sustainability

MDPI

Article

Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport

Miroslav Kelemen [1], Volodymyr Polishchuk [2,*], Beáta Gavurová [3], Rudolf Andoga [1], Stanislav Szabo [1], Wenjiang Yang [4], John Christodoulakis [5], Martin Gera [6], Jaroslaw Kozuba [7], Peter Kaľavský [1] and Matej Antoško [1]

[1] Faculty of Aeronautics, Technical University of Kosice, 04121 Kosice, Slovakia; miroslav.kelemen@tuke.sk (M.K.); rudolf.andoga@tuke.sk (R.A.); stanislav.szabo@tuke.sk (S.S.); peter.kalavsky@tuke.sk (P.K.); matej.antosko@tuke.sk (M.A.)

[2] Faculty of Information Technologies, Uzhhorod National University, 88000 Uzhhorod, Ukraine

[3] Research and Innovation Centre Bioinformatics, USP TECHNICOM, FBERG, Technical University of Košice, 04001 Kosice, Slovakia; beata.gavurova@tuke.sk

[4] School of Astronautics, Beihang University, Haidian District, Beijing 100191, China; yangwjbuaa@buaa.edu.cn

[5] Faculty of Physics, National Kapodistrian University of Athens, GR-15784 Athens, Greece; ichristo@phys.uoa.gr

[6] Faculty of Mathematics, Physics and Informatics, Comenius University in Bratislava, Bratislava, 84248 Mlynská Dolina, Slovakia; mgera@fmph.uniba.sk

[7] Faculty of Transport, Silesian University of Technology, 44100 Gliwice, Poland; jaroslaw.kozuba@polsl.pl

* Correspondence: volodymyr.polishchuk@uzhnu.edu.ua; Tel.: +380-664207484

Received: 14 June 2020; Accepted: 06 August 2020; Published: 7 August 2020

Abstract: One of the praxeological problems of safe and sustainable air transport (airfreight transport/air cargo, and air passenger transport) is the prevention and management of risks by competent staff, with the support of modern information and communication technologies. This paper presents an educational information model and software for the airport network and information systems risk assessment, primarily intended for aviation education and training of professionals for ensuring safe and sustainable air transport. The solution to the problem is based on the application of the fuzzy logic method in the air transport environment. Based on a fuzzy expert model, the selected scenario, and the input data established separately for airport assets by a group of 23 experts from aviation practice and a university, the following three assessments of airport network information system assets were constructed: Asset A_2 (meteorological information systems) has an insignificant risk with an estimated 0.1162, and assets A_1 (air traffic control and management (ATM), navigational aids and approach) and A_3 (runway monitoring system) received a low risk of airport network and information systems (NIS) security with ratings of 0.2623 and 0.2915, respectively. An airport NIS risk assessment was aggregated (0.2288), indicating a low degree of security risk to the airport's network and information systems. The aggregated risk assessment of airport NIS, including financial loss data, was calculated as 0.1438, representing a low degree of security risk to the airport's network and information systems. Scenarios for evaluating airport assets are changing for students during education. The results of the developed model and its software will be part of the Simulation Center of the Faculty of Aeronautics.

Keywords: airfreight transport; analysis of systems; processes and algorithms; sustainability; risk assessment; network and information systems (NIS); incident rate; airport assets

1. Introduction

In the context of the crisis caused by the COVID-19 pandemic and its consequences, the crucial importance of the sustainable transport of goods in the coordinated activities of international supply chain management has been highlighted more than ever. Airfreight transport (air cargo) is one of the key elements of the global transport system, and an important part of air transport is air passenger transport. According to the International Civil Aviation Organization, today's aircraft move well over USD 5 trillion worth of goods each year by air. Worldwide, air passenger numbers with a small cargo continued to rise, reaching 4.5 billion journeys annual, creating challenges for air cargo and mail security and facilitation, so maintaining or improving all aspects of air cargo safety and air passengers transport security and safety is essential.

The paper presents an information model and software for airport network and information systems risk assessment, primarily intended for aviation education and training of professionals to fulfill such roles for ensuring safe and sustainable air transport.

The focus of the proposed methodology is based mainly on our national 65 years' experience in aviation education and practice with the support of international experience of partners. The Slovak Republic faces specific problems including a lack of multi- and interdisciplinary education of specialists for integrated personal protection, data protection, information protection, airport security, air transport security and safety, flight safety, crisis management, and crime prevention for safe and sustainable air transport. The quality of the training of aviation specialists in this area is important, especially given the potential for loss of life for attacks on aircraft operating systems, air traffic control systems, airport network and information systems (NIS), etc. When we consider the sustainability of air transport, security and safety are at the forefront. Lastly, managing the risks in the field of antibacterial and antiviral protection of persons and contamination of material surfaces in air transport is a challenge, not only during this pandemic period, but also for everyday aviation practice. Finding solutions to the praxeological problem of educating these specialists with the support of current Software (SW) tools remains our challenge.

