NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROTECTING THE PERIMETER: UNMANNED AIRCRAFT SYSTEMS ENHANCE NATIONAL AIRPORT SECURITY

by

Robert L. Scott

December 2023

Co-Advisors: Rudolph P. Darken
Thomas J. Mackin (contractor)

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
PROTECTING THE PERIMETER: UNMANNED AIRCRAFT SYSTEMS ENHANCE NATIONAL AIRPORT SECURITY

5. FUNDING NUMBERS

6. AUTHOR(S) Robert L. Scott

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Airport perimeter security constitutes the first line of defense against unauthorized entry to restricted areas at airports, and it is crucial for ensuring overall safety and security at airports. Traditionally consisting of physical barriers and basic closed-circuit television monitoring, airport perimeter security systems have evolved to comprise multiple layers of innovative security technologies. These layered and integrated security solutions include advanced thermal and infrared cameras, modern video surveillance systems, and innovative perimeter intrusion detection systems such as fence disturbance sensors, microwave motion detection systems, electric field sensors, buried cable detection systems, ground based radar systems, and optical based detection and analytics. With advancements in science and technology, an increased number of technological innovations is expected to be utilized for enhancing existing perimeter security systems. In this study, a qualitative case study exploration is conducted to present evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States. Secondary data (i.e., gray and peer-reviewed literature) on technology usage for airport perimeter security are explored for the following three cases: unmanned aerial systems (UASs), biometric technologies, and miscellaneous technologies. The findings indicate the high potential of UASs, biometric technology-based security system

14. SUBJECT TERMS perimeter, airport, airport security, airport perimeter, UAV, UAS, drones, unmanned aerial systems, biometrics,	**15. NUMBER OF PAGES** 79
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

PROTECTING THE PERIMETER: UNMANNED AIRCRAFT SYSTEMS ENHANCE NATIONAL AIRPORT SECURITY

Robert L. Scott
Assistant Federal Security Director, Department of Homeland Security
BS, Daniel Webster College, 1994
MS, Embry-Riddle Aeronautical University, Worldwide, 2018

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2023

Approved by: Rudolph P. Darken
Co-Advisor

Thomas J. Mackin
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Airport perimeter security constitutes the first line of defense against unauthorized entry to restricted areas at airports, and it is crucial for ensuring overall safety and security at airports. Traditionally consisting of physical barriers and basic closed-circuit television monitoring, airport perimeter security systems have evolved to comprise multiple layers of innovative security technologies. These layered and integrated security solutions include advanced thermal and infrared cameras, modern video surveillance systems, and innovative perimeter intrusion detection systems such as fence disturbance sensors, microwave motion detection systems, electric field sensors, buried cable detection systems, ground based radar systems, and optical based detection and analytics. With advancements in science and technology, an increased number of technological innovations is expected to be utilized for enhancing existing perimeter security systems. In this study, a qualitative case study exploration is conducted to present evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States. Secondary data (i.e., gray and peer-reviewed literature) on technology usage for airport perimeter security are explored for the following three cases: unmanned aerial systems (UASs), biometric technologies, and miscellaneous technologies. The findings indicate the high potential of UASs, biometric technology-based security system

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACS	Access Control System
AI	Artificial Intelligence
CCTV	Closed-Circuit Television
CPTED	Crime Prevention Through Environmental Design
FAA	Federal Aviation Administration
IoT	Internet of Things
ML	Machine Learning
PIDS	Perimeter Intrusion Detection Systems
RFID	Radio Frequency Identification
SSA	Safe Skies Alliance
TSA	Transportation Security Administration
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicles
WSN	Wireless Sensor Network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Airport perimeter security constitutes the first line of defense against unauthorized entry to restricted and personnel-only areas at airports. It aims to prevent and address any potential perimeter breaches through deterrence, detection, delay, denial, defense, defeat, response, and recovery.[1] Perimeter security systems help avert internal accidents, delays, shutdowns, as well as terrorist attacks and hijackings which may result in the loss of life and capital. Several recent studies have been published pertaining to airport perimeter security issues, providing some insight into some of the barriers and limitations that still need addressing. Researchers have investigated topics like the use of optical fiber sensors for security threat detection, comprehensive security frameworks used to mitigate that common security threats, and the use of intelligent systems to guide security threat analysis.[2] Each of these studies has illustrated numerous limitations with respect to airport security, despite advancements in technology. Thus, this field desperately needs peer-reviewed research findings and relevant data to inform practice and enhance airport security by integrating technologies.

Despite the critical nature of perimeter security in airports, only limited scholarly works address this topic. Available works fail to explore the diverse technological systems and solutions that can enhance existing airport perimeter security systems.[3] Thus, this

[1] Mike Stokes, "Layer Surveillance Radar Technology into Physical Security Solutions for Real-Time Detection of Threats at Airport Sites," Aviation Pros, October 14, 2020, https://www.aviationpros.com/aviation-security/perimeter-security/article/21137832/layering-surveillance-radar-technology-into-physical-security-solutions-for-realtime-detection-of-threats-at-airport-sites.

[2] Youcheng Liang and Haitao Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device in Airport Perimeter Security System," in *2020 International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)* (Piscataway, NJ: IEEE, 2020), 150–52, https://doi.org/10.1109/ISCEIC51027.2020.00038; Endang Sugih Arti et al., "Airport Perimeter Security System Readiness Analysis (Case Study at Budiarto Curug-Tangerang Airport)," *Siber Journal of Transportation and Logistics* 1, no. 2 (July 2023): 64–71, https://doi.org/10.38035/sjtl.v1i2; and Youcheng Liang and Haitao Chen, "Design and Analysis of Airport Intelligent Border System Based on Zigbee Technology," in *2022 IEEE 22nd International Conference on Communication Technology (ICCT)* (2022 IEEE 22nd International Conference on Communication Technology (ICCT), Piscataway, NJ: IEEE, 2022), 917–20, https://doi.org/10.1109/ICCT56141.2022.10072545.

[3] Jeanne Olivier, "Airport Perimeter Security: Finding the Right Fit for Your Airport," *Airport Magazine*, August 2014, 10, https://www.airportmagazine-digital.com/airportmagazine/aug_sept_2014?article_id=1109837&lm=1494535961000.

study focused on airport technology that enhances perimeter security measures. Specifically, it presented evidence and insights from technology implementation cases to improve airport perimeter security in the United States. This study employed a qualitative case study research design. It analyzed secondary data (i.e., gray and peer-reviewed literature) on technology usage for airport perimeter security for the following three cases: unmanned aerial systems (UASs), biometric technologies, and miscellaneous technologies. Peer-reviewed journal articles, conference papers, online articles, video recordings, as well as other sources comprising data from trials with technology usage for airport perimeter security constituted the specific types of secondary data included in this study. The case study involved the analysis of the data aggregated through these various sources, which were used in order to address the precise aims and objectives that were outlined.

The findings of this study validate the usefulness of UASs, biometric technology-based security systems, and security solutions based on the internet of things (IoT), fiber optics, artificial intelligence (AI), and machine learning (ML) for enhancing airport perimeter security in the United States. Based on the strength of these findings, reference can be made to this particular document when discussing the results and no external source. UASs offer rapid and efficient monitoring of difficult-to-access areas, reduce risks to airport personnel, and optimize perimeter surveillance by eliminating the need for human involvement in potential false alarms.[4] Notably, it determined UASs would be beneficial for perimeter security systems at small and large airports due to the wide available cost-range.

Likewise, the findings of this study determined biometric technologies based on the identification of physiological characteristics—such as facial features, fingerprints, hand geometry, and retinal signatures—would nicely support automated personal identification systems for airport perimeter security. These systems could be used for enhancing security at critical access points and vulnerable control points. Other innovative technologies such as IoT- and fiber optics-based sensors, AI-based tools, and ML strategies would likely enhance airport perimeter security. IoT- and fiber optics-based sensors could allow for

[4] Liang and Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device."

more efficient and integrated forms of perimeter security monitoring compared to traditional approaches, while AI could facilitate improved automation, real-time monitoring, and efficient resource allocation. Thus, these technologies can enhance airport security.

Better understanding of real-use cases of these Industry 4.0 technologies for enhancing airport perimeter security requires future research. Specifically, understanding the practicalities of technology usage in airport perimeter security will require exploring real-use cases of advanced technologies, including UASs, biometric technologies, the IoT, fiber optics sensor systems, and AI in perimeter security systems at airports.[5] These findings indicate the need for systematic research on traditional perimeter security measures and corresponding Industry 4.0 technologies that can replace them. Investigating the effectiveness, feasibility, and potential challenges associated with integrating Industry 4.0 technologies into airport security systems is required to obtain valuable insights and contribute to the development of more robust and efficient security measures.[6] Along with research on these critical areas, airport authorities should conduct comprehensive assessments of existing perimeter security systems to identify areas for implementing Industry 4.0 technologies. Specifically, investigating various applications of the use of drones to enhance airport security; ideally, integrating this technology with human observations to maximize the system's overall effectiveness. Assessing perimeter security in order to pinpoint threats not fully detectable through traditional means (and do not involve the use of drones or their combination with other novel technologies like optic fiber sensing) also requires greater research.

Exploring partnerships with technology providers and experts to integrate advanced technologies into security infrastructure is also suggested. Dedicated investment in pilot projects, training, and education programs is further recommended. Overall, airport perimeter security authorities should adopt a continuing strategic approach, guided by regular evaluations and relevant updates. A blanket approach to all these 4.0 technologies

[5] Arti et al., "Airport Perimeter Security System."

[6] Liang and Chen, "Design and Analysis of Airport Intelligent Border System."

mentioned might obscure what airport authorities need to do in order to comprehensively mitigate security threats present. Findings from this study make a significant contribution to the understanding of airport perimeter security and advance literature related to this topic by illustrating the potential role that drones play in this endeavor. The other technologies shown, while not the direct focus of this study, also play an important role in airport security. In combining, a holistic airport security framework can be achieved.

ACKNOWLEDGMENTS

I must humbly and gratefully thank my wife, Dina Ellen Scott, and my daughter, Ariana Lee Scott, for their patience and support during my time away at the Naval Postgraduate School. This journey initially began as a personal goal to earn something I did not have. Over time, it became something different, something more: it allowed me to become a role model to my daughter, to teach her that learning is something that can be achieved throughout life. Ariana, I can only pray that my academic endeavors and how I live my life are good examples for you.

Also, I would be remiss if I did not acknowledge Dr. James C. Elmore, PhD, FRAeS, whom I hold in the highest regard. Sir, you inspired me to return to school after a twenty-one year absence to earn not just one master's degree, but a second one, too. The first degree was for me; this second one I dedicate to you and your ability to inspire continual growth and development.

Finally, I would like to extend my sincerest thanks to Professors Dr. Rudy Darken, PhD, and Dr. Thomas Mackin, PhD. Without your guidance and direction, I might still be in the library stacks and putting ideas on paper. You both offered the perfect balance of motivation and freedom to learn and create this thesis. It is an uncommon thing when you come across individuals who can teach students, while still being down-to-earth people whom their students want to emulate. Gentlemen, thank you is all I can offer, but I owe you so much more: how does one repay knowledge?

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Airport perimeter security constitutes a crucial aspect of the aviation sector. Multiple perimeter security breaches at United States (U.S.) airports every day demonstrates the significance of these security systems.[1] To address perimeter breaches and enhance perimeter security at airports, advancements in science and technology continually improve existing perimeter security systems.[2] In this regard, improving airport perimeter security requires a better understanding of the options, strategies, and barriers in implementing advanced technologies. This study focuses on exploring these implementation options.

A. PROBLEM STATEMENT

Airports are critical infrastructure and warrant strict protection. Airport perimeter security ensures their protection.[3] Such security aims include deterrence, detection, assessment, and action; airports also use a layered security model, which involves surveillance, personnel screening, and access control, among other strategies.[4] The most basic perimeter security systems in airports incorporate physical barriers, such as fencing topped by barbed or concertina wire, and closed-circuit television (CCTV) systems

[1] Mathilde Tisserand, "Violence, Crime and Difficult Passengers: Security Breaches at U.S. Aviation Facilities," Osprey Flight Solutions, November 1, 2022, https://www.ospreyflightsolutions.com/casestudy/violence-crime-and-difficult-passengers-security-breaches-at-us-aviation-facilities/; Sheldon H. Jacobson, "Are Airport Perimeter Security Breaches a Threat to Air Travelers?," The Hill, April 4, 2022, https://thehill.com/opinion/national-security/3258416-are-airport-perimeter-security-breaches-a-threat-to-air-travelers/.

[2] Jia Hao Tan and Tariq Masood, "Adoption of Industry 4.0 Technologies in Airports: A Systematic Literature Review," arXiv, 2021, 1, http://10.48550/arXiv.2112.14333; Nikos Papagiannopoulos, Konstantinos Loupos, and Christos Skoufis, "Iot-Based Airport Systems: A Unified Approach towards Establishing Trust for High Security and Integrity of Industrial Iot Platforms and Sensors," *Journal of Airport Management* 15, no. 3 (Summer 2021): 244, https://trid.trb.org/view/1870577.

[3] Jia Hao Tan and Tariq Masood, "Adoption of Industry 4.0 Technologies in Airports: A Systematic Literature Review," 12; Bert Willemsen and Menno Cadee, "Extending the Airport Boundary: Connecting Physical Security and Cybersecurity," *Journal of Airport Management* 12, no. 3 (Summer 2018): 242.

[4] Olivier, "Airport Perimeter Security," 10.

operated by employees observing a large set of monitors.[5] With modern computer and communication technology advancements, intelligent airport perimeter security systems integrate diverse collaborative and comprehensive detection technologies, such as sensors, data analytics, and the internet of things (IoT), as well as artificial intelligence (AI) for intrusion detection, which complement traditional perimeter security systems.[6] Using this array of tools and systems ensures greater protection of airport operation, as well as passenger and staff safety.

However, the large area within airports likely has multiple vulnerable locations. Security personnel infrequently patrol minor entrance points, such as fuel depots and remote or isolated areas within the airport. Other vulnerable locations present access points which can be breached, threatening perimeter security.[7] Breaches in airport perimeters can cause internal accidents, delays, and shutdowns, which impede the smooth functioning of the air transport system and incur substantial financial losses; such as the 9/11 terrorist attacks in 2001 that had catastrophic consequences.[8] This risk makes developing innovative security solutions imperative to allow a more thorough and complete monitoring of the airport perimeter and enable detection and interception of any possible breaches.

Despite the critical nature of perimeter security in airports, only limited scholarly works address this topic. Available works fail to explore the diverse systems and processes

---

[5] Xue Ming Cao, Chen Mei Jing, and Xiao Dan Zheng, "Design of the Airport Perimeter Security System Based on Internet of Things," *Applied Mechanics and Materials* 361–363 (2013): 2276, https://doi.org/10.4028/www.scientific.net/AMM.361-363.2276.

