

RESEARCH PROJECT EASA.2022.HVP.04

ASSESSMENTS PERFORMED, CONCLUSIONS AND
RECOMMENDATIONS

D-3.1.4

Impact of Security Measures on Safety

Research conducted by:



An Agency of the European Union



Disclaimer



This study has been carried out for EASA by consortium lead CAA International (CAAi) upon award of a specific contract for the provision of consultancy services. Consequently, it does not necessarily express the views of EASA itself, nor should it be relied upon as a statement, as any form of warranty, representation, undertaking, contractual, or other binding commitment upon EASA. Ownership of all copyright and other IPR in this material including any documentation, data, and technical information, remains vested to EASA. All logos, copyrights, trademarks, that may be contained within, are the property of their respective owners. Reproduction of this study, in whole or in part, is permitted under the condition that this Disclaimer remains clearly and visibly affixed in full at all times with such reproduced part.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

This deliverable has been carried out for EASA by an external organisation and expresses the opinion of the organisation undertaking this deliverable. It is provided for information purposes. Consequently, it should not be relied upon as a statement, as any form of warranty, representation, undertaking, contractual, or other commitment binding in law upon the EASA.

Ownership of all copyright and other intellectual property rights in this material including any documentation, data and technical information, remains vested to the European Union Aviation Safety Agency. All logos, copyrights, trademarks, and registered trademarks that may be contained within are the property of their respective owners. For any use or reproduction of photos or other material that is not under the copyright of EASA, permission must be sought directly from the copyright holders.

No part of this deliverable may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner. Should the owner agree as mentioned, then reproduction of this deliverable, in whole or in part, is permitted under the condition that the full body of this Disclaimer remains clearly and visibly affixed at all times with such reproduced part.

DELIVERABLE NUMBER AND TITLE: [Assessments performed, conclusions and recommendations – D-3.1.4]

CONTRACT NUMBER: EASA.2022.HVP.04

CONTRACTOR / AUTHOR: CASRA / Cédric Lüthi (Task Leader) – Adam Troczyński (Co-author) – Céline Delay (Co-author)

IPR OWNER: European Union Aviation Safety Agency

DISTRIBUTION: Public

APPROVED BY:	AUTHOR	REVIEWER	MANAGING DEPARTMENT
	CASRA / Adam Troczyński	CASRA / Cédric Lüthi	CASRA
	CASRA / Céline Delay		

DATE: 15/05/2025



CAA International Limited (CAAi) was established in April 2007 as a wholly owned subsidiary of the UK CAA. The UK Civil Aviation Authority (UK CAA) is the UK's specialist aviation regulator, directly reporting to the UK Government's Department for Transport (DfT). Through its skills and expertise, it is recognised as a world leader in its field. CAAi provides access to the UK CAA's wealth of expertise and experience within the five operating groups of the UK CAA (Safety & Airspace Regulation Group, Consumers and Markets Group, Security Group, Strategy and Policy Group and International Group). Its primary focus is providing advisory, training, examination and licencing services to agencies, fellow National Aviation Authorities and industry in over 140 countries. CAAi's work involves assessment and delivery of targeted safety, security and environmental improvements and offer unparalleled expertise stemming from insights into best practices defined by the CAA.



Apave's core business is to help companies and government services managing their technical, environmental and human risks in the areas of Oil & Gas / Nuclear / Industry / Transportation. In aviation, Apave is committed to offering a range of civil and military aviation safety services, covering oversight authority tasks, audits, technical control, training and consulting services, through specialised and dedicated entities. Apave's staff in aviation enjoy extensive knowledge of the International and European regulatory framework, with a focus on Airworthiness, Flight Operations and Safety Management Systems In 2022 Apave has strengthened its portfolio through the acquisition of Oppida a cyber-security specialist in many highly regulated domains and safety and security exposed businesses. Apave has organised its civil and military aviation risk management consulting services around a unique value proposition with a dedicated entity: Apave Aeroservices (hereafter referred to as "Apave") has been designated in 2009 as the Group centre of excellence to provide risk management solutions to the Aviation community, including aviation authorities, Air Operators, Industry, Maintenance Organisations (MROs - Maintenance, Repair & Overhaul) and Training Organisations.



APSS Software & Services Ltd is part of the Centre for Adaptive Security Research and Applications (CASRA), which was founded in 2008. CASRA emerged from the Visual Cognition Research Group of the University of Zurich, which was founded by Adrian Schwaninger in 1999. Today, CASRA APSS has a workforce of around 35 people, comprising of psychologists, economists, computer scientists, imaging specialists, software developers, aviation security experts, and more, most of which have an academic degree. The main objective of CASRA is to increase security and facilitation at airports and other environments involving people and technology. Through their studies and research on human – machine interaction, it was identified that visual abilities and training determine largely screeners' performance. As such CASRA has been working with a number of aviation security authorities and airports on selection, training and competency assessment processes providing advisory and research as well as their solutions globally.

TABLE OF CONTENTS

Abbreviations	5
1. Executive summary	7
2. Introduction	9
2.1. Context and background	9
2.2. Objectives of the document	9
3. Assessments performed	12
4. Conclusions	49
4.1. Physical security threats in relation to the aircraft design	49
4.2. Information security threats in relation to the aircraft design	49
4.3. Aircraft design requirements	50
4.4. Intertwinement of safety and security elements	50
4.5. Interconnection of risk assessments	53
4.6. Integration of stakeholder feedback	53
4.7. Cross-domain collaboration and communication	53
5. Recommendations	55
Bibliography	56

ABBREVIATIONS

ACRONYM	DESCRIPTION
ACARS	Aircraft Communications Addressing and Reporting System
ACI	Airports Council International
ADS	Aircraft Design Standards
AITRAP	Aviation Insider Threat Recognition and Prevention
AFDX	Avionics Full-Duplex Switch Ethernet
APT	Advanced Persistent Threats
AVSEC	Aviation Security
BA	Barrier Analysis
CAA	Civil Aviation Authority
CASRA	Center for Adaptive Security Research and Applications
CBR	Chemical, Biological or Radiological agents
CCA	Consequence Analysis
D	Deliverable
DAL	Development Assurance Levels
DG	Dangerous Goods
DME	Distance Measuring Equipment
EASA	European Union Aviation Safety Agency
EC	European Commission
ETA	Event Tree Analysis
EU	European Union
FAA	Federal Aviation Authority
FMEA	Failure Mode and Effects Analysis
FMS	Flight Management System
FTA	Fault Tree Analysis
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IID	Incendiary Improvised Device
IMA	Integrated Modular Avionics
IUEI	Intentional Unauthorized Electronic Interaction
LAGs	Liquids, Aerosols and Gels
MANPADS	Man Portable Air Defence System
OEM	Original Equipment Manufacturer
OTP	On-Time Performance
PETN	Pentaerythritol Tetranitrate
RE	Relative Effectiveness
RDX	Royal Demolition Explosive
RPAS	Remotely Piloted Aircraft System
RPN	Risk Priority Number

