NOVA IMS Information Management School

MGI

Master Degree Program in

Information Management

Digital Transformation within Airports Security Processes

New Security Technology Implementation Impact

Simão Botelho Batista

Project Work

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

DIGITAL TRANSFORMATION WITHIN AIRPORTS SECURITY PROCESSES

NEW SECURITY TECHNOLOGY IMPLEMENTATION IMPACT

by

Simão Botelho Batista

Project presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information Systems and Technologies Management

Supervised by

Maria Manuela Aparício, PhD, NOVA Information Management School

July, 2024

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledged the Rules of Conduct and Code of Honor from the NOVA Information Management School.

Simão Botelho Batista

Lisbon 15 July 2024

DEDICATION (OPTIONAL)

I want to sincerely thank my Supervisor Professor Manuela Aparicio which since the day one starting from the classes of Project Research and Methodologies and giving the extra leg also via meeting helps me setting the topic of this project and organize it with a structure of an Information Systems Management Project. All of the contributes have been crucial to the results that I have obtained particurarly all of the imputs and the push that have been made to sucessful deliver it on time.

ABSTRACT

The connection between the technological and aeronautical sectors, particularly in the security field, is crucial for economic and infrastructural development. The aeronautical market, integral to one of the most developed sectors globally, needs a robust strategy to sustain its role as a powerful economic engine. Studied country economy heavily relies on tourism, which contributes 16.5% to GDP and supports a substantial portion of the workforce. This sector drives revenue through various channels like hospitality and transportation. Concurrently, the aviation industry catalyzes infrastructure development, fosters technological innovation, and boosts exports. Despite its high security standards, the aviation industry must continually address threats such as terrorism and illicit acts, exemplified by events like September 11, 2001, and incidents like the Eurowings and Greece hijacking cases. Enhancing security remains imperative to maintaining user trust and industry reliability. Leads in advancing global airport security technology, and those were the focus for this work, which using a Database data will be strapulated resulting on fiability rates for this technologie use and implementation. This study suggested a conceptual model that may be used to govern services by utilizing a prototype model that was assessed by experts. Regarding the final results they have been obtained using DSR Methodology analysis which resulted on a realization of a Focus Group. As final results the Airport Tech Security Plan is performing well overall, with a Total Performance of 95.66%, driven by strong execution in Security Measures (98.25%) and a solid, though slightly lower, Level of Security Technology Efficiency (93.16%). Most security metrics surpass their targets, reflecting robust security infrastructure and adherence to protocols. However, there are critical areas in security technology, such as the high number of incidents due to security failures and inefficiencies in handling suspicious cases, that require immediate attention for further improvement.

KEYWORDS

Aviation Market; Technology; Security; Feasibility; Integration; AI

Sustainable Development Goals (SDG):

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AIT (Advanced Imaging Technology)

AI (Artificial Intelligence)

ANSAC (Autoridade Nacional de Segurança da Aviação Civil)

AVSEC (Aviation Security)

CCTV (Closed Circuit Television)

BD (Database)

DSR (Design Science Research)

EOS (European Organization for Security)

FM (Facilities Management)

IATA (Internation Air Transport Association)

ICAO (Internation Civil Aviation Organization)

IOT (Internet of Things)

KPIs (Key Performance Indicators)

OTP (On Time Password)

PNCQSAQ (Programa Nacional de Controlo da Qualidade da Segurança da Aviação Civil)

PNFSAC (Programa Nacional Formação Segurança Aviação Civil)

RFID (Radio Frequency Identification)

TSA (Transport Security Administration)

1. INTRODUCTION

The digital transformation at studied airports has markedly enhanced airports security performance through the deployment of advanced technologies. Sophisticated screening systems, such as advanced imaging technology (AIT) scanners and biometric identification, have streamlined the security screening process, reducing wait times and increasing accuracy in threat detection (Transportation Security Administration, n.d.). The integration of data analytics and artificial intelligence (AI) enables real-time threat detection and response (Homeland Security, 2021), while AI-powered surveillance and predictive analytics swiftly identify and mitigate potential security breaches (Airport Technology, n.d.). Digitalization also enhances coordination and communication between airport departments and security personnel through integrated communication systems and centralized data platforms, facilitating quicker decision-making and incident response (Digital Airport, 2020). Automated check-in and baggage drop-off systems reduce congestion, allowing security personnel to concentrate on critical tasks (ACI Insights, 2020). Real-time updates and information systems improve the passenger experience by reducing stress and potential conflicts (Passenger Experience, n.d.). Biometric technologies for boarding and identity verification further enhance security and convenience, ensuring that only authorized individuals access secure areas and expediting the boarding process (Biometric Update, n.d.). These technological advancements align with international security standards, significantly strengthening the airport's security infrastructure and contributing to a safer, more efficient, and more pleasant travel experience (IATA, 2020). The continued evolution and integration of digital technologies remain essential for maintaining and improving airport security in a technologically advanced world (ACI World, 2021).

The digital transformation at these airports aims to enhance airports security performance through the introduction of advanced technologies, and this project investigates its impact on security processes and operator satisfaction. To address research gaps, a comprehensive study will be developed to assess the integration and effectiveness of digital systems within security operations, focusing on advanced screening technologies, biometric identification systems, AI-powered surveillance, and enhanced communication among security personnel. Data from the questionnaire will populate a dashboard with specific Key Performance Indicators (KPIs) to measure reductions in wait times, accuracy of threat detection, responsiveness to security breaches, and overall satisfaction of operators and passengers. This approach aligns with studies highlighting the critical role of digital transformation in improving airport security and operational efficiency (Lohmann, Correia, & Costa, 2020; International Air Transport Association [IATA], 2021).This approach aligns with studies highlighting the critical role of digital transformation in improving airport security and operational efficiency (Lohmann, et al., 2020; IATA, 2021), ensuring that the integration of these technologies meets international security standards and enhances the travel experience .

Using a dashboard system, operators can evaluate how advanced technologies enhance their performance and passenger safety, focusing on metrics such as operational efficiency, communication reliability, speed and accuracy of identity verification, and real-time threat detection. While previous studies have explored the link between technology and operator performance, a research gap remains in understanding its specific impacts within aviation security.

This study aims to fill that gap by analyzing how digital transformation influences security operations and passenger safety, offering insights into the benefits and challenges of digital integration in airport security. According to other studies report, systems must be designed with inherent problem-solving abilities to adapt to disturbances, aligning with operators' skills and values to reduce complexity or match problem-solving knowledge (Espejo & Harnden, 1989). Prior study's findings underscore the importance of integrating technology and people as a single sociotechnical system, emphasizing the need to consider operators perceptions in system design. In order to contribute to the development of more secure and effective air travel, this project will use a PowerBI dashboard to assist airport operators and security management in evaluating the impact of new technologies on passenger security (Espejo & Harnden, 1989).

2. LITERATURE REVIEW

2.1. APPROVED PLANS AND GENERAL SECURITY

Any research effort must include a literature review since it sets the stage and provides background information for the topic being done. It assists in finding gaps in the literature, identifying themes and trends, and providing a summary of the present state of knowledge in the subject of aviation security technology. This shift aims to enhance operational efficiency but also introduces potential risks, such as inconsistent safety standards and regulatory gaps, underscoring the need for robust oversight to maintain safety. It makes sense to conduct a literature review on aviation security technology because it gives researchers a thorough understanding of the field, which helps them develop new studies that are relevant and answer unanswered problems (Creswell & Creswell, 2018). It also helps academics to understand the risks that the aviation sector faces today and assess how technology helps to reduce these threats (Neuman, 2014).

The discussed papers highlight the transition to performance-based regulations, the critical role of information technology in enhancing security, and the impact of digital transformation. This review provides a background for studying how evolving technologies and regulations influence aviation security, helping to identify best practices and challenges in the field. By synthesizing insights from these studies, researchers can design relevant and impactful studies that address previously unaddressed questions and improve aviation security measures (Creswell & Creswell, 2018; Neuman, 2014; Boote & Beile, 2005).

2.2. SECURITY ORGANIZATIONS AND OBJECTIVES

2.2.1 CIVIL AVIATION SAFETY GENERAL OBJECTIVES

The safeguarding and protection of people and property in aviation is a continuous endeavor that involves multiple layers of action and responsibility. This includes preventive measures against acts of unlawful interference, addressing potential risk or threat situations, and ensuring that all personnel in the sector receive adequate and up-to-date training. Preventive measures are crucial in preempting and mitigating threats before they manifest, while effective response strategies are essential for dealing with security risks as they arise. Ensuring that personnel are well-trained and current with the latest security protocols is fundamental to maintaining a robust security posture. This multi-faceted approach is critical to maintaining the safety and security of civil aviation operations (O'Brien & Bringezu, 2011; Taneja et al., 2014; Lahkani et al., 2008; Tamosaitis et al., 2014).

In the context of aviation safety and security, Taneja and Vashishth (2014) emphasize the complexity of maintaining security in a global aviation environment that demands continuous adaptation and innovation. Lahkani and Mann (2008) explore the regulatory framework for civil aviation security, highlighting the necessity of complying with international standards and integrating advanced technologies to address evolving threats. Tamosaitis and Barabanov (2014) focus on modern challenges and advocate for the adoption of cutting-edge technologies and proactive strategies to enhance threat detection and prevention. Together, these perspectives underscore the critical importance of preventive measures, regulatory compliance, and continuous innovation in effectively addressing aviation security challenges (Taneja & Vashishth, 2014; Lahkani & Mann, 2008; Tamosaitis & Barabanov, 2014).