[6] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports"; Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System," 12; and Nikos Papagiannopoulos, Konstantinos Loupos, and Christos Skoufis, "Iot-Based Airport Systems: A Unified Approach Towards Establishing Trust for High Security and Integrity of Industrial Iot Platforms and Sensors," 246.

[7] Akbota Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports Security Support UAS Operations" (master's thesis, Arizona State University, 2022), 1, https://keep.lib.asu.edu/items/171683/view; Mike Stokes, "Layer Surveillance Radar Technology into Physical Security Solutions for Real-Time Detection of Threats at Airport Sites," *Airport Business* 34, no. 8 (October 2020): 36, ProQuest.

[8] Joshua T. Cousins, "Policing the Aerotropolis: A Model for Securing the Nation's Large Airports" (master's thesis, Naval Postgraduate School, 2021), 26, https://hdl.handle.net/10945/67120; Michal Klenka, "Major Incidents That Shaped Aviation Security," *Journal of Transportation Security* 12, no. 1 (2019): 50, https://doi.org/10.1007/s12198-019-00201-2; and Nora Metzner, "A Comparison of Agent-Based and Discrete Event Simulation for Assessing Airport Terminal Resilience," *Transportation Research Procedia* 43 (2019): 209, https://doi.org/10.1016/j.trpro.2019.12.035.

that enhance airport perimeter security. The confidential nature of airport security measures—classified for national security—may limit access to airport security data and discourage researchers from conducting well-designed studies.[9] In this regard, research studies specific to airport infrastructure security are minimal, with available research focusing on passenger and baggage screening by the Transportation Security Administration (TSA).[10] Nevertheless, the literature on this topic illustrates the need for research on proactive security measures and integrating new technologies in airport security.[11] Thus, this paper focuses on airport technology usage to enhance perimeter security.

Among the emerging technologies relevant to airport security, particularly airport perimeter security, unmanned autonomous ground vehicles, unmanned aerial systems (UAS) or unmanned aerial vehicles (UAV)—more commonly known as drones—may add additional protection. According to Georgia Lykou, Dimitrios Moustakas, and Dimitris Grizalis, "UASs are multi-rotor or fixed-wing aircraft that may be autonomously piloted or operated by remote controllers and can have diverse shapes and sizes, ranging from small insect-like systems to large aerial systems weighing several tons."[12] In airport perimeter security, UASs may be a highly suitable tool because they can negotiate challenging terrain quickly, surveil more quickly than what is feasible on foot, and monitor areas inaccessible by personnel or vehicles.[13] Recent research, however, has primarily focused on the challenges and threats faced by the aviation sector due to UAS activity

[9] James Ford et al., "An Economic Study of the U.S. Post-9/11 Aviation Security," *Open Journal of Business and Management* 8, no. 5 (August 2020): 1941, https://doi.org/10.4236/ojbm.2020.85118.

[10] Cousins, "Policing the Aerotropolis," 11.

[11] Ford et al., "An Economic Study of the U.S. Post-9/11 Aviation Security"; Klenka, "Major Incidents That Shaped Aviation Security," 24.

[12] Georgia Lykou, Dimitrios Moustakas, and Dimitris Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors* 20, no. 12 (January 2020): 2, https://doi.org/10.3390/s20123537.

[13] Sarah Hubbard et al., "UAS to Support Airport Safety and Operations: Opportunities and Challenges," *Journal of Unmanned Vehicle Systems* 6, no. 1 (2018): 7, https://doi.org/10.1139/juvs-2016-0020.

rather than using them to enhance airport perimeter security.[14] How UAS technology can complement the existing perimeter security at airports is unknown.

Similar to the use of UASs for enhancing airport perimeter security, other technological innovations may apply. Recent research reveals that modern technologies includes the following:

- data analysis and data processing
- cloud computing
- mobile smart devices
- the IoT
- cyber-physical systems
- AI
- visualization
- modeling and simulation
- additive manufacturing

These technologies are being gradually adopted for use in areas such as:

- passenger handling services
- commercial services
- airside ground operations

[14] Chris Boselli et al., "Geo-Fencing to Secure Airport Perimeter against sUAS," *International Journal of Intelligent Unmanned Systems* 5, no. 4 (2017): 103, https://doi.org/10.1108/IJIUS-02-2017-0002; Lykou, Moustakas, and Gritzalis, "Defending Airports from UAS," 4; and Choon Seng Tan, Douglas L. Van Bossuyt, and Britta Hale, "System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment," *Systems* 9, no. 4 (November 2021): 1–27, https://doi.org/10.3390/systems9040079.2.

- air traffic control and management
- airport logistics
- airport planning
- design and construction
- airport security[15]

Specifically, recent reports highlight the development and adoption of advanced perimeter intrusion detection systems (PIDS), active and passive radar sensors, multi-sensor data fusion algorithms, and ML in airport perimeter security.[16] However, no recent literature focuses on airport perimeter security and the modern technological innovations that can enhance it. How modern technological innovations can complement the existing perimeter security systems at airports remains unknown. Although scholars have explored various technologies within the airport perimeter security system, implementing such technologies to improve its security requires a better understanding of the insights, including barriers, options, and best practices.[17] This thesis explores modern technology-based systems, applications, and strategies for enhancing airport perimeter security, including the use of AI to share the burden of systems surveillance and alert.

B. RESEARCH QUESTION

Which technologies might improve airport perimeter security by addressing unauthorized perimeter access, and to what effect?

C. LITERATURE REVIEW

This literature review surveys scholarly studies of current and future airport perimeter security protection against intrusions. It focuses on the promise of present and

[15] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports," 10.

[16] Tan and Masood, 12.

[17] Tan and Masood, 16; Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems"; and Lykou, Moustakas, and Gritzalis, "Defending Airports from UAS."

emerging technologies. It uses sources from the following databases: ERIC, ProQuest, JSTOR, and Google Scholar. The literature review emphasizes scholarly works published in the last five years (i.e., between 2019 and 2023). It also includes sources published before 2019 significant to the topic under investigation.

Airport perimeter security is a critical aspect of national security. Jia Hao Tan and Tariq Masood assert that improving airport operations in the airport security system requires reviewing the existing system to prevent perimeter breaches.[18] Chiao-Fe Shu et al. define an airport perimeter breach as a security incident wherein unauthorized individuals gain access to the airport grounds or personnel-only areas at the airport with the intent of engaging in malicious activities.[19] In his master's thesis, Joshua T. Cousins concludes that perimeter breaches at airports may, at best, lead to internal accidents, delays, and shutdowns, impeding the air transport system operations and, at worst, result in terrorist attacks and hijackings, causing the loss of life and capital.[20] Although incidents of airport perimeter breaches in the United States seem to have decreased in the last five years based on media reports, both Mathilde Tisserand and Sheldon H. Jacobson observed that multiple perimeter security breaches continue to occur at United States airports.[21] This trend underscores the need to improve airport perimeter security measures.

Over time, airport perimeter security has evolved from discrete physical barriers to digital and virtual monitoring. As Xue Ming Cao, Chen Mei Jing, and Xiao Dan Zheng note in their article, "Design of the Airport Perimeter Security System Based on Internet of Things," airport perimeter security traditionally comprises perimeter boundaries using

[18] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports," 14; Willemsen and Cadee, "Extending the Airport Boundary."

[19] Chiao-Fe Shu et al., "IBM Smart Surveillance System (S3): A [sic] Open and Extensible Framework for Event Based Surveillance," in *IEEE Conference on Advanced Video and Signal Based Surveillance, 2005.* (IEEE Conference on Advanced Video and Signal Based Surveillance, 2005., Piscataway, NJ: IEEE, 2005), 318, https://doi.org/10.1109/AVSS.2005.1577288.

[20] Cousins, "Policing the Aerotropolis"; Klenka, "Major Incidents That Shaped Aviation Security"; and Metzner, "A Comparison of Agent-Based and Discrete Event Simulation," 25.

[21] Tisserand, "Violence, Crime and Difficult Passengers"; Jacobson, "Are Airport Perimeter Security Breaches a Threat."

wire fencing, vehicular barriers, and manned CCTV systems.[22] They argue that technological advancements allow airports to use innovative security systems that integrate multiple detection levels. In this context, Tan and Masood advocate using sensors, data analytics, the IoT, PIDS, multi-sensor data fusion algorithms, and ML for various airport operations.[23] Likewise, Petr Dejdar et al. and Youcheng Liang and Haitao Chen investigate optical fiber technologies for long-distance monitoring of perimeter security systems. Sarah Hubbard et al. and Zbyšek Korecki, Miroslav Janošek, and Tomáš Pecháček propose using UAS or drones to optimize airport perimeter security.[24] Nevertheless, no recent in-depth qualitative research explores the diverse technologies used for airport perimeter security in the United States.

Airport perimeter security has an outsized role in national security. Joseph H. Szyliowicz and Luca Zamparini argue that the vast size of airports and their operational complexity make them vulnerable, and attackers consistently prefer them as targets because of the severe human, economic, and psychological tolls caused by a successful breach.[25] Steve Moody posits that airport perimeter security constitutes the crucial first layer of protection, enabling authorities to identify and intercept intruders before they can carry out any malicious acts.[26] In either case, reinforcing the physical barriers of the airport

---

[22] Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System," 2276.

[23] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports"; Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System"; and Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems," 12.

[24] Hubbard et al., "UAS to Support Airport Safety and Operations," 2; Zbyšek Korecki, Miroslav Janošek, and Tomáš Pecháček, "Use of Unmanned Aerial Systems in Airport Operations," in *2021 International Conference on Military Technologies (ICMT)* (Piscataway, NJ: IEEE, 2021), 4, https://doi.org/10.1109/ICMT52455.2021.9502756; Liang and Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device," 150; and Petr Dejdar et al., "Image Edge Detection Methods in Perimeter Security Systems Using Distributed Fiber Optical Sensing," *Sensors* 22, no. 12 (January 2022): 2, https://doi.org/10.3390/s22124573.

[25] Joseph S. Szyliowicz and Luca Zamparini, eds., "Introduction," in *Air Transport Security: Issues, Challenges and National Policies* (Cheltenham, UK: Edward Elgar Publishing, 2018), 5; Ann S. Barry and David S. Mazel, "Airport Perimeter Security: Where We've Been, Where We Are, and Where We're Going," in *2008 IEEE Conference on Technologies for Homeland Security* (Piscataway, NJ: IEEE, 2008), 62, https://doi.org/10.1109/THS.2008.4534423.

[26] Steve Moody, "Integrated Security," *Intersec: The Journal of International Security* 29, no. 6 (June 2019): 22, http://www.intersecmag.co.uk/integrated-security-2/; Galileo Tamasi and Micaela Demichela, "Risk Assessment Techniques for Civil Aviation Security," *Reliability Engineering & System Safety* 96, no. 8 (August 2011): 895, https://doi.org/10.1016/j.ress.2011.03.009.

perimeter with technologies further enhances the deter, detect, and defend goals of the airport operation.

Existing research on airport technology usage primarily focuses on operations and passenger and baggage security. Advanced technologies and processes have been explored in certain operational areas, such as "passenger operations, baggage handling, and border control by regulatory agencies."[27] Varied technological innovations also become part of security aspects at airports.[28] Gabriel Nowacki and Bohdan Paszukow underscore that since attackers consistently challenge the technical capabilities of existing airport security systems, airport perimeter security must take a proactive approach to uniformly apply technological innovations.[29] Current literature on airport perimeter security unanimously points to a need for enhanced security measures by using available specialized tools.

Airport perimeter security systems generally employ a layered model. According to Mike Stokes' applied research report on airport security (PARAS), the layered model fulfills the following functions:

- Deterring an intrusion before it occurs, detecting an intrusion if it happens
- Delaying an intrusion process to enable effective law enforcement response
- Responding promptly and effectively to an occurring intrusion
- Defending critical assets
- Defeating or neutralizing an intruder
- Providing situational awareness information to responders

[27] Aruna Rajapaksha and Nisha Jayasuriya, "Smart Airport: A Review on Future of the Airport Operation," *Global Journal of Management and Business Research* 20, no. 3 (2020): 32, https://doi.org/10.34257/GJMBRAVOL20IS3PG25.

[28] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports," 12.

[29] Gabriel Nowacki and Bohdan Paszukow, "Security Requirements for New Threats at International Airports," *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 1 (March 2018): 187, https://doi.org/10.12716/1001.12.01.22.

- Conducting recovery by effectively containing the threat and ensuring all processes and systems operate efficiently[30]

This layered approach to airport perimeter security reflects the idea that multiple individual layers of security are more effective than a single security mechanism. Even with a breach of one or more layers, others would still work. Based on the idea of multiple layers of protection, the Guidance for Airport Perimeter Security report published by PARAS in December 2018 presents the following physical, electronic, and operational airport perimeter security measures:

- Physical measures: These include "fences, walls, gates, maritime barriers for airports with waterfront perimeters, vehicle intrusion barriers, and crime prevention through environmental design (CPTED) concepts, such as natural surveillance, natural access control, territorial reinforcement, maintenance, and target hardening.[31]

- Electronic measures: These include PIDS such as CCTV cameras, access control system (ACS) devices, and, importantly, personnel for monitoring electronic system alarms and reporting potential incidents by following standardized procedures that support the use of the systems, the validation of the alarms, and central monitoring and dispatching of first responders. Specifically, PIDS technologies include "fence disturbance sensors, microwave motion detection, electric field sensors, buried cable detection systems, ground-based radar, and optical based detection/analytics."[32]

- Operational measures: These include perimeter patrolling by personnel.[33]

---

[30] Stokes, "Layer Surveillance Radar Technology."

[31] Ann S. Barry, *Guidance for Airport Perimeter Security* (Louisville, TN: National Safe Skies Alliance, Inc., 2018), https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf.

[32] Barry, 35.

[33] Barry, 16.

It is currently unknown as to whether this report provides any layout of the airport with these security systems in place, although this information would be beneficial in providing insight into these issues. According to Choon Seng Tan, Douglas L. Van Bossuyt, and Britta Hale, the adoption of technological innovations is gradually gaining traction within airport perimeter security, and advanced technology will likely become increasingly crucial in the future of airport security systems.[34] Hubbard et al. expanded on this perspective, and identified the untapped potential of UASs (i.e., drones). UASs can enhance perimeter security with minimal risk or impact on aeronautical activity by surveilling the extensive areas of airports with minimal personnel and maximum speed, with coverage of remote and isolated areas within airports.[35] Along with UASs, other technological innovations for enhancing airport perimeter security are worth exploring. Accordingly, this thesis considers the frameworks of layered airport perimeter security and security technology to adopt, such as UAS, biometrics, and other systems. Analyzing the existing and future airport perimeter security systems, particularly concerning technology usage, could provide valuable insights into how to enhance this first integral layer of protection.