SAL	Security Assurance Levels
TAWS	Terrain Avoidance and Warning System
TCAS	Traffic Collision and Avoidance System
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
VHF	Very High Frequency
VOR	VHF Omnidirectional Range

1. Executive summary

Problem area

The general objective of the project *Impact of security measures on safety* is to understand the nature and extent of interdependencies between safety and security. Through the research within this project, an attempt is made to produce the comprehensive knowledge base describing these interdependencies.

Executive Summary

This report serves as the **final assessment within the framework of subtask 3.1, summarising evaluations, key findings, and actionable recommendations**. It builds upon previous assessments, including an evaluation of current aircraft design requirements in relation to physical (D-3.1.1) and information security threats (D-3.1.3) and an analysis of the effectiveness of existing detection requirements for screening equipment in mitigating threats to aircraft structures (D-3.1.2). The objective of this report is to consolidate the findings from these assessments, derive meaningful conclusions, and provide clear recommendations to support informed decision-making.

The study focused on analysing key threat scenarios, both physical and related to information security, and their relationship with aircraft design requirements and mitigations. The research team examined to what extent existing safety and security standards already address these threats and identified remaining gaps. Furthermore, it investigated the relevance of current screening equipment detection standards in mitigating risks to aircraft structures. By exploring security regulations and their impact on the aircraft environment, the study also delved into the interdependencies between safety, security, and information security, highlighting their interconnected nature.

It was observed that certain aircraft design standards, although primarily focused on safety, may serve as security mitigations, with the extent of this role varying based on the context. The convergence of safety and security was particularly noted where a materialized threat or hazard manifests as a failure condition, distinguishable only by its intentional or unintentional origin.

In the context of screening equipment standards, the study examined the interdependencies between safety and security, particularly concerning the prevention of dangerous goods transport. The findings indicated that while detection capabilities have progressed, challenges remain in areas such as automation, human-machine interaction, and the evolving role of human operators in the screening process. It was confirmed that safety and security threats are closely interlinked, and effective prevention mechanisms are critical to avoiding significant structural damage to aircraft. Additionally, technical evidence suggests that existing screening equipment capabilities can be expanded to detect certain dangerous goods that are not currently actively screened, as they are not classified as security-prohibited items.

Given these interdependencies, it is recommended to establish a dedicated, permanent information exchange mechanism, such as a working group or committee. This platform would facilitate knowledge sharing on vulnerabilities and threats while ensuring safety and airworthiness considerations are integrated into security discussions. Enhancing communication and collaboration among stakeholders and regulatory authorities would improve proactive, integrated safety-security risk assessments and decision-making processes.

Encouraging interconnected risk assessment methodologies is crucial to identifying interdependencies between safety, security, and information security. In this regard, leveraging modern risk modelling tools, such as artificial intelligence, could enable more sophisticated simulations of physical threat impacts, particularly in airborne conditions. Investigating the potential effects of threats such as improvised explosive devices (IEDs),

incendiary improvised devices (IIDs), or unmanned aerial vehicles (UAVs) within the aircraft cabin could provide valuable insights for future risk mitigation strategies.

Technological advancements in screening equipment should be closely monitored and encouraged to identify areas where innovative solutions can help address evolving threats and hazards. At the same time, efforts should be made to reinforce screeners' threat detection capabilities and continuously adapt their qualifications to reflect the evolving role of automation in the screening process. Ensuring coherence and coordination among safety, security, and information security regulators is essential in developing sustainable and effective solutions. Any measures introduced in one domain should at the very least remain neutral in their impact on others, and all security measures should be assessed for their potential implications on aviation safety.

Prioritizing synergies between safety and security should be a key focus, aligning efforts to prevent the transport of dangerous goods and prohibited articles based on the potential severity of their consequences rather than their intentional or unintentional origins. Stakeholders should collaborate to ensure unauthorized dangerous goods are effectively prevented from entering the aviation transport system. Additionally, ongoing dialogue and further studies should explore the risks posed by class 6 and class 7 dangerous goods, aiming to develop preventive measures that safeguard both passengers and crew. Through these initiatives, aviation security and safety can be strengthened to address both current and emerging challenges in a coordinated and efficient manner.

2. Introduction

This chapter first provides the context and background of the project (section 2.1) and then objectives of the document are presented (section 2.2).

2.1. Context and background

The European Union Aviation Safety Agency (hereinafter “EASA”) is an agency of the European Union, which has been given specific regulatory and executive tasks in the field of aviation safety. The Agency constitutes a key part of the European Union’s strategy to establish and maintain a high uniform standard of safety and environmental protection in civil aviation at European level.

As part of the Horizon Europe Work Programme 2021-2022 on Cluster 5 Climate, Energy and Mobility, the European Commission has entrusted EASA with the management of one specific research action entitled “Impact of security measures on safety”.

As a result, EASA has awarded a public contract to a consortium of three companies:

- CAA International
- Apave Aeroservices
- CASRA

The contract details the four main tasks which are specified in order to achieve the expected outcome which is to understand the nature and extent of the interdependencies between safety and security in order to assess the impact of security measures on safety. In doing so, the research project should identify which processes and job roles are affected by safety–security interdependencies and which certification requirements and licensing activities are affected. In the medium term, safety risk management techniques that can be applied to security will produce harmonised risk assessment methods and support integrated policy and decision-making processes at national and EU level.

The project aims at developing a comprehensive knowledge base for the evaluation of the potential impact of security measures on the safety performances of aviation systems, personnel and operations, including the leading indicators for measuring such an impact (positive or negative) as well as the main factors playing a role in such safety - security dependencies.

