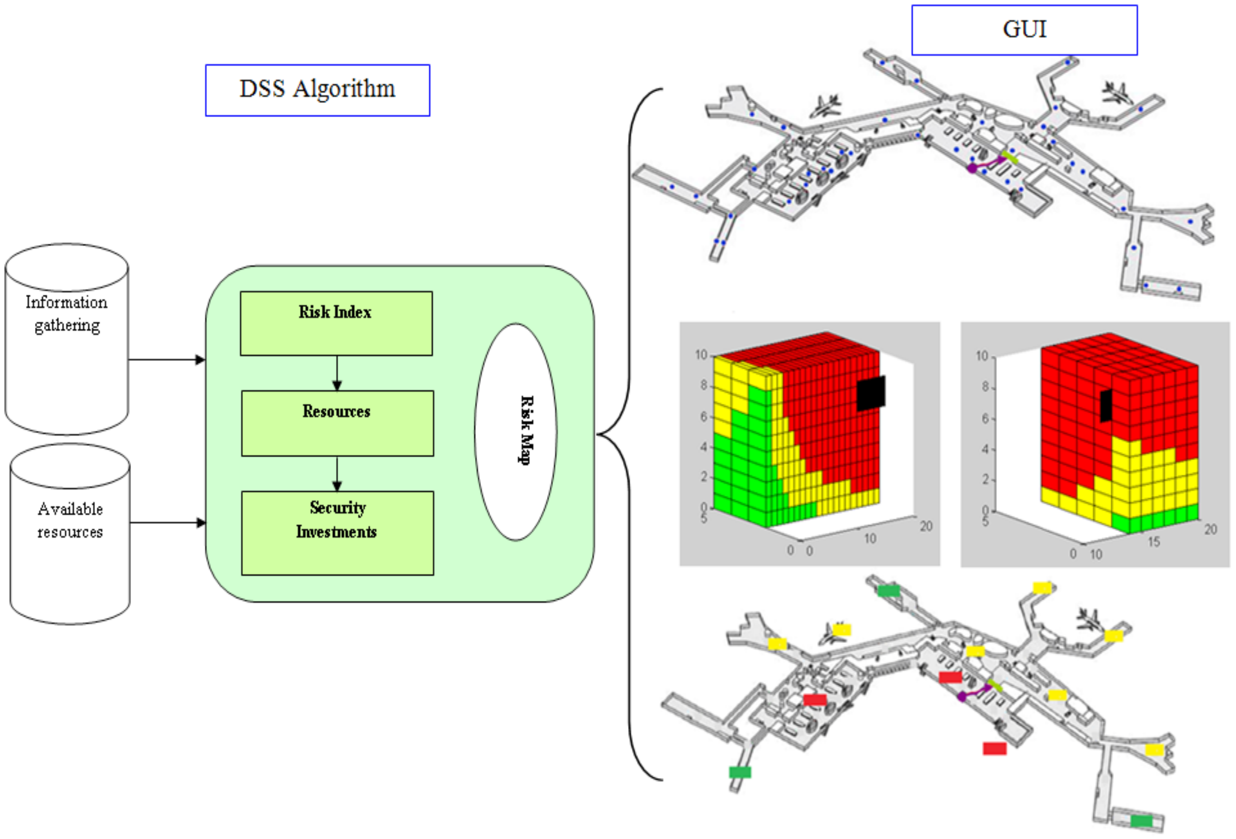
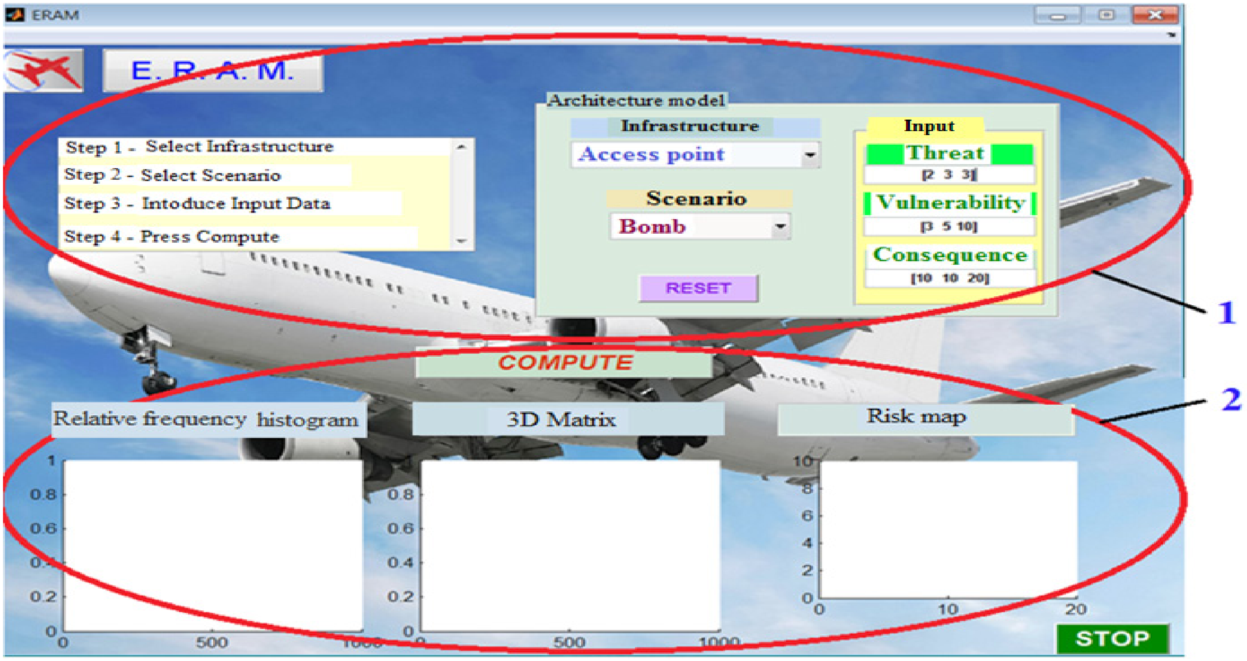