D. RESEARCH DESIGN

This study presents evidence and insights from technology implementation and usage cases for improving airport perimeter security in the United States. The intended outcomes of this thesis include policy and practice recommendations for use by TSA in implementing programs and using technology as a strategy for airport perimeter security.

This study employed a qualitative research methodology. According to John W. Creswell and Cheryl N. Poth, a qualitative inquiry helps obtain a comprehensive understanding of a complex issue through extensive data collection and analysis, which entails gathering and sorting through vast data sets and identifying relevant themes.[36]

[34] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports," 16.

[35] Hubbard et al., "UAS to Support Airport Safety and Operations," 1.

[36] John W. Creswell and Cheryl N. Poth, *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, 4th ed. (Thousand Oaks, CA: Sage, 2016).

Qualitative approaches may be narrative, phenomenological, ethnographic, grounded theories, or a case study. Among these, a case study research design is optimal for exploring an issue by considering one or more specific cases within a particular setting or context.[37] Case studies can describe, explain, or analyze phenomena and events in the everyday contexts within which they occur.[38] As such, a qualitative case study design fulfilled the objective of this thesis, which is to explore cases of technology usage for airport perimeter security in U.S. airports.

I used secondary data sources (i.e., gray and peer-reviewed literature) of cases of technology usage for airport perimeter security for this qualitative study. The data types included peer-reviewed journal articles, conference papers, online articles, video recordings, and other sources comprising data from trials with technology usage for airport perimeter security. I identified technology usage for airport perimeter security for the following cases: UAS/ drones, biometric technologies, and miscellaneous technologies.

Data collection and analysis followed these steps:

- Step 1: Identify gray and peer-reviewed literature on technology usage for airport perimeter security in the United States.
- Step 2: Classify the technologies used for airport perimeter security as per the identified literature into three cases: UAS/drones, biometric technologies, and miscellaneous technologies.
- Step 3: Case study analysis of the three technological cases as presented by Robert K. Yin.[39] The study does not use primary data; rather, it employed secondary data obtained from the identified gray and peer-reviewed literature.

[37] Creswell and Poth.

[38] Robert K. Yin, *Case Study Research: Design and Methods*, 3rd ed. (Thousand Oaks, CA: SAGE, 2003).

[39] Robert K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. (Thousand Oaks, CA: SAGE, 2018).

This chapter introduces the study. First, it defines the problem of airport perimeter security and provides a brief background of the topic. Then, it presents the research question and a concise review of the literature, followed by the research design. This introductory chapter forms a foundation for remaining chapters. Chapter II presents a more elaborate review of literature related to key constructs and variables of interest associated with airport perimeter security. Chapter III details the methodology and research design of the study. Chapter IV presents the key results of the study, a discussion of their meaning, and concludes the paper with recommendations for research and practice.

II. AIRPORT PERIMETER SECURITY AND TECHNOLOGY APPLICATIONS

A. INTRODUCTION

With rapid advancements in science and technology, airports are finding diverse applications for innovative tools and strategies. Digitizing and modernizing airports are attracting significant interest from the aviation sector and academia. Research on technological usage in the aviation industry is gradually gaining momentum, focusing on airport operations, passenger services, and aviation security.[40] Although researchers have studied the use of various technologies within the airport security system, improving airport perimeter security requires a better understanding of the insights, including barriers, options, and best practices, for implementing such technologies.[41] Specifically, how modern technological innovations might complement the existing perimeter security systems at airports is unknown. Thus, this study explores the use of integrated modern technology-based systems, applications, and strategies for enhancing the perimeter security system at airports. This study focuses on airport technology that enhances perimeter security measures. Specifically, it presents evidence and insights from technology implementation cases to improve airport perimeter security in the United States.

This chapter presents necessary background to this study. The discussion begins with a description of airport security and its various aspects, focusing on airport perimeter security. It then describes recent research related to technology adoption in airports, followed by a discussion on modern-day technological solutions in the context of airport security, specifically perimeter security. Based on the research, the chapter identifies the gap in the literature or the lack of knowledge regarding the use of drones to supplement airport perimeter security analysis.

[40] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports."

[41] Tan and Masood; Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems"; and Lykou, Moustakas, and Gritzalis, "Defending Airports from UAS."

B. AIRPORT SECURITY

Airports comprise critical infrastructures in terms of global transportation and connection. Any individual can use a number of airline services, purchase any number of tickets, and fly themselves or their freight shipments to numerous locations.[42] The ease and convenience of transport through the aviation sector make airports a prime target for attacks or the pathways for attacks.[43] The vulnerability posed by airports to national and international security is evident from the countless hijackings and ensuing acts of terrorism in different parts of the globe.[44] In the United States itself, the Dawson's Field hijackings of 1970, the 1988 bomb explosion on the Pan Am flight 103, and the hijacking and attacks on September 11, 2001 by the al-Qaeda terrorist network constitute only a small—albeit significant—fraction of aggressions in the aviation sector.[45] The consequences associated with such attacks in the aviation sector not only include horrific losses of life and property, but also include impediments in the smooth functioning of airports and airline services.

For these reasons, airports warrant strict measures of safety and security. Although often synonymously used, safety and security signify distinct aspects in the aviation sector. Safety refers to protection against aviation accidents, such as runway collisions, mid-air collisions, aircraft defects and malfunctioning, pilot and operator errors, and system failures.[46] The Federal Aviation Administration (FAA) agency of the U.S. government maintains aviation safety in the United States. The FAA establishes standards and regulations for the hiring, sobriety, and duty-time limit of pilots, rules for air traffic management, oversees air traffic control, and sets standards for the manufacture,

---

[42] Klenka, "Major Incidents That Shaped Aviation Security."

[43] Moody, "Integrated Security."

[44] Klenka, "Major Incidents That Shaped Aviation Security."

[45] Klenka.

[46] Arnold Barnett, "Aviation Safety and Security," in *The Global Airline Industry*, ed. Peter Belobaba, Amedeo Odon, and Cynthia Barnhart (West Sussex, UK: John Wiley & Sons, Ltd, 2009), 313–42, https://doi.org/10.1002/9780470744734.ch11; Heinz Wipf, "Safety versus Security in Aviation," in *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*, ed. Corinne Bieder and Kenneth Pettersen Gould (Cham, Switzerland: Springer International Publishing, 2020), 29–41, https://doi.org/10.1007/978-3-030-47229-0_4.

maintenance, and operation of aircraft.[47] Although aviation safety protects against the risks associated with day-to-day aviation activities, aviation security signifies protection against unlawful interference in aviation activities.[48] Security in the aviation sector encompasses measures for preventing intentional criminal acts that can harm airport operations, airport personnel, and air passengers, as well as broader regions in the country or abroad.[49] TSA is the primary regulatory body responsible for maintaining security at U.S. airports. It conducts passenger and baggage screening, random employee screenings, maintains passenger watchlists, pre-screens domestic air carrier flights, and installs detection systems for explosives, drugs, and certain hazardous materials.[50] These TSA functions help prevent illegal activities within airports, thus maintaining airport security.

In addition to these FAA and TSA functions for maintaining airport safety and security, a crucial aspect of the aviation sector, particularly airport security, is airport perimeter security. The TSA's function regarding airport perimeter security is ensuring that the perimeter security plans of U.S. airports meet federal standards, conducting necessary airport inspections such as joint vulnerability assessments, special emphasis inspections, and access control process checks, and analyzing airport inspection results to develop threat mitigation strategies for enhancing the integrity of perimeter security. Essentially, airport perimeter security is directly overseen by specific airport authorities and airport operators, who ultimately report to the TSA, which ensures security compliance and security effectiveness of the airports' perimeter security plans.[51] Along with the TSA and airport authorities and operators, relevant law enforcement agencies as well as private sector

[47] Claudia Culmone, "Safety vs. Security: Is There a Difference?," *NATACS Blog* (blog), July 25, 2018, https://info.natacs.aero/natacs-blog/safety-vs.-security-is-there-a-difference.

[48] Wipf, "Safety Versus Security in Aviation."

[49] Barnett, "Aviation Safety and Security."

[50] Culmone, "Safety vs. Security."

[51] H.R. TSA Oversight Part 2: Airport Perimeter Security: Hearing before the Subcommittee on National Security, Homeland Defense and Foreign Operations, House of Representatives 112 Cong., 1 (2011). https://www.govinfo.gov/content/pkg/CHRG-112hhrg71820/html/CHRG-112hhrg71820.htm.

security agencies work in tandem to maintain perimeter security at airports.[52] This study focused on the critical aspect of airport perimeter security. A closer look into airport perimeter security and its evolution over the years appears in the following section.

C. AIRPORT PERIMETER SECURITY

Airport perimeter security makes up a critical aspect of security in the aviation sector. Airport perimeter security systems include the measures in place for preventing unauthorized access to airport grounds or personnel-only areas at airports with malicious intents.[53] The objective of airport perimeter security is to prevent and address any possible perimeter breaches through deterrence, detection, delay, denial, defense, defeat, response, and recovery.[54] The significance of airport perimeter security lies with the current prevalence of perimeter breaches. Recent reports highlight the continual occurrence of perimeter breaches in airports across the United States.[55] Although recent breaches have not resulted in catastrophic hijackings or acts of terrorisms, constant vigilance is of the utmost importance.

Airport authorities and airport operators, under TSA oversight, handle perimeter security systems at airports. The former oversee facility-specific perimeter security measures depending on the size of the airport, financial availability, and security guidelines.[56] The perimeter security systems in most airports include boundary measures such as walls, fences, electronic boundaries (e.g., alarms and sensor lines), and other physical and/or natural barriers.[57] Additionally, airports that need or possess the means of

[52] Heather A. Panter, "Airport Security: Procedures in Secured Areas for TSA and Private Security," in *Encyclopedia of Security and Emergency Management*, ed. Lauren R. Shapiro and Marie-Helen Maras (Cham, Switzerland: Springer International Publishing, 2019), 7, https://doi.org/10.1007/978-3-319-69891-5_2-1.

[53] Shu et al., "IBM Smart Surveillance System (S3)."

[54] Stokes, "Layer Surveillance Radar Technology," October 2020.

[55] Tisserand, "Violence, Crime and Difficult Passengers"; Jacobson, "Are Airport Perimeter Security Breaches a Threat."

[56] Transportation Security Administration, *Security Guidelines for General Aviation Airport Operators and Users*, Information Publication A-001, Version 2 (Washington, DC: Department of Homeland Security, 2017), 10, https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf.

[57] Transportation Security Administration, 18.

more rigorous perimeter security measures use CCTVs, outdoor lighting, access point strategies, and PIDS.[58] As seen in Figure 1, security personnel for monitoring and surveillance, patrolling airport perimeters, reporting airport security violations, deterring criminal behavior, and reporting signs of threat or suspicious behavior also form a crucial part of airport perimeter security systems.[59]

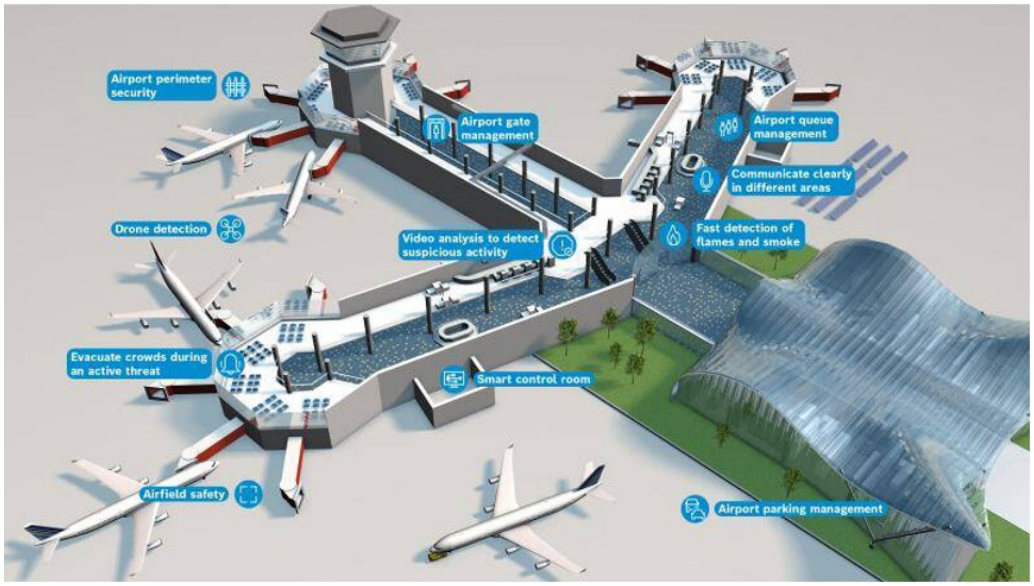

Figure 1. Perimeter Airport Security System[60]

As indicated in Figure 1, a perimeter airport security system protects the outer parameters of the facility. To this end, the layered approach of airport perimeter security is crucial. Based on it, multiple independent layers of security work together to create a comprehensive security system that is effective against any kind of perimeter breach.[61] The various layers in an airport perimeter security system usually include physical barriers, such as walls and fences topped with wires, as well as electronic devices, such as CCTV

[58] Transportation Security Administration, *Security Guidelines for General Aviation Airport*.

[59] Panter, "Airport Security," 7–8.

[60] Source: "Airport Security Solutions," Bosch Security and Safety Systems, accessed October 9, 2023, https://www.boschsecurity.com/us/en/industries/airports/.

[61] David Anderson, "Optimising Multi-Layered Security Screening," *Journal of Transportation Security* 14, no. 3–4 (December 2021): 249–73, https://doi.org/10.1007/s12198-021-00237-3.

systems for video surveillance.[62] To complement these security measures, airport personnel conduct perimeter patrols at scheduled and random intervals.[63] These layered and integrated security solutions deter, delay, detect, identify, classify, and locate potential or actual breaches in the airport perimeter in a timely manner, extending the response time of security personnel to prevent the intrusion and detain the suspect.[64]

Figure 2 illustrates the multiple steps involved in the layered security model. The layered approach of perimeter security enables many distinct strategies for protecting the airport perimeter.

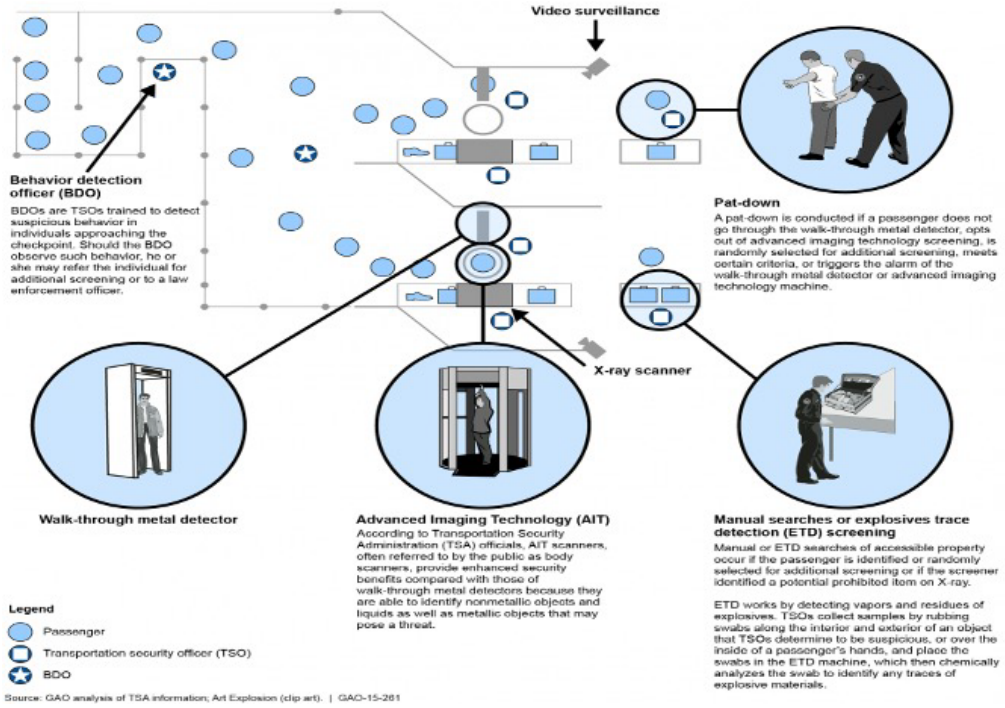

Figure 2. Layered Airport Security Model[65]

[62] Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System."

[63] Christopher Pheasant, Lorena de Rodriguez, and Don Zoufal, *Airport Security Training for Law Enforcement and Security Personnel* (Louisville, TN: National Safe Skies Alliance, Inc., 2020), 18.

[64] Stokes, "Layer Surveillance Radar Technology," October 14, 2020.

[65] Source: William Johnstone, "Passenger Aviation Security Layers," *SciTech Connect* (blog), October 6, 2015, https://scitechconnect.elsevier.com/passenger-aviation-security-layers/.

With advancements in science and technology, as well as the increasing threat from attackers, the layered model of airport perimeter security is evolving. Along with physical barriers, video surveillance systems, and security personnel, modern airport perimeter security systems may include thermal cameras, infrared cameras, and PIDS technologies, such as fence disturbance sensors, microwave motion detection, electric field sensors, buried cable detection systems, ground-based radar, and optical based detection/ analytics.[66] Each of these forms of technology, while potentially challenging to understand, plays a role in fostering enhanced airport security. With the increasing popularity of these innovative security solutions, other technological tools, such as UASs, the IoT, biometric technologies, optical fiber technologies, behavioral profiling, and big data analysis, are gaining prominence.[67] Biometric technologies detect security threats via body heat and other physiological indicators, while the IoT detects risks in technological connectedness across a range of different types of devices. To understand the incorporation of modern technologies in airport perimeter security systems, their current applications in the aviation industry warrant exploration. The following section discusses recent research of these uses.

D. TECHNOLOGY ADOPTION IN AIRPORTS

Major advancements in technology adoption for streamlining operations are taking place in airline security, improving travel experience, and enhancing security. Significant leaps in adopting technological innovations for operational purposes at airports include the use of UASs and digital technologies for ground operations, biometric technologies for customs and border protection, and biometric security gates for streamlining screening

66 Barry, *Guidance for Airport Perimeter Security*.

67 Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports"; Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports"; and Walter Matta and Alessandro Cantelli-Forti, "An Innovative Airport Physical-Cyber Security System (APSS)," *Information & Security* 43, no. 1 (2019): 285–93, https://doi.org/10.11610/isij.4321.

operations.[68] The adoption of digital services, such as biometric check-ins for passenger convenience, baggage handling, and border control has drastically improved travel experience.[69] The concept of smart airports—airports equipped with advanced technologies and processes for enhanced operations and passenger experience—comprise diverse tools and technologies, such as smart check-in, self-boarding, indoor navigation, biometric services, self-baggage tagging, radio frequency identification (RFID) baggage tags, and the use of smart wearables.[70]

All of these tools help detect security threats and/or expedite the security process by making it more efficient in some way. Social robots and self-service technologies have been explored for enhancing passenger handling services, cameras and sensors coupled with artificial intelligence technologies have been explored for improved airside ground operations, data analytics, ML, and automation technologies have been explored for more efficient air traffic control and management. The integration of RFID, wireless sensor network (WSN), and IoT has been explored for improved airport logistics.[71] Innovative

---

[68] Ivan Kovynyov and Ralf Mikut, "Digital Technologies in Airport Ground Operations," *Netnomics : Economic Research and Electronic Networking* 20, no. 1 (April 2019): 1–25, https://doi.org/10.1007/s11066-019-09132-5; Kim Cheong, Francis Joseph Costello, and Kun Chang Lee, "Integrating Qualitative Comparative Analysis and Support Vector Machine Methods to Reduce Passengers' Resistance to Biometric E-Gates for Sustainable Airport Operations," *Sustainability* 11 (2019): 1–22, https://doi.org/10.3390/su11195349; Kim Cheong, Kun Chang Lee, and Francis Joseph Costello, "The Intention of Passengers towards Repeat Use of Biometric Security for Sustainable Airport Management," *Sustainability* 12 (2020): 1–18, https://doi.org/10.3390/su12114528; Nimra Khan and Marina Efthymiou, "The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP)," *International Journal of Information Management Data Insights* 1 (2021): 1–14, https://doi.org/10.1016/j.jjimei.2021.100049; Thomas Mackie and Aaron Lawrence, "Integrating Unmanned Aircraft Systems into Airport Operations: From Buy-in to Public Safety," *Journal of Airport Management* 13, no. 4 (Autumn 2019): 380–90; and Sonal Seth and Qianmei Feng, "A Multi-Level Weighted Alarm Security System for Passenger and Checked-Baggage Screening," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 236, no. 5 (October 2022): 727–37, https://doi.org/10.1177/1748006X211042710.

[69] Rajapaksha and Jayasuriya, "Smart Airport"; Nathane Ana Rosa Negri, Giovanna Miceli Ronzani Borille, and Viviane Adriano Falcão, "Acceptance of Biometric Technology in Airport Check-In," *Journal of Air Transport Management* 81 (October 2019): 101720, https://doi.org/10.1016/j.jairtraman.2019.101720; and Joseph Amankwah-Amoah, "COVID-19 Pandemic and Innovation Activities in the Global Airline Industry: A Review," *Environment International* 156 (2021): 1–7, https://doi.org/10.1016/j.envint.2021.106719.

[70] Rajapaksha and Jayasuriya, "Smart Airport"; Negri, Borille, and Falcão, "Acceptance of Biometric Technology in Airport Check-In"; and Amankwah-Amoah, "COVID-19 Pandemic and Innovation Activities."

[71] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports."

security systems have been designed and studied for passenger and baggage screening, such as millimeter-wave advanced imaging technique, computed tomography technology, and explosive detection systems for cabin baggage screening, and research is being conducted to explore next-generation technologies, such as AI walk-through scanners, AI security gates, and behavioral biometric technology.[72] Technological innovations have thus changed diverse airport operations and passenger services. In the case of security enhancement at airports, technology adoption represents a promising and crucial factor and has research in diverse contexts. The following paragraphs discuss technology adoption for airport security, particularly technological innovations in airport perimeter security.

E. TECHNOLOGICAL SOLUTIONS FOR AIRPORT SECURITY

Airport security affords the opportunity for technological applications. Recent research on the topic of airport security and technology adoption highlights that technologies can improve the effectiveness and enhance the capabilities of airport security systems.[73] Diverse technological solutions have been explored in this regard, such as advanced imaging technologies, biometric identification technologies, computed tomography technology, and artificial intelligence technology.[74] It is only through the comprehensive integration of these security tools via an integrated framework that a sufficient detection framework is in place. The development of cyber security has been studied and advanced physical-cyber security control models have been proposed to cope

[72] Seth and Feng, "A Multi-Level Weighted Alarm Security System for Passenger and Checked-Baggage Screening"; Zhou Zhang, "Technologies Raise the Effectiveness of Airport Security Control," in *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)* (Piscataway, NJ: IEEE, 2019), 431–34, https://doi.org/10.1109/ICCASIT48058.2019.8973152; and Nicole Hättenschwiler et al., "Automation in Airport Security X-Ray Screening of Cabin Baggage: Examining Benefits and Possible Implementations of Automated Explosives Detection," *Applied Ergonomics* 72 (October 2018): 58–68, https://doi.org/10.1016/j.apergo.2018.05.003.

[73] Bruno Alencar Pereira, Gui Lohmann, and Luke Houghton, "Innovation and Value Creation in the Context of Aviation: A Systematic Literature Review," *Journal of Air Transport Management* 94 (July 2021): 102076, https://doi.org/10.1016/j.jairtraman.2021.102076; Zhang, "Technologies Raise the Effectiveness of Airport Security Control."

[74] Zhang, "Technologies Raise the Effectiveness of Airport Security Control"; Sena Kiliç, Caglar Ucler, and Luis Martin-Domingo, "Innovation at Airports: A Systematic Literature Review (2000–2019)," *Aviation* 25, no. 3 (2021): 220–31, https://doi.org/10.3846/aviation.2021.14917.

with the highly technical nature of the current aviation sector.[75] Scholarly works thus demonstrate the applicability of technological innovations for airport security and underscore the need for continual research in this regard.

A significant aspect of airport security is the perimeter security system at airports. Although few recent studies focus on airport perimeter security and corresponding technological adoptions, a few researchers have explored these topics. One modern-day technological innovation featured in recent research in the context of airport perimeter security is optical fiber-based perimeter technology.[76] Scholars, aviation industry professionals, and airport security experts have concluded that optical fiber perimeter technology is highly suitable for airport perimeter security systems because it enables long-distance monitoring, is corrosion-resistant, and adaptable to certain extreme locations, such as sea beds, fields, and underground, due to inherent properties.[77] As such, research on the optical fiber perimeter technology aims to improve its efficiency.[78] In this way, increased efficiency may be achieved through the performance of empirical investigations.

By the same token, the IoT holds promise to detect network intrusions across many systems. Another recent research focus for enhancing airport perimeter security is the IoT.[79] It integrates the internet and information sensing devices, such as RFID devices, global positioning systems, infrared sensors, and laser scanners to facilitate easy identification and management.[80] IoT-based sensor networks comprising intrusion

[75] Matta and Cantelli-Forti, "An Innovative Airport Physical-Cyber Security System (APSS)"; Briony Callander and Christian Kaunert, "Technological Innovation in Aviation Security: From Industries as Policy Entrepreneurs," *Politeja* 4, no. 79 (2022): 55–71, https://doi.org/10.12797/Politeja.19.2022.79.04.

[76] Zhenshi Sun et al., "Variational Mode Decomposition-Based Event Recognition in Perimeter Security Monitoring with Fiber Optic Vibration Sensor," *IEEE Access* 7 (2019): 182580–87, https://doi.org/10.1109/ACCESS.2019.2959788.

[77] Liang and Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device."

[78] Dejdar et al., "Image Edge Detection Methods."

[79] Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems"; Jialei Chen and Huan Zhang, "Study on the Internet of Things Discipline in Civil Aviation," in *Advances in Artificial Intelligence and Security: 8th International Conference on Artificial Intelligence and Security, ICAIS 2022, Qinghai, China, July 15–20, 2022, Proceedings, Part III*, ed. Xingming Sun et al. (Cham, Switzerland: Springer International Publishing AG, 2022), 586–94.

[80] Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System."

alarming systems, radio communication systems, video security monitoring systems, communication transmission network systems, and monitoring center management systems could enhance the perimeter security at airports.[81] Similarly, PIDS based on WSN, integrated radar-camera systems, and pattern recognition approaches based on neural network technology have been highlighted as the future of airport perimeter security.[82] PIDS in the form of virtual fencing, fencing sensor systems, mobile detection systems, visual spectrum video surveillance systems, infrared video surveillance systems, fingerprint readers, and unmanned ground and aerial drones stand out as effective perimeter security measures.[83] These technological tools may be critical for improved detection of possible perimeter breaches.

Figure 3 depicts various airport security tools that are commonly used to detect security risks. Along with monitoring and detection, the prevention of airport perimeter breaches requires regular and random patrolling. In this regard, technological adoption favors the use of UASs, which can rapidly traverse challenging terrain, surveil faster than possible on foot, and easily monitor remote or inaccessible areas.[84]

[81] Cao, Jing, and Zheng.

[82] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports."

[83] Jeffrey Price, "The Role of the Private Sector for Air Transport Security," in *Air Transport Security: Issues, Challenges and National Policies*, ed. Joseph S. Szyliowicz and Luca Zamparini (Cheltenham, UK: Edward Elgar Publishing, 2018), 63–84, https://www.e-elgar.com/shop/usd/air-transport-security-9781786435194.html.

[84] Hubbard et al., "UAS to Support Airport Safety and Operations."

Figure 3. Airport Security Tools[85]

Research has highlighted that UASs can complement traditional perimeter detection systems consisting of cameras and sensors to monitor airport perimeters, provide rapid response to security alarms, efficiently track threats, and patrol and inspect facilities.[86] Figure 4 depicts an airport security drone used to detect airport security threats around the perimeter. Some drones contain cameras and sensors.

[85] Source: Tony Smirnov, "WEB Monitoring and Social Listening Tools to Help Boost Security in Airports," LinkedIn, December 8, 2020, https://www.linkedin.com/pulse/web-monitoring-social-listening-tools-help-boost-security-smirnov.

[86] Lykou, Moustakas, and Gritzalis, "Defending Airports from UAS."

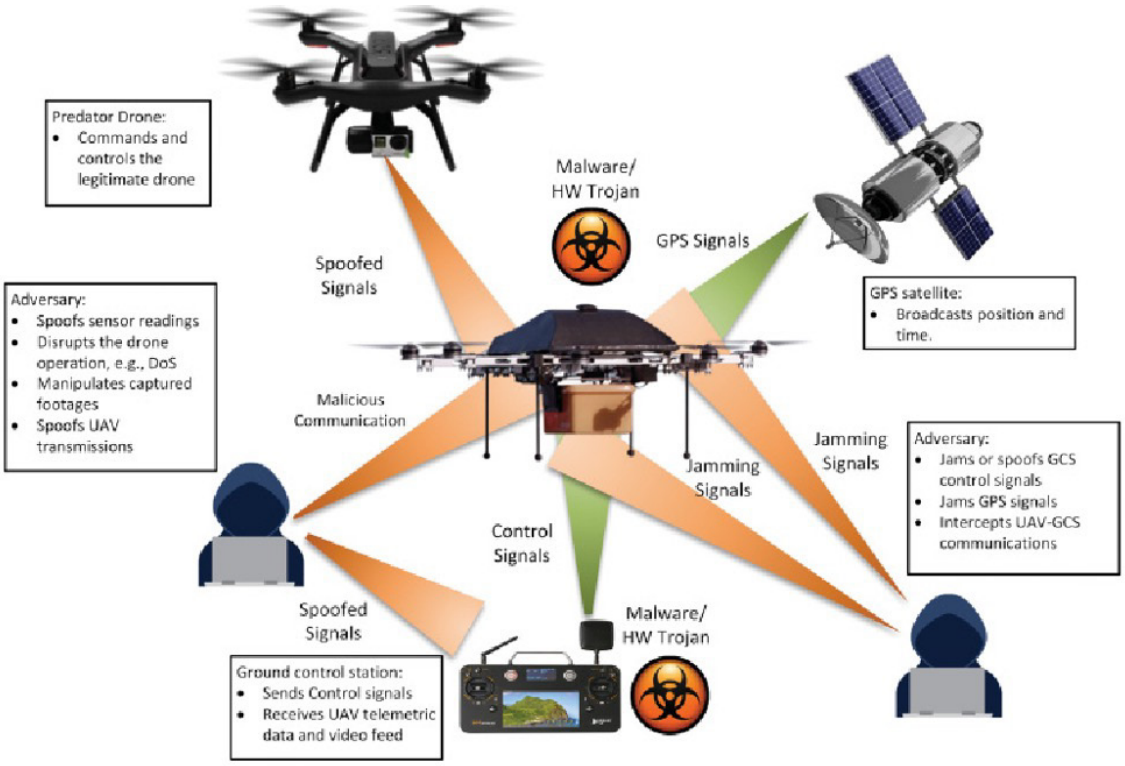

Figure 4. Airport Security Drone Schematic[87]

The use of UASs as active network elements connected to ground-based protection systems is expected to enhance airport perimeter security as well as facilitate airport operations cost reduction.[88] Thus, drones can have numerous potential benefits for airport security. Although the drones are promising, specific challenges accompany the adoption of technological innovations in the aviation industry. In this regard, research on technology adoption in the aviation sector underscores the need for organizational readiness, digital maturity, and airport sustainability to efficiently incorporate technological innovations at

[87] Source: Riham Altawy and Amr M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey," *ACM Transactions on Cyber-Physical Systems* 1, no. 2 (November 2016): 8, https://doi.org/10.1145/3001836.

[88] Korecki, Janošek, and Pecháček, "Use of Unmanned Aerial Systems in Airport Operations."

airports.[89] Developing a proactive and dedicated airport security system requires the appropriate consideration of these factors, which is crucial for preventing and addressing the increasing number of security threats and attacks.[90] In alignment with this, an exploration of current evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States is expected to provide critical perspectives.

F. DEFINITIONS

In alignment with this, an exploration of current evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States is expected to provide critical perspectives. For this exploration, this section presents key definitions.

- Airport Perimeter: Boundary of an airport, comprising the airside and landside areas.
- Airport Perimeter Breach: A security incident wherein unauthorized individuals gain access to the airport grounds or personnel-only areas at airports with the possible intent of engaging in malicious activities that can result in operational disruption, internal accidents, delays, shutdowns, and even terrorist attacks and hijackings.
- Airport Perimeter Security: Security measures specifically aimed at detecting, deterring, and addressing perimeter breaches at airports.

[89] Nigel Halpern et al., "Ready for Digital Transformation? The Effect of Organisational Readiness, Innovation, Airport Size and Ownership on Digital Change at Airports," *Journal of Air Transport Management* 90 (2021): 1–11, https://doi.org/10.1016/j.jairtraman.2020.101949; Nigel Halpern et al., "Conceptualising Airport Digital Maturity and Dimensions of Technological and Organisational Transformation," *Journal of Airport Management* 15, no. 2 (2021): 1–27, https://dspace.lib.cranfield.ac.uk/handle/1826/16634; and S. Sreenath, K. Sudhakar, and AF Yusop, "Sustainability at Airports: Technologies and Best Practices from ASEAN Countries," *Journal of Environmental Management* 299 (December 2021): 1–15, https://doi.org/10.1016/j.jenvman.2021.113639.

[90] Cousins, "Policing the Aerotropolis."

- Airport Security: Measures of protection at airports for the prevention of intentional criminal acts that can harm airport operations, airport personnel, and air passengers, as well as broader regions in the country or abroad.
- Federal Aviation Agency: Agency of the United States government that performs the role of maintaining aviation safety in the United States.
- Internet of Things: A system of integration between the internet and information sensing devices for simplified identification and management.
- Neural network/AI-enabled system management*:* A method of artificial intelligence that trains computers to process and respond to information in a manner like the human brain.
- Perimeter Intrusion Detection System: A security system that detects intruders aiming to breach the perimeters of buildings, properties, or critical infrastructure areas.
- Transport Security Administration: Primary regulatory body in charge of maintaining security at airports in the United States.
- Unmanned Aerial System: Fixed-wing or multi-rotor aircrafts of diverse shapes, sizes, and weights that can be autonomously piloted or operated by remote controllers.
- Wireless Sensor Network: A collection of spatially-distributed sensors that are connected through a network to facilitate data collection by individual sensors and data communication between sensors and the end-user.

G. SUMMARY

The main emphasis of this chapter was to provide an overview of the current evidence related to airport security technology. Technology offers improvements to airport perimeter security, although implementation requires much more research. Technology

adoption in the context of airport security can use recent studies to illustrate diverse technological innovations and their use in various security aspects.[91] Despite recent work about adoption, technology use for enhancing airport perimeter security has received limited attention. A handful of studies have focused on airport perimeter security system innovations, such as the use of optical fiber perimeter systems, the IoT, and UASs.[92] Mentions of other technological tools—such as PIDS, WSN, radar-camera systems, and neural network technology—have been made in the context of airport perimeter security.[93] However, no single study has qualitatively explored the diverse technological tools that can be specifically adopted for enhancing airport perimeter security. Therefore, further research needs to examine the efficacy and efficiency of the use of drones for the enhancement of airport perimeter security.

[91] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports."

[92] Liang and Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device"; Dejdar et al., "Image Edge Detection Methods."; Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems"; Chen and Zhang, "Study on the Internet of Things Discipline in Civil Aviation"; and Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System."; and Hubbard et al., "UAS to Support Airport Safety and Operations"; Lykou, Moustakas, and Gritzalis, "Defending Airports from UAS"; and Korecki, Janošek, and Pecháček, "Use of Unmanned Aerial Systems in Airport Operations."

[93] Tan and Masood, "Adoption of Industry 4.0 Technologies in Airports."

III. METHODS

A. INTRODUCTION

This study aims to present evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States. The intended outcomes of this study include policy and practice recommendations for use by TSA in implementing and using technology as a strategy for airport perimeter security. This chapter elaborates on the methodology adopted for this study. First, the chapter describes the research approach and design of this study and discusses the rationale for selecting the specific research approach and design. Next, it describes the data sources and the data collection procedure, then presents the data analysis plan. Finally, it discusses the measures in place to validate the reliability of the study. The chapter ends with a summary.

B. RESEARCH DESIGN

This study employs a qualitative research methodology. As presented by Creswell and Poth, a qualitative inquiry facilitates a comprehensive understanding of a complex issue through data collection and data analysis processes, which entail gathering and sorting through vast sets of data and identifying relevant themes.[94] Qualitative approaches may be narrative, phenomenological, ethnographic, grounded theories, or have a case study design. Among these, a case study research design is optimal for exploring an issue by considering one or more specific cases within a particular setting or context.[95] Case studies can describe, explain, or explore phenomena and events in the everyday contexts within which they occur.[96] As such, a qualitative case study design aligns with the objective of

[94] John W. Creswell and Cheryl N. Poth, "Designing a Qualitative Study," in *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, by John W. Creswell and Cheryl N. Poth, 4th ed. (Thousand Oaks, CA: SAGE Publications, 2016), 38.

[95] John W. Creswell and Cheryl N. Poth, "Five Qualitative Approaches to Inquiry," in *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, by John W. Creswell and Cheryl N. Poth, 4th ed. (Thousand Oaks, CA: SAGE Publications, 2016), 78.

[96] Yin, *Case Study Research and Applications*, 1.

this study, which is to explore cases of technology usage for airport perimeter security in U.S. airports. Thus, this qualitative case study research design fits the goals of the study.

1. Data Sources

As data sources for this qualitative case study research, the study considered secondary data (i.e., gray and peer-reviewed literature) on cases of technology usage for airport perimeter security. The types of data included peer-reviewed journal articles, conference papers, online articles, video recordings, and other sources comprising data from trials with technology usage for airport perimeter security. This process identified technology usage for airport perimeter security: UAS/drones, biometric technologies, and miscellaneous technologies.

2. Data Collection Procedure

This study followed the following procedure for data collection in this study:

1. Online databases helped identify the relevant literature for this study. These databases included ERIC, JSTOR, ScienceDirect, ProQuest, and Google Scholar.
2. The following keywords directed the literature search in the selected databases: airport security, airport perimeter security, perimeter technology, perimeter security technology, perimeter intrusion detection, perimeter technology use, perimeter security technology use, airport technology use, airport perimeter security technology, UAS airport perimeter security, airport perimeter security drones, airport perimeter security biometric technology, and modern technology in airport perimeter security.
3. This researcher examined the literature obtained by searching the selected databases with the above keywords. For this, he read the abstracts or summaries of the literature thoroughly and established the relevance of the works.

4. After selecting a relevant work for this study, the researcher read the entire content of the work at least twice to identify its major focus.

5. Lastly, the researcher classified the literature into one of the three following categories: UAS/drones, biometric technologies, miscellaneous technologies.

3. Data Analysis Plan

The case study analysis followed the protocols of Yin regarding data analysis.[97] The first step of data analysis involved becoming familiar with the collected data. This step essentially made the researcher thoroughly aware and informed about the information within the collected data. In this study, familiarization with the collected data occurred during the data collection procedure: reading the entire content of the selected literature works through at least twice to determine the major focuses of the literature works, and classifying the literature into one of the three pre-defined categories (i.e., UAS/drones, biometric technologies, or miscellaneous technologies).

The next step analyzed the three distinct cases of technology usage in airport perimeter security (i.e., UAS/drones, biometric technologies, miscellaneous technologies). This case analysis step involved reading through all the identified research works of a single case of technology usage and making a note of the relevant points. Relevant points of a technology usage case included the reported benefits of the technological tool in airport perimeter security systems, its applicability and potential in airport perimeter security, and any available information on real-use cases of the technology in United States airports.

The final step of data analysis included drafting the data analysis report. Each case of technology usage became an independent study, as per the case study analysis proposed by Yin, and the findings of the individual cases were aggregated and synthesized.[98] Thus, as each case was an independent study, a separate step was implemented to aggregate and

[97] Robert K. Yin, "Analyzing Case Study Evidence," in *Case Study Research: Design and Methods*, by Robert K. Yin, 3rd ed. (Thousand Oaks, CA: SAGE, 2003), 133.

[98] Yin, 133–34.

synthesize data cross case studies. The major points reported in association with the three categories of technology usage created Figure 9; the figure illustrates the key takeaways from the exploration of the three cases of technology usage for enhancing existing perimeter security systems at airports.

C. RELIABILITY MEASURES

Reliability is a critical aspect of qualitative research and signifies the degree of confidence that can be attributed to the study and its findings.[99] Yvonna S. Lincoln and Egon G. Guba consider the most common measures of reliability in qualitative research as: confirmability, dependability, credibility, and transferability.[100] Confirmability signifies the extent to which the study findings are neutral and objective and not the researcher's bias; dependability signifies the extent of the study's replicability; credibility signifies the extent to which the study participants can depend on study findings; transferability signifies the applicability of the study findings to other similar contexts. In this study, a major support for reliability comes from case triangulation.[101] The study involves data collection and analysis for three technological cases (i.e., UAS/drones, biometric technologies, or miscellaneous technologies), and the use of these three cases facilitated triangulation, which supports confirmability, dependability, and credibility of the study.[102] In essence, the analysis of the three cases provided separate and comparable insights with regard to technology implementation and usage for improving airport perimeter security in the United States. For supporting transferability of the study, I maintained a reflective journal throughout the data collection and data analysis procedures which allowed for me to develop reflexivity related to potential biases and served as an audit trail to determine the reliability of the findings, and facilitate replication.

---

[99] Nicola J. Petty, Oliver P. Thomson, and Graham Stew, "Ready for a Paradigm Shift? Part 2: Introducing Qualitative Research Methodologies and Methods," *Manual Therapy* 17, no. 5 (October 2012): 4, https://doi.org/10.1016/j.math.2012.03.004.

[100] Yvonna S. Lincoln and Egon G. Guba, "Doing What Comes Naturally," in *Naturalistic Inquiry*, by Yvonna S. Lincoln and Egon G. Guba (Newbury Park, CA: SAGE Publications, 1985), 219.

[101] Petty, Thomson, and Stew, "Ready for a Paradigm Shift?," 5.

[102] Petty, Thomson, and Stew, 5.

D. SUMMARY

This chapter elaborated on the methodology adopted in this study. First, it discussed a rationale for selecting a qualitative case study design for this study. It then established the data sources for secondary data (i.e., gray and peer-reviewed literature) related to three technological cases: UAS or drones, biometric technologies, and miscellaneous technologies for enhancing airport perimeter security at U.S. airports. Next, it described the steps to be adopted for data collection and data analysis. Finally, it explained the measures in place for supporting the reliability of the study. The next chapter discusses the key results of the study.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS, DISCUSSION, AND RECOMMENDATIONS

A. INTRODUCTION

This study aimed to present evidence and insights from cases of technology implementation and usage for improving airport perimeter security in the United States. It considered three distinct cases of technology usage for enhancing airport perimeter security: UAS/drones, biometric technologies, miscellaneous technologies. This chapter presents the key findings obtained from the review of gray and peer-reviewed literature works for each technological case. Further, based on the findings, it makes relevant recommendations for future research and practice.

B. RESULTS

1. UAS/Drones

UASs or drones have emerged as a promising application for perimeter security enhancement technology for airports. A drone is an unmanned aircraft that can be controlled remotely. Equipped with cameras and sensors, these tools can play a valuable role in any airport security system. Drones represent a fresh approach to perimeter security and have been demonstrated to be an efficient security tool.[103] UASs that are equipped with cameras and sensors can be are integrated into airport security programs, serving various functions, including conducting perimeter patrols, monitoring PIDS, responding to alarm systems, tracking potential threats, visually inspecting remote areas of the airport, and performing numerous other tasks.[104] UASs have the potential to streamline fence and gate lock inspections and enhance existing security measures by conducting random perimeter checks throughout the day.[105] The rapid deployment, surveillance capabilities, and object tracking abilities of UAS make them a valuable "force multiplier" that enhances

[103] Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports," 1–2.

[104] Ashirbek, 2.

[105] Hubbard et al., "UAS to Support Airport Safety and Operations," 7.

and complements existing airport security systems in multiple ways.[106] With advanced technology on board, UASs can provide real-time visual information from a safe distance (approximately 25 feet above ground level). Mounting a bird's eye view type camera significantly enhances situational awareness, offering wider-ranging views and exceptional levels of detail to human operators who perform inspections using the UASs.[107] Such technology is critical to detect modern airport security threats.

UASs offer a set of advantages for airport perimeter security. Some sections of airport perimeters might be difficult to patrol regularly due to topographical configurations; however, deploying UASs over these areas provides aerial surveillance capabilities that traditional security measures cannot match.[108] The use of UASs in perimeter patrol at airports also reduces the need for humans to respond to false alarms. Such alarms, which happen daily, often require dispatching security personnel to check the airport perimeter, even for minor triggers like a plastic bag or wildlife. By using UASs, airport security personnel can verify breaches more quickly, navigate directly to the location of the breach, and gain valuable situational awareness. This approach not only improves response time but also helps alleviate personnel shortages by allowing security officers to focus on necessary inspections.[109] Therefore, the integration of this technology could advance the safety of passengers and workers in the airport industry.

UASs offer airports the advantage of reducing personnel requirements and optimizing the efficiency of existing systems. For instance, UASs can complete runway pavement inspections within a mere 30 minutes, whereas traditional methods would take up to eight hours and necessitate the closure of the runway. Akbota Ashirbek maintains that using UASs in a well-planned manner can avoid runway closure entirely.[110] He further contends the approach eliminates the need for human presence in safety-critical areas because the UAS can be operated from a safe distance. He points out this distance is

[106] Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports," 10.

[107] Ashirbek, 11.

[108] Ashirbek, 11.

[109] Ashirbek, 12.

[110] Ashirbek, 10.

particularly valuable in airport environments because individuals or physical obstacles in critical areas may disrupt navigational systems and introduce errors. UASs can improve inspection efficiency, which can yield significant annual benefits, especially considering that even smaller hub airports may need to perform up to six inspections daily. Given the expansive size of many airports and the presence of non-populated areas distant from active runways, UASs can serve as a suitable tool for bolstering security with minimal risk or disruption to aeronautical operations.[111] Thus, UASs reduce several security limitations regarding manpower in airport security.

Considering the several benefits of UASs, the adoption of the UAS technology has already begun in U.S. airports. Airports such as the Dallas/Fort Worth International and Savannah/Hilton Head International have included UAS-based processes in their routine operations for conducting inspection, maintenance, and law enforcement programs.[112] Further, Hartsfield-Jackson Atlanta International Airport has effectively used drones for 3D mapping of runway surfaces to identify cracks as part of their runway repair and resurfacing projects. Traditionally, conducting such inspections would necessitate closing the runway for several hours, with airport staff employing specialized equipment.[113] Although these airports have begun to leverage the capabilities of the UAS technology, use cases of UASs in airport security, and specifically airport perimeter security, are currently limited.

Non-airport authorities have explored the use of UASs for airport perimeter security operations. In 2019, the Safe Skies Alliance (SSA) conducted a case study involving the integration of autonomous UAS for security support.[114] The study took place at one of the SSA's test facilities near the McGhee Tyson Airport in Tennessee, which had a fence-mounted perimeter detection system. During the trials, various missions assessed the capabilities of the autonomous drones. For instance, in one test flight, an autonomous UAS

111 Hubbard et al., "UAS to Support Airport Safety and Operations," 7.

112 Ashirbek, "Analysis of the FAA's Small UAS Regulations for Airports," 1–2.

113 Ashirbek, 13.

114 Ashirbek, 13–15.

followed a predetermined route using GPS coordinates to investigate the test site of another UAS, which served as a target object to track. The autonomous UAS provided a panoramic view of the area adjacent to the target the UAS's launch site and notified the operator when the target object appeared, initiating the tracking of the threat. The security personnel could monitor real-time video transmission and assess the danger. The mission was successfully completed, demonstrating the autonomous the UAS's ability to fly pre-programmed routes and switch to manual control when needed.[115] Thus, this study validated the effective use of drones.

Studies continue to reveal the benefits of using drones for security purposes. In an earlier report in 2013, the Office of Inspector General of the Department of Justice announced that small UASs, with weights up to 55 pounds, can have significantly cheaper operational and maintenance costs compared to manned aircraft. The report highlighted the significant cost advantage of UASs, with an estimated cost of $25/hour, compared to $650/ hour for manned aircraft operations.[116] The specific models of UASs highlighted for airport security measures are the SkyRanger quadcopter and the hybrid FireFLY6 PRO UAS.

Figure 5 shows the SkyRanger quadcopter. The SkyRanger quadcopter sets itself apart from other quadcopters by offering an extended flying duration of 50 minutes, which exceeds the capabilities of other quadcopters.[117] As a result, it is well-suited for missions that require longer periods of operation. Furthermore, it demonstrates enhanced durability in inclement weather circumstances, as it possesses the capacity to survive wind gusts of up to 65 kilometers/hour and withstand temperatures ranging from -22 to 122 degrees Fahrenheit.

[115] Ashirbek, 13–15.

[116] Ashirbek, 11.

[117] Source: "SkyRanger R70," Unmanned Aerial Systems, accessed October 9, 2023, https://www.flir.com/products/skyranger-r70/?vertical=uas&segment=uis.

Figure 5. SkyRanger Quadcopter[118]

In contrast, the hybrid FireFLY6 PRO UAS—which combines fixed-wing and vertical takeoff and landing functionalities—offers a cost-effective solution for conducting perimeter inspections within a range of around seven miles. This UAS costs less than $10,000/unit. Nevertheless, certain restrictions in terms of operating conditions, such as restricted range capabilities and decreased tolerance to windy conditions accompany the price of these systems. Although a rudimentary surveillance system may solely offer video capabilities, a more extensive configuration could encompass automated video detection and alerts to augment its functionality.[119] As the UAS technology continues to advance, the airport perimeter security system is expected to witness gradual incorporation of UASs in perimeter security operations and an increasing number of law enforcement agencies will likely have the opportunity to adopt UASs as a cost-effective alternative to manned aircraft.

2. Biometric Technologies

Biometric technologies may offer valuable solutions for enhancing airport perimeter security. A biometric system is a technology that detects and analyzes human

[118] Source: "SkyRanger R70," Unmanned Aerial Systems, accessed October 9, 2023, https://www.flir.com/products/skyranger-r70?vertical=uas&segment=uis.

[119] Hubbard et al., "UAS to Support Airport Safety and Operations," 7–8.

biological systems and indicators of potential security threats, such as heat and perspiration. Biometric systems may replace traditional access cards or PIN codes, using unique biometric identifiers like fingerprints, iris scanning, or facial recognition to grant access to secure areas within the airport perimeter.[120] These technologies can facilitate precise identification and authentication of individuals, improving access control measures and reducing the risk of unauthorized entry. Physiological characteristics such as facial features, fingerprints, hand geometry, handwriting, voice, and retinal and vein recognition signatures have been identified as traceable biometric features, which can be used in automated personal identification systems for perimeter security at vulnerable control points.[121] Figure 6 shows a biometric system that is commonly used in airport security.

Figure 6. Biometric System for Airport Security[122]

[120] Amankwah-Amoah, "COVID-19 Pandemic and Innovation Activities," 4.

[121] Rajapaksha and Jayasuriya, "Smart Airport," 29.

[122] Source: Chris Burt, "Airport Biometrics at a Potential Turning Point," Biometric Update, June 4, 2018, https://www.biometricupdate.com/201806/airport-biometrics-at-a-potential-turning-point.

This screening process ensures that only authorized personnel can enter restricted zones or sensitive facilities.[123] In addition to access control, biometric technologies verify the identities of airport employees and visitors. By integrating biometric systems at entry and exit points, airports can ensure that only authorized individuals gain access, preventing unauthorized personnel from entering or leaving the premises. This restriction helps maintain a secure environment and enables effective tracking of personnel movements within the airport.

Implementing biometric technologies throughout various stages of passenger movement within airports can significantly enhance security levels.[124] By using biometric identifiers such as fingerprints or facial recognition, airports can verify the identity of individuals entering the airport premises, thereby enhancing perimeter security measures. Although biometric technology applications in perimeter security systems in U.S. airports are limited, the deployment of biometric approaches in airport perimeter security will likely improve accuracy, efficiency, and the ability to detect potential threats. By streamlining access control processes, enhancing surveillance capabilities, and strengthening identity verification, biometric technologies may play a vital role in safeguarding airports and ensuring the safety of passengers, employees, and facilities.

3. Other Technologies: IoT, Fiber Optics,

Along with UAS and biometric technologies, many other innovative technological tools are gradually becoming popular for enhancing existing airport perimeter security measures. Primary among these are advanced sensor systems which incorporate modern technologies, including the IoT and fiber optics. The IoT refers to a network of diverse physical devices that are connected to each other through the internet, enabling integration among all these devices and facilitating easy identification and management. In the airport perimeter security domain, various information sensing devices, such as laser scanners, global positioning systems, infrared sensors, and RFID devices link through the IoT

[123] Hubbard et al., "UAS to Support Airport Safety and Operations," 8.

[124] Sreenath, Sudhakar, and Yusop, "Sustainability at Airports," 11–12.

network to integrate these devices and enhance traditional perimeter security systems.[125] These forms of technology allow the automatic identification and transmission of signals that allow remote tracking of tags. In the IoT system, RFID devices have gained substantial interest for airport perimeter security enhancement because of their potential to improve existing access control systems.[126] The IoT technology is gradually being implemented in various sensor systems at airports and is on the way to become a critical part of airport perimeter security.[127] Thus, the integration of these technologies can significantly enhance airport security. Figure 7 demonstrates the use of RFID in airport security.

Figure 7. Airport RFID for Security Purposes[128]

[125] Cao, Jing, and Zheng, "Design of the Airport Perimeter Security System," 2277.

[126] Cao, Jing, and Zheng, 2277.

[127] Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems," 244.

[128] Source: "Newark Airport Improves Travel Experience with RAIN RFID," Innovating IoT Solutions in Air Transportation with RAIN RFID, accessed October 9, 2023, https://www.impinj.com/industries/airlines-airports.

Fiber optics sensing systems are another recent technological advancement suitable for airport perimeter security systems because they enable automatic breach detection. These sensing systems use fiber optic cables, which are essentially thin cables made of glass or plastic, transmitting data through light signals.[129] The installation of fiber optics cables along the airport perimeter facilitates the detection and location of disturbances or intrusions through the fiber optics sensing system. The principle behind fiber optics sensing systems involves measuring changes in the light signal transmitted through the fiber optic cables. When an intrusion occurs, it disrupts the light signal, and the system can pinpoint the exact location of the disturbance.[130] It then relays information to a central monitoring station, where security personnel can assess the situation and take appropriate action. Fiber optics sensing systems provide more efficient long-distance monitoring compared to traditional technologies as the fiber optics cables can be used as both signal acquisition and signal transmission units.[131] Therefore, this form of technology can play an important role in airport security.

Further, fiber optics sensing systems offer high levels of sensitivity and accuracy, allowing for precise detection and localization of intrusions. Identification rates of 100.0 percent and 96.9 percent have been obtained for detecting wind disturbances as well as three typical patterns of human intrusions (i.e., waggling the perimeter fencing, climbing the perimeter fence, and knocking the fence) using fiber optics sensing systems, demonstrating the potential of this technology.[132] Fiber optics sensing systems are immune to electromagnetic interference, can operate over long distances without any performance loss, and are resistant to harsh environmental conditions, such as extreme temperatures, moisture, and electrical interference. For all these reasons, fiber optics are highly sought after in airport perimeter security advancements. As can be seen in Figure 8, fiber optics contain multiple layers and components.

[129] Rajapaksha and Jayasuriya, "Smart Airport," 29.

[130] Papagiannopoulos, Loupos, and Skoufis, "Iot-Based Airport Systems," 244.

[131] Liang and Chen, "Analysis on Signal Sensing Principle of Optical Fiber Device," 150.

[132] Sun et al., "Variational Mode Decomposition-Based Event," 182580.

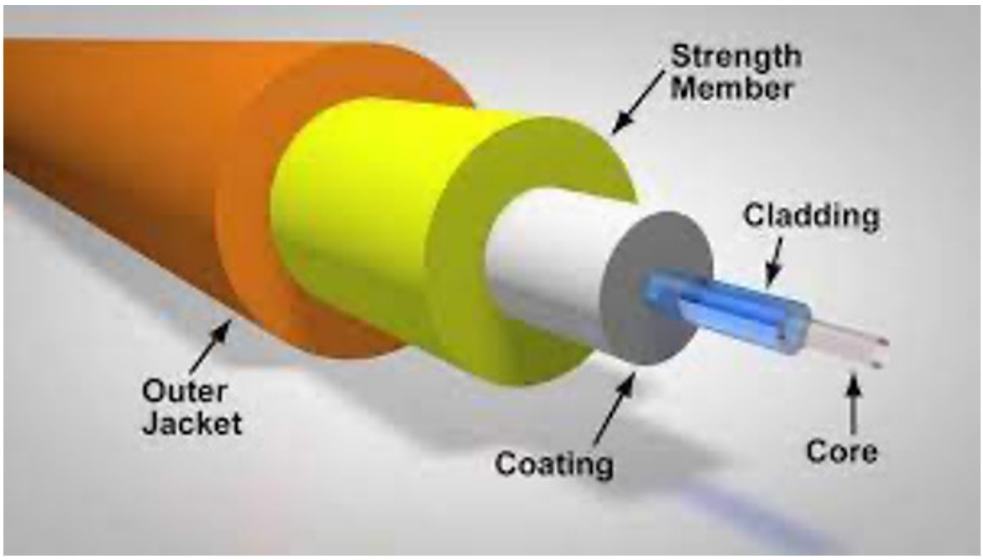

Figure 8. Fiber Optics[133]

In addition to the innovative, efficient, and powerful sensor systems, technological advancements in the field of AI will likely become crucial in modern-day airport perimeter security. Advancements in the integration of technology, automation, and AI may decrease the need for human involvement in airport perimeter security monitoring.[134] In the airport perimeter security domain, AI-based facial recognition technology can identify individuals on watchlists or persons of interest; it can also map human images into law enforcement database files, enabling the identification of perpetrators.[135] By comparing live or recorded facial images against databases, security systems can quickly flag potential threats and alert airport authorities.