The four main tasks are:

- Task 1: Identify the interdependencies between security and safety
- Task 2: Assessment of the impact of security measures on safety
- Task 3: Analysis of certification standards
- Task 4: Integrated risk management

The intention of this activity is to provide a basis for better understanding of where security threats have safety consequences in a more granular way than is currently understood.

2.2. Objectives of the document

The present report is an output of Task 3, which covers the analysis of certification standards in the context of safety-security interdependencies and the assessment of the impact of security measures on safety. Subtask 3.1 focuses on interdependencies between the security landscape, in particular physical and information

security threats and aircraft design standards (ADS) as well as existing screening equipment detection requirements.

The present report is the deliverable **D-3.1.4** of Task 3: “*Assessments performed, conclusions and recommendations*”. This document presents the **final assessment within the framework of subtask 3.1 [Impact of security threats on aircraft structure]**, summarizing the evaluations conducted, key findings, and actionable recommendations. It builds upon the two previous deliverables in this subtask (Figure 1).

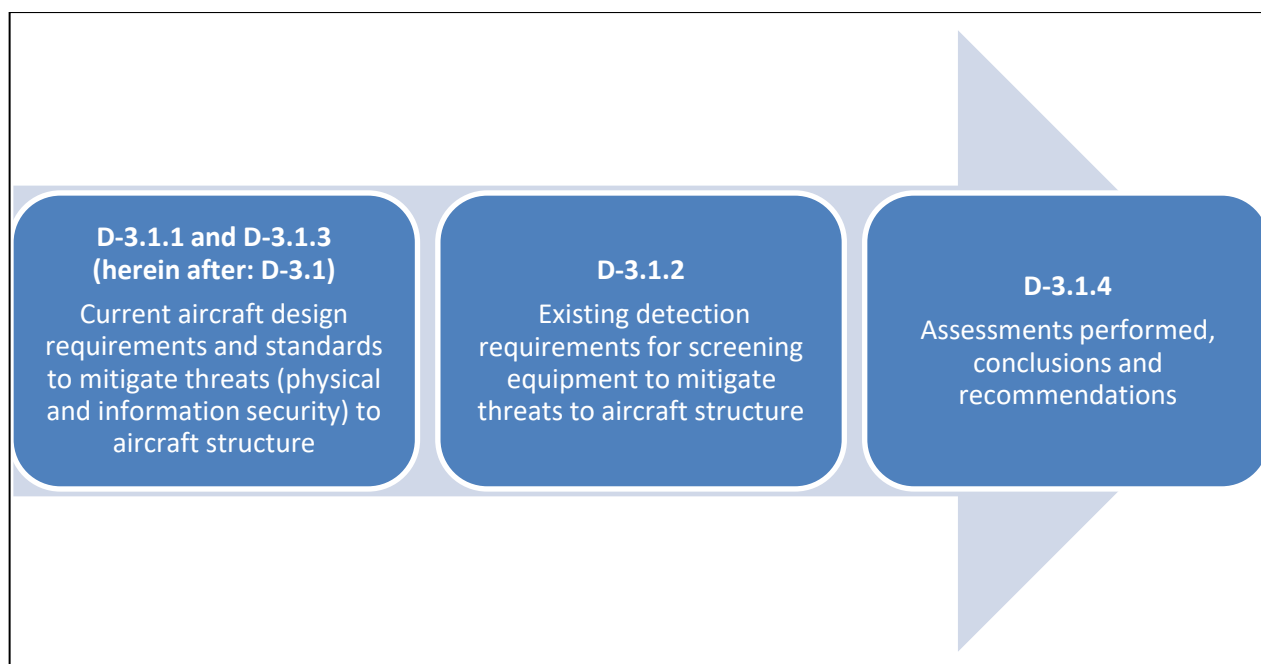


Figure 1 – Process of work in subtask 3.1 (Impact of security threats on aircraft structure)

Deliverable **D-3.1** outlined an assessment on the current aircraft design requirements and their relevance for mitigating physical and information security threats, including a gap analysis of aircraft design standards (see Figure 2 for the methodology overview). The objectives were to analyse the main applicable threat scenarios (both physical threats and cyberthreats), identify their impact on aircraft design requirements and propose effective solutions for preventing or mitigating the safety impact.

Deliverable **D-3.1.2** outlined an assessment on the relevance of the existing detection requirements for screening equipment to mitigate threats to the aircraft structure (see Figure 3 for the methodology overview). The objectives were to investigate how the existing detection requirements for screening equipment contribute to minimising the negative impact of security threats on aircraft structure and integrity.

The primary objectives of this report therefore are:

- To summarize the **assessments performed**, including methodologies and key findings ([Chapter 3](#)).
- To present **conclusions** based on the analyzed data and observations ([Chapter 4](#)).
- To provide **recommendations** for future actions, improvements, or strategic decisions ([Chapter 5](#)).

The results will support stakeholders in implementing effective measures based on the assessment outcomes.