Fig. 1 The architecture of decision support system

The main menu is divided into two parts: the configuration section of the input data (1) and the results section (2) (Figure 2).

The application contains a number of four steps, as follows: selecting infrastructure element under evaluation, selection risk scenario, assessing risk parameters, displaying the results.

In order to cover the first two stages is required that the user selects from a list of predefined evaluated elements (3).



Step 1 - Select Infrastructure
Step 2 - Select Scenario
Step 3 - Intoduce Input Data
Step 4 - Press Compute

Infrastructure: Access point

Scenario: Bomb

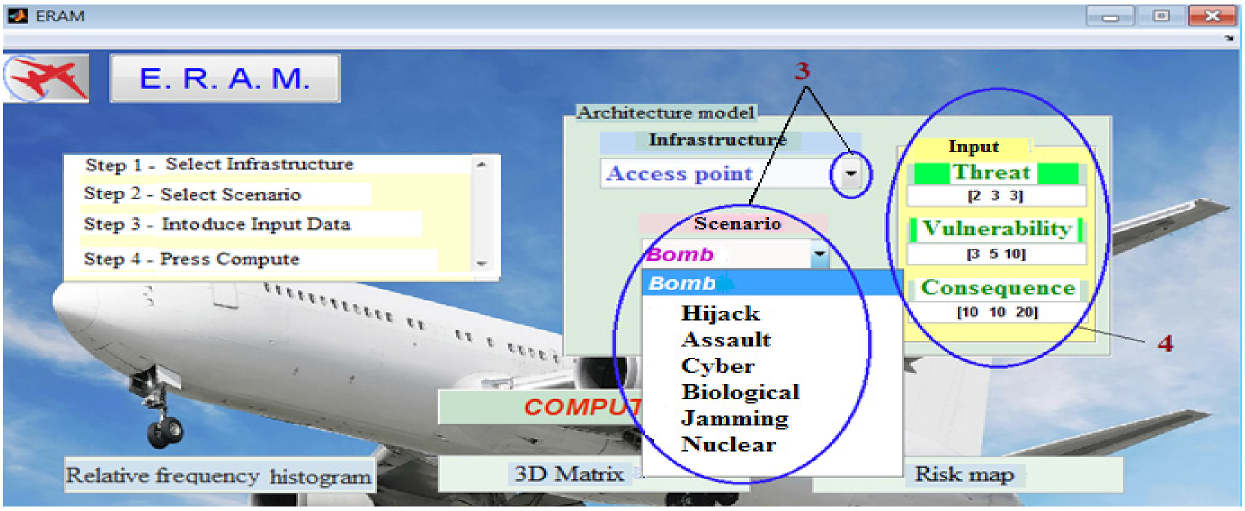
Input

Threat [2 3 3]