2.2.2 Civil Aviation Safety Objectives

The safeguarding and protection of people and property in aviation is an ongoing effort that requires a multi-layered approach, including preventive measures against unlawful interference, effective response to security threats, and continuous training for personnel. According to Ismail and Haryadi (2020), the implementation of robust security protocols and technological advancements is essential for preempting potential threats and ensuring passenger safety. Additionally, effective risk management strategies are critical for addressing security challenges in real-time (Kusuma & Sumanto, 2021). Moreover, the integration of advanced security technologies and comprehensive training programs for aviation personnel are crucial for enhancing overall security measures (Corpuz & Cruz, 2022). This holistic approach ensures that aviation operations remain secure and resilient against evolving threats.

The Aviation Security (AVSEC) system, a sub-system of the national internal security system, is regulated by the National Civil Aviation Safety Authority (ANSAC). The AVSEC training and certification framework involves ANSAC, entities, and trainers. ANSAC's objectives include developing, implementing, and promoting the National Civil Aviation Safety Training Program (PNFSAC) and the National Civil Aviation Safety Quality Control Program (PNCQSAC), certifying and approving personnel and entities, approving regulations and procedural rules, and licensing and accrediting public or private activities. Entities are responsible for ensuring all personnel under their supervision receive the required training and qualifications as stipulated in the PNFSAC, while trainers are tasked with delivering high-performance training actions and maintaining up-to-date qualifications necessary for effective training delivery. This comprehensive structure ensures that aviation security personnel are well-trained, certified, and capable of maintaining high standards of safety and security in civil aviation.

2.3. THE EVOLUTION TO RISK BASED AVIATION SECURITY

Major transition from conventional, standardized security measures to a more flexible and dynamic method that allocates resources according to evaluated risks is represented by the evolution of risk-based aviation security. This shift resulted from the need for a more effective strategy to handle a wider spectrum of threats due to the growing complexity and interconnectedness of international aviation (Lohmann, Correia, & Costa, 2020; International Air Transport Association [IATA], 2021). In contrast to the one-size-fits-all approach, risk-based security focuses on areas with the most risk and thus more effectively distributes resources, improving overall security outcomes without needless spending or delays (European Union Agency for Cybersecurity [ENISA], 2021).

Central to risk-based aviation security is the identification and mitigation of the most significant threats. This involves comprehensive risk assessments and intelligence-driven decision-making, supported by advanced technologies (Homeland Security, 2021). Continuous threat assessment, based on intelligence and data analytics, identifies likely and severe threats. Differentiated passenger screening processes, such as the TSA's PreCheck and the EU's Registered Traveller Programme, expedite low-risk travellers while conducting more thorough checks on higher-risk individuals (Transportation Security Administration, n.d.; European Commission, n.d.). Additionally, integrating technologies like biometrics, advanced imaging technology (AIT) scanners, and automated data analysis tools enhances the accuracy and efficiency of threat detection (Biometric Update, n.d.; Airport Technology, n.d.).

The successful implementation of risk-based aviation security also relies on optimizing resource allocation and fostering international cooperation. Security resources, including personnel and technology, are deployed based on risk levels associated with different flights, routes, and passengers, ensuring higher-risk areas receive more attention (European Union Aviation Safety Agency [EASA], 2021). Enhanced collaboration among international aviation security agencies is crucial for sharing intelligence and best practices to manage threats that cross borders (International Civil Aviation Organization [ICAO], 2020). Furthermore, updating and harmonizing regulatory frameworks support the adoption of these measures, ensuring consistency and effectiveness (IATA, 2021). This strategic shift not only boosts security efficiency but also improves the overall passenger experience, making air travel safer and more efficient (Homeland Security, 2021).

Table 1 - Risk Based Aviation Security

Identified Risks	Risk Mitigation
Passenger Flow at Border Crossings	Enhancing passenger flow through the Automated Border Crossing (ABC) project.
Passenger Screening Processes	Optimizing screening procedures at targeted security checkpoints for efficiency and passenger satisfaction.
Support from Airports and Regulators	Securing backing from airports and national regulators to advance the Checkpoint of the Future project.
Airline and Airport Cooperation	Facilitating cooperation on Common Use Self Service (CUSS) systems between airlines and airports.
Common Technical Specifications	Establishing standardized technical specifications for data exchange at airports.
Best Practices in Ground Handling	Implementing safety and productivity best practices in ground handling operations.
Baggage Handling Improvements	Reducing mishandled bags and introducing innovations like permanent and home-printed bag tags for passengers.

In 2014, IATA and ACI established a memorandum of understanding, prioritizing collaboration on enhancing "*airline airport interface, airport throughput capacity and efficiency*" to advance next-generation aviation security. Currently, both organizations are finalizing annexes to the agreement, targeting specific areas for improvement.

The Transportation Security Administration (TSA), responsible for aviation security and industry regulation, is often cited as a reason why some argue that the current governance structure in the United States is inadequate. Advocates for change suggest adopting a system similar to that used in the UK, where local airports have the option to provide security screening services themselves or to contract them out (Poole, 2019). Furthermore, critics of the current system point out that US behavioural screening programs have not proven effective to date (General Accountability Office [GAO], 2017).

Here is an explanation of the statistics that highlight the impact and effectiveness of risk-based aviation security:

Table 2 - Impact and Effectiveness of Risk-Based Aviation Security

Category	**Aspect**	**Data/Statistics**	**Impact/Effectiveness**
Passenger Screening Efficiency	TSA PreCheck	Enrollment: Over 10 million passengers (2023)	Wait Times: Less than 5 minutes in PreCheck lanes, highlighting efficiency
Global Entry Program		Enrollment: Over 8 million members (2022)	Processing Times: Under 5 minutes, streamlining customs clearance
Technological Enhancements	CT Scanners	Deployment: Over 300 CT scanners planned for U.S. airports by 2020	Detection Rate: Improved detection of prohibited items, reducing manual bag checks
Biometric Systems		Facial Recognition: Implemented at 20 busiest U.S. airports by 2021	Efficiency Gains: Speeds up boarding process, processing passengers in under 2 seconds with 98% accuracy
Data-Driven Risk Assessment	Advanced Passenger Information System (APIS)	Coverage: Data on over 4 billion passengers annually worldwide	Risk Identification: Identifies high-risk individuals for targeted security measures
Passenger Name Record (PNR)		Global Usage: Used by over 60 countries	Effectiveness: Significant improvements in identifying high-risk individuals, reducing security incidents by up to 20%
Resource Optimization	Security Personnel Allocation	Focused Deployment: 15-20% increase in checkpoint efficiency in some airports	Cost Savings: 10-15% reduction in security-related expenditures
International Cooperation	ICAO Standards	Adoption Rates: Over 190 member states encouraged to adopt risk-based measures	Compliance and Effectiveness: Improved compliance and reduction in security breaches

2.4. AGREEMENT IN USE OF OPEN ARCHITECTURE

2.4.1. Security data share and technology recognition

The chief executives of the Transportation Security Administration (TSA), ACI EUROPE (Airports Council International), and other key organizations, along with prominent airports and industry stakeholders such as London Heathrow, Avinor, and the European Organization for Security (EOS), convened in Brussels to reinforce their commitment to ongoing collaboration on open architecture for airport security systems. This initiative aims to create a cohesive technology framework that promotes teamwork, resource sharing, and the achievement of common objectives (ACI EUROPE, 2021; European Organization for Security, 2021). By facilitating seamless data exchange and simplifying the integration, modification, and upgrading of system modules, open architecture eliminates significant commercial and technical barriers (TSA, 2021). Thus, it is important to study the following benefits of Open Architecture in Aviation Security Systems:

1) Innovation and Technological Diversity

The implementation of open architecture in aviation security systems introduces a plethora of benefits to the airport industry. Primarily, it fosters innovation by offering operators a wider selection of technology options from multiple providers (Airport Technology, n.d.). This flexibility enables airports to meet diverse operational requirements effectively, ensuring that they are not confined to a single vendor's solutions. As a result, airports can adopt cutting-edge technologies that best suit their unique security needs (ACI EUROPE, 2021).

2) Rapid Adaptation to Emerging Threats

Open architecture facilitates quicker and more effective responses to emerging threats and technological advancements. The adaptable nature of open systems allows for timely updates and modifications, ensuring that security measures remain robust and resilient in the face of new challenges (Airport Technology, n.d.). This adaptability is crucial for maintaining the highest standards of security in an ever-evolving threat landscape.

3) Operational and Business Efficiency

Operational, business, and procurement efficiencies are significantly enhanced through the adoption of open architecture. The ability to swiftly adjust screening technologies in response to changing threat environments and resource demands streamlines operations (Airport Technology, n.d.). This flexibility leads to cost savings and improved allocation of resources, optimizing the overall efficiency of airport security systems.