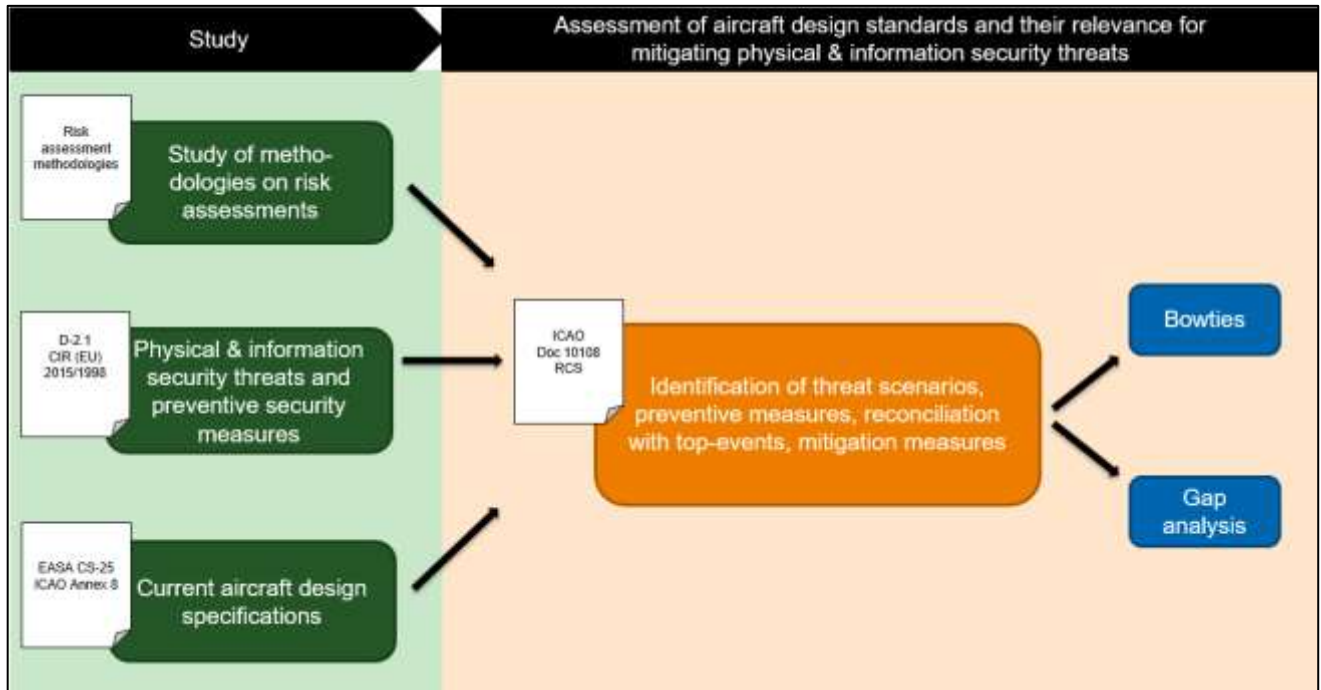


Figure 2 – Methodology for D-3.1

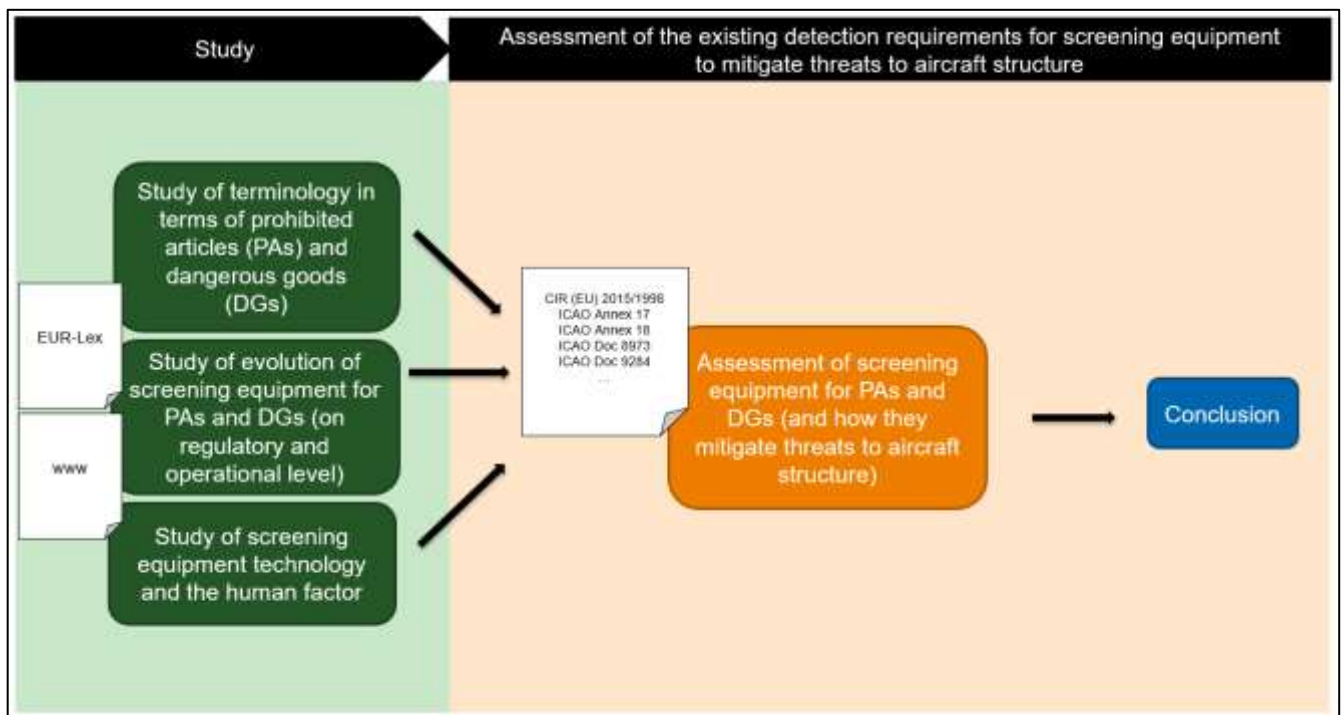


Figure 3 – Methodology for D-3.1.2

3. Assessments performed

INTENTIONALLY REMOVED FROM PUBLIC RELEASE

4. Conclusions

This chapter first presents the most important of key insights from the subtask 3.1:

- Physical security threats in relation to the aircraft design (section 4.1)
- Information security threats in relation to the aircraft design (section 4.2)
- Aircraft design requirements (section 4.3)
- Intertwinement of safety and security elements (section 4.4)
- Interconnection of risk assessments (section 4.5)
- Integration of stakeholder feedback (section 4.6)
- Cross-domain collaboration and communication (section 4.7)

4.1. Physical security threats in relation to the aircraft design

Physical security threats are constantly evolving, necessitating ongoing discussions about vulnerabilities and the role of both aircraft design and, perhaps even more importantly, ground-based measures in enhancing mitigation strategies. Manufacturers have demonstrated their responsiveness by implementing oxygen generator requirements to address specific security risks. As threats evolve, it is crucial for all aviation actors to seek proactive solutions to address vulnerabilities for threat scenarios, where gaps in preventive security measures may still exist. Such channels exist and are actively working in the information security domain (e.g. WG-72 of EUROCAE) and it appeared concerning no equivalent arrangements could be identified in the course of the research with regards to the traditional physical security domain (especially after the ISAD discontinued).

Additionally, the research revealed that most adequate prevention achieved through existing screening equipment detection requirements exists against PAs that are simultaneously classified as specific DGs. For the remaining DGs (which are not PAs) although there is common concern over the threat they could cause, there is no clear consensus on how this could be integrated within the existing security screening process and therefore equally prevented.

4.2. Information security threats in relation to the aircraft design

Historically, safety and security considerations did not have intersections related to aircraft systems and data protection, particularly before the advent of e-enabled airplanes. While technological advancements have significantly improved safety, they have simultaneously exposed systems to new vulnerabilities, calling for expertise in information security beyond traditional IT security.

Information security in aviation requires specialized considerations, as illustrated by the aircraft software patching process, which must be conducted differently from conventional IT systems to preserve type certification, airworthiness and safety assurance. Additionally, security control verifications must be coordinated with the aircraft manufacturer. Information security risks can also be mitigated through active threat monitoring and early-stage interventions, thereby preventing threats before they reach critical proximity to aircraft systems.

In this context, strengthening the *supply chain* security is essential, with the implementation of Part-IS regulations potentially enhancing the aviation industry's overall security capabilities. Aviation security can also benefit from the dynamic response capabilities developed within information security domain, particularly through a risk-based, and more agile approach.

4.3. Aircraft design requirements

The analysis indicated that the aircraft design may not necessarily be most relevant placeholder to address specific issues. Adding additional physical security features, especially if alternatively, preventive measures could apply on the ground (for physical threats), does not seem to be a reasonable approach. Applying preventions on the ground may be more efficient than designing measures in the aircraft. Aircraft design alone will not achieve the goal of improved security system if measures applicable on the ground are not taken into consideration as preventions and/or mitigations.

4.4. Intertwinement of safety and security elements

The research team showed safety and security elements are intertwined and interrelated even if no specific and substantial aircraft design gaps requiring intervention within this research framework were identified. The analysis showed that safety-oriented design requirements contain security components which the security domain shall comprehend and study to understand ultimate vulnerabilities of an aircraft. It also exemplified measures or requirements introduced as safety mitigations can play a role in containing security events. Therefore, more interconnected risk assessments especially utilising modern tools (e.g. exploring capabilities of the artificial intelligence modelling) and simulation modelling can build value-added for combined enhanced safety and security posture reducing the risk of unintended gaps.

Figure 4 illustrates interrelations between safety and information security in terms of risk assessments.

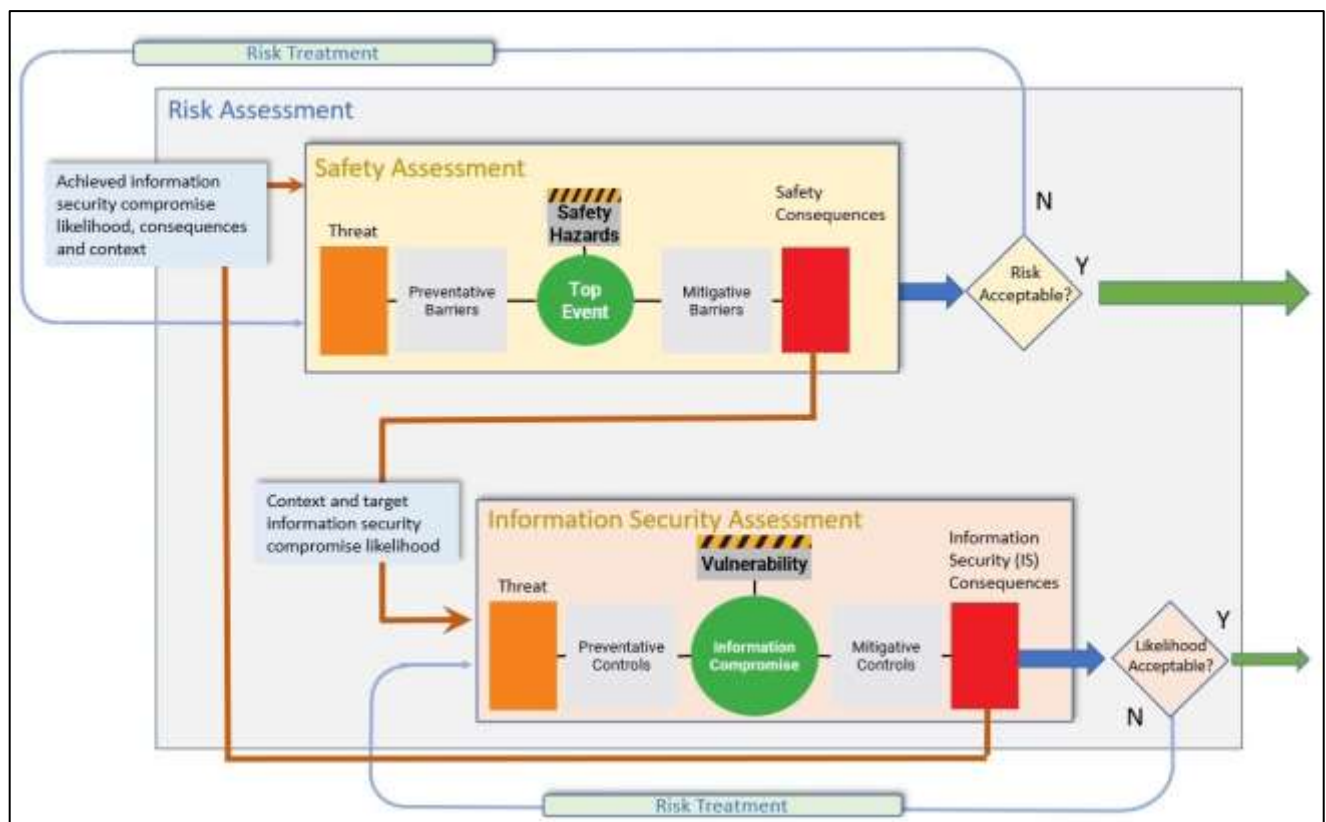


Figure 4 – Information Security Risk Assessment implications for Safety Risk Assessment (Source: Source: ICAO Manual on Aviation Information Security (MAIS), Doc 10204)

Subsequent Figures 24 and 25 leverage on this approach and propose illustration of interrelations between safety and aviation security and vice-versa. This interrelation means that when an occurrence triggers a risk assessment within one domain (e.g. safety), it is essential to share the outcomes of that assessment, including any implemented mitigations, with the other domain (e.g. security). This enables evaluation of the potential impact on risk beyond the originating area and helps identify any unintended or unknown consequences, including the emergence of new risks or an increase in existing ones. Following this, a feedback loop should be established to ensure that insights and outcomes from the second domain are communicated back to the first. Such reciprocal information exchange supports a holistic approach to risk management across interconnected domains.