Vulnerability [3 5 10]

Consequence [10 10 20]

Fig. 2 The main menu of users interface



Step 1 - Select Infrastructure
Step 2 - Select Scenario
Step 3 - Intoduce Input Data
Step 4 - Press Compute

Access point

Scenario: Bomb

Threat [2 3 3]
Vulnerability [3 5 10]
Consequence [10 10 20]

Fig. 3 Stages 2 and 3 of application

The necessary data for step 3 are obtained in real time from the members of the evaluation team, according to the algorithm described in section 4.3 (4) (Figure 3).

Once the input data is entered by pressing the Compile button, the application generates results in three graphs: relative frequency histogram (5) 3D matrix of risk (6) and updated risk map (7) (Figure 4).

Cumulative relative frequency distribution (5) provides decision makers the opportunity to read in terms of probability the risk level composite index.

Positioning the index associated with a scenario and risk facilities on three-dimensional matrix (6) in the red zone because of the potential consequences and vulnerability, it must be interpreted as adopting those measures that allow the option of moving this scenario out of the red zone.

Being an unacceptable risk, the risk map associated scenario (eg. bomb attack on the gateway) is updated (Figure 5).

MASTER application of extreme risk management is installed on a desktop computer at the organization, entering the responsibility of a system administrator, who is part of the security department.

The station becomes the main avenue of the application, while the data storage is the base of future evaluation.

At the request of policy makers (members of the committee cell crisis) risk analysis of terrorism or the emergence of new information about the threat (provided by specialized structure information), the system administrator uses the application to produce a temporary database that together with other data (eg. plan airport security procedures, positioning systems security) developed during the pre-assessment, are sent via intranet to the evaluation team members.