4) Standardization and Interoperability

Standardized and interoperable interfaces between security systems and business management tools are a cornerstone of open architecture. These standardized interfaces ensure seamless integration and cooperation between airport operators and regulators, promoting data accuracy and adherence to testing procedures (ACI EUROPE, 2021). Additionally, interoperability reduces the ongoing expenses associated with complex system integrations, providing long-term financial benefits (European Organization for Security, 2021).

5) Data Availability and Advanced Applications

Open architecture establishes a foundation for readily available data and outputs, which are essential for advanced applications such as data analytics, machine learning, and artificial intelligence (Airport Technology, n.d.). These technologies can significantly enhance corporate resources, providing valuable insights that support decision-making processes. Furthermore, the integration of advanced data analytics improves the overall passenger experience by enabling more efficient and effective security measures.

The collaborative effort to implement open architecture in aviation security systems represents a significant advancement in the industry. By fostering innovation, facilitating rapid adaptation to emerging threats, enhancing operational efficiency, promoting standardization, and enabling advanced data applications, open architecture offers a comprehensive solution to the challenges faced by modern airports (ACI EUROPE, 2021). As airports and industry stakeholders continue to work together, the benefits of open architecture will become increasingly evident, ultimately leading to improved security, efficiency, and passenger satisfaction.

2.5. PROPOSED FEATURES FOR AIRPORT SECURITY SYSTEMS OPEN ARCHITECTURE

The development of an architecture for aviation security systems must adhere to specific standards and considerations to ensure effectiveness and efficiency. According to Smith (2023), the system architecture should align with actual system requirements, allowing for necessary modifications in design implementation to remain flexible and adaptable to changing security needs (Smith, 2023). Critical interfaces, including detection, imaging, security protocols, incident alerting, and system health monitoring, are essential for integrating and operationalizing all critical security operations. Service interfaces are also crucial for providing non-critical support functions such as data access and training, enhancing the system's usability and maintenance (Smith, 2023). Resource control mechanisms enable system services software to manage resources for processing information and controls, ensuring optimal performance (Smith, 2023). Additionally, the principle of commonality emphasizes using common hardware and software components to maximize efficiency, with any deviations requiring approval from the relevant authority (Smith, 2023). By adhering to these standards, aviation security architectures can ensure robustness, interoperability, and optimal performance in safeguarding airport operations and passengers (Smith, 2023).

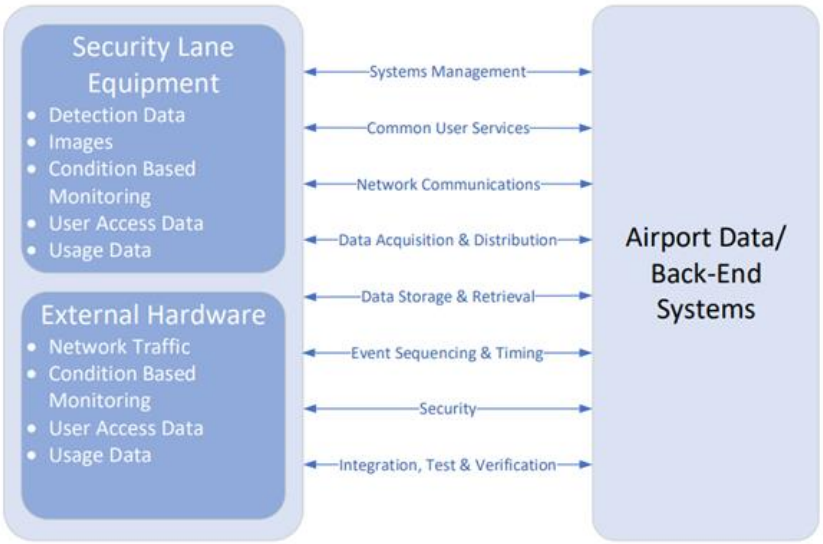


Figure 1 – Security Technology Association. (2024). *Proposed high-level features of security equipment open architecture*. Security Technology Association.

How to use dual recognition documents on open architecture system

The electronic passport, or e-passport, represents an advanced identification document that incorporates relevant biographic and biometric data about its bearer. Embedded with cryptographic capabilities within a Radio Frequency Identification (RFID) chip, the e-passport aims to enhance border security by reducing the likelihood of passport fraud and facilitating easier verification of the document holder's identity. The integration of RFID and biometric technology has the potential to lower fraud, simplify identity checks, and improve overall security, although it also introduces new security and privacy challenges. Radio Frequency Identification (RFID) technology, which uses wireless communication for identification, is central to the e-passport system. The primary distinguishing feature of RFID applications is their identification goal. The RFID system for biometric passport validation, known as the digital passport, combines traditional paper passports with electronic passports, embedding biometric data that can be used to verify a traveler's identity. The e-passport uses contactless smart card technology, which is less sophisticated but effective, employing a microprocessor chip and antenna to power and communicate with the chip. The antenna is typically embedded within the passport's front, rear, or center page, and the RFID cards contain personal information about the passport holder, including details about the issuing institution and the date of issuance (Honade et al., 2018).

Technologies approved by the International Civil Aviation Organization (ICAO) for use as security mechanisms include RFID and biometric systems. RFID technology, which encompasses automatic identification, extracts data from radio waves. This technology is useful in various forms, such as barcodes and integrated chips. An RFID tag, a tiny microchip, is used to transmit data wirelessly, containing details such as the passport holder's name, nationality, gender, place of birth, and digital photo, as well as their unique passport ID number. The passive RFID card operates by wirelessly emitting electricity and communicating through its antenna, typically integrated with RFID tags and readers to enhance signal strength. The chip circuitry's intended operating range is narrow, requiring the card to be held within 10 centimeters of the reader (Honade et al., 2018). Biometric systems in e-passports involve the automated measurement of biological or behavioral features that identify a person. According to ICAO, the three primary biometric features used in e-passports are fingerprint recognition, face recognition, and iris recognition. Fingerprint recognition, the technique implemented in this project, involves digitally capturing the ridges and furrows at the tips of each finger using a compact sensor. The captured fingerprint image is then compared to a live scan image to verify identity (Honade et al., 2018).

In summary, the use of e-passports incorporating RFID and biometric technologies enhances border security by reducing fraud and simplifying identity verification processes. Despite the introduction of new security and privacy risks, these advanced systems offer a robust solution for modern border control challenges.

2.8 Future Developments

The future development of e-passport technology promises several enhancements to improve security, reliability, and convenience. One proposed improvement is the introduction of a One-Time Password (OTP) or personal identification number (PIN) option. This feature would serve as a fallback mechanism in case biometric verification fails. By providing an alternative method of authentication, the OTP or PIN ensures that travelers can still verify their identities securely and continue their journey without undue delays (Honade, Sarwar, Kanawade, & A. H., 2018).

In addition to the OTP/PIN option, face recognition technology could be employed to enhance security further. Face recognition, already used in various security applications, offers a non-intrusive and highly accurate method of verifying a person's identity. This technology can be integrated into e-passports to provide an additional layer of security, ensuring that only the rightful owner can use the passport. Studies have shown that face recognition systems can achieve high levels of accuracy and reliability, making them a valuable addition to the suite of biometric tools used in border security (Jain, Ross, & Prabhakar, 2004).

Another significant advancement would involve storing all biometric and biographic data in a centralized database or cloud. This approach allows for real-time verification and validation of passport data against a secure, centralized repository. Centralized data storage can streamline the verification process, reducing the time required for identity checks and improving overall efficiency. Additionally, it can provide a more robust system for detecting and preventing fraudulent activities by enabling cross-referencing of data from multiple sources (Juels, Molnar, & Wagner, 2005).

Eye scan technology, such as iris recognition, could also be integrated into e-passports to enhance biometric identification further. Iris recognition is known for its high accuracy and resistance to spoofing, making it an ideal candidate for inclusion in advanced security systems. By adding eye scan capabilities, the security of e-passports can be significantly increased, providing a more comprehensive biometric profile of the passport holder. This technology has been successfully deployed in various high-security environments, demonstrating its potential for widespread use in border control applications (Daugman, 2004).

In conclusion, the future developments in e-passport technology aim to create a more secure and efficient system for verifying traveller identities. The introduction of OTP/PIN options, face recognition, centralized data storage, and eye scan technology represents significant steps forward in enhancing the robustness and reliability of e-passports. These advancements, supported by ongoing research and technological innovation, will help ensure that e-passports remain a vital tool in maintaining global security and facilitating international travel.

3. METHODOLOGY

3.1 Design Science Research Methodology

The idea is to suggest a design science research methodology model to help with the project's outcomes. In this model, the research question is addressed by producing creative artifacts, in this case an excel performance management model with specific metrics that will be evaluated by inquiries via survey. DSR is a multistage process that involves the identification of a research problem, the design and development of an artifact to address that problem, the evaluation of the artifact, and the communication of the results. The goal of DSR is to contribute to the development of a body of knowledge that can be used to improve practice in each given field. According to the nature of the work each question is related within the security market, and with these answers inserted on PM Model we can understand how the new technology is applied into the security market influencing their role of work and contributing to greater awareness of aviation security.

Figure 2 depicts a conceptual framework for understanding, conducting, and evaluating design science research. In 2004 Hevner et al. identified the area of difficulty where intriguing occurrences exist is determined by the situation. It consists of people, teams, and technology that has already been used or will be used in the future.