What is novel in the presented approach? The idea of using fuzzy logic in the security models is not new. The paper expands upon the applications of fuzzy logic theory to the digital space of risk assessment of information systems and data protection within airports and air transport, which it also offers within the simulation center and internationalization of these processes as part of the digital aviation education of aviation specialists. Traditionally, experts are included in the risk assessment strategy and valuation of different aspects of security and safety risks, which is common practice. However, we lack the tools for the multi- and interdisciplinary education of students, the new and future specialists who must be competent and skilled for incorporation into teams for risk assessment strategies and validation of various aspects of security and safety risks in aviation practice. To fulfill these roles in the future, staff need to be selected, educated, and trained, and as members of a multi- and interdisciplinary team of aviation risk assessment experts they must be prepared within multi- and interdisciplinary teams of students from the beginning of their professional careers. The results of the study provide practical tools to support these educational processes of air transport personnel.

The plan was to compare at least three relevant methods with metrics for the objective and comprehensive assessment of the risks and incidents of airport network and information systems (NIS) in the air transport sector. The first part of the study focused on innovative solutions used by fuzzy methods and models for civil airport NIS risk assessment. This paper presents the risk assessment in the first part of the ongoing study. In the second part of the study, we used a fuzzy multi-criterion decision-making method (FMCMD) that we developed. In the third part of the study, we used a selected expert system (rule-based expert system). The knowledge gained in individual research questions allowed the relevant methods for these purposes to be compared and practical conclusions to be drawn. We intend to use these study conclusions for a complex solution for the education at the Simulation Center of the Faculty of Aviation of the Technical University in Košice, Slovak Republic, for the training of aviation specialists in this agenda, and to support the development of methodologies for the creation of intelligent systems for measuring and assessing security aspects of civil airport NIS.

In any intelligent decision support systems, a final decision maker (DM) is required. These systems should help, advise, and raise the level of validity of decision-making. Therefore, the decision support is improved with the formalization of expertise together with the quantitative assessments of various aspects of the assessed object. Air transport businesses need to complement the existing solutions with components responsible for security analysis, attack detection, and risk management in cybercrime prevention to align the information security systems with the current requirements [1,2]. Our research focused on developing risk management technologies with the involvement of NIS expertise in an adaptive approach to airport network security for civil aviation, primarily for air transport.

Overview of Domestic and Foreign Research Studies

The urgency of this task is demonstrated by major global studies and scientific publications assessing the risks of NIS security against various threats related to cybercrime prevention.

Simulation technologies and modeling techniques effectively support the assessment of cyber security risks in aviation [3]. To achieve this, it is recommended to develop, maintain, and apply simulation models and cyber-attack modeling scenarios to connect and develop simulation models from gate to gate, and integrate human interaction with cyber-attack modeling scenarios. Thorough evaluations and reviews of cyber risks for companies with internet access have already been explored, such as a recent study presenting a cyber risk vulnerability management software platform for simplifying and improving automation and continuity in cybersecurity assessment [4], also offering risk assessment and classification to the user. Bayesian networks, with various types of induced uncertainty with simplicity of criteria, have also been successfully used in the construction of an expert model for the analysis of cyber threats [5]. This means a fuzzy set of theories should be used to reflect knowledge of an object [6].

To properly assess the risk of airport NIS, it is necessary to learn how to scientifically model information uncertainty by drawing the formally described boundaries between reliable knowledge, knowledge with a certain level of reliability, and what is unknown [7]. To do this, the fuzzy-plural descriptions are used to model uncertainty [8,9]. For example, the fuzzy-plural description works on current information systems and technology [10] or artificial intelligence systems and decision support [11] on fixed point theorems in fuzzy metric spaces [12] or expert information using fuzzy logic [13], considering the general ideas and benefits underlying the current views on the use of fuzzy logic in the decision support systems, as Skorupski J. and Uchrońsk P. [14] presented a model fuzzy logic model supporting the management of a security screening checkpoint's organization at an airport, but only the role of the human factor was considered.