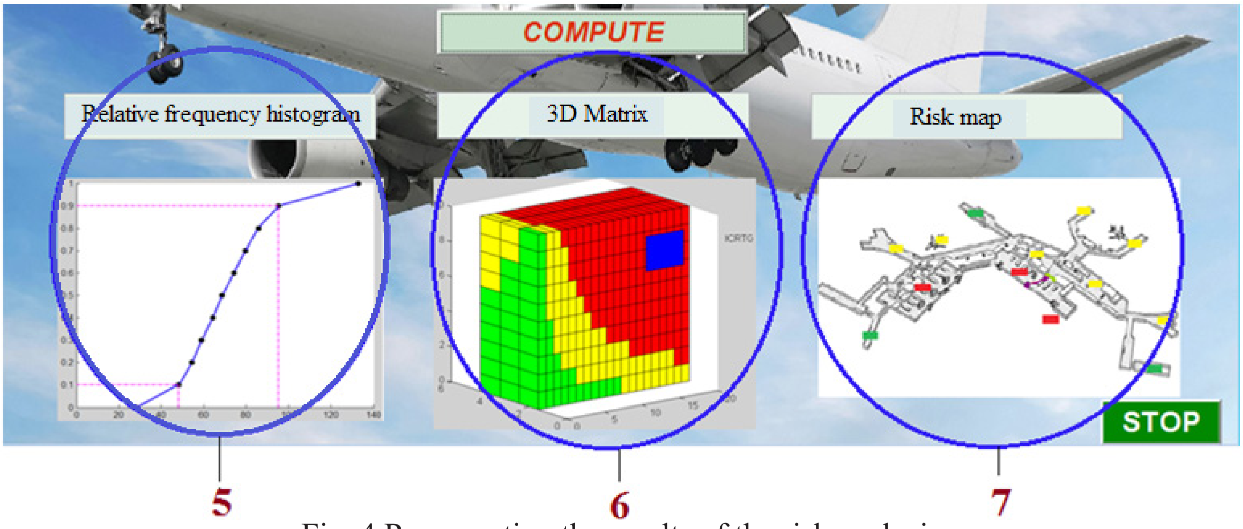


Fig. 4 Representing the results of the risk analysis

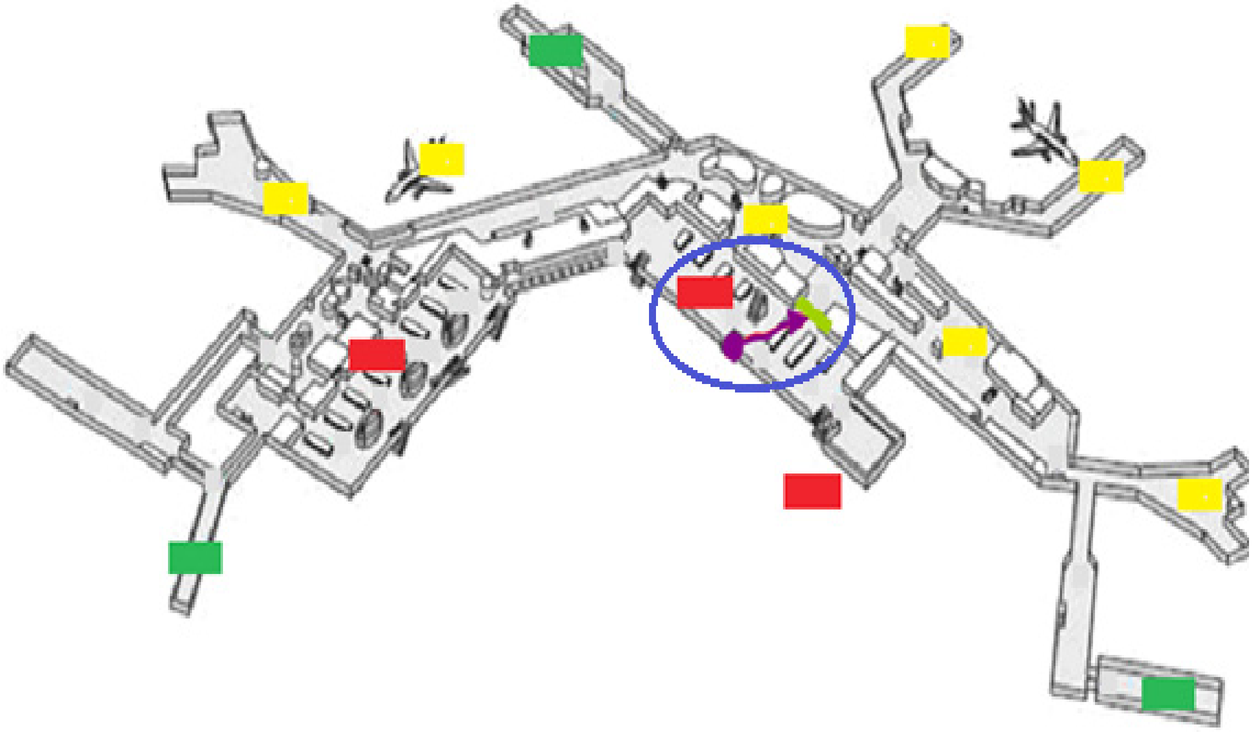


Fig. 5 Updating the risk map for the bomb attack at the gateway scenario

Evaluators who are equipped with tablets or laptop, perform the analysis of the new information and record the results in one database, which is transmitted to the system administrator.

The administrator then loads it into the program and transmits the data to the security manager for print and analysis.

After initiating the request for data, access to database risk assessment becomes limited only to those users who have permission to access the database granted by the system administrator.

Also, data can be viewed by all authorized users and data changes can be made only by those who have been granted permission.

All information flow takes place through a secure intranet.

Security risk analysis in aircraft systems by applying the MASTER instrument provides the following benefits: identifying and assessing security risks extreme risk prioritization based on the composite index of terrorist risk, risk map building based on hierarchical levels, the possibility of evaluating multiple attack scenarios, achieving a database of quantitative and qualitative risk assessments required for further statistical data, uniform treatment of terrorism risk in the critical infrastructure of Romania, integrating information collected from multiple sources into a coherent, efficient connection (information packages restricted network secure intranet) with other information systems.

4. CONCLUSIONS

Assessing the risk level is a key issue of assessment methods. Risk levels classification is the first step in establishing security objectives and security measures that an organization decides to adopt.

These measures are complemented by implementing measures such as technical improvements, implement new features, adapting work procedures and establish staff training programs, all aimed at reducing the level of risk to an acceptable level.

Contributions to tackling decisions under uncertainty for managing extreme risk events are essential in practice because, in the context of technological progress (especially in the field of Communications and Information), the management of these events remains quite inefficient.

In addition, it still lacks a systematic problem-solving of the decisional support at a strategic, tactical or operational level.

MASTER application complements the proposed risk assessment methodology, providing a particularly useful tool for policy makers, efficient and easy to use, with personalization and improvement.

This is the answer to the current requirement of end users to effectively exploit a modular platform, flexible, adaptable and scalable by security managers situated on different levels, including policy makers, central and local authorities in the field.

Through the design and architecture of the instrument's structure an effective technology transfer and a significantly impact on users can be obtained.

The proposed solution enables the rapid improvement of databases in order to reduce the search area track parameters for achieving security.

Inter-connection of input data transfer and exchange of data and displaying the results are controlled by a special sub-operating system (acting as data management, exchange of information between modules and interaction between users).

Flexibility of the system is independent from the further development of subsystems/ security procedures. Dialogue with the user can be done automatically (slideshow maker relevant information in relation to the original data) and interactive (change data and parameters).

The main result is the conception, design and realization of a decision-making tool used to manage extreme risk events.

Decision support is offered at different levels for: data acquisition and processing; analysis and prediction of the risk situation (spatial and temporal distribution) based on modeling and simulation; ranking sets of counter-measures, determining the feasibility and quantify the advantages/ disadvantages; assessing and prioritizing security investment strategies.

MASTER can be used as a decision tool by the national airspace security authorities (Air Force Staff, Ministry of Transport, Ministry of Interior, the Romanian Intelligence Service) aviation security (Aviation Security and Facilities Directorate, ROMATSA administrators airports, airline operators) and air traffic management (Autonomous Civil Aviation Authority, Air Force Staff) in the process of asymmetric extreme crisis management. The application also can be used for educational purposes, proving good information support for research on security and safety in aviation.

BIBLIOGRAPHY

1. Brooks, N., (2003), Vulnerability, Risk and Adaptation: A conceptual framework, Tyndall Centre for Climate Change Research, Working paper no. 38, Norwich, 10-11.

2. Cioacă, C., Boscoianu, M., (2013), Predictive models for extreme risk assessment in aviation system, Proceeding of International Conference on Military Technologies 2013, Faculty of Military Technology, University of Defence in Brno.

3. CSES (Centre for Strategy and Evaluation Services), (2011), Aviation Security and Detection Systems – Case Study, Ex-post Evaluation of PASR Activities in the field of Security & Interim Evaluation of FP7 Research Activities in Space and Security, 3. Available on: http://ec.europa.eu/ enterprise/ policies/ security/files/doc/ aviation_case_study__cses_ en.pdf.

4. Dillon, R.L., Liebe, R. M., Bestafka, T., (2009), Risk-Based Decision Making for Terrorism Applications, Risk Analysis, Vol. 29, No. 3, 329.

5. Druzdel, M.J., Flynn, R.R., (2002), Decision Support Systems, Encyclopedia of Library and Information Science, Editura A. Kent.

6. Haimes, J.Y., Horowitz, B.M., (2004), Adaptive two-players Hierarchical Holographic Modeling Game for Counterterrorism Intelligence Analysis, Journal of Homeland Security and Engineering Management, Vol. 1, No. 3, art. 302.

7. Kahneman, D., (2012), Gândire rapidă, gândire lentă, D. Crăciun version, Publica Publishing House, Bucuresti, 409-528.

8. Smith, V., Mansfield, C.A., Clayton, L.J., (2009), Valuing a homeland security policy: Countermeasures for the threats from shoulder mounted missiles, Journal of Risk and Uncertainty, 38(3), 215-243.

9. Willis, H., Morral, A., Kelly, T., Medby, J., (2005), Estimating Terrorism Risk, MG-388, RAND Corporation, 5-11.