It includes the goals, tasks, problems, and opportunities that, in the eyes of organization stakeholders, define requirements. Needs are assessed and analyzed taking into account corporate strategies, structures, cultures, and current work processes. They are positioned in relation to the existing technical infrastructure, development capabilities, communication structures, and applications. The "research challenge" as perceived by the researcher is described by these components taken together. Stakeholder requests are addressed via framing activities to ensure research relevance.

The knowledge base consists of Methodologies and Foundations. The build phase of a research project uses foundational theories, frameworks, instruments, constructs, models, techniques, and instantiations that are derived from previous studies and conclusions from reference disciplines. Guidelines provided by methodologies are used in the evaluation phase. Rigor is achieved through the proper use of previous foundations and procedures.

DSR Method

Numerous process models, such as those created by Nunamaker, Chen, and Purdin in 1991, Walls, Widmeyer, and El Sawy in 1992, Hevner in 2007, and Kuchler and Vaishnavi in 2008, have been essential to the success of DSR programs. (2008). The most often mentioned model is the one proposed by Peffers, Tuuanen, Rothenberger, & Chatterjee (2008). The process paradigm for design science research methodology (DSRM) is shown in Figure 2. The six-step DSR process has four possible entry points: problem identification and motivation, solution objectives formulation, design and development, demonstration. Additionally, there are four entrance points: client/context, problem-centered, objective-centered, and design and development-centered. As part of the process it also includes assessment, and communication.

A brief description of each DSR activity follows.

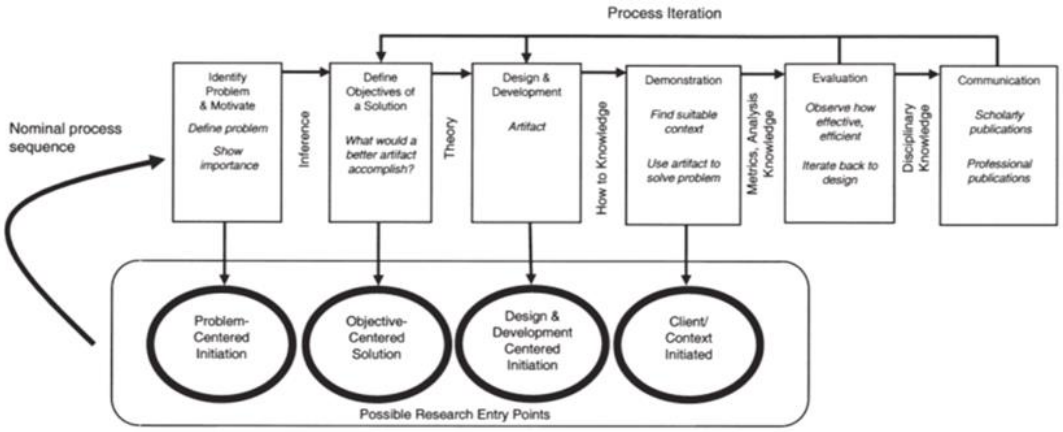


Figure 2 - **"Design Science in Information Systems Research."** Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004).

DESIGN SCIENCE RESEARCH METHOD

The DSR Method helps researchers plan, coordinate, and communicate about their DSR projects in an effective manner (vom Brocke & Maedche 2019). The goal of the DSR grid is to provide a one-page summary of a DSR project, highlighting its essential components to accurately represent and communicate its extent. A DSR project representation like this helps with improved planning and communication, early stakeholder input collection, and challenging and updating the project scope as it advances. The six most important dimensions of a DSR project comprise the DSR Method, as Figure 2 illustrates.

Problem Description: What problem needs to be investigated through a DSR study in order to identify possible solutions? In this case the focus points were to address a database with relevant KPIs in order to be accepted and answers problem statements. These consists of how is the level of feasibility on airport security technologies perceived by the security managers and operations - all contribute to the context, which is defined by research (vom Brocke et al. 2020).

Understanding of Input: What prior knowledge will be used to the DSR initiative? Design Science Research (DSR) in the context of aviation security technologies involves creating and evaluating artifacts designed to solve identified problems. To understand the inputs needed for a project in this area, it's essential to consider several key elements.

In a Design Science Research project for aviation security technologies, problem identification involves a stakeholder analysis to understand needs and priorities, alongside a threat assessment to identify security vulnerabilities and limitations of existing measures (Bajpai & Ravindran, 2018). Solution objectives include preventing unauthorized access, detecting contraband, and ensuring passenger safety, with performance metrics such as detection rates and false alarm rates (Wang, 2016). Design and development require detailing technological requirements (e.g., scanners, biometric systems) and ensuring system compatibility and usability (Gourdin, 2006). Theoretical foundations draw from cybersecurity, risk management, criminology, and design science frameworks (Hevner et al., 2004). Artifact creation involves developing prototypes and pilot programs for real-world evaluation (Peffers et al., 2007). Evaluation includes field testing, stakeholder feedback, and benchmarking against existing solutions (March & Smith, 1995). Iteration focuses on continuous improvement and scalability (Gregor & Jones, 2007). Implementation plans phased rollouts, comprehensive training, and maintenance protocols (Gill & Hevner, 2013). Impact assessment measures security improvements, operational impacts, and cost-benefit analysis (Gregor & Hevner, 2013). Documentation and dissemination record processes and publish findings to advance the field (Peffers et al., 2007).

Research Process: To achieve the intended outcomes in a Design Science Research (DSR) project focused on digital transformation within airport security processes, it is crucial to organize and carry out several key actions. Building and evaluating are essential steps when the desired contribution involves designing new entities (Hevner et al., 2004). Meta-analyses (Denyer, Tranfield, & Van Aken, 2008) and literature reviews (Webster & Watson, 2002; von Brocke et al., 2020) are foundational tasks supporting the design phase. These reviews help synthesize existing knowledge and identify gaps that the new technology aims to address.

Solution Description: Introducing innovative security technology into airport security procedures is the DSR project's approach to solving the challenge. As per the findings of Brocke et al. (2020), the solution description has to clarify the basic functions of the suggested technologies and their positioning in the solution domain. Constructs (theoretical frameworks defining digital transformation and security technologies), models (conceptual representations of how these technologies integrate with current processes), techniques (specific methods for implementing and using these technologies), and instantiations (actual implementations of the technologies in airport settings) are all combined to represent the solution in this context. With this thorough approach, you can be sure that the solution is well-defined and positioned to properly solve the problems that have been identified.

Problem Identification: The primary problem addressed in this project is the inefficiency and vulnerability of current airport security processes. Traditional security measures often lead to long wait times, passenger inconvenience, and potential security breaches due to outdated technologies and methods. The challenge is to enhance these processes through digital transformation, leveraging new security technologies to improve efficiency, accuracy, and overall security.

Process Definition: The process for this Design Science Research (DSR) project involves several critical steps to ensure the effective integration of new security technologies within airport security processes. The initial phase comprises conducting an extensive literature review and meta-analysis to identify gaps and opportunities in existing research on digital transformation and security technologies. This is followed by the design speculation phase, where speculative designs and hypotheses are developed to address the identified gaps. Subsequently, the construction phase involves building prototypes or models of the proposed security technologies and integrating them into current airport security processes. The effectiveness of these prototypes is then assessed through empirical research, which includes both qualitative and quantitative methods. Throughout this process, meticulous documentation of all steps, findings, and modifications is essential to maintain transparency and reproducibility.

Key concepts for the DSR project on digital transformation within airport security processes include digital transformation, security technology implementation, airport security processes, and impact assessment. Digital transformation refers to the comprehensive integration of digital technology into all areas of airport security, fundamentally altering how security operations are conducted. Security technology implementation involves the adoption and integration of new technologies, such as biometrics, RFID, and advanced scanning systems, into existing security frameworks. Airport security processes encompass the set of procedures and protocols employed by airport security to ensure passenger safety and regulatory compliance. Impact assessment evaluates the effects of these new security technologies on efficiency, accuracy, passenger experience, and overall security performance. By focusing on these concepts and following a structured research process, the DSR project aims to develop and validate innovative solutions that significantly enhance airport security operations.

The output knowledge for the DSR project on digital transformation in airport security encompasses several key constructs. The Digital Transformation Framework outlines the necessary steps and considerations for integrating digital technologies into airport security processes. This framework includes an assessment phase to evaluate current security processes and identify areas for improvement, technology selection based on this assessment, and integration planning to develop a detailed plan for incorporating the selected technologies into existing processes. Following this, the implementation phase executes the integration plan while ensuring minimal disruption to ongoing operations, and finally, continuous monitoring and evaluation are conducted to assess the performance of integrated technologies and make necessary adjustments. Security Technology Constructs are also defined, specifying new technologies relevant to airport security such as biometrics for facial recognition and fingerprint scanning, RFID for tracking luggage and personnel, and advanced scanning systems for high-resolution imaging.

Additionally, the project includes the development of integration and process models. Integration Models conceptually represent how new security technologies can be integrated with existing processes. These models show how digital technologies fit into current security workflows, how data from these technologies are collected, processed, and utilized, and the overall architecture of integrated systems. Process Models provide detailed representations of airport security procedures incorporating new technologies to streamline operations, including pre-screening processes using digital technologies for passengers and luggage, real-time screening with advanced scanning systems, and post-screening analysis using data analytics to evaluate the effectiveness of screening processes and identify potential improvements.