ML and AI offer some decided advantages in airport perimeter security. Furthermore, AI in the form of ML is gaining significant popularity in cyber surveillance, which has proven to be less labor-intensive compared to traditional human surveillance

[133] Source: "Introduction to Fiber Optics," Fiber & Fiber Patch Cables Technical Publications, accessed October 9, 2023, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=10759.

[134] Barry, *Guidance for Airport Perimeter Security*, 69.

[135] Nikolay Radulov, "Artificial Intelligence and Security. Security 4.0," *Security & Future* 3, no. 1 (2019): 3, https://stumejournals.com/journals/confsec/2019/1/3.

methods.[136] AI is the use of technology to solve complex and human-like problems, while ML refers to the analysis of complex and large sets of data to improve the functionality of a technological device or system like AI. Along with ML, the capabilities of AI in behavioral data collection, pattern recognition, and probabilistic estimations can be highly applicable in the airport perimeter security domain.[137] AI can analyze vast amounts of data, including historical and real-time information, to identify potential security risks or vulnerabilities. By leveraging ML algorithms, AI systems can recognize patterns and trends, helping security teams proactively mitigate threats and allocate resources effectively. The incorporation of AI-based sensors in existing perimeter security systems can help process the large amount of surveillance data being collected, with AI-based deep neural networks facilitating image classification.[138] Despite being in its early stages of development, AI technology is anticipated to gain widespread popularity in the field of airport perimeter security, as it offers promising approaches for enhancing security measures in modern airports.

4. Major Takeaways

The major takeaways from the exploration of technology usage for the enhancement of airport perimeter security appear in Figure 9. Figure 9 shows the three technological cases discussed in this chapter (i.e., UAS/drones, biometric technologies, and miscellaneous technologies), the existing information regarding the benefits, applicability, and potential of these technological cases, and the future directions needed to better incorporate these technologies into airports to enhance existing perimeter security systems.

Figure 9 also highlights the diverse benefits and strong potential of the three technologies (i.e., UAS/drones, biometric technologies, and miscellaneous technologies) in airport perimeter security enhancement. Exploring the integration of these highly applicable technological tools into the layered perimeter security system of airports may

[136] Michael Horowitz et al., *Artificial Intelligence and International Security* (Washington, DC: Center for a New American Security, 2018), 2, ProQuest.

[137] Horowitz et al., 3.

[138] Horowitz et al., 7.

provide valuable insights. Notably, research on real-use cases of these technologies is critically required to comprehensively understand how their incorporation can help improve existing perimeter security systems and enhance airport security.

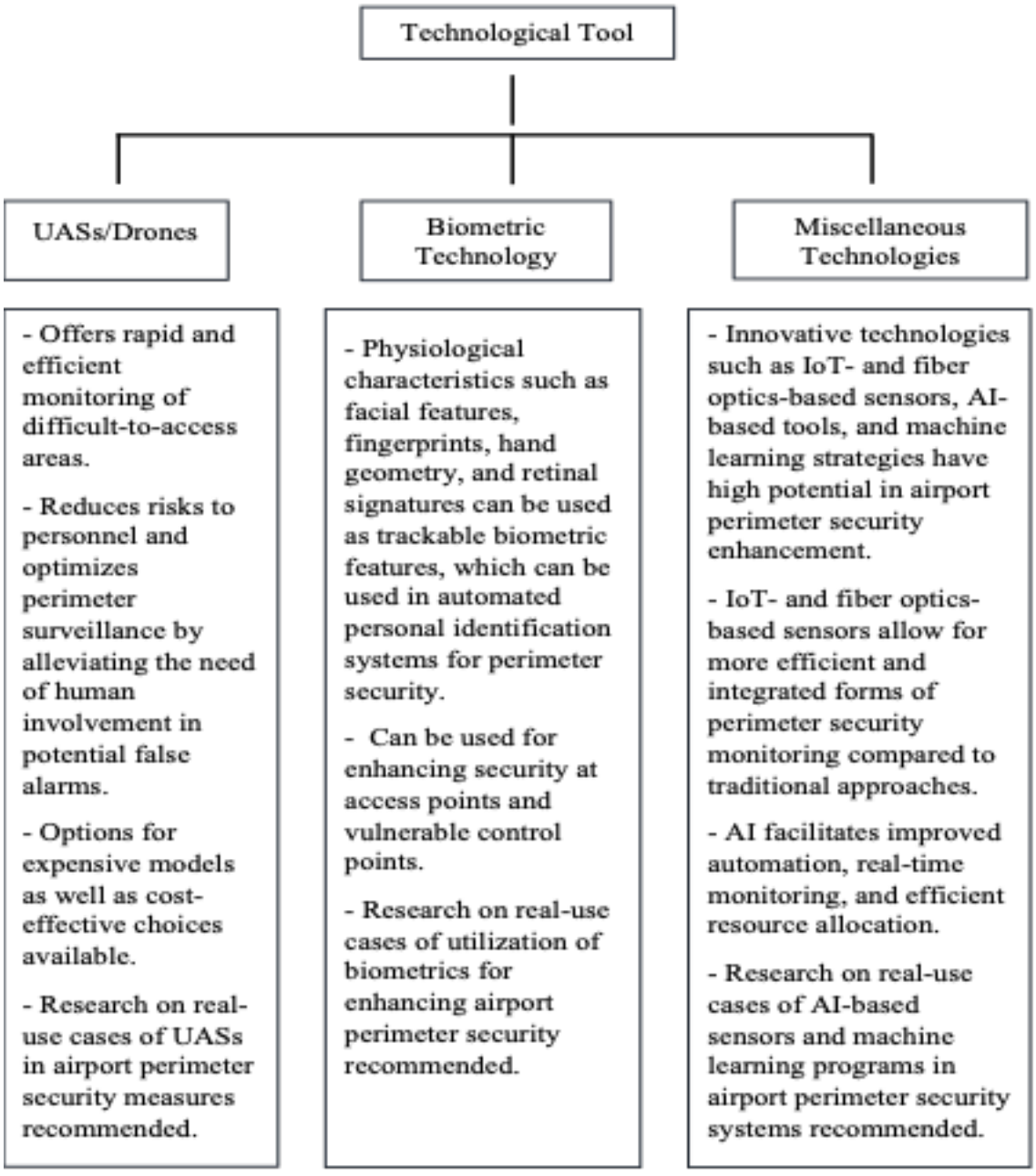

Figure 9. Technology Usage for Airport Perimeter Security Enhancement

5. Potential Extent of Technology Usage for Enhanced Perimeter Security

The potential of these technological tools—UASs, biometrics, IoT, AI and ML—for enhancing airport perimeter security indicates that an integrated technology-driven perimeter security model could offer significant benefits. Such an integrated perimeter security model could combine UASs, biometric tools, IoT, AI, and ML capabilities to provide the most effective and cost-efficient strategy for preventing and addressing potential perimeter breaches. The optimal combination of these technologies for designing an effective and cost-efficient perimeter security strategy would involve identifying and leveraging the individual benefits of these technologies.

A possible technology-driven airport perimeter security system might consist of the following elements:

- UASs that offer rapid and efficient monitoring of difficult-to-access areas could patrol the airport perimeter fencing as well as restricted access points. Airports could tailor the number and type of UASs being used to their specific budgets, given the wide range of options available for expensive models and cost-effective choices. The use of UASs would reduce the number of personnel required for perimeter patrolling, allowing the reallocation of funding for other technology in the perimeter security system.

- The video feed of the patrolling UASs could be integrated with AI and machine capabilities for matching with biometric data obtained at airport control points, thereby facilitating an effective technology-driven perimeter security system that offers improved automation, efficient resource allocation, and enhanced security.

C. RECOMMENDATIONS FOR RESEARCH

Future research is recommended on several aspects of technology usage in airport perimeter security enhancement. First, Industry 4.0 technologies and their application potential in specific aspects of existing airport perimeter security systems requires further

study. Systematic research work is also recommended on traditional perimeter security measures and corresponding replacement Industry 4.0 technologies. Investigating the effectiveness, feasibility, and potential challenges associated with integrating Industry 4.0 technologies into airport security systems is necessary to obtain valuable insights and contribute to the development of more robust and efficient security measures. Exploration of real-use cases of advanced technologies, including UASs, biometric technologies, the IoT, fiber optics sensor systems, and AI, in perimeter security systems at airports is also crucial for understanding the practicalities associated with technology usage in airport perimeter security. Conducting focused research in these areas, could achieve a deeper understanding regarding how to effectively employ these technologies to ensure the security of airport perimeters.

D. RECOMMENDATIONS FOR PRACTICE

Based on the findings of this study, the following recommendations for practice could strengthen airport perimeter security using technological advancements. First, airport authorities can consider conducting comprehensive assessments of their existing perimeter security systems to identify potential areas to implement Industry 4.0 technologies. This evaluation should involve an examination of the effectiveness and efficiency of traditional security measures in comparison to the potential benefits offered by advanced technologies. Additionally, airport management can explore partnerships with technology providers and experts in the field to gain insights into best practices for integrating Industry 4.0 technologies into their security infrastructure.

Airports can also invest in pilot projects to test the practical applications of UASs, biometric technologies, the IoT, fiber optics sensor systems, and AI in their specific perimeter security context. These projects could involve collaboration with relevant stakeholders, such as security agencies, technology vendors, and regulatory bodies, to ensure compliance with legal and operational requirements. By implementing these advanced technologies in real-life scenarios, airports can assess their efficacy, address any operational challenges, and refine their security protocols accordingly. Additionally, airport personnel need ongoing training and education programs to equip them with the

necessary skills and knowledge to operate and maintain these advanced security systems. Such personnel development includes providing specialized training on the use of UASs, biometric technologies, and AI-based systems, and promoting a culture of cybersecurity awareness to mitigate potential risks associated with interconnected technologies.

To recap, the following list contains implications of this study:

- Airport authorities can perform more comprehensive assessments of existing perimeter security threats.
- Partnerships with technology companies can be explored.
- Ongoing training and educational programs can be established to ensure technological skill in these areas.
- The adoption of drones can greatly enhance overall airport security at a low cost to airports.

Overall, the adoption of advanced technologies in airport perimeter security should be a strategic and continuous effort, guided by regular evaluations and updates based on the industry's best practices and emerging innovations. By implementing these recommendations, airports can strengthen their security posture, enhance situational awareness, and mitigate potential threats to ensure the protection of airport perimeters.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Altawy, Riham, and Amr M. Youssef. "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey." *ACM Transactions on Cyber-Physical Systems* 1, no. 2 (November 2016): 1–25. https://doi.org/10.1145/3001836.

Amankwah-Amoah, Joseph. "COVID-19 Pandemic and Innovation Activities in the Global Airline Industry: A Review." *Environment International* 156 (2021): 1–7. https://doi.org/10.1016/j.envint.2021.106719.

Anderson, David. "Optimising Multi-Layered Security Screening." *Journal of Transportation Security* 14, no. 3–4 (December 2021): 249–73. https://doi.org/10.1007/s12198-021-00237-3.

Arti, Endang Sugih, Nunuk Praptiningsih, Rinosa Ari Widagdo, and Dini Wagini. "Airport Perimeter Security System Readiness Analysis (Case Study at Budiarto Curug-Tangerang Airport)." *Siber Journal of Transportation and Logistics* 1, no. 2 (July 2023): 64–71. https://doi.org/10.38035/sjtl.v1i2.

Ashirbek, Akbota. "Analysis of the FAA's Small UAS Regulations for Airports Security Support UAS Operations." Master's thesis, Arizona State University, 2022. https://keep.lib.asu.edu/items/171683/view.

Barnett, Arnold. "Aviation Safety and Security." In *The Global Airline Industry*, edited by Peter Belobaba, Amedeo Odon, and Cynthia Barnhart, 313–42. West Sussex, UK: John Wiley & Sons, Ltd, 2009. https://doi.org/10.1002/9780470744734.ch11.

Barry, Ann S. *Guidance for Airport Perimeter Security*. Louisville, TN: National Safe Skies Alliance, Inc., 2018. https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf.

Barry, Ann S., and David S. Mazel. "Airport Perimeter Security: Where We've Been, Where We Are, and Where We're Going." In *2008 IEEE Conference on Technologies for Homeland Security*, 57–62. Piscataway, NJ: IEEE, 2008. https://doi.org/10.1109/THS.2008.4534423.

Bosch Security Systems. "Airport Security Solutions." Bosch Security and Safety Systems. Accessed October 9, 2023. https://www.boschsecurity.com/us/en/industries/airports/.

Boselli, Chris, Jason Danis, Sandra McQueen, Alex Breger, Tao Jiang, Douglas Looze, and Daiheng Ni. "Geo-Fencing to Secure Airport Perimeter against sUAS." *International Journal of Intelligent Unmanned Systems* 5, no. 4 (2017): 102–16. https://doi.org/10.1108/IJIUS-02-2017-0002.

Burt, Chris. "Airport Biometrics at a Potential Turning Point." Biometric Update, June 4, 2018. https://www.biometricupdate.com/201806/airport-biometrics-at-a-potential-turning-point.

Callander, Briony, and Christian Kaunert. "Technological Innovation in Aviation Security: From Industries as Policy Entrepreneurs." *Politeja* 4, no. 79 (2022): 55–71. https://doi.org/10.12797/Politeja.19.2022.79.04.

Cao, Xue Ming, Chen Mei Jing, and Xiao Dan Zheng. "Design of the Airport Perimeter Security System Based on Internet of Things." *Applied Mechanics and Materials* 361–363 (2013): 2276–81. https://doi.org/10.4028/www.scientific.net/AMM.361-363.2276.

Chen, Jialei, and Huan Zhang. "Study on the Internet of Things Discipline in Civil Aviation." In *Advances in Artificial Intelligence and Security: 8th International Conference on Artificial Intelligence and Security, ICAIS 2022, Qinghai, China, July 15–20, 2022, Proceedings, Part III*, edited by Xingming Sun, Xiaorui Zhang, Zhihua Xia, and Elisa Bertino, 586–94. Cham, Switzerland: Springer International Publishing AG, 2022.

Cheong, Kim, Francis Joseph Costello, and Kun Chang Lee. "Integrating Qualitative Comparative Analysis and Support Vector Machine Methods to Reduce Passengers' Resistance to Biometric E-Gates for Sustainable Airport Operations." *Sustainability* 11 (2019): 1–22. https://doi.org/10.3390/su11195349.

Cheong, Kim, Kun Chang Lee, and Francis Joseph Costello. "The Intention of Passengers towards Repeat Use of Biometric Security for Sustainable Airport Management." *Sustainability* 12 (2020): 1–18. https://doi.org/10.3390/su12114528.

Cousins, Joshua T. "Policing the Aerotropolis: A Model for Securing the Nation's Large Airports." Master's thesis, Naval Postgraduate School, 2021. https://hdl.handle.net/10945/67120.

Creswell, John W., and Cheryl N. Poth. "Designing a Qualitative Study." In *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, by John W. Creswell and Cheryl N. Poth, 41–64, 4th ed. Thousand Oaks, CA: SAGE Publications, 2016.

———. "Five Qualitative Approaches to Inquiry." In *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, by John W. Creswell and Cheryl N. Poth, 65–110, 4th ed. Thousand Oaks, CA: SAGE Publications, 2016.

———. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*. 4th ed. Thousand Oaks, CA: Sage, 2016.

Culmone, Claudia. "Safety vs. Security: Is There a Difference?" *NATACS Blog* (blog), July 25, 2018. https://info.natacs.aero/natacs-blog/safety-vs.-security-is-there-a-difference.

Dejdar, Petr, Pavel Záviška, Soběslav Valach, Petr Münster, and Tomáš Horváth. "Image Edge Detection Methods in Perimeter Security Systems Using Distributed Fiber Optical Sensing." *Sensors* 22, no. 12 (January 2022): 1–13. https://doi.org/10.3390/s22124573.

Ford, James, Ardeshir Faghri, Dian Yuan, and Saumabha Gayen. "An Economic Study of the U.S. Post-9/11 Aviation Security." *Open Journal of Business and Management* 8, no. 5 (August 2020): 1923–45. https://doi.org/10.4236/ojbm.2020.85118.

Halpern, Nigel, Thomas Budd, Pere Suau-Sanchez, Svein Bråthen, and Deodat Edward Mwesiumo. "Conceptualising Airport Digital Maturity and Dimensions of Technological and Organisational Transformation." *Journal of Airport Management* 15, no. 2 (2021): 1–27. https://dspace.lib.cranfield.ac.uk/handle/1826/16634.

Halpern, Nigel, Deodat Mwesiumo, Pere Suau-Sanchez, Thomas Budd, and Svein Bråthen. "Ready for Digital Transformation? The Effect of Organisational Readiness, Innovation, Airport Size and Ownership on Digital Change at Airports." *Journal of Air Transport Management* 90 (2021): 1–11. https://doi.org/10.1016/j.jairtraman.2020.101949.

Hättenschwiler, Nicole, Yanik Sterchi, Marcia Mendes, and Adrian Schwaninger. "Automation in Airport Security X-Ray Screening of Cabin Baggage: Examining Benefits and Possible Implementations of Automated Explosives Detection." *Applied Ergonomics* 72 (October 2018): 58–68. https://doi.org/10.1016/j.apergo.2018.05.003.

Horowitz, Michael, Paul Scharre, Gregory C. Allen, Frederick Kara, Anthony Cho, and Edoardo Saravalle. *Artificial Intelligence and International Security*. Washington, DC: Center for a New American Security, 2018. ProQuest.

Hubbard, Sarah, Andrew Pak, Yue Gu, and Yan Jin. "UAS to Support Airport Safety and Operations: Opportunities and Challenges." *Journal of Unmanned Vehicle Systems* 6, no. 1 (2018): 1–17. https://doi.org/10.1139/juvs-2016-0020.

IMPINJ. "Newark Airport Improves Travel Experience with RAIN RFID." Innovating IoT Solutions in Air Transportation with RAIN RFID. Accessed October 9, 2023. https://www.impinj.com/industries/airlines-airports.

Jacobson, Sheldon H. "Are Airport Perimeter Security Breaches a Threat to Air Travelers?" The Hill, April 4, 2022. https://thehill.com/opinion/national-security/3258416-are-airport-perimeter-security-breaches-a-threat-to-air-travelers/.

Johnstone, William. “Passenger Aviation Security Layers.” *SciTech Connect* (blog), October 6, 2015. https://scitechconnect.elsevier.com/passenger-aviation-security-layers/.

Khan, Nimra, and Marina Efthymiou. “The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP).” *International Journal of Information Management Data Insights* 1 (2021): 1–14. https://doi.org/10.1016/j.jjimei.2021.100049.

Kiliç, Sena, Caglar Ucler, and Luis Martin-Domingo. “Innovation at Airports: A Systematic Literature Review (2000–2019).” *Aviation* 25, no. 3 (2021): 220–31. https://doi.org/10.3846/aviation.2021.14917.

Klenka, Michal. “Major Incidents That Shaped Aviation Security.” *Journal of Transportation Security* 12, no. 1 (2019): 39–56. https://doi.org/10.1007/s12198-019-00201-2.

Korecki, Zbyšek, Miroslav Janošek, and Tomáš Pecháček. “Use of Unmanned Aerial Systems in Airport Operations.” In *2021 International Conference on Military Technologies (ICMT)*, 1–8. Piscataway, NJ: IEEE, 2021. https://doi.org/10.1109/ICMT52455.2021.9502756.

Kovynyov, Ivan, and Ralf Mikut. “Digital Technologies in Airport Ground Operations.” *Netnomics : Economic Research and Electronic Networking* 20, no. 1 (April 2019): 1–25. https://doi.org/10.1007/s11066-019-09132-5.

Liang, Youcheng, and Haitao Chen. “Analysis on Signal Sensing Principle of Optical Fiber Device in Airport Perimeter Security System.” In *2020 International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, 150–52. Piscataway, NJ: IEEE, 2020. https://doi.org/10.1109/ISCEIC51027.2020.00038.

———. “Design and Analysis of Airport Intelligent Border System Based on Zigbee Technology.” In *2022 IEEE 22nd International Conference on Communication Technology (ICCT)*, 917–20. Piscataway, NJ: IEEE, 2022. https://doi.org/10.1109/ICCT56141.2022.10072545.

Lincoln, Yvonna S., and Egon G. Guba. “Doing What Comes Naturally.” In *Naturalistic Inquiry*, by Yvonna S. Lincoln and Egon G. Guba, 187–220. Newbury Park, CA: SAGE Publications, 1985.

Lykou, Georgia, Dimitrios Moustakas, and Dimitris Gritzalis. “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies.” *Sensors* 20, no. 12 (January 2020): 1–40. https://doi.org/10.3390/s20123537.

Mackie, Thomas, and Aaron Lawrence. "Integrating Unmanned Aircraft Systems into Airport Operations: From Buy-in to Public Safety." *Journal of Airport Management* 13, no. 4 (Autumn 2019): 380–90.

Matta, Walter, and Alessandro Cantelli-Forti. "An Innovative Airport Physical-Cyber Security System (APSS)." *Information & Security* 43, no. 1 (2019): 285–93. https://doi.org/10.11610/isij.4321.

Metzner, Nora. "A Comparison of Agent-Based and Discrete Event Simulation for Assessing Airport Terminal Resilience." *Transportation Research Procedia* 43 (2019): 209–18. https://doi.org/10.1016/j.trpro.2019.12.035.

Moody, Steve. "Integrated Security." *Intersec: The Journal of International Security* 29, no. 6 (June 2019): 20–22. http://www.intersecmag.co.uk/integrated-security-2/.

Negri, Nathane Ana Rosa, Giovanna Miceli Ronzani Borille, and Viviane Adriano Falcão. "Acceptance of Biometric Technology in Airport Check-In." *Journal of Air Transport Management* 81 (October 2019): 101720. https://doi.org/10.1016/j.jairtraman.2019.101720.

Nowacki, Gabriel, and Bohdan Paszukow. "Security Requirements for New Threats at International Airports." *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 1 (March 2018): 187–92. https://doi.org/10.12716/1001.12.01.22.

Olivier, Jeanne. "Airport Perimeter Security: Finding the Right Fit for Your Airport." *Airport Magazine*, August 2014. https://www.airportmagazine-digital.com/airportmagazine/aug_sept_2014?article_id=1109837&lm=1494535961000.

Panter, Heather A. "Airport Security: Procedures in Secured Areas for TSA and Private Security." In *Encyclopedia of Security and Emergency Management*, edited by Lauren R. Shapiro and Marie-Helen Maras, 1–9. Cham, Switzerland: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-69891-5_2-1.

Papagiannopoulos, Nikos, Konstantinos Loupos, and Christos Skoufis. "Iot-Based Airport Systems: A Unified Approach towards Establishing Trust for High Security and Integrity of Industrial Iot Platforms and Sensors." *Journal of Airport Management* 15, no. 3 (Summer 2021): 244–57. https://trid.trb.org/view/1870577.

Pereira, Bruno Alencar, Gui Lohmann, and Luke Houghton. "Innovation and Value Creation in the Context of Aviation: A Systematic Literature Review." *Journal of Air Transport Management* 94 (July 2021): 102076. https://doi.org/10.1016/j.jairtraman.2021.102076.

Petty, Nicola J., Oliver P. Thomson, and Graham Stew. "Ready for a Paradigm Shift? Part 2: Introducing Qualitative Research Methodologies and Methods." *Manual Therapy* 17, no. 5 (October 2012): 378–84. https://doi.org/10.1016/j.math.2012.03.004.

Pheasant, Christopher, Lorena de Rodriguez, and Don Zoufal. *Airport Security Training for Law Enforcement and Security Personnel*. Louisville, TN: National Safe Skies Alliance, Inc., 2020.

Price, Jeffrey. "The Role of the Private Sector for Air Transport Security." In *Air Transport Security: Issues, Challenges and National Policies*, edited by Joseph S. Szyliowicz and Luca Zamparini, 63–84. Cheltenham, UK: Edward Elgar Publishing, 2018. https://www.e-elgar.com/shop/usd/air-transport-security-9781786435194.html.

Radulov, Nikolay. "Artificial Intelligence and Security. Security 4.0." *Security & Future* 3, no. 1 (2019): 3–5. https://stumejournals.com/journals/confsec/2019/1/3.

Rajapaksha, Aruna, and Nisha Jayasuriya. "Smart Airport: A Review on Future of the Airport Operation." *Global Journal of Management and Business Research* 20, no. 3 (2020): 25–34. https://doi.org/10.34257/GJMBRAVOL20IS3PG25.

Seth, Sonal, and Qianmei Feng. "A Multi-Level Weighted Alarm Security System for Passenger and Checked-Baggage Screening." *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 236, no. 5 (October 2022): 727–37. https://doi.org/10.1177/1748006X211042710.

Shu, Chiao-Fe, A. Hampapur, M. Lu, L. Brown, J. Connell, A. Senior, and Yingli Tian. "IBM Smart Surveillance System (S3): A [Sic] Open and Extensible Framework for Event Based Surveillance." In *IEEE Conference on Advanced Video and Signal Based Surveillance, 2005.*, 318–23. Piscataway, NJ: IEEE, 2005. https://doi.org/10.1109/AVSS.2005.1577288.

Smirnov, Tony. "WEB Monitoring and Social Listening Tools to Help Boost Security in Airports." LinkedIn, December 8, 2020. https://www.linkedin.com/pulse/web-monitoring-social-listening-tools-help-boost-security-smirnov.

Sreenath, S., K. Sudhakar, and AF Yusop. "Sustainability at Airports: Technologies and Best Practices from ASEAN Countries." *Journal of Environmental Management* 299 (December 2021): 1–15. https://doi.org/10.1016/j.jenvman.2021.113639.

Stokes, Mike. "Layer Surveillance Radar Technology into Physical Security Solutions for Real-Time Detection of Threats at Airport Sites." *Airport Business* 34, no. 8 (October 2020): 36–37. ProQuest.

———. “Layer Surveillance Radar Technology into Physical Security Solutions for Real-Time Detection of Threats at Airport Sites.” Aviation Pros, October 14, 2020. https://www.aviationpros.com/aviation-security/perimeter-security/article/21137832/layering-surveillance-radar-technology-into-physical-security-solutions-for-realtime-detection-of-threats-at-airport-sites.

Sun, Zhenshi, Kun Liu, Junfeng Jiang, Pengfei Ma, Zhongyuan Xu, Hairuo Guo, Zichun Zhou, and Tiegen Liu. “Variational Mode Decomposition-Based Event Recognition in Perimeter Security Monitoring with Fiber Optic Vibration Sensor.” *IEEE Access* 7 (2019): 182580–87. https://doi.org/10.1109/ACCESS.2019.2959788.

Szyliowicz, Joseph S., and Luca Zamparini, eds. “Introduction.” In *Air Transport Security: Issues, Challenges and National Policies*, 1–11. Cheltenham, UK: Edward Elgar Publishing, 2018.

Tamasi, Galileo, and Micaela Demichela. “Risk Assessment Techniques for Civil Aviation Security.” *Reliability Engineering & System Safety* 96, no. 8 (August 2011): 892–99. https://doi.org/10.1016/j.ress.2011.03.009.

Tan, Choon Seng, Douglas L. Van Bossuyt, and Britta Hale. “System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment.” *Systems* 9, no. 4 (November 2021): 1–27. https://doi.org/10.3390/systems9040079.

Tan, Jia Hao, and Tariq Masood. “Adoption of Industry 4.0 Technologies in Airports: A Systematic Literature Review.” arXiv, 2021. http://10.48550/arXiv.2112.14333.

Teledyne FLIR. “SkyRanger R70.” Unmanned Aerial Systems. Accessed October 9, 2023. https://www.flir.com/products/skyranger-r70?vertical=uas&segment=uis.

Tisserand, Mathilde. “Violence, Crime and Difficult Passengers: Security Breaches at U.S. Aviation Facilities.” Osprey Flight Solutions, November 1, 2022. https://www.ospreyflightsolutions.com/casestudy/violence-crime-and-difficult-passengers-security-breaches-at-us-aviation-facilities/.

Transportation Security Administration. *Security Guidelines for General Aviation Airport Operators and Users*. Information Publication A-001, Version 2. Washington, DC: Department of Homeland Security, 2017. https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf.

Willemsen, Bert, and Menno Cadee. “Extending the Airport Boundary: Connecting Physical Security and Cybersecurity.” *Journal of Airport Management* 12, no. 3 (Summer 2018): 236–47.

Wipf, Heinz. “Safety versus Security in Aviation.” In *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*, edited by Corinne Bieder and Kenneth Pettersen Gould, 29–41. Cham, Switzerland: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-47229-0_4.

Yin, Robert K. “Analyzing Case Study Evidence.” In *Case Study Research: Design and Methods*, by Robert K. Yin, 109–40, 3rd ed. Thousand Oaks, CA: SAGE, 2003.

———. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: SAGE, 2018.

———. *Case Study Research: Design and Methods*. 3rd ed. Thousand Oaks, CA: SAGE, 2003.

Zhang, Zhou. “Technologies Raise the Effectiveness of Airport Security Control.” In *2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, 431–34. Piscataway, NJ: IEEE, 2019. https://doi.org/10.1109/ICCASIT48058.2019.8973152.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE