

Modelling of information security threats for airport infrastructure based on digital twin technology

Zarina Poberezhna^{1,*†}, Tetiana Konrad^{2†}, Dmytro Malnov^{1†} and Ladislav Dorotik^{3†}

¹Transport Academy of Ukraine, Omelyanovich-Pavlenko Str., 1, Kyiv, 02000, Ukraine

²University of the National Education Commission, Podchorazych Str. 2, Krakow, 30-084, Poland

³Tomas Bata University in Zlin, T. G. Masaryk Sq., 5555, Zlin, 76001, Czech Republic

Abstract

The paper investigates the use of digital twins in the formation of airport infrastructure information security. A conceptual model of airside areas of a digital twin using the A-I-T triad is formed, which is based on the classic CIA triad of information security for operational management of airport infrastructure. It is proven that increasing the level of airport information security allows not only to resist attacks, minimize operating costs, but also to quickly restore work in the event of an attack. It is established that the operational and information resilience index (OIRI) of the airport has a direct dependence on the level of one of the components of the triad. Digital twins are the main tool for predicting and increasing OIRI, because they continuously collect data from various types of networks, servers and channels, and instantly calculate the index level. The author's methodology for determining OIRI depending on the impact of information threats, and possible measures to increase the resilience of airport infrastructure are proposed. Within the framework of simulation modelling of four types of information threats, it was found that a coordinated attack reduces OIRI by 45.6–59.4% depending on the airport. The sensitivity analysis of OIRI confirmed the robustness of the ranking when the weights of the triad components vary. For one airport, access to personal data of passengers and check-in systems may be critical, for another – the integrity of data on control traffic in the airport control zone.

Keywords

digital twin, airport infrastructure, information security, cyberattacks, information threats, airside areas, A-I-T triad, operational information resilience index, OIRI, threat modelling

1. Introduction

In modern conditions, the level of airport information security is subject to constant threats that disrupt operational functioning, which is determined not only by the level of physical infrastructure (runways, aprons, ground equipment), but also by the main information flows of the airport system Airport Collaborative Decision Making (A-CDM), Departure/Arrival Manager (DMAN/AMAN), Surface Movement Guidance and Control System (SMGCS). Violation of the functioning of the information system leads to a decrease in operational indicators (delayed flights, departure time deviation, increased waiting time in the transit zone). It is worth noting that the airport information system is a complex cyber-physical system that is exposed to cyber incidents, which can manifest not only in the failure of some IT services, but also in the deterioration of air traffic management.

In this context, the development of new approaches to increase the level of airport information security in order to minimize the impact of threats becomes particularly relevant. The technology of digital doubles acts as one of the key tools in the fight against threats to the information environment of the airport, and allows combining observational operational data with the forecast of the consequences of the impact of threats. Most scientific approaches to the assessment of information security of airport

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ zarina_www@ukr.net (Z. Poberezhna); tetiana.konrad@uken.krakow.pl (T. Konrad); dmalnov@gmail.com (D. Malnov); l_dorotik@utb.cz (L. Dorotik)

ORCID 0000-0001-6245-038X (Z. Poberezhna); 0000-0001-6283-1967 (T. Konrad); 0009-0006-9731-885X (D. Malnov); 0009-0006-0408-1743 (L. Dorotik)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

infrastructure are based on the analysis of regulatory requirements, cyber defense architecture and the description of attack types, however, the quantitative analysis between information threats and operational resilience remains poorly studied.

Therefore, the use of digital duplicates makes it possible to form an analytical and simulation model capable of reproducing changes in the operational activity of the airport under the influence of a system malfunction due to potential threats.

2. Literature review

The application of digital twin technology has been used in many scientific works, most of which investigated the issues of operational activities of the transport industry using digital twin technology [1, 2, 3]. However, the application of this technology is not only described in airport infrastructure, in the paper [4] the application of digital twin in the port industry is described, which allowed to form a methodological three-level architecture (object, virtual model, two-way communication), which can also be applied to aviation infrastructure. It is worth noting that in some studies on the construction of composite indicators of critical infrastructure, which allows to aggregate and normalize indicators of different types (technical, economic, security) to a single coefficient [5, 6, 7].

However, the issues of increasing information stability, which allow to ensure the continuity of processes in crisis conditions in security management, remain unexplored. In paper [8], a four-dimensional approach (robustness, redundancy, resourcefulness, rapidity) to the resilience of critical infrastructure is proposed, however, it does not include information and cognitive resilience, which are critically important for modern cyber-physical systems in the face of hybrid threats.

When studying the level of information security of aviation infrastructure, the priority is to focus on the provisions and standards of EUROCAE ED-205, EASA Part-IS, and ENISA reports [9, 10]. In the aviation industry, the application of the smart airport concept includes A-CDM, DMAN, AMAN systems, digital services, automated resource management platforms, ground services, which require a certain level of information security depending on international standards [11]. The vast majority of studies in this area describe the technological component of the infrastructure or the overall efficiency of operations, while the issue of information resilience of the airside circuit remains less studied.

In the paper [12], the issue of information security and resilience to threats is investigated through a three-level approach (Confidentiality, Integrity, Availability) enshrined in the ISO/IEC 27000 standards, however, the issues of not preventing incidents, but the ability of the infrastructure to function in a vulnerable state during failures from attacks, require attention. It is worth noting that information security is directly related to economic security, their interdependence and main components have been studied in the papers [13, 14, 15, 16]. However, most studies describe the technological components of the infrastructure or the overall efficiency of operations, while the issue of determining the level of information stability using a stability indicator, which can serve as a tool for comparing the activities of different airports and responding to different threat scenarios, remains poorly studied, which confirms the relevance of the chosen direction of research.

The purpose of the study is to develop models of information security of airport infrastructure depending on the impact of threats based on digital twin technology and assessment of the airport operational and information stability index.

3. Materials and methods

3.1. The A-I-T analytical triad as the basis of the airside area conceptual model of the digital twin

Airport infrastructure usually consists of two main areas: airside and landside. The airside areas include a set of operational processes that directly ensure the movement of aircraft in the airport area, i.e., arrival and departure halls, runways, waiting rooms, landing and actual departure of aircraft. The landside

areas include operations related to passenger service, commercial areas of the terminal, baggage packing services and other types of services for passengers. That is why the development and application of digital twins should include a full cycle of operations, starting from servicing passenger traffic, baggage, and ensuring aviation security both in the airport area and on the aircraft.

Ensuring information security of the airside areas plays a key role, because any failures and interruptions in its work significantly affect the availability of operating time, flight frequency, airport throughput, leading to long-term delays and possible flight cancellations, as well as creating an excessive load on dispatch services and ground personnel. Failures in aviation equipment, inconsistencies in technological procedures and operational inefficiency reduce the level of increasing the stability of aviation systems [17, 18]. The stability of information support is determined by the reliability and efficiency of operational processes [19].

Classical approaches to information security include the components of the CIA triad (Confidentiality, Integrity, Availability) enshrined in the ISO/IEC 27000, NIST SP 800-12 standards and are the basis for modern approaches to information security. Operational data on traffic, flight delays, slot adherence are important in the formation of a digital twin, as they affect the assessment of operational time availability [20, 21]. However, the most important data is the Timeliness of operational decisions, which is separately prescribed in aviation standards EUROCAE ED-205, ICAO Doc 10101 [22].

According to EUROCONTROL aviation statistics, flight delay data consists of: Arrival Sequencing and Metering Area (ASMA) additional time, which shows the state of the incoming load to the airport area, Taxi-out additional time, which characterizes the waiting time of the aircraft before departure, has received permission, but is in the take-off queue, Air Traffic Control (ATC) pre-departure delay and ALL pre-departure delays, which reflect the timeliness of pre-departure decisions [23].

Within the framework of the study, the author proposed the analytical triad A-I-T (Availability, Integrity, Timeliness), which is based on the classical CIA approach, however, the Confidentiality attribute was replaced by Timeliness, which is of critical importance in airport operations. The proposed author's methodology is consistent with the EUROCONTROL Key Performance Areas (KPA) concept, where the digital twin performs three functions. The first, representative, which combines heterogeneous data into a single structured model. The second, diagnostic, allows to determine the airport's operating profile based on *A*, *I*, and *T* components. The third, simulation, allows to check the effectiveness of the airport infrastructure under the influence of information threats.

The proposed replacement of Confidentiality with Timeliness does not deny the importance of confidentiality in aviation cybersecurity, the security of personal, commercial or classified service data, but examines the operational resilience of the airside areas to disruption of its state during the impact of threats. In this context, Timeliness becomes a key component of security, since even correct data received late may lose its management value for pre-flight coordination and ground traffic control.

The essential value of the components of the A-I-T triad and specific operational processes according to EUROCONTROL to the components of the triad is presented in Table 1.

Table 1

The Essential Meaning of the Components of the A-I-T Triad According to EUROCONTROL [24]

Triad component	Essential definition	EUROCONTROL
Availability (A)	The ability of the airport system to handle an aircraft in the scheduled time slot	ATFM slot adherence
Integrity (I)	Compliance of actual trajectories and timing with planned ones (absence of movement deformations caused by data violations)	ASMA additional time; Taxi-out additional time
Timeliness (T)	Timeliness of pre-departure operational decisions (conformity of departure time with the plan)	ATC pre-departure delay; ALL pre-departure delays

3.2. Formation of the airport operational and information resilience index (OIRI) depending on information threats

Aviation is a critical industry, and its criticality is enhanced by the strong connection between ground and mobile objects that require protection and the development of appropriate security measures [25, 26]. Modern international airports are complex multifunctional systems that, like most systems, are exposed to various kinds of threats. Increasing the level of airport information security allows not only to resist attacks, minimize operating costs, but also to quickly restore work in the event of an attack.

Using the airport's operational and information resilience index (OIRI) allows to quantify the level of security and the ability to continuously ensure aviation security. Information threats directly reduce this index by destabilizing key airport systems, so monitoring the OIRI level allows to prepare and develop an action plan in advance for flights in conditions of cyberattacks, technical failures or data distortion.

Digital twins are the main tool for predicting and improving OIRI, as they continuously collect data from various networks, servers and channels, and instantly recalculate the index level [27]. The complexity and scalability of cyberattacks are becoming increasingly large, this leads to the cessation of the functioning of the airport system, the index drops rapidly, and then the digital twin offers certain options and scenarios for protection, identifies weaknesses in protection and helps to adjust actions without any risk to real flights, which allows to return the resilience index to stable indicators as quickly as possible.

Methodological tools for determining the OIRI of an airport when exposed to information threats include four main stages:

Stage 1. Normalization of heterogeneous data to a common metric. According to EUROCONTROL data, each of the airport indicators has different units of measurement: Slot adherence is measured in percentages $[0; 100\%]$, and ASMA, Taxi-out, ATC and ALL delay in minutes per flight $[0; +\infty)$. To convert them into dimensionless scores $s \in [0; 1]$, the Sigmoid s-function is used to determine the flight delay due to information threats:

$$x \in \{x_{ASMA}, x_{taxi}, x_{ATC}, x_{all_delay}\}, s_x = 1 - \frac{1}{1 + e^{-\alpha(x-\beta)}} \quad (1)$$

where β is critical delay threshold (for which the score is 0.5); α is model sensitivity coefficient to delay increase; e is Euler number.

A delay of 1-2 minutes is considered acceptable, but a delay of more than 15 minutes and every subsequent minute brings catastrophic damage to the efficiency of the airport's operation.

Stage 2. Determination of the operational inefficiency index (I):

$$I = \left(\frac{(s_{ASMA})^p + (s_{taxi})^p}{2} \right)^{\frac{1}{p}} \quad (2)$$

where p is the sensitivity coefficient. The higher this indicator, the higher the operational inefficiency index becomes and the worst value is reached, which leads to management in the operational response mode, ignoring all kinds of successes in other directions.

Stage 3. Determination of the weight coefficients of the airport operational and information stability index. We use the entropy method, where the weight of each index is proportional to the change in the data of this indicator over time and depending on m airports (or days) and n indices ($j \in \{A, I, T\}$), normalized values for each object:

$$p_{ij} = \frac{y_{ij}}{\sum_{i=1}^m y_{ij}} \quad (3)$$

where y_{ij} is the value of the index A, I or T for the i -th object. The calculation of each index E_j will be as follows:

$$E_j = -\frac{1}{\ln m} \sum_{i=1}^m p_{ij} \ln p_{ij}$$

while the degree of diversification (data usefulness) d_j :

$$d_j = 1 - E_j$$

and the weighting factors of the operational and information stability index $\omega_A, \omega_I, \omega_T$:

$$\omega_j = \frac{d_j}{\sum_{k=1}^n d_k} \quad (4)$$

in this case $\omega_A + \omega_I + \omega_T = 1$

Stage 4. Determination of the overall operational and information efficiency index (I_{OIRI}):

$$I_{OIRI} = A^{\omega_A} \cdot I^{\omega_I} \cdot T^{\omega_T}$$

To combine the three main indices into a single indicator, a weighted geometric aggregation is used, in which a change in one index or its approach to 0 leads to a sharp change in the overall airport index, which makes it impossible to cover up failures and destructive airport functioning with other high indicators.

The operational information efficiency index (I_{OIRI}) is defined as:

$$I_{OIRI} = \left(\frac{1}{1 + e^{-\gamma(x_{slot} - \delta)}} \right)^{\omega_A} \cdot \left(\frac{\left(1 - \frac{1}{1 + e^{-\alpha_1(x_{ASMA} - \beta_1)}} \right)^p + \left(1 - \frac{1}{1 + e^{-\alpha_2(x_{taxi} - \beta_2)}} \right)^p}{2} \right)^{\frac{\omega_1}{p}} \quad (5)$$

The proposed methodology allows to adapt the airport system depending on the impact of information threats, and ensure the stability and efficiency of the airport's operation in modern conditions.

4. Results of empirical testing and simulation modelling

To test the proposed methodology, the three largest airports in Europe by traffic volume in 2025 were selected: Istanbul (LTFM), Amsterdam-Schiphol (EHAM) and London-Heathrow (EGLL) [24]. The total volume of flights at these three airports is more than 1.517 million flights per year, which is about 8.8% of the total European traffic (17.188 million). For calculations, were used EUROCONTROL statistical data in the Python programming environment according to the given formulas (1)-(5). Empirical data for constructing a digital twin of the airside zone are given in Table 2.

The given input data are the basis for testing the proposed methodology for determining the role of the digital twin in the proposed author's concept of calculating the A-I-T components and the OIRI index, in order to determine the level of airport resistance to information attacks. The resulting data for three airports are presented in Table 3.

Table 2

Empirical Data from Three Airports Used to Construct a Digital Twin of the Airside Area

Airport	Annual Flights	Daily Flights	Slot Adherence	ASMA add. time, min	Taxi-out add. time, min	ATC delay, min	All delays, min
Istanbul (LTFM)	544 121,0	1 490,742	0,899	4,239	4,766	1,177	13,186
Amsterdam-Schiphol (EHAM)	493 042,0	1 350,800	0,986	2,607	3,282	2,382	19,555
London-Heathrow (EGLL)	480 072,0	1 315,266	0,985	6,293	6,495	1,954	12,458

Table 3

Basic Airport Operational KPIs and Components of the A-I-T Concept

Indicator	LTFM (Istanbul)	EHAM (Amsterdam)	EGLL (Heathrow)
Annual traffic, flights	544 121	493 042	480 072
Slot adherence, %	89,88	98,59	98,49
ASMA add. time, min/flight	4,239	2,607	6,293
Taxi-out add. time, min/flight	4,766	3,282	6,495
ATC pre-dep. delay, min/flight	1,177	2,382	1,954
ALL pre-dep. delays, min/flight	13,186	19,555	12,458
Component A	0,8988	0,9859	0,9849
Component I	0,0602	0,3893	0,0000
Component T	0,4890	0,1896	0,3022
Integral OIRI	0,4826	0,5216	0,4291

Table 4Determination of OIRI and Δ OIRI Levels by Types of Information Attacks

Scenario	LTFM (Istanbul)	EHAM (Amsterdam)	EGLL (Heathrow)
(S0) Baseline	0,4826	0,5216	0,4291
(S1) DDoS DMAN/AMAN	0,3382 (-29,9%)	0,3359 (-35,6%)	0,3260 (-24,0%)
(S2) GPS-spoofing	0,3918 (-18,8%)	0,3445 (-34,0%)	0,3892 (-9,3%)
(S3) Ransomware A-CDM	0,2867 (-40,6%)	0,3165 (-39,3%)	0,3231 (-24,7%)
(S4) Combined APT attack	0,1961 (-59,4%)	0,2120 (-59,4%)	0,2333 (-45,6%)

The analysis of the obtained results shows the heterogeneity of the stability indicators for the three airports. Thus, EHAM airport has the highest integral OIRI (0.5216) due to the combination of high components A (0.9859) and I (0.3893), which is explained by the high level of operational processes and compliance with discipline between the time of flight stay in the TMA. However, for EHAM airport, the T component has the lowest indicator among the three airports (0.1896), which characterizes the high level of pre-departure delays at this airport. LTFM airport has an intermediate OIRI value (0.4826) due to the combination of a high indicator of the T component (0.4890) with an almost zero component I

(0.0602). For the EGLL airport, the lowest OIRI indicator (0.4291) is due to the zero value of component I (0.0000), which characterizes the high vulnerability of the airport or the complete inability to withstand failures in operation due to information threats or cyberattacks. The results of modeling scenarios for four types of information attacks on the OIRI level of three airports are presented in Table 4.

The simulation modeling conducted in the Python programming environment allowed to formulate the main conclusions. The combined APT attack (S4) scenario reduces OIRI by 45.6–59.4% depending on the airport, which confirms the statement about the vulnerability of the airport airside area to various types of attacks. It was found that under the (S0) scenario, the airport with a higher baseline OIRI index (EHAM) has higher decline rates during an information attack, since it has a large number of operational processes, while the EGLL airport with a lower OIRI resilience index demonstrates a smaller relative decline. The (S2) scenario demonstrates a special role of data integrity, especially for EHAM airport the OIRI level is 34.0%, while for EGLL airport it is 9.3%. This gap in the data is explained by the fact that in the baseline (S0) scenario EGLL airport has a zero value of component I, therefore additional deterioration of this block changes the integral result less, Fig 1. In this context, the digital twin allows not only to compare airports, but also to form different management mechanisms depending on the level of vulnerability. For one airport, access to personal data of passengers and check-in systems may be critical, for the second the integrity of data on the control movement in the airport control area.

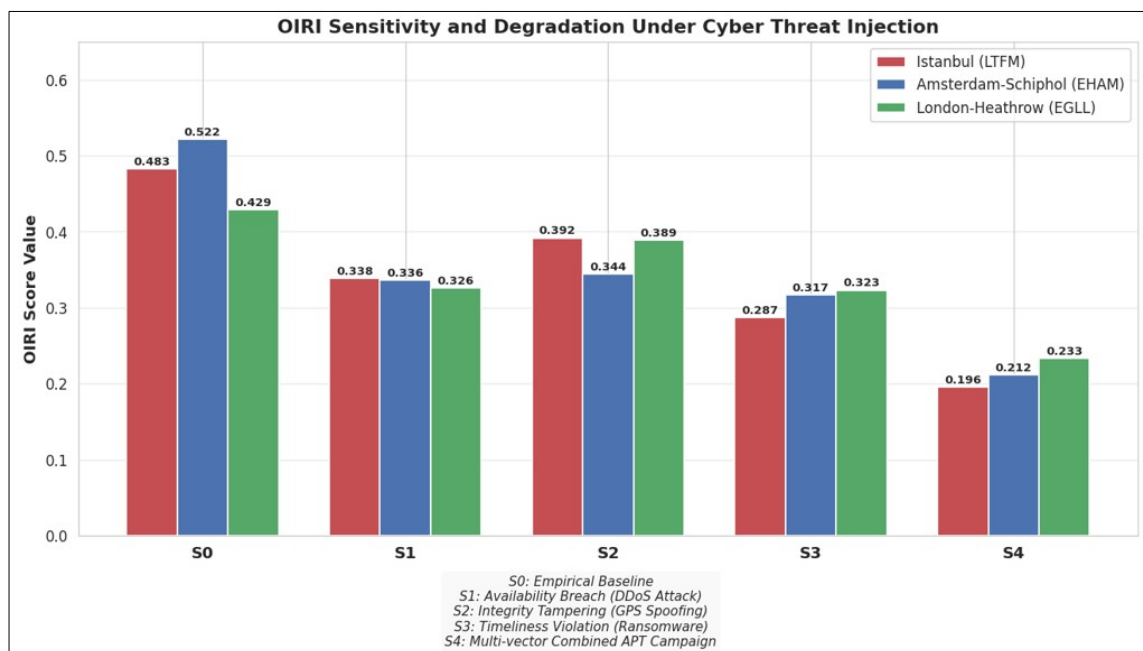


Figure 1: Change in the OIRI index according to information threat scenarios.

If we consider the impact of the most dangerous information attacks on the functioning of airports, then the first place belongs to ransomware attacks, which cause the greatest harm to the timeliness of operational processes for the airside area. Relative changes in the OIRI index under information attack scenarios have certain levels of sensitivity, low sensitivity to a separate scenario may sometimes indicate not the level of resilience, but the level of the normalized component reserve. Different types of information threats pose the greatest risk of degradation for each specific airport, Fig. 2

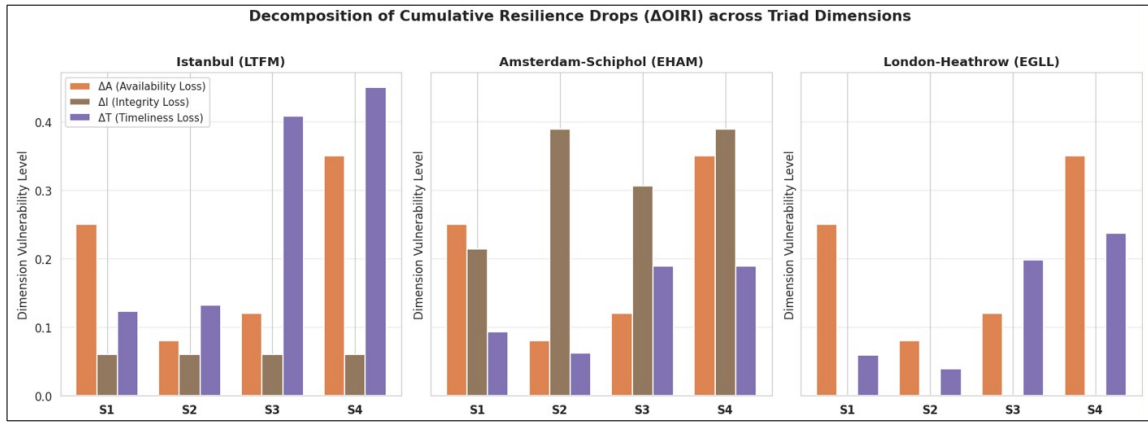


Figure 2: Decomposition of cumulative stability reduction into components A , I and T .

As can be seen from Table 5, the value of the index after the impact of threats and their scale relative to the losses from the baseline allows us to determine which types of information threats pose the greatest risk for each specific airport.

Table 5

The Absolute and Relative Change in the OIRI Index by Information Threat Scenarios

Airport	S0 (OIRI)	S1 (ΔOIRI)	S2 (ΔOIRI)	S3 (ΔOIRI)	S4 (ΔOIRI)
Istanbul (LTFM)	0,4826	-0,144 (-29,9%)	-0,091 (-18,8%)	-0,196 (-40,6%)	-0,287 (-59,4%)
Amsterdam-Schiphol (EHAM)	0,5216	-0,186 (-35,6%)	-0,177 (-34,0%)	-0,205 (-39,3%)	-0,310 (-59,4%)
London-Heathrow (EGLL)	0,4291	-0,103 (-24,0%)	-0,040 (-9,3%)	-0,106 (-24,7%)	-0,196 (-45,6%)

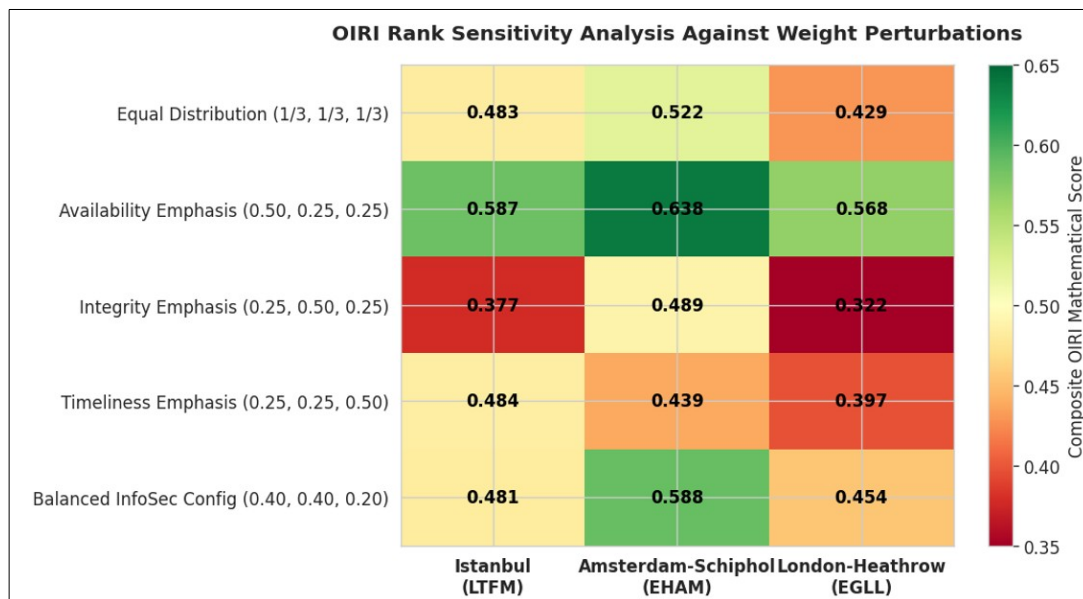


Figure 3: Sensitivity analysis of OIRI to changes in the weights of the A-I-T triad components

Within the framework of the study, an experiment was conducted to determine the level of OIRI sensitivity of airports according to five alternative sets of weights: levels (1/3, 1/3, 1/3); *A*-emphasis (0.5; 0.25; 0.25); *I*-emphasis (0.25; 0.5; 0.25); *T*-emphasis (0.25; 0.25; 0.5); Balanced InfoSec Config (0.4; 0.4; 0.2). The results are presented in Fig. 3.

Analysis of the results shows sufficient robustness in four out of five weight options: $EHAM > LTFM > EGLL$. A change in ranking is observed only in the *T*-emphasis option, where the LTFM airport indicators take first place due to the higher *T* component. This confirms that the level of the OIRI integral indicator is directly intertwined with the level of the component, since different airports may have different vulnerability structures even with close integral values.

5. Conclusions

The results obtained demonstrate the use of a digital twin to ensure a high level of information security when forming operational KPIs of airports. The proposed model allows to determine the OIRI level depending on the type of information threats and form certain management decisions to minimize the negative impact of their damage.

The results of calculations for the three main airports in Europe showed that information threats can manifest themselves not only through a complete shutdown of the information system and disruption of the airport's operational activities, but also through deterioration of data quality. This is critically important for the airside area, as a decrease in slot adherence, distortion of ASMA data, and an increase in Taxi-out time can cause large congestion for departures at the airport and reduce its throughput capacity and operational and information stability.

The proposed analytical triad A-I-T showed that large airports do not have a universal resilience profile, EHAM airport has a better integral OIRI result, but a weaker *T* component, LTFM airport demonstrates a high level of *T* components, but a lower *I* component, this means that there is no general mechanism for forming airport resilience, it should differ depending on the management priorities for different airports. In this context, the use of digital twins is one of the main tools for forming certain management scenarios for each specific airport depending on the type of information threats.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] M. Grieves, Digital twin: Manufacturing excellence through virtual factory replication (2015).
- [2] F. Tao, H. Zhang, A. Liu, A. Y. C. Nee, Digital twin in industry: State-of-the-art, IEEE Transactions on Industrial Informatics 15 (2019) 2405–2415. doi:10.1109/TII.2018.2873186.
- [3] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within CNS/ATM systems, in: I. Ostroumov, M. Zalisky (Eds.), Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development, volume 992 of *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5_20.
- [4] J. Neugebauer, L. Heilig, S. Voß, Digital twins in seaports: Current and future applications, in: Computational Logistics: 14th International Conference, ICCL 2023, Berlin, Germany, September 6–8, 2023, Proceedings, Springer-Verlag, 2023, pp. 202–218. doi:10.1007/978-3-031-43612-3_12.
- [5] OECD, Handbook on Constructing Composite Indicators: Methodology and User Guide, OECD Publishing, Paris, 2008. doi:10.1787/9789264043466-en.

- [6] V. Volkogon, T. Konrad, O. Kolganova, L. Tereshchenko, Situational synthesis of algorithmic support of regional transport systems based on expert system, in: Proceedings of the International Workshop on Advances in Civil Aviation Systems Development, volume 736 of *Lecture Notes in Networks and Systems*, 2023, pp. 321–333. doi:10.1007/978-3-031-38082-2_25.
- [7] S. Smerichevska, L. Ivanenko, Z. Poberezhna, S. Smerichevskyi, T. Konrad, D. Dudko, Matrix-vector approach to assessing the competitiveness of logistics enterprises in the context of economic security and information risks, in: CEUR Workshop Proceedings, volume 4024, 2025, pp. 440–451.
- [8] M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, D. Winterfeldt, A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra - EARTHQ SPECTRA* 19 (2003). doi:10.1193/1.1623497.
- [9] EUROCAE ED-205, Process standard for security certification and declaration of ATM/ANS ground systems, European Organisation for Civil Aviation Equipment (2024).
- [10] ENISA, ENISA threat landscape 2024, European Union Agency for Cybersecurity (2024). doi:10.2824/0710888.
- [11] A. Rajapaksha, N. Jayasuriya, Smart airport: A review on future of the airport operation, *Global Journal of Management and Business Research* (2020) 25–34. doi:10.34257/GJMBRAVOL20IS3PG25.
- [12] Y. Cherdantseva, J. Hilton, A reference model of information assurance & security, in: 2013 International Conference on Availability, Reliability and Security, 2013, pp. 546–555. doi:10.1109/ARES.2013.72.
- [13] O. Solomentsev, M. Zaliskyi, Z. Poberezhna, O. Zuiev, Predictive analytics of decision-making for aviation operation enterprise, in: I. Ostroumov, K. Marais, M. Zaliskyi (Eds.), *Advances in Civil Aviation Systems Development*, Springer Nature Switzerland, Cham, 2025, pp. 348–363. doi:10.1007/978-3-031-91992-3_23.
- [14] A. Dziubynskyi, Z. Poberezhna, O. Shehynskyi, O. Pakholiuk, D. Riznyk, Management of transport and logistics systems: Problems under conditions of military operations, in: A. Bahaaeddin, H. Allam (Eds.), *Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation*, Springer Nature Switzerland, Cham, 2024, pp. 363–373. doi:10.1007/978-3-031-67444-0_35.
- [15] O. Solomentsev, M. Zaliskyi, O. Zuiev, Estimation of quality parameters in the radio flight support operational system, *Aviation* 20(3) (2016) 123–128. doi:10.3846/16487788.2016.1227541.
- [16] O. Solomentsev, et al., Method of optimal threshold calculation in case of radio equipment maintenance, in: S. Shukla, X. Gao, J. Kureethara, D. Mishra (Eds.), *Data Science and Security*, volume 462 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2024, pp. 69–79. doi:10.1007/978-981-19-2211-4_6.
- [17] J. Al Azzeh, A. Mesleh, M. Zaliskyi, R. Odarchenko, V. Kuzmin, A method of accuracy increment using segmented regression, *Algorithms* 15 (2022) 24. doi:10.3390/a15100378.
- [18] V. Ivannikova, M. Zaliskyi, O. Solomentsev, I. Ostroumov, N. Kuzmenko, Statistical data processing technologies for sustainable aviation: A case study of ukraine, *Sustainability* 17 (2025). doi:10.3390/su17135781.
- [19] M. Zaliskyi, O. Solomentsev, Z. Poberezhna, O. Chioma Okoro, B. Chumachenko, S. Chumachenko, Information technologies of data processing for linear deterioration process during aviation equipment operation, in: I. Ostroumov, K. Slimani, M. Zaliskyi, L. Tereshchenko (Eds.), *International Workshop on Computational Methods in Systems Engineering*, volume 3732, Kyiv, Ukraine, 2024, p. 32–44. URL: <https://ceur-ws.org/Vol-3732/paper03.pdf>.
- [20] International Electrotechnical Commission, ISO/IEC 27000:2018 "Information technology — Security techniques — Information security management systems — Overview and vocabulary" (2018). URL: <https://www.iso.org/standard/73906.html>.
- [21] National Institute of Standards and Technology (NIST), An introduction to information security (2017). doi:10.6028/NIST.SP.800-12r1.
- [22] International Civil Aviation Organization (ICAO), Cybersecurity action plan (2022). URL: https://www.icao.int/sites/default/files/sp-files/SAM/Documents/2022-CIBER/Cybersecurity_

Action_Plan_EN.pdf.

- [23] Performance Review Commission, Performance review report (2024). URL: <https://www.eurocontrol.int/publication/performance-review-report-prr-2024>.
- [24] EUROCONTROL, Performance Review Unit Data (2026). URL: <https://ansperformance.eu/data/>.
- [25] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, R. Odarchenko, Hybrid encryption model of aes and elgamal cryptosystems for flight control systems, in: 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), 2018, pp. 229–233. doi:10.1109/MSNMC.2018.8576289.
- [26] S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency increasing method for quantum secure direct communication protocols, in: 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), volume 1, 2015, pp. 468–472. doi:10.1109/IDAACS.2015.7340780.
- [27] Y. Liu, S. Pan, E. Ballot, Unveiling the potential of digital twins in logistics and supply chain management: Services, capabilities, and research opportunities, Digital Engineering 3 (2024) 100025. doi:10.1016/j.dte.2024.100025.