Techniques for implementing and using new security technologies are also detailed. Implementation Techniques include specific methods and procedures for deploying new technologies in airport settings, such as installation guidelines, training programs for security personnel on how to use and maintain the technologies, and maintenance protocols for ensuring continued functionality. Usage Techniques cover best practices for the day-to-day use of new security technologies by airport security personnel, including operational procedures for different phases of security checks, troubleshooting guidelines for addressing common issues, and comprehensive user manuals detailing the functionality and features of the technologies. The project also features instantiations in the form of prototype systems and demonstrations, showcasing the practical feasibility and effectiveness of new security technologies in real-world scenarios. These instantiations highlight efficiency gains, such as reduced wait times and faster processing of passengers and luggage, enhanced security with improved detection capabilities and reduced security breaches, and improved passenger experience with greater convenience and satisfaction.

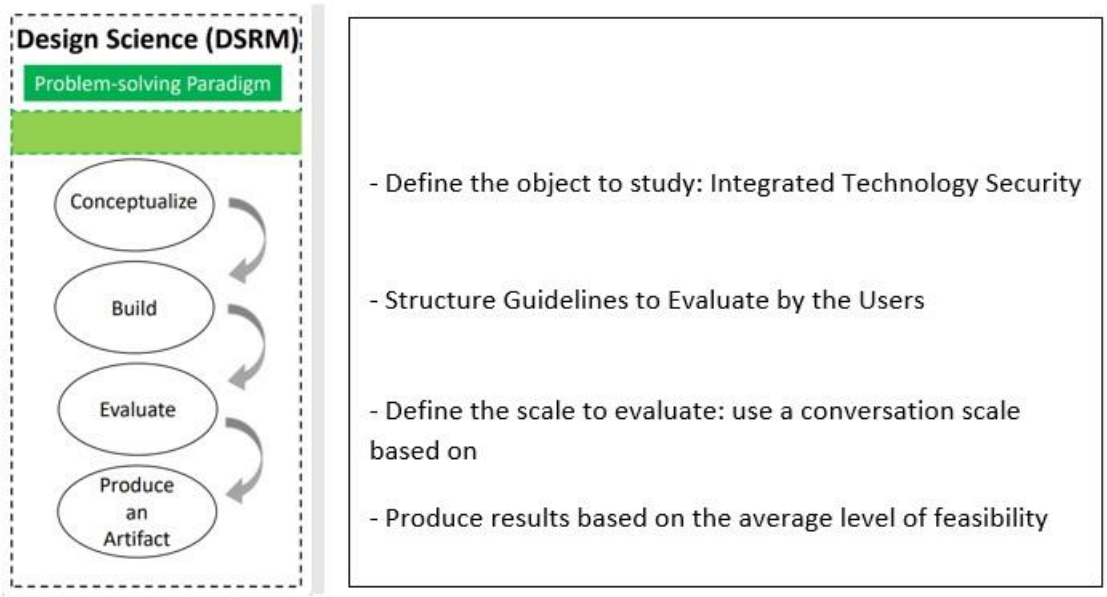


Figure 3 - Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). **"Design Science in Information Systems Research."** MIS Quarterly, 28(1), 75-105.

Creating a Focus Group

A focus group is a qualitative research method involving a structured group interview to explore concepts with participants, guided by a specific topic and a moderator (Morgan, 1988). It allows face-to-face communication, adaptability in discussing different design concepts, and provides rich, diverse data, facilitating a clear understanding of the design and generating new ideas or identifying issues (Stewart et al., 2006; Tremblay et al., 2010). The process involves planning (setting objectives, preparing questions, recruiting participants), execution (moderating discussions), and analysis (evaluating data and summarizing results) as outlined by Morgan (1988) and Stewart et al. (2007).

In this case the target group have been identified among aviation operators and its based o testimonies of aviation security specialists and security operators. In specific a Security Management team composed of 4 elements and a Group of Scaled Security Staff for a shift around 12 elements. For these elements the dashboard was introduced with the porpoise of evaluation the impact of security technology equipments in use and evaluate his performance. The questions made correspond to the KPIs and on a rate from 1 to 10 the given answers introduced on a excel sheet and then the calculated average introduced on the DB to obtain the final results.

3.2 Data & Results

3.2.1 Performance Management Model (KPIs BASED)

This chapter's goal is to outline the recent 10-15 years worth of new approaches and work styles that organizations have adopted, as well as the professional development brought on by a bet on organizational performance business models. The use of techniques for motivating employees at work, such as performance management procedures.

Description of a large variety of performance management practices, their theoretical underpinnings resulting on the setting of KPIs becomes a relevant discipline, and their application to understand human behavior and their position in the labor market.

3.2.2 The Role of KPIs

Due to the broad definition of key performance indicators, both private and public sector organizations find it challenging to establish KPIs. Performance indicators should be applied carefully because they are not an end in themselves. Behn (2003) addresses the topic of why managers should evaluate performance. He added that they might find such tactics useful in reaching managerial goals in his response. Valins and Slater (1996) discuss the difficulties in assessing how buildings affect people's feelings, attitudes, behaviors, performance levels, and satisfaction in relation to the functional performance of the facility and the organizational objectives.

The majority of KPIs in facilities management deal with costs of operation, running a facility, managing revenue-generating space, managing the environment, and dealing with health and safety concerns. KPIs are essential for enhancing the reputation of the construction sector.

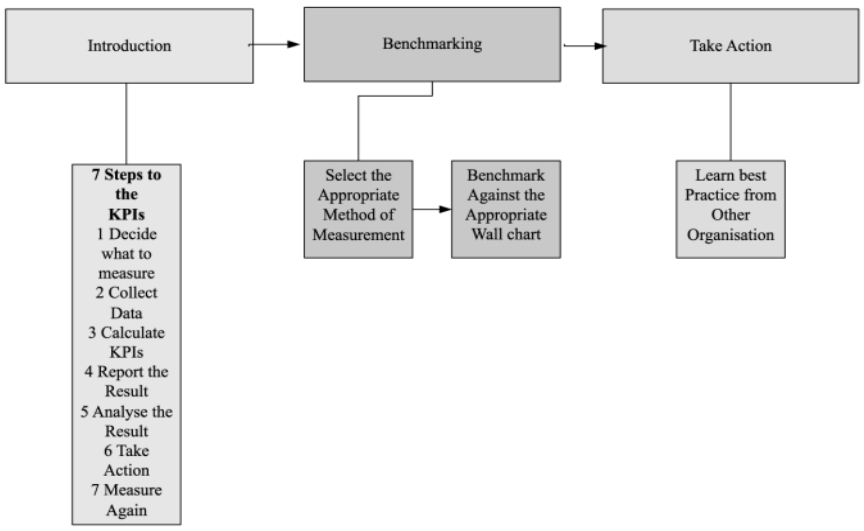


Figure 4 - KPI development and implementation Parmenter, D. (2015). *Key Performance Indicators: Developing, Implementing, and Using Winning KPIs*. John Wiley & Sons.

Gauging performance in the aviation sector involves a straightforward process: starting with the seven KPI steps, comparing project and performance data with others, and using the results to identify areas for improvement. It's essential to monitor performance trends and contrast them with data from other sources to maintain accuracy and relevancy.

There is no consensus on performance metrics within the aviation sector. Doganis and Graham (1987) noted that while few airports have developed and utilized performance indicators, agreement on which indicators to use or their value is lacking. This thesis aims to address this gap by developing and testing KPIs specifically for airport security.

Doganis and Graham's study primarily focused on the potential application and reliability of performance indicators as tools for airport management. In contrast, this research will develop and test KPIs for airport security and explore the role of facilities management (FM) in enhancing airport performance. These KPIs are designed for comparison, allowing for the evaluation of security across different airports regardless of size or location.

Performance indicators help analyze historical data, guiding management in resource allocation and benchmarking decisions. For instance, if results highlight shortcomings in airport facility maintenance response times, management can use this information to plan future maintenance activities and set performance goals for staff. KPIs can identify necessary data, highlight limitations in current data, and establish criteria for comparing and evaluating other measurements. A Performance Management Model will facilitate like-for-like comparisons of operations across multiple airports and within the same airport over time.

It's crucial to ensure that KPIs for airport safety are interpreted by those with in-depth knowledge of the specific measurements. Without expert interpretation, the indicators may be misunderstood or misused, despite being user-friendly and easy to comprehend.

Furthermore, the demand for airport services is highly inelastic; passengers prioritize safety and security over cost. They will avoid airports where they feel unsafe, regardless of pricing. This study aims to develop a general set of KPIs for facilities management, which will be used to monitor airport security design. These KPIs should not only be accepted by airport operators and aviation experts but also reflect passengers' trust in the implemented security technologies.

3.2.3 Support Methodology to justify the use of KPIs

Set of a Literature Review: Following an extensive preliminary literature review, a multifaceted approach was employed to develop, test, and validate a comprehensive set of Key Performance Indicators (KPIs) for airport security. This methodology was meticulously designed to incorporate a blend of case studies (Yin, 2017), structured interviews with key airport personnel (Kvale & Brinkmann, 2009), and a series of questionnaires (Bryman, 2016). In addition, observational techniques (Angrosino, 2007) and interactive workshops (Kolb, 2014) were integral to this process. Each component of this methodology played a critical role: the case studies provided in-depth insights into real-world applications, the structured interviews elicited valuable expert opinions, the questionnaires gathered quantifiable data from a broader audience, and the observations and workshops facilitated a dynamic exchange of ideas and practical feedback. This holistic approach ensured a robust and thorough examination of the KPIs, ultimately leading to their effective validation and refinement for implementation in the aviation security sector.

Pilot study (Prior to the KPIs Questionnaire): Following the initial literature review, the pilot study marked the beginning of the questionnaires process. Within empirical research, a variety of methodologies are employed, such as case studies, factor analysis, experiments, and surveys. Pfleeger and Kitchenham (2001) emphasize that it is crucial to focus on organizing, executing, and analyzing the study to yield meaningful and applicable results. The pilot questionnaires in this study provided valuable insights into what could be expected in the full-scale questionnaires.

This stage is critically important as it involves theoretical justification. In this context, the use of a Design Science Research Methodology was pivotal in determining whether the developed list of KPIs was sufficiently tailored to the aviation sector and whether prior research was too broad for the scope of the investigation. The findings from the pilot survey were instrumental in shaping the design of subsequent interviews, questionnaires, and the overall set of KPIs. This iterative process ensured that the tools and methods employed were both relevant and specific to the needs of airport security.

KPIs Questionnaire: During the questionnaire phase, multiple managers and operators were contacted at different times on the airport premises. We set aside about an hour for questions and answers, and as additional information was found and investigated, the process became iterative. A total of 16 surveys with pre-given KPIs that each specialist had to rate on a scale of 1 to 10 in order to complete the excel response sheet were sent out. The same set of questions were then added to a database and assessed based on the weight assigned to each KPIS. These questions and their responses are critical since they are related to the airport's daily operations.

The Workshops: Prior accepting the KPIs and use them on the DB it is important to test and validate the proposed KPIs.

A revised list of KPIs was identified and further developed at several workshops that aimed to validate the safety and security KPIs based upon two major classes of incidences: "airport incidence," which refers to any breach or emergency that takes place inside the airport, and "aircraft incidence," which refers to incidents that take place outside the airport but inside the aircraft. At the conclusion of this paper, this modified list is discussed, and it is suggested that this amended list will be further studied and it will be conducted with the airport teams to identify the following in relation to each KPI after a list of KPIs has been produced and authorized. This results on, priorities definition, identification of measures of success and set of targets for performance improvement.

Priorities were established to detail the operational practices employed during incidents involving the identified KPIs, which themselves acted as benchmarks for measuring the system's effectiveness and efficiency, as well as the adequacy of resources to address arising issues. The KPIs functioned as indicators of success, providing data on performance and resource utilization. Targets were set to monitor progress, indicating how effectively the airport was leveraging its resources. Following the approval of the KPI list, further research with airport teams was planned to assess each KPIs impact on airport facilities and any potential design implications. This process culminated in a final set of KPIs, which were then validated through expert opinions.

3.3 KPIs

3.3.1 Analysis of Proposed KPIs prior KPIs definition

In the case of a breach of security, the priorities are the speed of identifying and dealing with the breach, using CCTV, airport control centers, communication between officers, and uniform direction of passenger movement. The measure of success is the shutdown and reopening time of the airport after a breach. The target is to reduce the time required for shutdown and reopening based on past trends. The justification for this KPI is its feasibility, as it uses existing technologies like CCTV and airport control centers. It is accepted by authorities because it ensures safety and quick resolution, which are critical for public safety and airport operations.

For evacuation in the case of an emergency, the priorities are the speed and efficiency of evacuation, clear communication, signage, and officer effectiveness. The measure of success is the time taken for business operations to resume after an incident. The target is to eliminate threats within control and implement emergency measures for uncontrollable threats. This KPI is feasible because clear protocols and communication channels can be effectively implemented. It is accepted by authorities as it prioritizes passenger safety and ensures a quick return to normal operations, essential for maintaining public trust and operational continuity.

Hysteria control has priorities such as the speed of control and support for affected individuals, effective communication, setting up support zones, and smooth transition from aircraft to support areas. The measure of success is the effectiveness of handling and resolving incidents with minimal destruction and quick return to normalcy. The target is to reduce incident occurrences and implement measures to handle situations efficiently. The feasibility of this KPI lies in establishing support systems and communication protocols, which are manageable with proper training. Authorities accept it as essential for managing public perception and ensuring the emotional and physical safety of passengers and staff.

When addressing attacks on airport facilities or installations, the priorities are the speed of restoring services, availability of backups, easy repair or replacement, and a strong workforce. The measure of success is the time taken to resume normal service after incidents. The target is to eliminate occurrences by enhancing protection and surveillance. This KPI is feasible because enhancing security measures and preparing contingency plans are achievable. Authorities find it vital for maintaining airport infrastructure and operational integrity.

For destructive or criminal behavior by passengers or directed at cargo, the priorities are the speed and manner of dealing with the incident, clear communication, and early support services. The measure of success is the time taken for normal service to begin. The target is to eliminate incidents within control and ease the effects of uncontrollable incidents. This KPI is feasible as training staff and implementing clear communication strategies are practical steps. It is accepted by authorities because it ensures swift handling of disruptions and minimizes the impact on airport operations and safety.

Overall, the feasibility of these KPIs is supported by the fact that each one leverages existing infrastructure and protocols, making implementation straightforward. Clear, actionable measures ensure that progress can be tracked and improvements made. Authorities accept these KPIs because they focus on safety, efficiency, and quick recovery, aligning with regulatory and operational priorities. Emphasis on reducing disruption and maintaining public confidence is crucial for airport authorities. In summary, these KPIs are accepted by authorities and have a good feasibility rate because they are practical, focused on critical aspects of airport operations, and ensure that there are clear, measurable targets for improvement.

3.3.2 Defined KPIs

Number of security checks

Number of technical support teams

Number of surveillance cameras

Number of security staff

Surprise security visits

Security I-cards

Security Standard procedures

Security Reeinforced check procedures

Number of suspicious cases

Time taken for security checks

Number of incidents due to security failure

Access granted cases per day

Non-Access granted cases per day

Contribute of Technology Security to alertness level

Level of Trust on Tech Security Equipment’s

4. RESULTS AND DISCUSSION

4.1 Answers and Analysis

A total of sixteen intervenients were interviewed throughout the data gathering phase. The KPIs listed below were the ones that the aviation expert needed to rate, and table 3 displays the results as follows. As part of the process for results collection a focus group was identified and invited to measure each KPIs on a scale of importance from 1 to 10 where 1 poor/relevant and 10 adequate/not relevant. The answered questions were Number of security checks with an average rate of 5, Number of technical support teams with an average rate of 7, Number of surveillance cameras with an average rate of 4, Number of security staff with an average rate of 5, Surprise security visits with an average rate of 6, Security I-cards with an average rate of 6, Security Standard procedures with an average rate of 8 and Security Reinforced check procedures with an average rate of 7. These were the first set of questions where we can affirm the lowest score was 4 and the highest 8. For the next set of questions the answers were as follows, Number of suspicious cases with an average rate of 5, Time taken for security checks with an average rate of 6, Number of incidents due to security failure with an average rate of 2, Access granted cases per day with an average rate of 8, Non Access granted cases per day with an average rate of 4, Contribute of Technology Security to alertness level with an average rate of 7 and Level of Trust on Tech Security Equipment's with an average rate of , for this set of questions the lowest score was 2 and the highest 8.

Table 3 – Aviation Security Survey Answers

KPIS	RATES
Number of surveillance cameras	4
Number of security checks	5
Number of security staff	5
Surprise security visits	6
Security I-cards	6
Security Reeinforced check procedures	7
Security Standard procedures	8

Number of incidents due to security failure	2
Non-Access granted cases per day	4
Number of suspicious cases	5
Time taken for security checks	6
Contribute of Technology Security to alertness level	7
Level of Trust on Tech Security Equipments	7
Acess granted cases per day	8

As the first data was collected, the first conclusions which are represented as follows: General Feedback on Digital Transformation and New Security Technology Implementation

Table 4 – Aviation Security Procedures Optimization

Strengths
Standardized Procedures and Reinforced Checks: These are highly valued, suggesting that structured and rigorous security protocols are critical to the perceived effectiveness of airport security.
Technical Support and Use of Technology: The high ratings for technical support teams and the contribution and trust in security technology reflect positive perceptions and satisfaction with the technological aspects of security.
Areas of Improvement
Security Incident Management: The low score for incidents due to security failures is a red flag, indicating a need for better measures to prevent security breaches.
Surveillance Camera Utilization: The lower importance placed on surveillance cameras may suggest a need for reassessment of their deployment or integration with other security measures
Efficiency in Security Checks and Staffing: The moderate relevance scores for the number of security checks and staff suggest potential areas for optimization to ensure both thoroughness and efficiency.
Overall Impact
The feedback suggests that while digital transformation and new security technologies are well-regarded and seen as enhancing security, there are critical areas needing attention, particularly in preventing security failures and optimizing surveillance. Strengthening these areas will further bolster the perceived effectiveness and reliability of airport security processes.

