MODEL OF RELIABILITY OF SECURITY CONTROL OPERATION AT AN AIRPORT

Artur Kierzkowski

Preliminary communication

The aim of the operation of the security control system at an airport is the prevention of the introduction of forbidden objects to the restricted area of the airport or onto the plane. All passengers and their luggage undergo security control. The security control system is a very specific system. On the one hand, the security control must be performed effectively so as to eliminate forbidden objects during the inspection and, on the other hand, it should be efficient so that the passenger who has checked in his/her luggage does not cause the aircraft to be delayed by a long wait. The criteria mentioned above are in conflict. For this reason, the study proposes a multi-criteria model of reliability of the security control operation, which takes into account both the timeliness and effectiveness of the control process as well as the reliability of devices that are used to perform security control. The developed model was used to evaluate the operation of the security counters at the Wrocław airport. The model makes it possible to assess the influence of security control operators' qualifications (their effectiveness) on the reliability of the control.

Keywords: airport; case analysis; reliability; security control; socio-technical system

Model pouzdanosti djelovanja sigurnosne provjere na aerodromu

Prethodno priopćenje

Cilj sigurnosne provjere na aerodromu je sprječavanje unošenja zabranjenih predmeta na ograničeno područje aerodroma ili u zrakoplov. Svi putnici i njihova prtljaga prolaze sigurnosnu provjeru. Sustav te provjere je vrlo specifičan sustav. S jedne strane sigurnosna se provjera mora obaviti učinkovito kako bi se odstranili zabranjeni predmeti tijekom pregleda, a s druge strane treba biti učinkovita tako da zbog putnika koji je prijavio pregled prtljage avion ne treba kasniti. Gore spomenuti kriteriji su proturječni. Zbog toga se u radu predlaže model pouzdanosti sigurnosne provjere s više kriterija koji uzima u obzir pravovremenost i učinkovitost postupka provjere kao i pouzdanost uređaja koji se koriste za sigurnosnu provjeru. Razvijeni je model primijenjen u procjeni funkcioniranja sigurnosnih pultova na aerodromu u Wrocławu. Model omogućuje procjenu utjecaja kvalifikacija djelatnika sigurnosne provjere (njihovu učinkovitost) na pouzdanost provjere.

Ključne riječi: aerodrom; analiza slučaja; društveno-tehnički sustav; pouzdanost; sigurnosna provjera

1 Introduction

The security control system at an airport is the key element of the air transport system operation. The necessity to perform security control is regulated by a number of international regulations, which define procedures related to the passenger flow and baggage control at airports. The Regulation of the Minister of Transport [1] is the main act defining the responsibility for keeping an appropriate level of air transport security in Poland. This act refers to regulations [2, 3, 4] that define detailed security control procedures the airport operator is obliged to follow.

The commission on implementing Regulation No. (EU) 2015/1998 [4] imposes on airport managers the obligation to designate boundaries between the landside and the airside. Access to the landside area of an airport is possible after checking authorized persons and after a security check. The aim of the security control process is the prevention of forbidden objects specified in [1].

The influence of various factors on the efficiency of the process of securing an airport is described in the study by [5]. An interesting conclusion drawn from the analysis conducted was that the assignment of weights to specific activities carried out within security systems showed that the security of passengers and luggage is the priority of activities aimed at ensuring an appropriate level of safety.

Security control of passengers can be conducted using [1]:
- a walk-through metal detector (WTMD),
- a manual search,
- security scanners,
- devices for detecting trace amounts of explosives (ETD) combined with a hand-held metal detector,

- dogs detecting explosives in combination with a manual search.

Security control of cabin baggage is conducted using [1]:
- an X-ray device,
- a manual search,
- systems for the detection of explosives,
- dogs detecting explosives in combination with a manual search.

Dogs and devices for detecting trace amounts of explosives can be used only as additional security control measures. Both passenger and luggage control will have a positive result only if the process operator can unambiguously decide that the requirements of the control process have been met. Each negative signal from control devices must be identified and eliminated. Otherwise, the passenger or the luggage goes through subsequent control or is refused admittance onto the aircraft.

As shown in the report [6], the problem of timely passenger service at an airport does not only concern large airports, but also small ones with low traffic. The London Heathrow airport, which serves over 70 million passengers a year, was ranked among 20 airports with the greatest delays, as was the Lisbon airport, which serves only 16 million passengers. Among the top 20 airports generating the greatest disturbances in departures, there were airports causing delays within the range of 34 to 55 % of the served air operations. Passenger service delays are generated at various stages of their service: check-in, security control, ground handling.

The security control system is highly specific as:

- security control must be performed in a way that guarantees the elimination of all forbidden objects in air transport,
- security control must be efficient to prevent generation of delays in the aircraft departure.

The security control system may be described as a socio-technical system, which is defined as the Man-Technical Facility pair performing its task in the surrounding area. The surrounding area includes everything that is situated outside the Man-Technical Facility System [7]. A technical facility, on the other hand, is an object of human activity intended for the performance of specific tasks with certain features and functions purposefully assigned to it by man [7]. The system is a collection of elements and relationships between them [7]. Man, in the socio-technical system, fulfils the role of an element of the system on the one hand, while on the other hand he fulfils the function of the technical facility operator in relation to the surrounding area.

The socio-technical system (*STS*) can be defined as [7]:

$$STS = \langle O; T; P; R \rangle, \tag{1}$$

where:
$O = \{O_i\}$, $i = 1, 2, …, n$ - the set of all operators in the socio-technical system,
$T = \{T_j\}$, $j = 1, 2, …, m$ - the set of all technical facilities in socio-technical system,
$P = \{P_k\}$, $k = 1, 2, …, o$ - the set of all tasks in the socio-technical system,
$R = \{R_l\}$, $l = 1, 2, …, p$ - the set of all relationships in the socio-technical system,

Operators $\{O_i\}$ of the system are security control employees who take care of passenger service and the baggage-handling process. Technical facilities $\{T_j\}$ are passenger control devices (e.g. WTMD) and baggage control devices (e.g. X-ray).

The reliability of the socio-technical system depends on:
- reliability of the technical facility - R_T,
- reliability of the operator – R_O,
- reliability of timely performance of the task – R_P.

The reliability of the technical facility (e.g. a WTMD device), R_T, is defined as a property characterising the ability of the facility to perform complex functions within specified time limits and defined on operational conditions. The most frequently used indices of the assessment of reliability of a technical facility include: the reliability function, the damage intensity function, etc.

The operator's reliability, R_O, is related to the operator of the technical facility (e.g. the operator of the X-ray device). The following methods are usually used in the literature to assess the operator's reliability: HRA, THERP, HEART, HCR etc. These methods allow for defining the probability of an error being committed by the operator.

The reliability of timely performance of the task, R_P, is defined as the probability that a task will be performed sooner than assumed.

2 Overview of the state of research

The literature review is divided into three basic areas:
- the operation of the security control system as an element of airport operation,
- the principles of socio-technical system modelling,
- modelling of human factor reliability.

The essential features of a system supporting the operation of the airport terminal are presented in [8]. The authors pay special attention to the security control system as an element, which, as a result of research, generates the greatest delay among elements of the terminal infrastructure. Apart from the model of the security control system operation, statistical data concerning the operation of this subsystem is presented. Wilson et al. [9] present a two-lane security control counter model. The developed model, together with models of check-in desks, was implemented in a simulation environment. The developed application allowed an analysis of a passenger flow and the pinpointing of bottlenecks. A microscopic model of the security control system based on the control process diagram is presented in [10]. Data concerning the implementation of the control process on individual devices (WTMD, ETD etc.) was presented. Input data for the model (pre-screening, alarm rates etc.) was presented together with results. The model made it possible to determine the passenger's waiting time for the security check, depending on the number of employees performing the manual search. The developed model [10] made it possible to designate: average wait time [min./PAX], average maximum wait time [min./PAX], average service time [min./PAX], average queue length [PAX], and average maximum queue length [PAX]. The model for the assessment of the effectiveness of the security control system is presented in [11]. The model, which is based on fuzzy logic, takes into account both technical and human factors. The developed model was used for the evaluation of the operation of the security control checkpoint at the Katowice airport. As a result, quantitative ratings of the level of safety were obtained, expressed as the efficiency of the system for detecting prohibited articles in cabin baggage. Kierzkowski et al. [12] present characteristics of the security control system operation. The developed model was verified on the basis of the security control system at the Wrocław airport. The developed model made it possible to estimate the throughput of the security control, depending on its configuration. Sample characteristics of the security control system are presented in [13]. In the study [13], density functions of the probability of the time of performing activities by security control operators and passengers were presented. Security control procedures were identified in accordance with [2], [3]. Maintaining the desired security level is an important functional aspect of the air transport system operation. These aspects were discussed in [14, 15, 16]. The reliability of the implementation of security control by the operator is assessed by the analysis of the TIP system. TIP (Threat Image Projection) is a system installed in an X-ray device, which has a built-in library of over 1,000 3-dimensional objects [14], which are dangerous in air transport (e.g. weapons). At random moments, this system

plots the image of one of the objects that is dangerous in air transport on the image of the baggage. The security control operator's task involves marking the image, in which a forbidden object can be seen within the assumed time ranging from 3 to 5 seconds [15]. According to [4], the airport administrator has to store data for a year. Each security control operator has his/her number, for which the system allows for preparing reports on the response time and reliability. In [14, 16], the authors indicate high diversity of security control reliability. There is a group of operators for whom the probability of detecting a dangerous object ranges from 0.98 to 1; however, there are single operators for whom this value is only 0.8.

The modelling of the socio-technical system is broadly discussed in world literature. In [17], the authors present a literature review of socio-technical system modelling methods. Comments on currently-used methods are presented and guidelines for the modelling of such systems are defined. The quantitative approach to the assessment of the socio-technical system operation is described in [7]. It has been shown that human perception is a function that depends on personal experience and mental flexibility. The authors claim it is necessary to assign weights to individual variables. Instead of the classical approach (the social, technical and natural environment), the authors in [18] propose a division of the socio-technical system into three groups of objects: static objects (object relationships, object definition), dynamic objects (events, activities, processes) and behaviour objects (performance, matrices). Thus, for SCO, these are security control objects and procedures influencing the level of security and capacity. In this way, the study [18] became the basis for developing a model of security control system readiness. The division of the system was implemented in the following models: the Business Process Modelling Notation (BPMN) model, Hybrid Queue-Based Bayesian Network (HQBN) model and the Agent-Based Model (ABM).

The current status of knowledge on human reliability analysis is very broad. Over 70 methods have been developed according to the world literature [19]. A large number of models based on the developed methods reveal that a large number of the models rely on basic methods, which are adjusted to the assessment of the functioning of selected systems. TESEO and HEART belong to basic methods used. The TESEO method (Tecnica Empirica Stima Errori Operatiori) was presented in [20]. This method assumes that the probability of the operator's error – human error (HE) depends on five factors: the type of action taken, the time available to perform an action, the operator's preparation, the operator's emotional state, ergonomic characteristics of the environment. The application of the method is presented in [21], where the assessment of committing an error involving an attempt at take-off at an inappropriate speed has been done. The HEART method (Human error assessment and reduction technique) is presented in [22]. This technique takes into consideration the operator's tasks as well as the environment (ergonomic and environmental factors). Conditions that have a disadvantageous effect on human actions are also considered. The HCR method (Human Cognitive Reliability) is presented in [23]. Just like the TESEO method, the HCR method allows for determining

the operator's reliability, taking into account time limitations. This method takes into account the operator's experience of the stress level and its ergonomic quality. The THERP method (Technique of Human Error Rate Prediction) was presented in [24]. This method proposes an approach based on event trees. On their basis, it is possible to determine the probability of succeeding in performing a specific task. Also, the Performance Shaping Factors (PSF) are taken into consideration. The determination of the probability of successful task performance involves the construction of a tree of events and the determination of nominal probabilities of human errors. The THERP method can be compared to the decomposition approach, as a result of which this method has a significantly broader scope of analysis than other techniques.

An analysis of the literature on the assessment of the security control system operation shows that there is no model that would take into account both aspects of reliability of the device and reliability of timely task performance as well as aspects of correct performance of the security control process. It is particularly important that the timely performance of the passenger service process in the security control system should be considered together with the effectiveness of the control to identify hazardous (forbidden) objects in air transport (both for baggage and passengers).

3 Multi-criteria model of the reliability of the security control system at the airport

The reliability of the security control system is described by three events:
- A − an event involving timely performance of the passenger's security check,
- B − an event involving the absence of an error committed by the security control operator during the process of acceptance, analysis and decision-making,
- C − an event involving the absence of damage to a technical device in the security control system within specified time limits.

The reliability of the security control system should be defined as:

$$R = P(A \cap B \cap C). \tag{2}$$

Assuming the independence of events, the reliability of the security control system will have the following form:

$$R = P(A) \cdot P(B) \cdot P(C). \tag{3}$$

The reliability of the security control system can be considered according to two variables: time and the number of passengers. It is more advantageous to consider the reliability of a security control according to the number of passengers served, as it is a system with high fluctuations of intensity of passenger reports for the control in time. While considering the reliability of the security control in relation to the number of passengers, the assessment of its operation is independent of the

intensity of reports in time. Such analyses were performed in [25, 26].

The reliability of timely passenger service R_P in the security control model is defined as the probability that the passenger is n^{th} served in a timely manner.

$$R_P = P(A). \tag{4}$$

Thus, the function of a timely security control process $R_P(n)$ has the following form:

$$R_P(n) = P(N_P \geq n), \tag{5}$$

where: N_P is a random variable of the number of passengers served in a timely manner.

Reliability of effective security control R_O is the probability that operators will not commit an error for passenger n^{th}. Security control operators can commit various errors defined by events $\overline{B}_1$, $\overline{B}_2$, $\overline{B}_3$, $\overline{B}_4$.

The event $\overline{B}_1$ means that the RTG operator will have a projection of the TIP image and will not indicate it. The probability of such an event is marked as $P(\overline{B}_1)$. For an event defined in this way, the reliability function has the following form:

$$R_O^{B1}(n) = 1 - P(N_{\overline{B}_1} \geq n), \tag{6}$$

where: $N_{\overline{B}_1}$ is a random variable of the number of passengers for whom foreign objects were displayed on the screen of the device, and the baggage control operator did not take action to identify them.

The event $\overline{B}_2$ means that the RTG operator will not have a projection of the TIP image; however, he will indicate that there was such a projection. The probability of such an event is marked as $P(\overline{B}_2)$. For an event defined in this way, the reliability function has the following form:

$$R_O^{B2}(n) = 1 - P(N_{\overline{B}_2} \geq n), \tag{7}$$

where: $N_{\overline{B}_2}$ is a random variable of the number of passengers, for whom no foreign objects were displayed on the screen of the device, but the baggage control operator took action to identify it.

The event $\overline{B}_3$ means that the operator, after referring baggage to a manual search, will not detect a forbidden object. The probability of such an event is marked as $P(\overline{B}_3)$. For an event defined in this way, the reliability function has the following form:

$$R_O^{B3}(n) = 1 - P(N_{\overline{B}_3} \geq n), \tag{8}$$

where: $N_{\overline{B}_3}$ is a random variable of the number of passengers for whom the operator did not detect a forbidden object in air transport after referring baggage to a manual search.

The event $\overline{B}_4$ means that the operator, after referring a passenger to a manual search, will not detect a forbidden object by them. The probability of such an event is marked as $P(\overline{B}_4)$. For an event defined in this way, the reliability function has the following form:

$$R_O^{B4}(n) = 1 - P(N_{\overline{B}_4} \geq n), \tag{9}$$

where: $N_{\overline{B}_4}$ is a random variable of the number of passengers for whom the manual search operator did not detect a forbidden object in air transport.

Assuming the independence of events, the reliability of effective security control R_O has the following form:

$$R_O = \bigcap_{i=1}^{4} \left(1 - P\left(\overline{B}_i\right)\right). \tag{10}$$

The function of a timely security control process $R_O(n)$ has the following form:

$$R_O(n) = \prod_{i=1}^{4} \left(1 - P\left(N_{\overline{B}_i} \geq n\right)\right). \tag{11}$$

The reliability of security control devices R_T (X-ray device and walk-through detector) is defined as the probability that the device will become damaged while serving passenger n^{th}.

$$R_T = P(C). \tag{12}$$

Thus, the reliability function of the security control device $R_T(n)$ has the following form:

$$R_T(n) = P(N_T \geq n), \tag{13}$$

where: N_T is a random variable of the number of passengers for whom the device worked in a failure-free manner.

The function of the reliability of the security control system that takes into account the assumptions above has the following form:

$$R_{SC}(n) = R_P(n) \cdot R_O(n) \cdot R_T(n). \tag{14}$$

4 Model application – Wrocław airport

The security control system at the Wrocław airport is based on two-lane security control counters. The diagram of a two-lane counter is presented in Fig. 1.

A passenger queuing for security control checks the availability of one of the entry areas. If it is available, the preparation process for the security control begins in accordance with the security control employee's instructions (Operator 1). At the next stage, the passenger prepares for the metal detector (WTMD) control. What is important, the availability of one of two operators (Operator 4) allows the passenger to pass through to the walk-through metal detector. If the detector did not

indicate the necessity for a manual inspection, the passenger goes to the baggage-waiting area. If the metal detector has shown the necessity for performing a security control, it is done in the manual control area by one of two operators (Operator 4). The metal detector is not available for the next passengers when two operators are performing a manual inspection. After the manual control, the passenger goes to the baggage-waiting area or to the baggage collection area. At the same time, the baggage is checked on an X-ray device by Operator 2. If this operator indicates that it is necessary to perform a manual search of the baggage, it is performed by Operator 3 in the presence of the passenger to whom the baggage belongs.
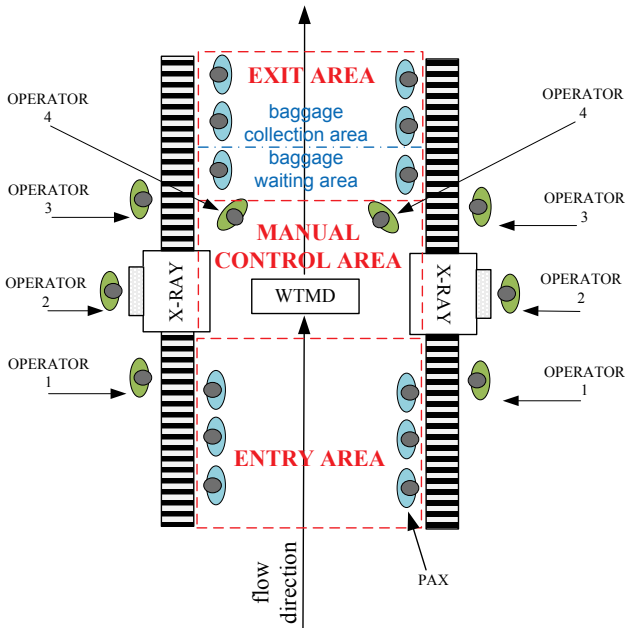
Figure 1 The diagram of security processes control implementation at a two-stream point

The reliability of timely performance of the passenger service process, R_P in the security control system was determined on the basis of research performed at the Wrocław airport. It results from the research performed that the security control process is performed in a timely manner if it does not last longer than 8 minutes [13] (from the time the passenger approaches the point until they leave with their baggage to the checkpoint), assuming the service time of 8 minutes results from the research conducted. Passengers served in a period shorter than 8 minutes indicated in surveys that the service took a short amount of time. Using the simulation model of the security control [12], the reliability function of a two-lane security control counter was determined, which has the following form:

$$P_P(n) = 1 - \phi\left(\frac{\ln(n - 3.2) - 26.2}{0.74}\right), \qquad (15)$$

where:

$$\phi(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_0^x e^{-\frac{t^2}{2}} \, dt.$$

The input data of the simulation model [13] was estimated on the basis of a sample including 15,000 passengers. The tests were performed at the Wrocław Airport in 2016. The obtained characteristics were implemented into the model [13]. One thousand repetitions of the computer simulation were performed. On the basis of the observations made, the function of the reliability of timely security control was determined. Compliance between theoretical and empirical courses was verified using the λ-Kolmogorov test at the significance level of $\alpha = 0.05$. The value of test statistics was 0.516 for the limit value $\lambda_{0.05} = 1.36$. The compliance test showed correct approximation of the empirical distribution indicated by the theoretical distribution. The function of the reliability of timely security control, together with a 95 % confidence interval, which was determined in accordance with [27], is presented in Fig. 2.
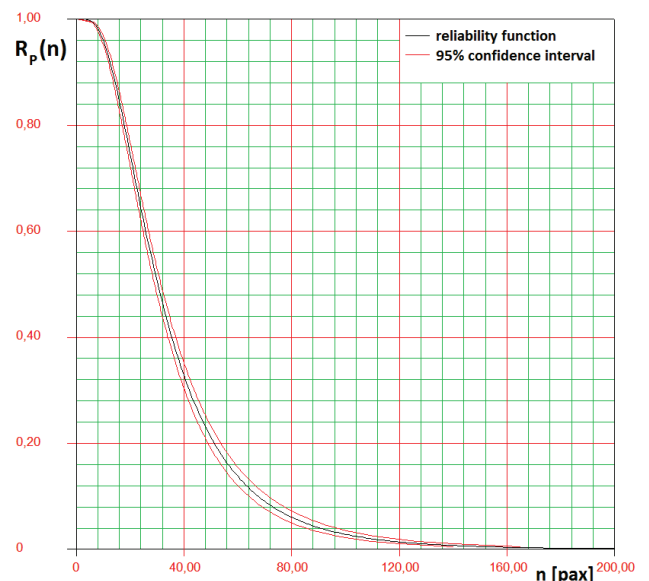

Figure 2 Function of reliability of timely security control

The function of the reliability of timely security control is close to zero for $n = 125$. If the number of persons waiting for a control is higher than this value, the probability that they will be served in a timely manner is very low. For values $n = 20$, the probability of a failure to perform a timely security control is as high as 25 %.

The reliability of effective security control was determined:
- theoretically using the TESEO and HEART methods,
- empirically on the basis of statistics of effectiveness of the security control by the operator as shown in [11, 28].

On the basis of the TESEO tables [21], the following assumptions were adopted that best describe the system under analysis:
- $K_1 = 0.01$ – operation requires concentration,
- $K_2 = 10$ – the available time is longer than 2 seconds,
- $K_3 = 0.5$ – the operator is an expert,
- $K_4 = 2$ – a potential threat situation may occur,
- $K_5 = 1$ – ergonomic factors at a good level.

On the basis of the assumptions above, the unit probability of committing an error by the operator:

$$P = K_1 K_2 K_3 K_4 K_5 = 0.01 \cdot 10 \cdot 0.5 \cdot 2 \cdot 1 = 0.1 \qquad (16)$$

By analysing the reliability of the security control operator's work using the HEART method, the following assumptions were adopted on the basis of [29]:
- Class G = 0.0004 tasks – Routine tasks, well-practised,
- Additionally, corrective factors were selected: a short detection time $E = 11$ and $P = 1$ due to the fact that the detection time is limited significantly.

The value of influence coefficients was calculated according to:

$$AE = ((E-1) \cdot P) + 1 = ((11-1) \cdot 1) + 1 = 11 \qquad (17)$$

The unit probability of committing an error by the operator:

$$P = G \cdot AE = 0.004 \cdot 11 = 0.044 \qquad (18)$$

On the basis of empirical data [11, 28] and on the basis of the research performed, the probabilities of events were determined:
- $P(\overline{B}_1) = 0.0055$,
- $P(\overline{B}_2) = 0.0143$,
- $P(\overline{B}_3) = 0.0005$,
- $P(\overline{B}_4) = 0.0010$.

Table 1 Probability values for individual events and of reliability of effective security control, depending on the method of its designation

| Probability of event / Reliability	A method for determining probability values		
	TESEO	HEART	Empirical
$P(\overline{B}_1)$			0.0055
$P(\overline{B}_2)$	0.1	0.044	0.0143
$P(\overline{B}_3)$			0.0005
$P(\overline{B}_4)$			0.001
R_O	0.6561	0.8353	0.9788

The reliability value of the security control for theoretical and empirical data differs significantly. The TESEO and HEART methods lead to considerable errors in the assessment of the checkpoint operation.

The function of reliability of timely security control was determined using empirical data due to a large amount of data and its resultant high reliability. The function has the following form:

$$R_O(n) = e^{-0.0212n}. \qquad (19)$$

The function of reliability of effective security control was estimated on the basis of a sample including 15,000 passengers. It was checked whether the security control operator committed an error and, if applicable, what kind of error it was. Additionally, the results of research described in [11, 28] were used. Compliance

between theoretical and empirical courses was verified using the λ-Kolmogorov test at the significance level of α = 0.05. The value of test statistics was 0.239 for the limit value $\lambda_{0.05} = 1.36$. The compliance test showed the correct approximation of the empirical distribution indicated by the theoretical distribution. The function of the reliability of effective security control, together with a 95 % confidence interval, which was determined in accordance with [30], is presented in Fig. 3.
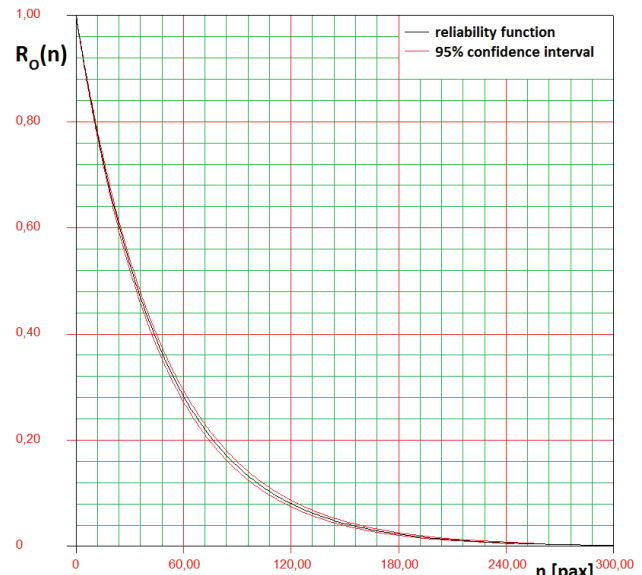
Figure 3 Function of reliability of effective security control

The function of reliability of effective security control is close to zero for n = 240. If a checkpoint serves more than 240 persons, it is virtually certain that the security control operator commits one of the errors listed above. For the value n = 20, the probability of committing one of such errors is as high as 35 %.

The reliability of the security control device (an X-ray device and a walk-through detector) was determined on the basis of empirical data obtained during the research [13]. The probability of the lack of damage to the device is:

$$R_T = P(C) = 0.999 \qquad (20)$$

The reliability function of the security control device has the following form:

$$R_T(n) = e^{-0.001n}. \qquad (21)$$

The reliability function of the security control device was estimated on the basis of a sample of approx. 1 million passengers. Information was collected on how many passengers were tested by the WTMD gate and how many passengers were checked by an X-ray device. Also, data concerning the breakdowns of devices were collected. Compliance between theoretical and empirical courses was verified using the λ-Kolmogorov test at the significance level of α = 0.05. The value of test statistics was 0.349 for the limit value $\lambda_{0.05} = 1.36$. The compliance test showed correct approximation of the empirical distribution indicated by the theoretical distribution. The

function of the reliability of the device together with a 95 % confidence interval, which was determined in accordance with [30] is presented in Fig. 4.
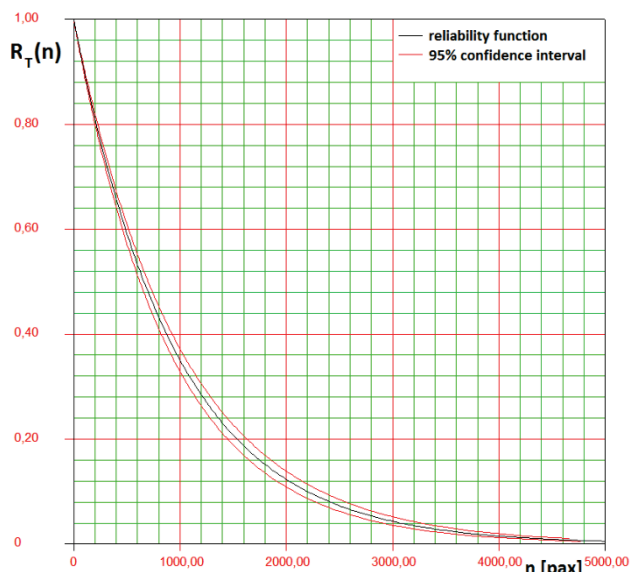

Figure 4 Function of reliability of the security control device

The values obtained from the security control device reliability are several orders of magnitude higher than for (15) and (19). Thus, the influence of the reliability of the device is rather small.

The reliability function of the security control will have the following form:

$$R_{SC}(n) = R_P(n) \cdot R_O(n) \cdot R_T(n). \tag{22}$$

The function of the reliability of the control together with a 95 % confidence interval, which was determined in accordance with [30], is presented in Fig. 5.
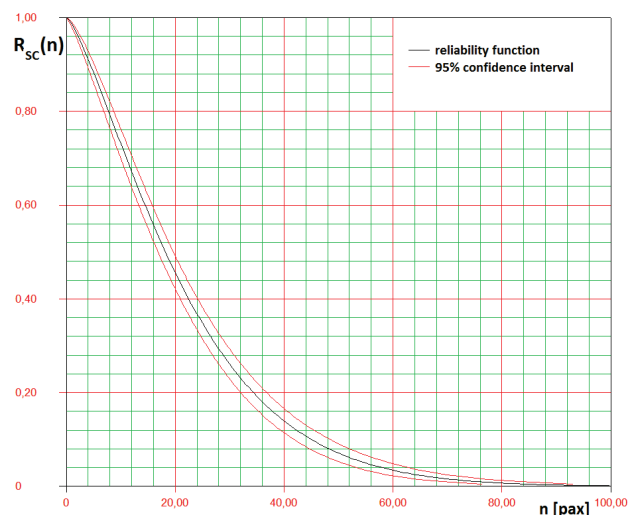

Figure 5 Function of security control reliability

As it can be noticed in Fig. 5, the reliability of the security control if $n = 20$ passengers is approx. 0.45, while for $n = 40$, it amounts only to 0.14. The key aspect of the possibility of analysing the results obtained is narrow (± 0.02) confidence limits.

5   Conclusion

The study presents a model of the security control reliability, which takes into account the timeliness and effectiveness of the security control process implementation as well as reliability of devices. The proposed model was used for the evaluation of the operation of the security control checkpoint at the Wrocław airport. For this system, individual functions of reliability and their confidence intervals were determined on the basis of empirical data. Additionally, the probability of committing an error by the security control operator obtained from the theoretical TESEO and HEART methods was compared with empirical values. The operator's error was assessed in a group of security control operators. This group included both experienced operators and beginners. The developed model also makes it possible to estimate the influence of the operator's qualifications and reliability of the device on the reliability of the security control.

Furthermore, the developed model of the security control will also make it possible to develop guidelines pertaining to the configuration of a security control system (which consists of m lanes). Characteristics of the reliability function have a significant influence on decisions made by the manager of the security control system. In particular, they answer the question of whether it will be a better solution to raise the operators' qualifications and how this will affect the reliability of the system, or perhaps it is necessary to increase the number of security control lanes or replace devices.

Further work will be performed to develop a modelling method for the security control system to obtain an acceptable reliability level, taking into account the stream of passenger reports. The research will be conducted to check for the existence of independent events and the influence of the reliability of the device on the timeliness of the passenger's security control.

Acknowledgements

6   References

[1] Dziennik Ustaw. The Regulation of the Minister of Transport, Construction and Maritime Economy of 31 July 2012 on the National Civil Aviation Security Program. Journal of Laws of the Republic of Poland 2012, Item 912.
[2] EC, Commission Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.
[3] EC, Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council.

[4] EU, Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security

[5] Yu M.M., Assessment of airport performance using the SBM-NDEA model. Omega, 38, 2010: 440-452. https://doi.org/10.1016/j.omega.2009.11.003

[6] Eurocontrol, CODA Digest, All-Causes Delay and Cancellations to Air transport in Europe. 2013. URL: https://www.eurocontrol.int/sites/default/files/publication/files/coda-digest-annual-2013.pdf

[7] Schöttl, F.; Lindemann, U. Quantifying the Complexity of Socio-technical Systems – A Generic. // Interdisciplinary Approach, Procedia Computer Science, 44, (2015), pp 1-10, https://doi.org/10.1016/j.procs.2015.03.019

[8] Schultz, M.; Fricke, H. Managing passenger handling at airport terminals. // Proceedings of Ninth USA/Europe Air Traffic Management Research and Development Seminar / Berlin, 2011.

[9] Wilson, D.; Roe, E. K.; So, S. A. Security checkpoint optimizer (SCO): an application for simulating the operations of airport security checkpoints. // Proceedings of Int. Winter Simulation Conference / 2006, pp. 529-535. https://doi.org/10.1109/WSC.2006.323126

[10] van Boekhold, J.; Faghri, A.; Li, M. Evaluating security screening checkpoints for domestic flights using a general microscopic simulation model. // J. Transport. Security. 7, (2014), pp. 45-67. https://doi.org/10.1007/s12198-013-0129-8

[11] Skorupski, J.; Uchroński, P. A fuzzy reasoning system for evaluating the efficiency of cabin baggage screening at airports. // Transportation Research Part C: Emerging Technologies. 54, (2015), pp. 157-175. https://doi.org/10.1016/j.trc.2015.03.017

[12] Kierzkowski, A.; Kisiel, T. An impact of the operators and passengers behaviour on the airport's security screening reliability. // Safety and Reliability: Methodology and Applications, Proceedings of the European Safety and Reliability Conference, ESREL 2014 / Wrocław, 2015, pp. 2345-2354.

[13] Kierzkowski, A.; Kisiel, T. Determination of the basic characteristics for security screening in winter air season, using simulation model of combined counter. // Scientific Papers of Warsaw University of Technology. Transport, 103, (2015), pp. 113-123. (in Polish)

[14] Hofer, F.; Schwaninger, A. Using threat image projection data for assessing individual screener performance. // Safety and Security Engineering. WIT Transactions on The Built Environment. 82, (2005), pp. 417-426.

[15] Schwaninger, A. Increasing effectiveness and efficiency in airport security screening. // Safety and Security Engineering. WIT Transactions on the Built Environment. 82, (2005), pp. 405-416.

[16] Schwaninger, A. Training of airport security screeners. // Airport. 5, 2003, pp. 11-13.

[17] Baxter, G.; Sommerville I. Socio-technical systems: From design methods to systems engineering. // Interacting with Computers, 23, 1(2011), pp. 4-17. https:// doi.org/10.1016/j.intcom.2010.07.003

[18] Wu, P. P. Y.; Fookes, C.; Pitchforth, J.; Mengersen, K. A framework for model integration and holistic modelling of socio-technical systems // Decision Support Systems, 71, (2015), pp. 14-27. https:// doi.org/10.1016/j.dss.2015.01.006

[19] Bell, J.; Holroyd, J. Review of human reliability assessment methods, Health and Safety Laboratory, HSE Books, 2009.

[20] Bello, G.C.; Colombari, C. The human factors in risk analyses of process plants: the control room operator model, TESEO. // Reliability Engineering. (1980), pp. 13-14. https://doi.org/10.1016/0143-8174(80)90010-4

[21] Cacciabue, P. C. Risk Analysis in Take-Off Procedure with Electronic Flight Bag. Politecnico Di Milano Books, 2012.

[22] Williams, J. C. HEART – A proposed method for achieving high reliability in process operation by means of human factors engineering technology. // Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society (SaRS) / Birmingham, 1985.

[23] Hannaman, G. W.; Spurgin, A. J.; Lukic, Y. D. Human cognitive reliability model for PRA analysis. // Draft Report NUS-4531, EPRI Project RP2170-3. Electric Power and Research Institute: Palo Alto / CA, 1984.

[24] Swain, A. D.; Guttmann H. E. Handbook of human reliability analysis with emphasis on nuclear power plant applications. // US Nuclear Regulatory Commission / Washington, 1983. https://doi.org/10.2172/5752058

[25] Kowalski, M.; Magott, J.; Nowakowski T.; Werbińska-Wojciechowska S. Exact and approximation methods for dependability assessment of tram systems with time window. // European Journal of Operational Research. 235, 3(2014), pp. 671-686. https://doi.org/10.1016/j.ejor.2014.01.031

[26] Nowakowski, T. problems with analysing operational data uncertainty. // Archives of Civil and Mechanical Engineering. 10, 3(2010), pp. 95-109. https://doi.org/10.1016/S1644-9665(12)60139-3

[27] Smith, D. L.; Naberejnev, D. G. Confidence intervals for the lognormal probability distribution // Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment. 518, 3(2004), pp. 754-763. https:// doi.org/10.1016/j.nima.2003.09.068

[28] Skorupski, J.; Uchroński, P. Telematic support of baggage security control at the airport. // Communications in Computer and Information Science. 471, (2014), pp. 215-224. https://doi.org/10.1007/978-3-662-45317-9_23

[29] Sandom, C.; Harvey, R. S. Human Factors for Engineers, IET Books, London, 2004. https://doi.org/10.1049/PBNS032E

[30] Ross, S. M. Introduction to Probability and Statistics for Engineers and Scientists, 5th Edition Books, 2014.

Authors' addresses

Artur Kierzkowski, PhD, Eng.
Faculty of Mechanical Engineering
Wrocław University of Science and Technology
27 Wybrzeze Wyspianskiego,
50-370 Wrocław, Poland
E-mail: artur.kierzkowski@pwr.edu.pl