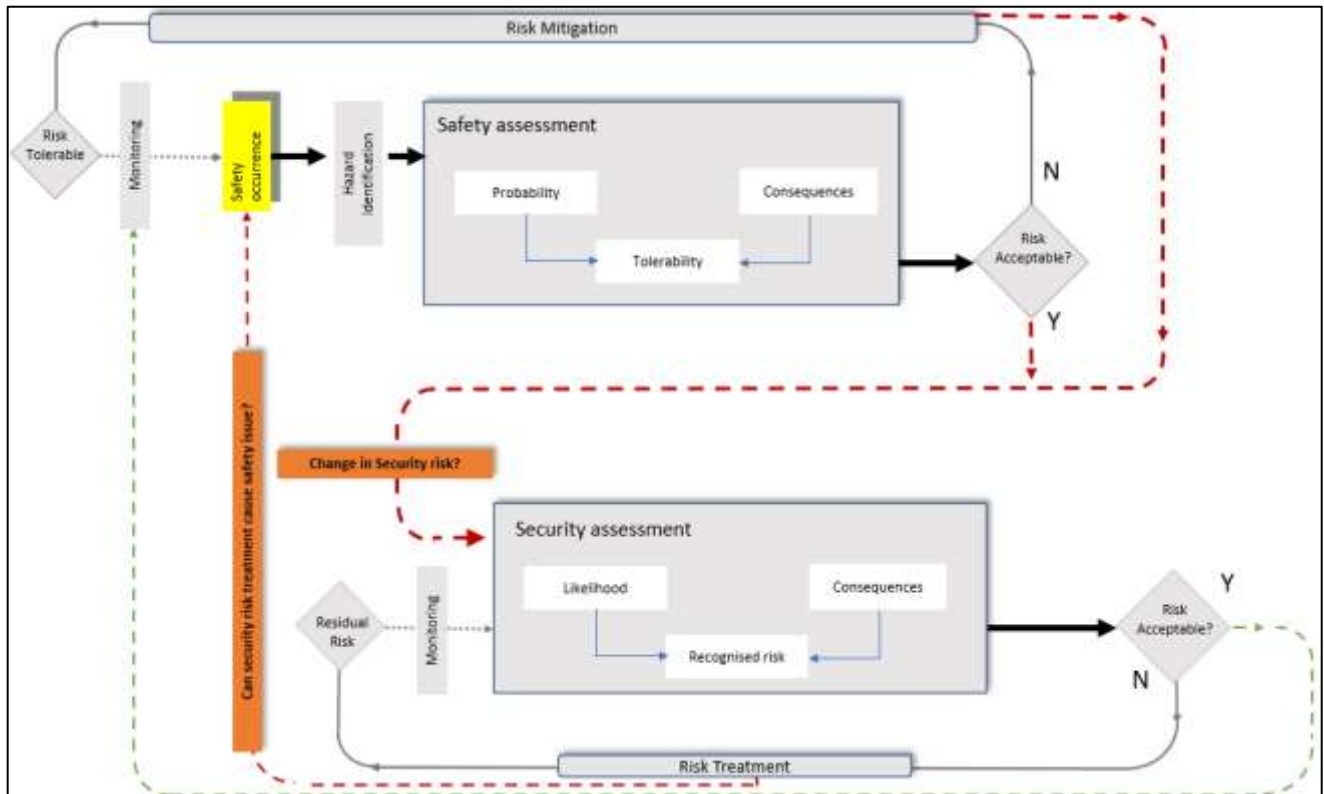


Figure 5 – Security Risk Assessment implications for Safety Risk Assessment

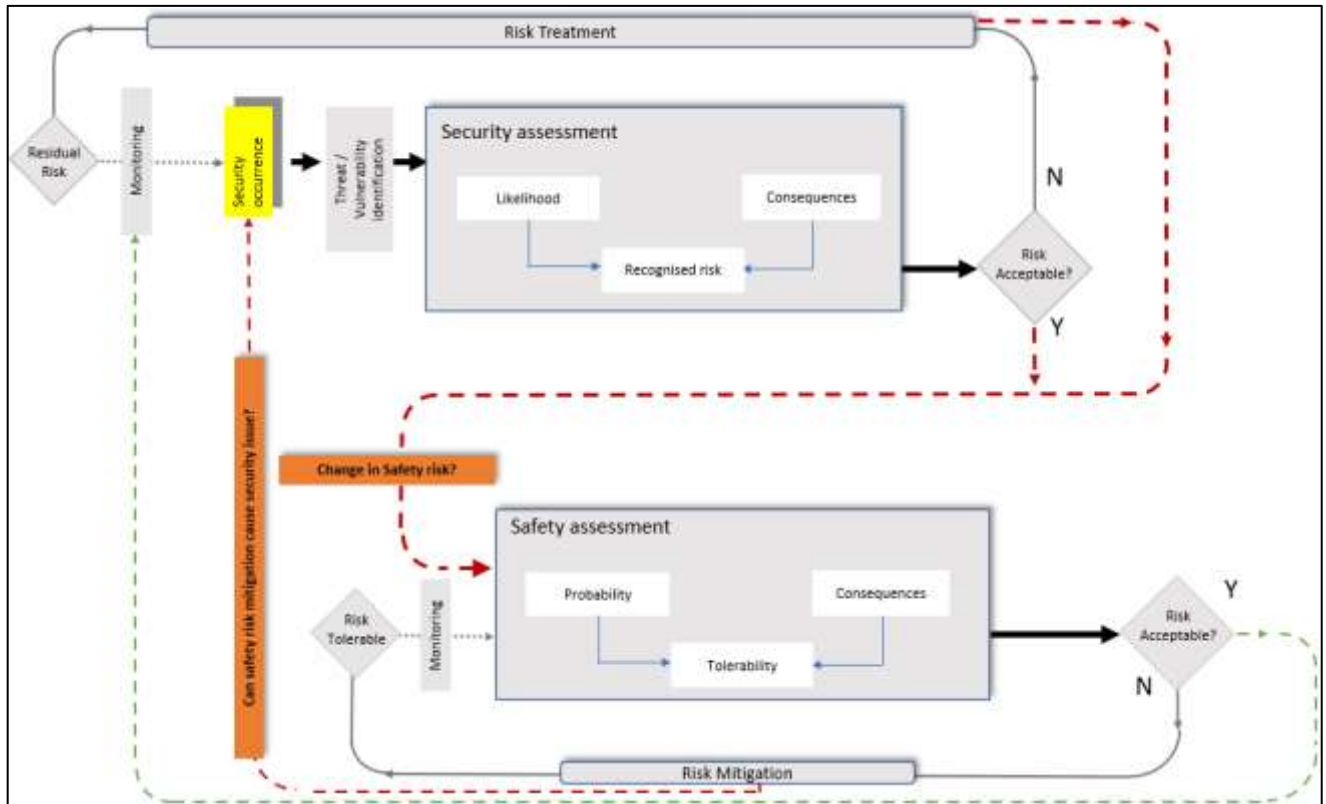


Figure 6 – Safety Risk Assessment implications for Security Risk Assessment

4.5. Interconnection of risk assessments

Traditional safety and security risk assessments were developed over time by either domain following rather isolated methodologies. This report underscores the importance of cross-domain methodology and leveraging on each other's expertise. Threat in security is defined as combination of intent and capability. These are both external and difficult to measure. Vulnerability is the second component of the security risk formula. The vulnerability seems easier to measure but it actually is not. What is measured is actually past and known vulnerabilities. This is because the reference is typically made to events that happened where evidences of weaknesses existed and were identified. A common approach is also anchored in the believe that since the vulnerability was exploited similar attacks can be expected. In many cases past vulnerabilities are patched by new or amended regulations so the vulnerability level gets actually measured through the optic of compliance instead of the actual exposure to threats.

This approach towards vulnerabilities is sensible, however it contains potential loopholes. Such an analysis:

- does not account for unknown risks with no past data to analyse or examples to refer to
- lacks anticipation of the evolution of attack methods, new tactics which may exploit vulnerability in new way or exploit preventive barrier not previously identified as vulnerability
- changed conditions where changes to one part of the system may create cascading vulnerability elsewhere
- overly relies on compliance as an indicator of the degree of vulnerabilities.

From the perspective of this research, it appears that other existing structured methods could be mostly either directly applicable or adapted from models used in safety like e.g. Bowtie. An adapted Bowtie method allows to record threat scenarios, together with existing security measures (preventive barriers) but also accounting for recorded (known from history) as well as potential vulnerabilities (defined in the Bowtie as escalating factors) which can be linked to escalation factor barriers. As the bowtie is rather qualitative than quantitative method the process does not finish with any specific score. It provides however a more comprehensive, dynamic and scalable situational picture.

It also allows to target more specifically threat scenarios, identified vulnerabilities or changes in the threat tactic as these both would fall into the category of escalating factors (or as a new threat scenario in some cases).

4.6. Integration of stakeholder feedback

Surveys serve as a fundamental tool for collecting structured feedback from stakeholders. Workshops facilitate direct engagement and in-depth discussions among stakeholders. By fostering collaborative dialogue, workshops enable the identification of challenges and the exploration of potential solutions. The research team evidenced broad ongoing consultation with stakeholders is necessary to foster collaborative approach and information exchange.

4.7. Cross-domain collaboration and communication

Lastly, this report underscores the importance of cross-domain collaboration and communication to address the misconception that safety and security are isolated concerns. In reality, these domains are closely interwoven. The catastrophic consequences of a worst-case incident remain equally severe, regardless of whether the root cause is categorized as a "safety" or "security" issue. To facilitate cross-domain learning and

maintain situational awareness, channels of communication must remain open between aviation security, safety, aircraft design, and airworthiness stakeholders.

5. Recommendations

Recommendations in this section should be considered in conjunction with section 6 of the deliverables [D-3.1](#) and [D-3.1.2](#)

Given the interdependencies between safety, security, and information security, and the need for domain-specific expertise to provide adequate input, it is recommended to establish a permanent, dedicated information exchange mechanism - such as a working group or committee. This forum could facilitate the sharing of information on vulnerabilities and threats while providing essential safety and airworthiness-related insights. Ensuring that the outcomes of these discussions are shared with Member State authorities could enhance their ability to conduct proactive integrated safety-security risk assessments, improve communication and collaborative decision making.

An interconnected risk assessment should be encouraged to assist in enhanced capability to identify safety, security and information security interdependencies. In this context, enhanced risk modelling using modern tools such as artificial intelligence should be explored to investigate possibilities of simulating the impact of different physical threats in the aircraft cabin in airborne conditions (especially for IEDs, IIDs, impact of UAVs).

Technology developments for screening equipment should be closely monitored and encouraged to evaluate areas where innovative solutions may help in addressing evolving threats and hazards. At the same time, a range of reinforcement activities should be developed and maintained to bolster screeners' threat detection capabilities as well as to adjust their qualifications to the changing role in the evolution and automation of the screening process.

Coordination and coherence are needed between safety, security and information security regulators to develop sustainable and effective solutions where measures developed with the primary mission or objective in one domain are at least neutral for the other domain. In this context, impact assessment of security measures on safety should be encouraged for both, information and traditional aviation security.

Seeking for synergies should be prioritised and alignment opportunities explored to synchronise the prevention of DGs and PAs, prioritising similarities of the worst-possible outcome rather than focusing on differences related to intentional (for security) or unintentional (for safety) behaviour. All stakeholders involved are encouraged to collaborate and prevent unauthorized DGs from the transport.

An ongoing dialogue including potential future studies should take place with regards to threats caused by class 6 or 7 DGs to understand the potential for development of preventive measures to ensure the safety of passengers and the crew.

BIBLIOGRAPHY

AMC-20 Amendment 18

Aust, J., & Pons, D. (2019). Bowtie methodology for risk analysis of visual borescope inspection during aircraft engine maintenance. Aerospace, 6(10), 110.

Bond, A. H., & Ricci, R. J. (1992). Cooperation in aircraft design. Research in Engineering Design, 4(2), 115-130.

Ch. M. Fuchs, The Evolution of Avionics Networks. From ARINC 429 to AFDX, Network Architectures and Services, August 2012

Commission Delegated Regulation (EU) 2020/2034 of 6 October 2020 supplementing Regulation (EU) No 376/2014 of the European Parliament and of the Council as regards the common European risk classification scheme.

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

Commission Staff Working Document. Working towards an enhanced and more resilient aviation security policy: a stocktaking. SWD(2023) 37 final

Computational modelling and forensic analysis for terrorist airplane bombing: A case study, J. Yeh,et al. Engineering Fracture Mechanics 211 (2019) 137-160

D. Kritzinger, The Aircraft System Safety. Assessments for Initial Airworthiness Certification, 2016

EASA CS-25 Easy Access Rules for Large Aeroplanes.

EASA Notice of Proposed Amendment (NPA), No 2009-07, Draft Decision of the Executive Director of the EASA, Amending Decision No. 2003/2/RM of 17 October 2003 on Certification Specifications for Large Aeroplanes (CS-25), July 2009

EUROCAE ED-202B Airworthiness Security Process Specification, October 2024

EUROCAE ED-203A Airworthiness Security Methods and Considerations, June 2018

EUROCAE ED-204A Information Security Guidance for Continuing Airworthiness, September 2020

European Commission (2011). Flightpath 2050 – Europe’s Vision for Aviation.

FAA Advisory Circular (AC) 25.795-1A, Flightdeck Intrusion Resistance, October 2008

FAA Advisory Circular (AC) 25.795-2A, Flightdeck Penetration Resistance, October 2008

FAA Advisory Circular (AC) 25.795-3, Flight deck Protection (smoke and fumes), October 2008

FAA Advisory Circular (AC) 25.795-4, Passenger Cabin Smoke Protection, October 2008

FAA Advisory Circular (AC) 25.795-5, Cargo Compartment Fire Suppression, October 2008

FAA Advisory Circular (AC) 25.795-6, Least Risk Bomb Location, October 2008

FAA Advisory Circular (AC) 25.795-7, Survivability of Systems, October 2008

FAA Advisory Circular (AC) 25.795-8, Interior design to facilitate searches, October 2008

FAA Final Rule Security Related Considerations in the Design and Operation of Transport Category Airplanes, Federal Register, Vol. 73, No. 209, 28 October 2008

Further review of proposals for the Amendment of Annex 6, Part I and Annex 8 to incorporate security into aircraft design and construction , Working Paper AN-WP/7594, December 2000

GAO-21-86 report Aviation Cybersecurity, October 2020

Hättenschwiler N, Sterchi Y, Mendes M, Schwaninger A (2018) Automation in Airport Security X-Ray Screening of Cabin Baggage: Examining Benefits and Possible Implementations of Automated Explosives Detection. Applied Ergonomics 2018(72):58 -68

Hättenschwiler, N., Mendes, M., & Schwaninger, A. (2019). Detecting bombs in X-ray images of hold baggage: 2D versus 3D imaging. Human factors, 61(2), 305-321.

Huegli D, Merks S, Schwaninger A (2020) Automation Reliability, Human-Machine System Performance, and Operator Compliance: A Study with Airport Security Screeners Supported by Automated Explosives Detection Systems for Cabin Baggage Screening. Applied Ergonomics 2020 86:103094

IATA Security Management System (SeMS) Manual.

ICAO Guidance - Protection of Civil Aviation Infrastructure against Unmanned Aircraft, 2023

ICAO Annex 17 Security, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, July 2022.

ICAO Doc 10108 - Aviation Security Global Risk Statement - Edition 03, 2022.

ICAO Annex 18. The Safe Transport of Dangerous Goods by Air.

ICAO Doc 8973. Aviation Security Manual.

ICAO Doc 9284. Technical Instructions for the Safe Transport of Dangerous Goods by Air.

ICAO Doc 9859 - Safety Management Manual (SMM)

ICAO Doc 10147. Guidance on a Competency-based Approach to Dangerous Goods Training and Assessment

Impact Assessment of Cybersecurity threats, Final Report. EASA_REP_RESEA_2016_1, July 2018

Infantry Antiaircraft Missiles, Steven J. Zaloga, 2023

Iovea, M., Neagu, M., Dului, O. G., & Mateiasi, G. (2007, June). High accuracy x-ray dual-energy experiments and non-rotational tomography algorithm for explosives detection technique in luggage control. In Proc DIR.

Lambert M. Surhone, Miriam T. Timpledone, Susan F. Marseken Relative Effectiveness Factor: Explosive Material, Demolition, Table of Explosive Detonation Velocities, Trinitrotoluene, Amatol, Ammonium Nitrate, ANFO, Gunpowder, C-3 (Plastic Explosive), 2010

MANPADS – Scale and Nature of the Threat, Loren Thompson 2003

MANPADS, A terrorist threat to Civilian Aircraft, brief 47. Bonn International Center for Conversion, February 2013

Nabiev Sh Sh, Palkina A, Russian Journal of Physical Chemistry B, 2017, Vol. 11, No. 5 p. 729-776

Nicolai, L. M., & Carichner, G. E. (2010). *Fundamentals of aircraft and airship design: Volume I—aircraft design*. American Institute of Aeronautics and Astronautics, Inc.

Pan Am Fight 103 Publications Collection, Syracuse University
https://library.syracuse.edu/digital/guides_pa103/html/pa103_publications.htm

Preliminary Review of Proposals for the Amendment of Annex 6, Part I and Annex 8 to incorporate security into aircraft design and construction, Working Paper AN-WP/7544, June 2000

Price, J., & Forrest, J. (2016). *Practical aviation security: predicting and preventing future threats*. Butterworth-Heinemann.

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

Sterchi, Y., & Schwaninger, A. (2015). *A First Simulation on Optimizing EDS for Cabin Baggage Screening Regarding Throughput. Proceedings of the 49th IEEE International Carnahan Conference on Security Technology, Taipei Taiwan, September 21-24, 2015, 55-60.*

Sterchi, Y., & Simonetti, A. (2023). *Report on commercial AI systems (update August 2023)*

Torenbeek, E. (2013). *Advanced aircraft design: conceptual design, analysis and optimization of subsonic civil airplanes*. John Wiley & Sons. p.3.

Vukadinovic, D., & Anderson, D. (2022). *X-ray baggage screening and artificial intelligence (AI)*. Publications Office of the European Union.



European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3

50668 Cologne

Germany

Mail EASA.research@easa.europa.eu

Web www.easa.europa.eu