4.2 Security Equipment's in Scope for Open Architecture

The following table defines the security equipment that Open Architecture will include for Airport Operators and Regulators:

Table 5 – Security Equipment in Scope for Open Architecture - Transportation Security Administration. (2023). Open architecture for airport security systems. TSA Publications.

Security Equipment	Algorithms	Data	External References
Security Scanner	In Scope	In Scope	In Scope
X-Ray technology (eg Computed Tomography [CT], traditional 2D and diffraction)	In Scope	In Scope	In Scope
ATRS	In Scope	In Scope	In Scope
Shoe Metal Detection (SMD) and Shoe Explosive Detection (SED) equipment	tbc	In Scope	In Scope
Explosive Trace Detection (ETD)	tbc	In Scope	In Scope
Walk Through Metal Detector (WTMD)	tbc	In Scope	In Scope
Common Viewing Station	In Scope	In Scope	In Scope
Other technology, eg CCTV, optical trace detection, Liquid Explosive Detection Systems (LEDS)	tbc	tbc	tbc

4.3 Database and KPIs Answers Analysis

The provided performance dashboard for the Airport Tech Security Plan (Figure 5), presenting various key performance indicators (KPIs) across two main perspectives: Security Measures and Level of Security Technology Efficiency.

In the Security Measures perspective, the dashboard highlights several metrics such as the number of security checks, security staff, surveillance cameras, technical support teams, security I-cards, and specific procedures like reinforced checks and standard protocols. Most of these indicators show strong performance, with actual values surpassing their targets. For instance, the number of security checks and security staff are both performing at 106.12% of the target, indicating a slight overachievement in these areas. The number of technical support teams is also significantly above target at 125%, suggesting robust support in technical aspects. Standard procedures and surprise security visits are notably higher than the target, achieving 135.71% and 79.37%, respectively, which reflects thorough adherence to and enforcement of security protocols.

The Level of Security Technology Efficiency perspective shows varied performance. Metrics like access granted cases per day, contribution of technology security to alertness level, and level of trust in tech security equipment are either meeting or exceeding their targets, with access granted cases per day exactly at target (100%) and trust in tech security equipment slightly above target at 101.11%. However, areas such as non-access granted cases per day are just at 80% of the target, which could imply stricter control or possible inefficiencies. Notably, the number of incidents due to security failure is substantially high at 300%, indicating a critical area that needs immediate attention and improvement to prevent future security breaches. Furthermore, the number of suspicious cases is performing negatively at -50%, and the time taken for security checks is at 0%, highlighting significant issues in these areas which could affect overall security efficiency.

Overall, while the majority of security measures are performing well, demonstrating a strong security framework at the analyzed Airport, the efficiency of security technology shows mixed results with some critical areas needing improvement. Specifically, addressing the high number of incidents due to security failure and the efficiency of resolving suspicious cases should be prioritized to enhance the overall effectiveness of the security technology system.

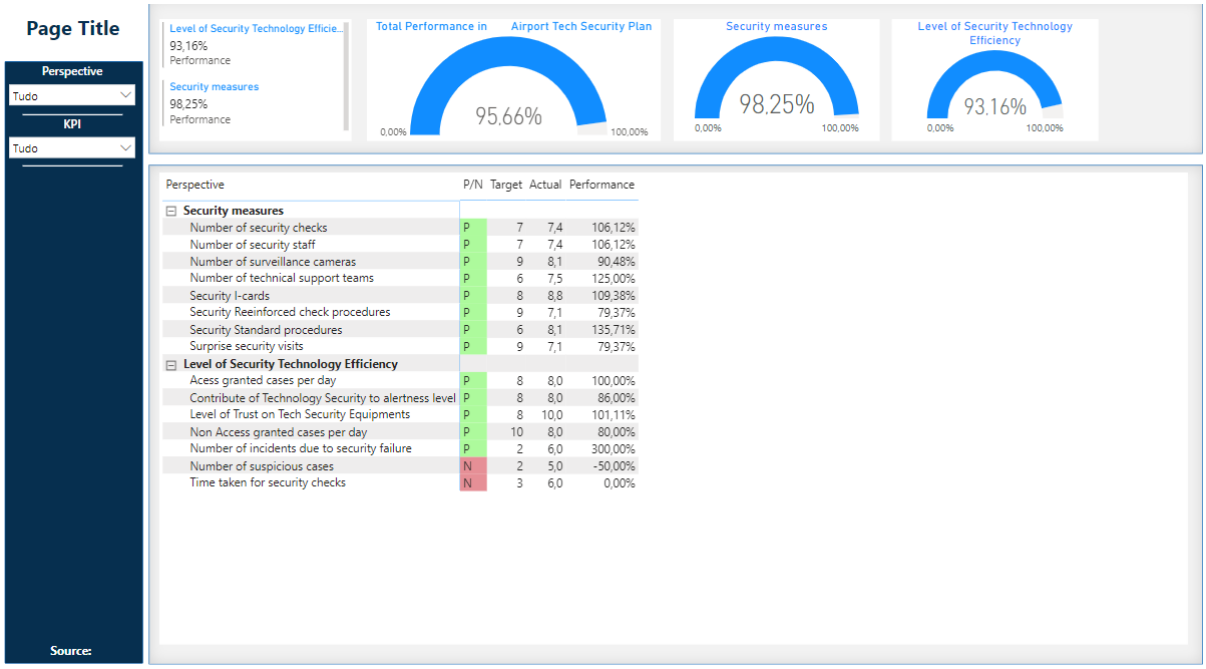
Key summary metrics reflect the overall performance of the Airport Tech Security Plan. The primary indicators highlighted include Total Performance, Security Measures, and the Level of Security Technology Efficiency.

Total Performance in the Airport Tech Security Plan stands at 95.66%. This high percentage suggests that the overall implementation and execution of the security plan are largely effective, approaching the target of 100%. This metric provides a consolidated view of all the individual components' performances, indicating that the airport's security plan is functioning at a highly satisfactory level.

Security Measures are performing exceptionally well, with a performance metric of 98.25%. This nearly perfect score indicates that the various aspects of security measures, such as security checks, staffing, surveillance, and procedures, are being executed with high efficiency and effectiveness. The strong performance in these fundamental security components underlines a well-maintained and robust security infrastructure at the airport.

The Level of Security Technology Efficiency is measured at 93.16%. While slightly lower than the Security Measures, it still represents a high level of efficiency in the application and integration of security technology. This metric encompasses the efficiency of access controls, the contribution of technology to security alertness, and trust in security equipment. Although the performance is commendable, it also points to some areas where there may be room for improvement, particularly in handling incidents due to security failures and suspicious cases.

The blue sections of the dashboard depict an overall strong performance of the Airport Tech Security Plan. The high percentages across Total Performance, Security Measures, and Security Technology Efficiency reflect an effective and well-implemented security strategy, although continuous monitoring and improvements, particularly in technology-related incidents, will ensure sustained security excellence.



Perspective	P/N	Target	Actual	Performance
Security measures				
Number of security checks	P	7	7,4	106,12%
Number of security staff	P	7	7,4	106,12%
Number of surveillance cameras	P	9	8,1	90,48%
Number of technical support teams	P	6	7,5	125,00%
Security I-cards	P	8	8,8	109,38%
Security Reeinforced check procedures	P	9	7,1	79,37%
Security Standard procedures	P	6	8,1	135,71%
Surprise security visits	P	9	7,1	79,37%
Level of Security Technology Efficiency				
Acess granted cases per day	P	8	8,0	100,00%
Contribute of Technology Security to alertness level	P	8	8,0	86,00%
Level of Trust on Tech Security Equipments	P	8	10,0	101,11%
Non Access granted cases per day	P	10	8,0	80,00%
Number of incidents due to security failure	P	2	6,0	300,00%
Number of suspicious cases	N	2	5,0	-50,00%
Time taken for security checks	N	3	6,0	0,00%

Figure 5 - Airport Database Results

Finally, in light of this database's contribution, sixteen professionals who were interviewed were asked to score the provided KPIs on a scale of 1 to 10 according to how they felt about the used technologies. Security operations, which integrates security activities on a daily basis, and security managers were the intervenients. This database shows their stated level of satisfaction with each KPIs and attempts to illustrate how they feel generally about the effectiveness of the use of technology in aviation security procedures.

5. CONCLUSIONS AND FUTURE WORKS

The analysis of the Dashboard designed to evaluate airport tech security plan performance metrics and the focus group's evaluation provides a comprehensive view of the airport's security infrastructure, highlighting both strengths and areas for improvement. The focus group's ratings and the performance dashboard collectively offer a nuanced understanding of the current state of security measures and technology efficiency at the airport.

Comparing this analysis with similar works in airport security, it is evident that studied Airport is performing well in terms of standardized procedures, technical support, and the implementation of technology. These aspects are often highlighted in industry reports and academic studies as critical components of a robust airport security framework. For instance, research emphasizes the importance of standardized procedures and technological integration in enhancing airport security, which aligns with the high ratings for security standard procedures and the contribution of technology to alertness levels at the Analized Airport.

However, the critical areas needing improvement, such as the high incidence of security failures and the inefficiencies in handling suspicious cases, are also commonly identified in the literature. Studies have pointed out that while technological advancements and increased staffing can enhance security, the human element and procedural adherence remain significant challenges. The focus group's low rating for the number of incidents due to security failure (average rate of 2) and the negative performance in suspicious case management reflect these ongoing challenges.