Cyber-attacks and incidents cause financial losses, but obtaining this business information is difficult. For example, Zurich Insurance Company in the U.K. reported that nearly 850,000 small- and medium-sized businesses were being hit by cyber-attacks, with more than one-fifth of the companies suffering losses of more than USD 13,000 and 1 in 10 companies losing more than USD 69,000 [15]. The 2017 Ponemon data leak damage study found that the average total cost for large companies was approximately USD 3.62 million. According to the findings of the study on global costs related to data leaks, the average cost of cyber-attacks more than doubled between 2014 and 2015, while the average cost of lost or stolen records increased slightly to nearly USD 41 [16]. In the 2018 study, the average cost of a data breach per compromised record was USD 148, and it took an average of 196 days for organizations to detect breaches. The 2019 report found that the average total cost of a breach ranges from USD 2.2 million for incidents with less than 10,000 compromised records to USD 6.9 million for incidents with more than 50,000 compromised records [17]. The 2018 study covered 477 organizations, including data on mega breaches for the first time. Although the cost per record remained consistent at USD 148, large-scale breaches of 50 million records could cost companies over USD 350 million [18]. As DeBrusk Ch. and Mee P. [19] correspondingly reported, the amounts spent by companies in an attempt to protect themselves is also large, estimated at approaching USD 1 trillion annually on a global basis by 2022.

Today, no single method is available for creating risk management technologies by involving expertise using an adaptive approach. An expert model for assessing the risks and incidents of airport NIS using fuzzy sets is an urgently required task to improve civil aviation information security.

This paper is organized as follows. In Section 2, we describe the formal problem statement and the model of input data for assessment of the situation provided by a group of experts based on their knowledge, skills, and at least 15 years of practical experience. We present the fuzzy expert model for incident and risk assessment of airport NIS security for civil aviation. In Section 3, we outline the simulation experiment. In Section 4, we discuss the results of the expert model and its SW developed in the study. In Section 5, we conclude the paper and present the main results. We expand the ideas for future work and improvements.

2. Model of Experts' Input Data for Selected Airport Assets Assessment Scenarios

2.1. Formal Problem Statement, and Model of Input Data

Suppose we have a set of information assets of civil aviation security [2] $A = \{A_1; A_2; \ldots; A_n\}$, for which many threats to the security of personal data of network and information systems have been identified (the airport network threats in real-time, malicious or anomalous patterns, airport security threats, air transport security and safety threats, aviation communication systems threats, air traffic control threats, the threat of fraudulent acquisition and use of air passengers' private identification information, airport health threats including antibacterial and antiviral protection, etc.) $K = \{K_{i1}; K_{i2}; \ldots; K_{im}\}$, $i = \overline{1, n}$. Every security threat K_{ij} for an asset A_i, $(i = \overline{1, n}, j = \overline{1, m})$ is assessed by a group of experts in the form of the input data $(T_{ij}; \mu_{ij})$, $(i = \overline{1, n}; j = \overline{1, m})$. The input data have the following meanings:

- T represents the consequences of threat implementation K of airport NIS personal data security. This indicator is defined as the value of the next term set: $T = \{M; \quad A; \quad H; \quad C\}$, where M is the minimal consequences of the threat, A is the average consequences of the threat, H is the maximum consequences of the threat, and C is the critical consequences of the threat.
- μ is the degree of possibility of occurrence of an NIS airport threat. This parameter belongs to the interval [0; 1], with different values having the following content: 0 indicates it is impossible that the threat will occur, 0.4 indicates a minimal possibility of the occurrence of the threat, 0.6 indicates average threat occurrence possibility, 0.8 indicates high threat occurrence possibility, and 1 indicates critical occurrence of the threat.

For each asset, we have L, which indicates the severity of the incident's consequences for the asset. This indicator is defined as the value of the next term set: $L = \{V; \quad C; \quad U\}$, where V is vital (if its failure lasts more than 2 h as too many flights will be delayed immediately and then canceled), C is critical (if its failure cannot last more than 24 h because too many flights will be delayed), and U is useful or not applicable [2].

Based on the input of expert data, we assessed the security risk of personal data of airport NIS $R = \{R_1; R_2; \ldots; R_n\}$ separately for assets, calculated financial loss incidents (probability of occurrence of risk) for assets $Z = \{Z_1; Z_2; \ldots; Z_n\}$, and constructed one aggregate estimate $Y \in [0; 1]$ to make additional decisions to prevent cybercrime. The solution to this problem can be demonstrated in the form of a structural diagram of the expert model for evaluation of the civil airport NIS security to support security management with ensuring safe and sustainable air transport (Figure 1).