All off the given results were only possible because this database was created and agreed among the professional, as this study aims to answer a set of important KPIs that globally permits this dashboard to be accepted as a model to measure Airport Tech Security Plan global satisfaction.

The future guidelines for improving airport security should focus on several key areas. First, enhancing the integration and utilization of surveillance cameras can address the lower importance placed on this aspect by the focus group (average rate of 4). Advanced surveillance technologies, including AI-powered analytics, can significantly improve the monitoring and detection capabilities, as suggested by recent advancements in security technology research. Second, improving incident management protocols is crucial. The high number of incidents due to security failures (300% of the target) indicates a need for robust incident response strategies, including regular training and simulations for security personnel to handle breaches effectively.

Additionally, optimizing the efficiency of security checks and staffing is essential. The moderate relevance scores for the number of security checks and security staff suggest a need for better balancing thoroughness with efficiency. Implementing streamlined processes and leveraging technology such as biometric screening and automated check-in systems can help achieve this balance.

In terms of broader implications and future research, the ongoing evolution of digital transformation in airport security must be closely monitored. The positive feedback on the use of technology and technical support teams underscores the importance of continued investment in these areas. Future studies should explore the long-term impacts of digital security measures and the integration of emerging technologies such as blockchain for secure data management and Internet of Things (IoT) devices for real-time monitoring.

In conclusion, while the Dashboard designed to evaluate airport tech security plan demonstrates strong performance in many areas, continuous improvement is necessary to address the highlighted weaknesses. By enhancing surveillance, improving incident management, and optimizing security procedures, the airport can further strengthen its security infrastructure. Future research and industry practices should focus on leveraging technological advancements and ensuring rigorous adherence to security protocols to maintain and enhance airport security effectiveness.

BIBLIOGRAPHICAL REFERENCES

ACI Europe :, E. (2023). Open architecture for airport security systems. Aci-europe.org. Obtido 24 de julho de 2024, de https://www.aci-europe.org/downloads/resources/TSA-230504-7_4.1%20Attachment%201%20OA%20for%20Airport%20Security%20Systems%202nd%20Edition%20%20FINAL.pdf

Airports Council International Europe. (2023). Aci-europe.org. Retrieved July 24, 2024, from https://www.aci-europe.org/media-room/468-inaugural-guidance-on-open-architecture-for-airport-security-systems-establishes-detailed-recommendations-for-implementation-across-national-regulators-airport-operators-manufacturers-and-service-providers.html

Airports Council International. (2001). *AVIATION SECURITY TECHNOLOGY - Airport Requirements*. Aci-Europe. https://www.acieurope.org/downloads/resources/Aviation%20Security%20Technology%20-%20European%20Airport%20Requirements.pdf

Ana Aeroportos de Portugal. (2010). Segurança da Aviação Civil: Nível 13 e 14. Obtido 24 de julho de 2024,https://www.ana.pt/sites/default/files/documents/normas_de_seguranca_na_plataforma_ahd_versao_2_nov2019.pdf

ANAC. (2013). Programa Nacional de Controlo de Qualidade da Segurança da Aviação Civil. 76.

ANAC. (2010). Programa Nacional de Formação em Segurança na Aviação Civil (p. 34).

Angrosino, M. (2007). Doing Ethnographic and Observational Research. SAGE Publications.

ASQ Awards and recognition. (sem data). ACI World. Obtido 24 de julho de 2024, de https://aci.aero/programs-and-services/asq/asq-awards-and-recognition/

Aviation security and facilitation. (sem data). Icao.int. Obtido 24 de julho de 2024, de https://www.icao.int/Security/Pages/default.aspx

Baker, J. (2019, janeiro 2). How can AI help speed up airport security? Airport Technology. https://www.airport-technology.com/features/ai-at-airports-security/

Biometric update: Biometrics news, companies and explainers. (2012, maio 7). Biometric Update | Biometrics News, Companies and Explainers. https://www.biometricupdate.com/

Bryman, A. (2016). Social Research Methods. Oxford University Press.

Daugman, J. (2004). How Iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology: A Publication of the Circuits and Systems Society, 14(1), 21–30. https://doi.org/10.1109/tcsvt.2003.818350

European Data Protection Supervisor. (2013). Entry/Exit System (EES) and Registered Traveller Programme (RTP). Obtido 24 de julho de 2024, de https://www.edps.europa.eu/data-protection/our-work/publications/opinions/entryexit-system-ees-and-registered-traveller_en

European Organization for Security (Retrived July 24,2024). What is EOS?. https://www.eos-eu.com/

European Union. ENISA - Risk management remains an important tool for classifying and assessing current risks and threats. (2016, January 20). https://www.enisa.europa.eu/topics/risk-management

Future travel experience. (sem data). Future Travel Experience. Obtido 24 de julho de 2024, de https://www.futuretravelexperience.com/

Gillen, D., & Morrison, W. G. (2015). Aviation security: Costing, pricing, finance and performance. Journal of Air Transport Management, 48(c), 1–12. https://doi.org/10.1016/j.jairtraman.2014.12.005

Honade, S., Sarwar, A., Kanawade, S., & Hawle, A. (2018). Electronic passport using RFID. Ijisrt.com. Obtido 24 de julho de 2024, de https://ijisrt.com/wp-content/uploads/2018/03/Electronic-Passport-using-RFID.pdf

(2020). Iata.org. Obtido 24 de julho de 2024, de https://www.iata.org/contentassets/cb691a38573642d0bbfd2ba380eaf04e/no2-americas-focus-october-2020.pdf

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology: A Publication of the Circuits and Systems Society, 14(1), 4–20. https://doi.org/10.1109/tcsvt.2003.818349

Janson, M. (2023). Enhancing cyberspace monit enhancing cyberspace monitoring in the United States aoring in the United States aviation viation industr industry: A multi-lay: A multi-layered appryered approach for addroach for addressing emeressing emerging ging thr threats eats. Erau.edu. Obtido 24 de julho de 2024, de https://commons.erau.edu/cgi/viewcontent.cgi?article=1772&context=edt

Juels, A., Molnar, D., & Wagner, D. (2005). Security and privacy issues in E-passports. First international Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 2005, pp. 74-88, doi: 10.1109/SECURECOMM.2005.59.

Kolb, D. A. (2014). Experiential Learning: Experience as the Source of Learning and Development. Pearson Education.

Kvale, S., & Brinkmann, S. (2009). InterViews: Learning the craft of qualitative research interviewing, 2nd ed. Thousand Oaks, CA, US: Sage Publications, Inc InterViews: Learning the Craft of Qualitative Research Interviewing, 2, 354. https://psycnet.apa.org/fulltext/2008-15512-000.pdf

Lo, C. (2020, October 16). Open architecture: a new vision for airport security. Airport Technology. https://www.airport-technology.com/features/open-architecture-airport-security/

Paper, A. F. &. S. (2018). *Digital Transformation Of Airport Airside Operations Airports Invest In Digitalisation Of Airside Operations To Achieve Operational Efficiencies And Reduce Impact Of Disruptions*. Adbsafegate.com. https://adbsafegate.com/media/4hxibx1n/digital-transformation-of-airport-airside-operationswhite-paper.pdf

Programa Nacional de Formação em Segurança na Aviação Civil. (2010). Obtido 24 de julho de 2024, https://www.anac.pt/vPT/Generico/LegislacaoRegulamentacao/LegislacaoConsultaPublica/Paginas/LegislacaoemConsultaPublica.aspx

Safety risk management. (sem data). EASA. Obtido 24 de julho de 2024, de https://www.easa.europa.eu/en/domains/safety-management/safety-risk-management

TSA PreCheck®. (n.d.). Tsa.gov. Retrieved July 24, 2024, from https://www.tsa.gov/precheck

United States Government. TSA (s.d). Security Screening. Obtido 24 de julho de 2024, de https://www.tsa.gov/travel/security-screening

VisionBox. (2021). Manuais de Processos e Procedimentos. Obtido 24 de julho de 2024, de https://www.vision-box.com/airports

Yin, R. K. (2017). Case Study Research and Applications: Design and Methods. SAGE Publications.

APPENDIX A

In order to obtain results for this project it has been conducted a focus group, all of the conduct rules from Nova IMS have been respect and no identity of the inquiries is being shared. To certify this information, there is a proof submitted to Ethics Committee in annex.

This is to certify that
Project No.: **INFSYS2024-7-35745**
Project Title: **Digital Transformation within Airport Security Processes New Security Technology Implementation Impact**
Principal Researcher: **Simão Batista**

according to the regulations of the Ethics Committee of NOVA IMS and MagIC Research Center this project was considered to meet the requirements of the NOVA IMS Internal Review Board, being considered **APPROVED** on 7/3/2024.

It is the Principal Researcher's responsibility to ensure that all researchers and stakeholders associated with this project are aware of the conditions of approval and which documents have been approved.

The Principal Researcher is required to notify the Ethics Committee, via amendment or progress report, of
- Any significant change to the project and the reason for that change;
- Any unforeseen events or unexpected developments that merit notification;
- The inability of the Principal Researcher to continue in that role or any other change in research personnel involved in the project.

Lisbon, 7/3/2024

NOVA IMS Ethics Committee
ethicscommittee@novaims.unl.pt

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa