EASA
European Union Aviation Safety Agency

This project has received funding
from the European Union's Horizon Europe Programme

RESEARCH PROJECT EASA.2022.HVP.04

ASSESSMENT ON THE CURRENT AIRCRAFT DESIGN REQUIREMENTS AND THEIR RELEVANCE FOR MITIGATING PHYSICAL AND INFORMATION SECURITY THREATS, INCLUDING GAP ANALYSIS OF AIRCRAFT DESIGN STANDARDS

D-3.1.1 & D-3.1.3 (D-3.1)

Impact of Security Measures on Safety

Research conducted by:

UK Civil Aviation Authority International
apave Aeroservices
CASRA

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:	[Assessment on the current aircraft design requirements and their relevance for mitigating physical and information security threats, including gap analysis of aircraft design standards – D-3.1.1 & D-3.1.3 (D-3.1)]
CONTRACT NUMBER:	EASA.2022.HVP.04
CONTRACTOR / AUTHOR:	CASRA / Sarah Merks (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
EASA	CASRA / Adam Troczyński CASRA / Céline Delay	CASRA / Sarah Merks	CASRA CAA International

DATE: 12/12/2024

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

ACRONYM	DESCRIPTION
A/C	Aircraft
AAE	Aircraft & Aircraft Equipment
AAO	Aerodrome / Airport Operations
ACARS	Aircraft Communication Addressing and Reporting System
ADBM	Aircraft Design-Based Mitigations
ADR	Aircraft design requirements
ADS	Aircraft design standards
AI	Artificial Intelligence
AMC	Acceptable Means of Compliance
AO	Air Operations
AOC	Air Operator Certificate
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
AUI	Act of Unlawful Interference
BA	Barrier Analysis
CAA	Civil Aviation Authority
CAD	Computer Aided Design
CAMO	Continuing Airworthiness Management Organisation
CASRA	Center for Adaptive Security Research and Applications
CBT	Computer-Based Training
CCA	Consequence analysis
CIR	Commission Implementing Regulation
CS	Certification Specifications
D	Deliverable
DAL	Design Assurance Level
DoS	Denial of Service
EASA	European Union Aviation Safety Agency
ECAM	Electronic Centralised Aircraft Monitor
EF	Escalation Factor
ETA	Event Tree Analysis
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FHA	Functional Hazard Assessment
FMS	Flight Management System
FOD	Foreign Object Damage
FTA	Fault Tree Analysis
GASeP	Global Aviation Security Plan
GNSS	Global Navigation Satellite System
GO	Ground Operations

I	Insider
IA	Intelligent Assistant
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IED	Improvised Explosive Device
ILS	Instrument Landing System
IUEI	Intentional Unauthorized Electronic Interaction
LRBL	Least Risk Bomb Location
LoC	Loss of Control
MANPAD	Man Portable Air Defence System
MRO	Maintenance and Repair Organisation
NIST	National Institute for Standards and Technology
NTP	Non-Travelling Person
P	Passenger
PBIED	Person-borne Improvised Explosive Device
RCS	Aviation Security Global Risks Context Statement (ICAO Doc 10108)
RPAS	Remotely Piloted Aircraft System
RTCA	Radio Technical Commission for Aeronautics
SAL	Security Assurance Level
SeMS	Security Management System
SMM	Safety Management Manual
UGV	Unmanned Ground Vehicle
VOR	Very High Frequency Omnidirectional Range Station

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.

Task 3 focuses on the analysis of certification standards with subtasks 3.1.1 and 3.1.3 investigating areas related to aircraft design requirements.

The aircraft design process is guided by mission requirement and shall ensure that the aircraft meets its intended purpose effectively and safely. From the purpose perspective, there are different types of aircraft: civil/commercial transport, military operations, general aviation, and specialised (e.g. firefighting). The focus of this task is on large civil aircraft intended for commercial transport of passengers and cargo.

Previous tasks of this project (D-1.1. and D-1.2) created foundations for more specific discussions in these tasks through e.g. identifying safety areas affected by security and job-roles with safety-security interdependency.

This report provides a more specific analysis of the area "aircraft design and certification" identified as one of these affected by security measures.

Executive Summary

The present report is the combination of deliverables D-3.1.1 "*Assessment on the current aircraft design requirements and their relevance for mitigating physical security threats, including a gap analysis of aircraft design standards*" and D-3.1.3 "*Assessment on the current aircraft design requirements and their relevance for mitigating information security threats, including a gap analysis of aircraft design standards*" of task 3 and is herein referred to as D-3.1 "*Assessment on the current aircraft design requirements and their relevance for* ***mitigating physical and information security threats****, including gap analysis of aircraft design standards*".

The objective of this document is to describe the analysis process which explores interdependencies between safety and security from the perspective of aircraft design standards. To achieve this, first threats and threat scenarios were identified. Next, the analysis covered the identification of preventive security measures and finally aircraft-design based mitigations. Mitigations analysed do not cover those based on training, procedures and coordination with other relevant entities. At the last stage the research attempts to identify gaps which later will be used to formulate conclusions and recommendations.

The analysis in this document highlights conditions, assumptions and specifications impacting aircraft design process in relation to both, aviation and information security and in the context of safety.

The research examined security standards and regulations and their impact on the environment the aircraft functions in. It also delved into the interconnections between safety, security, information security and explored interdependencies and interactions of these three domains in relation to the aircraft itself. For instance, the research notes that certain safety related aircraft-design standards, though primarily focused on safety, may play a role as security mitigations (extent of that role could vary). In this context safety and security converge at the aircraft where a materialised threat or hazard manifests a "failure condition" distinguishable only by its intentional or unintentional origin.

The report explores also if there are gaps in relation either to the aircraft design itself or at the intersections between safety and security. It investigates whether unknown relationships between preventive security measures and mitigations exist along with undocumented, obsolete or missing preventive strategies. The analysis underscores the importance of strong information sharing between security and safety within the aircraft design, harmonization of terminology, education and exchange of expertise leading towards integrated safety/security analysis for enhanced risk assessment, conducting broader situational analysis that incorporates diverse inputs, and fostering communication among stakeholders. Strengthened information exchange is essential for understanding possibilities and limitations, formulating optimal solutions, and developing sustainable strategies that ensure aircraft design safety and security.

The discussions and assessments within this document provide valuable insights into the interconnectedness of safety and security as they relate to potential physical and information security threats affecting aircraft. This analysis aims to enhance the understanding of these relationships to support a more resilient and secure aircraft design.

The content of this report could potentially foster a holistic and comprehensive analysis of positive or detrimental impact, security measures could have on overall safety. It may also encourage further investigations in specific technical domains and thereby enable identification of opportunities for improvement.

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. This approach will enable a holistic and comprehensive analysis of the positive or detrimental impact security measures are having on overall safety and the identification of opportunities for improvement.

2.2. Objectives of the document

The present report is an output of task 3.

Task 3 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 and aircraft design standards (ADS) and best practices.

The present report is the combination of:

- Deliverable D-3.1.1 - "Assessment on the current aircraft design requirements and their relevance for mitigating physical security threats, including a gap analysis of aircraft design standards"
- Deliverable D-3.1.3 - "Assessment on the current aircraft design requirements and their relevance for mitigating information security threats, including a gap analysis of aircraft design standards"

Therefore, it is after herein referred to as **D-3.1 "*Assessment on existing detection requirements for screening equipment & current aircraft design requirements and their relevance for mitigating physical and information security threats to aircraft structure (including gap analysis of aircraft design standards)*".**

The objective of this document is to collect information on the following topics:

- Current aircraft design requirements
- Physical and information security threats that concern the aircraft
- Methodologies which can help to assess the relationship between aircraft design standards and mitigation of threats

Furthermore, the report combines the studies in form of:

- Diagrams and other most suitable assessment method(s)
- Gap analysis

The output of this document is therefore diagrams and a gap analysis that indicate the role of current aircraft design requirements (ADR) in relation to physical and information security threats.

In the broader context, this report can contribute to the vision outlined in the European Commission document Flightpath 2050 (European Commission, 2011)[1]. In the scope of "Ensuring safety and security", one of the aspirational goals described therein is that "*air vehicles (are) resilient by design to current and predicted on-board and the on-the-ground security threat evolution, both internally and externally to the aircraft*". Deliberations in this report may potentially inform further discussions and actions related to this goal. In this context, the project OPTICS2[2] should also be mentioned. Its objective was to make aviation safety and security

[1] https://www.arcs.aero/sites/default/files/downloads/Bericht_Flightpath_2050.pdf

[2] https://www.optics-project.eu/optics2-final-safety-security-integrated-recommendations/

research more effective in achieving Flightpath 2050 goals in the scope of European Aviation Safety and Security Research and Innovation. Recommendations are not determined at this stage as this will be covered in deliverable D-3.1.4. For purposes of this report it is however essential to recall some recommendations:

- Research (…) needed to determine how humans and Intelligent Assistant (IA)[3] can work together productively (…) and safely (e.g. IAs assisting pilots during flight upsets or "startle events"), including human supervision and recovery on case of "*aberrant behaviour*" by Artificial Intelligence (AI) systems
- Research is required on how to achieve security resilience in design including aspects such as software and maintenance, covering the entire lifecycle phase from concept design through to deployment, operation and decommissioning and covering the various aspects of the supply chains which can become mission critical as recent events have shown.

3. Methodology

This chapter outlines the process of work conducted for the creation of this report in the scope of subtasks 3.1.1 and 3.1.3.

Figure 1 shows the process undertaken in order to assess the relevance of aircraft design requirements (ADRs) for mitigating physical and information security threats.

The following elements were studied:

- Risk assessment methodologies
- Physical and information security threats and related preventive security measures
- Aircraft design specifications[4]

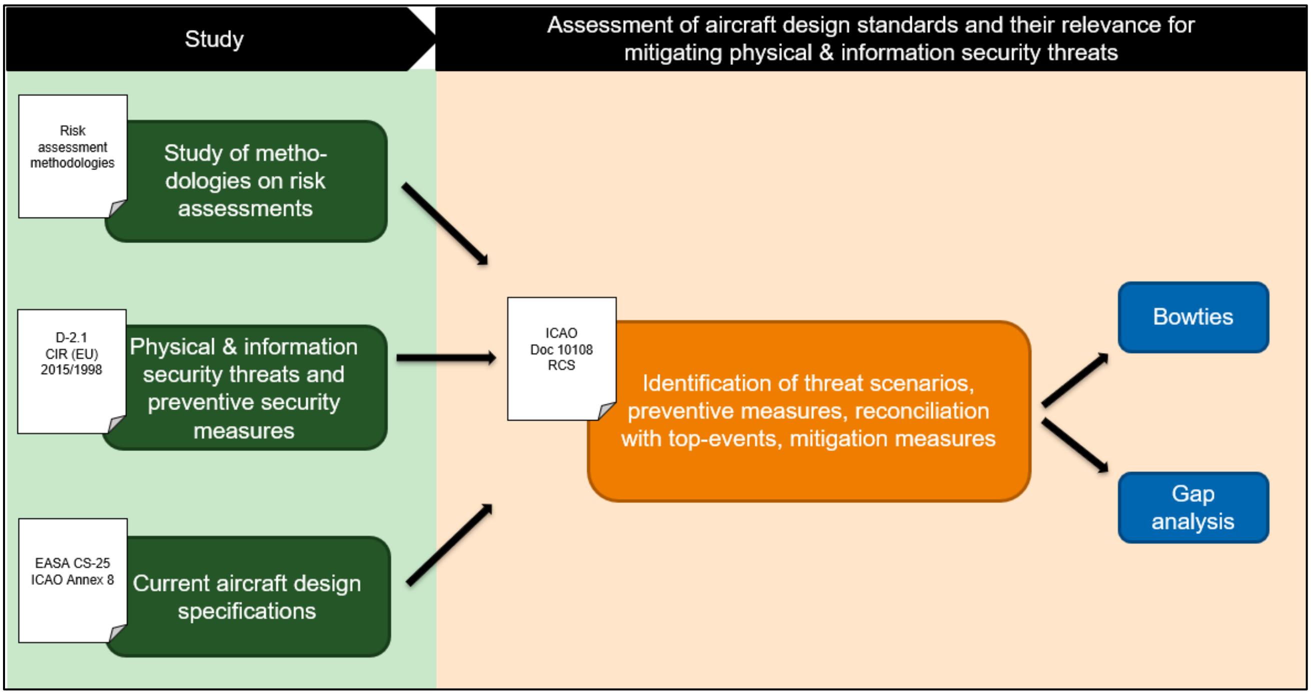

Study
Assessment of aircraft design standards and their relevance for mitigating physical & information security threats
Risk assessment methodologies
Study of metho-dologies on risk assessments
D-2.1 CIR (EU) 2015/1998
Physical & information security threats and preventive security measures
EASA CS-25 ICAO Annex 8
Current aircraft design specifications
ICAO Doc 10108 RCS
Identification of threat scenarios, preventive measures, reconciliation with top-events, mitigation measures
Bowties
Gap analysis

Figure 1 – Process of work

Details on individual study steps are described in this Chapter 3 whereas the study output is described in Chapter 4. Chapter 5 covers collected, analysed and collated information that was next used to assess the

[3] Intelligent Assistant refers to Artificial Intelligence (AI)

[4] Specifications here are understood broadly as standards, regulations, guidance material and industry recommendations

relevance of aircraft design standards in mitigating physical and information security threats. This chapter includes also a gap analysis.

3.1. Study of risk assessment methodologies

Functional Hazard Assessment (FHA) is one of the central processes conducted in aircraft design and with the central role to determine hazards. Assessment is conducted in reference to aircraft functions and subsequently aircraft system functions to identify “failure conditions”. Each failure condition is assigned a severity classification. These classifications are closely related to Development (Design) Assurance Levels (DAL) for software and hardware:[5]

- DAL A – Catastrophic severity of the failure condition
- DAL B – Hazardous severity of the failure condition
- DAL C – Major severity of the failure condition
- DAL D – Minor severity of the failure condition
- DAL E – No impact on safety of the failure condition

The DAL classification will be referred to further in the report in relation to information security threat scenarios.

Other well-established risk assessment methodologies exist across different domains. The scope of this project guided the research team specifically to these related to aviation. In the scope of aviation safety, the following seem to be most frequently used:

- risk matrix
- decision tree
- failure modes and effects analysis
- bowtie model / analysis
- what-if analysis

3.1.1. Bowtie model / analysis

For the purposes of this research, the bowtie model was selected as the preferred initial framework for further analysis. Bowtie seemed not only well-established in the aviation domain, but also was assessed as a model risk management tool that provides clear and intuitive visual representation of processes leading to unwanted events, including controls in place to prevent or mitigate them. Through its visual format if facilitates effective communication and understanding of topic for non-expert readers.

Further advantages of bowtie include:

- Structured approach – the model shows relationships between different elements in a systematic manner
- Focus on prevention and mitigation – in its holistic approach the model distinguishes between prevention and mitigation which has been particularly useful for this research
- Flexibility and adaptability – as a versatile tool the model can be tailored to specific needs

Accordingly, the research team examined this specific model and conducted a feasibility assessment to determine its applicability. This process involved analysing the potential use of the bowtie model, leading to several adaptations to align it effectively with the objectives of the assigned task.

[5] Development (Design) Assurance levels are explained in the EUROCAE ED-80 and ED-12C or their RTCA equivalents DO-254 and DO-178C

The bowtie analysis was chosen as a starting point in the development of the methodology. The adapted model combines:

- security threats
- threat scenarios
- preventive measures (preventive barriers)
- escalation factors (and their barriers)
- top event
- mitigations (recovery barriers)
- consequences

This is described in detail in Section 4.1.1.

3.1.2. Top safety events

The "top safety event" concept was used to identify a harmonised approach to a point in time when the controlled state of a hazard (or threat, using aviation security terminology) is lost. This was based on Key Risk Areas in accordance with the European Common Risk Classification scheme outlined in Regulation (EU) 2020/2034[6].

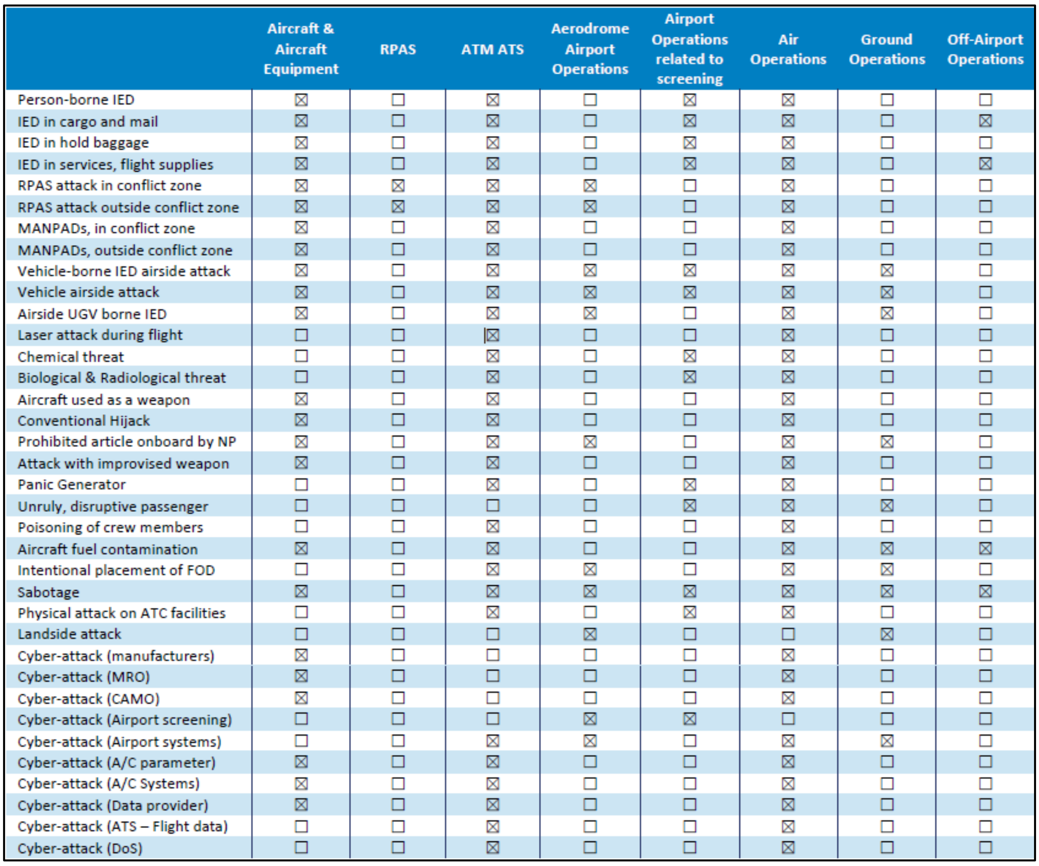
This is described in detail in Section 4.1.2.

3.2. Study of physical & information security threats

3.2.1. List of security threats

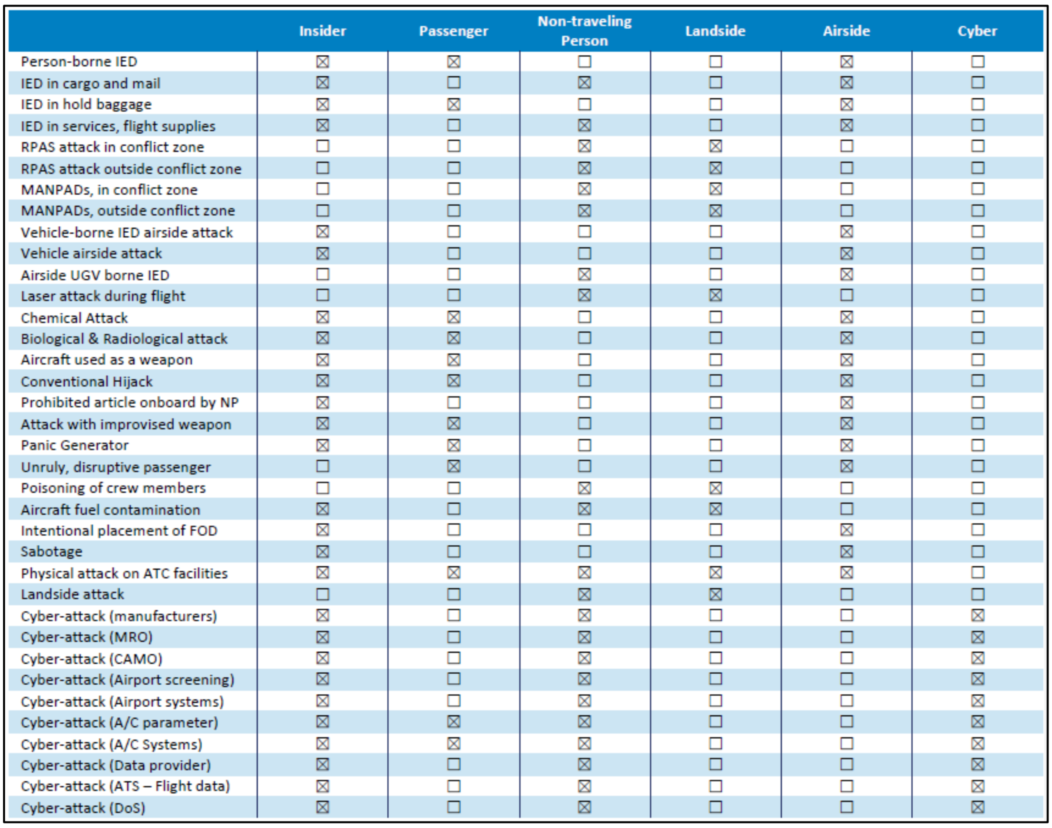
Threats were sourced from deliverable D-2.1 of task 2 "*Identification of the main security threats and scenarios (physical threats and information security threats) having an impact on aircraft safety*" (Figure 2 and Figure 3). It was used to develop threat scenarios and was contextualised by outcomes of the ICAO Doc 10108 Global Risk Context Statement (RCS) as well as based on stakeholder's consultation.

[6] https://www.easa.europa.eu/en/document-library/regulations/commission-delegated-regulation-eu-20202034



	Aircraft & Aircraft Equipment	RPAS	ATM ATS	Aerodrome Airport Operations	Airport Operations related to screening	Air Operations	Ground Operations	Off-Airport Operations
Person-borne IED	☒	☐	☒	☐	☒	☒	☐	☐
IED in cargo and mail	☒	☐	☒	☐	☒	☒	☐	☒
IED in hold baggage	☒	☐	☒	☐	☒	☒	☐	☐
IED in services, flight supplies	☒	☐	☒	☐	☒	☒	☐	☒
RPAS attack in conflict zone	☒	☒	☒	☒	☐	☒	☐	☐
RPAS attack outside conflict zone	☒	☒	☒	☒	☐	☒	☐	☐
MANPADs, in conflict zone	☒	☐	☒	☐	☐	☒	☐	☐
MANPADs, outside conflict zone	☒	☐	☒	☐	☐	☒	☐	☐
Vehicle-borne IED airside attack	☒	☐	☒	☒	☒	☒	☒	☐
Vehicle airside attack	☒	☐	☒	☒	☒	☒	☒	☐
Airside UGV borne IED	☒	☐	☒	☒	☐	☒	☒	☐
Laser attack during flight	☐	☐	☒	☐	☐	☒	☐	☐
Chemical threat	☐	☐	☒	☐	☒	☒	☐	☐
Biological & Radiological threat	☐	☐	☒	☐	☒	☒	☐	☐
Aircraft used as a weapon	☒	☐	☒	☐	☐	☒	☐	☐
Conventional Hijack	☒	☐	☒	☐	☐	☒	☐	☐
Prohibited article onboard by NP	☒	☐	☒	☒	☐	☒	☒	☐
Attack with improvised weapon	☒	☐	☒	☐	☐	☒	☐	☐
Panic Generator	☐	☐	☒	☐	☒	☒	☐	☐
Unruly, disruptive passenger	☐	☐	☐	☐	☒	☒	☒	☐
Poisoning of crew members	☐	☐	☒	☐	☐	☒	☐	☐
Aircraft fuel contamination	☒	☐	☒	☐	☐	☒	☒	☒
Intentional placement of FOD	☐	☐	☒	☒	☐	☒	☒	☐
Sabotage	☒	☐	☒	☒	☒	☒	☒	☒
Physical attack on ATC facilities	☐	☐	☒	☐	☒	☒	☐	☐
Landside attack	☐	☐	☐	☒	☐	☐	☒	☐
Cyber-attack (manufacturers)	☒	☐	☐	☐	☐	☒	☐	☐
Cyber-attack (MRO)	☒	☐	☐	☐	☐	☒	☐	☐
Cyber-attack (CAMO)	☒	☐	☐	☐	☐	☒	☐	☐
Cyber-attack (Airport screening)	☐	☐	☐	☒	☒	☐	☐	☐
Cyber-attack (Airport systems)	☐	☐	☒	☒	☐	☒	☒	☐
Cyber-attack (A/C parameter)	☒	☐	☒	☐	☐	☒	☐	☐
Cyber-attack (A/C Systems)	☒	☐	☒	☐	☐	☒	☐	☐
Cyber-attack (Data provider)	☒	☐	☒	☐	☐	☒	☐	☐
Cyber-attack (ATS – Flight data)	☐	☐	☒	☐	☐	☒	☐	☐
Cyber-attack (DoS)	☐	☐	☒	☐	☐	☒	☐	☐

Figure 2 – D-2.1 – Security threat scenarios vs areas of interdependencies



	Insider	Passenger	Non-traveling Person	Landside	Airside	Cyber
Person-borne IED	☒	☒	☐	☐	☒	☐
IED in cargo and mail	☒	☐	☒	☐	☒	☐
IED in hold baggage	☒	☒	☐	☐	☒	☐
IED in services, flight supplies	☒	☐	☒	☐	☒	☐
RPAS attack in conflict zone	☐	☐	☒	☒	☐	☐
RPAS attack outside conflict zone	☐	☐	☒	☒	☐	☐
MANPADs, in conflict zone	☐	☐	☒	☒	☐	☐
MANPADs, outside conflict zone	☐	☐	☒	☒	☐	☐
Vehicle-borne IED airside attack	☒	☐	☐	☐	☒	☐
Vehicle airside attack	☒	☐	☐	☐	☒	☐
Airside UGV borne IED	☐	☐	☒	☐	☒	☐
Laser attack during flight	☐	☐	☒	☒	☐	☐
Chemical Attack	☒	☒	☐	☐	☒	☐
Biological & Radiological attack	☒	☒	☐	☐	☒	☐
Aircraft used as a weapon	☒	☒	☐	☐	☒	☐
Conventional Hijack	☒	☒	☐	☐	☒	☐
Prohibited article onboard by NP	☒	☐	☐	☐	☒	☐
Attack with improvised weapon	☒	☒	☐	☐	☒	☐
Panic Generator	☒	☒	☐	☐	☒	☐
Unruly, disruptive passenger	☐	☒	☐	☐	☒	☐
Poisoning of crew members	☐	☐	☒	☒	☐	☐
Aircraft fuel contamination	☒	☐	☒	☒	☐	☐
Intentional placement of FOD	☒	☐	☐	☐	☒	☐
Sabotage	☒	☐	☐	☐	☒	☐
Physical attack on ATC facilities	☒	☒	☒	☒	☒	☐
Landside attack	☐	☐	☒	☒	☐	☐
Cyber-attack (manufacturers)	☒	☐	☒	☐	☐	☒
Cyber-attack (MRO)	☒	☐	☒	☐	☐	☒
Cyber-attack (CAMO)	☒	☐	☒	☐	☐	☒
Cyber-attack (Airport screening)	☒	☐	☒	☐	☐	☒
Cyber-attack (Airport systems)	☒	☐	☒	☐	☐	☒
Cyber-attack (A/C parameter)	☒	☒	☒	☐	☐	☒
Cyber-attack (A/C Systems)	☒	☒	☒	☐	☐	☒
Cyber-attack (Data provider)	☒	☐	☒	☐	☐	☒
Cyber-attack (ATS – Flight data)	☒	☐	☒	☐	☐	☒
Cyber-attack (DoS)	☒	☐	☒	☐	☐	☒

Figure 3 – D-2.1 – Security threat scenarios vs threat actors’ profile and type of threat

Table 1 that combines the information from both Figure 2 and Figure 3 was then created as a starting point.

Table 1: Recapturing of threats listed in D-2.1 (Figures 2 and 3 combined). I = Insider, P = Passenger, NTP =Non-Travelling Person, AAE = Aircraft & Aircraft Equipment, ATM ATS = Air Traffic Management / Air Traffic Services, AAO = Aerodrome / Airport Operations, AO = Air Operations, GO = Ground Operations, RPAS = Remotely Piloted Aircraft System)

	Threat	Adversary	Threat type	Safety area affected
1	IED on body (person-borne IED, PBIED) IED in cabin baggage	I / P	Airside	AAE / ATM ATS / Screening / AO
2	IED in cargo IED in mail	I / NTP	Airside	AAE / ATM ATS / Screening / AO / Off-AO
3	IED in hold baggage	I / P	Airside	AAE / ATM ATS / Screening / AO
4	IED in services and flight supplies	I / NTP	Airside	AAE / ATM ATS / Screening / AO / Off-AO
5	RPAS (inside conflict zone)	NTP	Landside	AAE / RPAS / ATM ATS / AAO / AO
6	RPAS (outside conflict zone)	NTP	Landside	AAE / RPAS / ATM ATS / AAO / AO
7	MANPADS (inside conflict zone)	NTP	Landside	AAE / ATM ATS / AO
8	MANPADS (outside conflict zone)	NTP	Landside	AAE / ATM ATS / AO
9	IED (vehicle-born)	I	Airside	AAE / ATM ATS / AAO / Screening /AO / GO
10	Vehicle attack	I	Airside	AAE / ATM ATS / AAO / Screening /AO /GO
11	IED (UGV-borne)	I	Airside	AAE / ATM ATS / AAO / AO /GO
12	Laser attack during flight	NTP	Landside	ATM ATS / AO
13	Chemical attack	I / P	Airside	ATM ATS / Screening / AO
14	Biological & radiological attack	I / P	Airside	ATM ATS / Screening / AO
15	Aircraft used as weapon	I / P	Airside	AAE / ATM ATS / AO
16	Conventional hijack (taking hostages and making demands)	I / P	Airside	AAE / ATM ATS / AO
17	Prohibited article onboard by NTP	I	Airside	AAE / ATM ATS / AAO / AO / GO
18	Attack with improvised weapon	I / P	Airside	AAE / ATM ATS / AO
19	Panic generator	I / P	Airside	ATM ATS / Screening /AO
20	Unruly, disruptive passenger	P	Airside	Screening /AO / GO
21	Poisoning of crew members	NTP	Landside	ATM ATS / AO
22	Aircraft fuel contamination	I / NTP	Landside	AAE / ATM ATS / AO / GO / Off-AO
23	Intentional placement of FOD	I	Airside	ATM ATS / AAO / AO / GO
24	Sabotage	I	Airside	AAE / ATM ATS / Screening /AO / GO / Off-AO
25	Physical attack on ATC facilities	I / P / NTP	A / L	ATM ATS / AAO / Screening /AO
26	Landside attack	NTP	Landside	AAO / GO
27	Cyber-attack (manufacturers)	I / NTP	Cyber	AAE / AO
28	Cyber-attack (MRO)	I / NTP	Cyber	AAE / AO
29	Cyber-attack (CAMO)	I / NTP	Cyber	AAE / AO
30	Cyber-attack (airport screening)	I / NTP	Cyber	AAO / Screening
31	Cyber-attack (airport systems)	I / NTP	Cyber	ATM ATS / AAO / AO / GO
32	Cyber-attack (A/C parameter)	I / P / NTP	Cyber	AAE / ATM ATS / AO
33	Cyber-attack (A/C systems)	I / P / NTP	Cyber	AAE / ATM ATS / AO
34	Cyber-attack (data provider)	I / NTP	Cyber	AAE / ATM ATS / AO
35	Cyber-attack (ATS - flight data)	I / NTP	Cyber	ATM ATS / AO
36	Cyber-attack (DoS)	I / NTP	Cyber	ATM ATS / AO

The selection process of threat scenarios which consider the top safety event and consequences of threats in terms of aircraft safety and survivability as well as loss of lives (passengers and crew) is described in detail in Section 4.2.1.

3.2.2. Preventive security measures

The approach toward this subtask requires the recapitulation of the difference between terms *prevention* and *mitigation* as the report captures "preventive" security measures and "mitigations".

Prevention means *stopping something from happening*, while mitigation means *making the situation, or effects of something less harmful or serious*. In this context, the preventive nature of security measures is prominent and confirmed in the Annex 17 definition of acts of unlawful interference (AUIs). These AUIs are defined as *acts to jeopardize the safety of civil aviation*, therefore it can be generally concluded security measures contribute to the safety by preventing AUIs.

The research validated this approach with stakeholders by receiving feedback which confirmed this assumption (see Figure 4). Respondents were asked to choose one out of three statements which reflects their opinion best and the overwhelming majority of them, selected "security contributes to safety" (88%) while only a small percentage selected either of the remaining two answers. Out of these two, the smallest share of respondents selected "safety and security are completely separated".

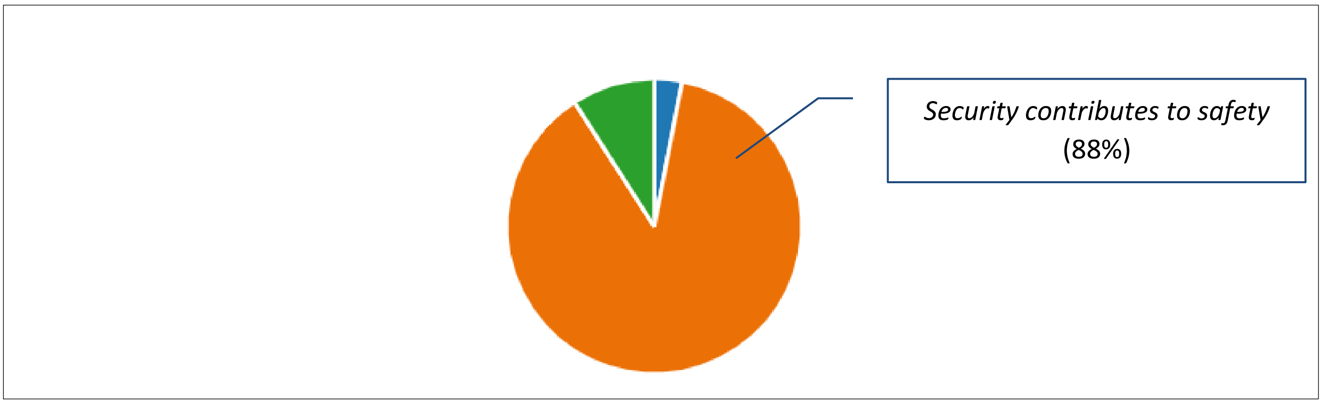


Figure 4 – Results of stakeholder survey question "Select the answer that reflects your opinion best"

Stemming from the global baseline of Annex 17, preventive measures referred to in this report were mostly sourced from two regulations applicable in the EU and European Economic Area:

- 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[7]
- 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[8]

For the purpose of assessments in this report, it was considered sufficient to look into these preventive measures grouped around certain aviation security activities or outcomes, rather than looking into each single measure and provision separately. Also, a more detailed analysis of the screening topic is covered in the separate report D-3.1.2 "*Relevance of the existing detection requirements for screening equipment to mitigate threats to aircraft structure*", which investigates screening methods and their relevance to mitigate threats to aircraft structure. All these are aggregated and described in detail in Section 4.2.2 .

[7] OJ L 97, 9.4.2008, p. 72–84

[8] Consolidated text including subsequent amendments: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015R1998-20240901

In case of several types of threat scenarios preventive security measures in Regulation (EU) 2015/1998 did not provide sufficient input to the study. This has been the case for threats related to:

- Remotely Piloted Aircraft System (RPAS)
- Man Portable Air Defence System (MANPAD)
- Chemical, Biological or Radiological agents (CBR)
- Intentional Unauthorized Electronic Interaction (IUEI)

In these instances, the research explored other sources of regulations, standards and recommendations to provide information on existing preventive measures.

Additionally, due to their sensitive nature, preventive measures are presented in descriptive form rather than focused of listing specific, individual security controls.

3.3. Study of aircraft design standard (as security mitigations)

Relevant aircraft design standards were sourced from EASA CS-25 *Easy Access Rules for Large Aeroplanes* with the support of other sources found through the literature search.

Main conditions ruling the design of aircraft were investigated, together with the most important environment / surrounding considerations in the context on the aircraft design process. These aircraft design standards were reviewed to understand which of them may play a role in mitigating physical and information security threats in case preventive measures would not cope with them.

These are described in detail in Section 4.3.

4. Study of aircraft design standards and their relevance for mitigating physical & information security threats

This chapter provides critical information that is later used for the assessment of aircraft design standards and their relevance for mitigating physical & information security threats in the form of:
- Methodology (Section 4.1)
- Physical and information security threats and related preventive security measures (Section 4.2)
- Current aircraft design standards and their relevance for mitigating physical and information security threats (Section 4.3)

4.1. Methodology of assessment

4.1.1. The bowtie method

As mentioned in section 3.1, bowties were selected by the research team as most adequate to analyse and visualise interdependencies between threat scenarios, preventive security measures, and aircraft design-based mitigations (ADBM). In the next step, the research looked into the theoretical background of the bowtie method and the use case of aviation.

4.1.1.1. Theoretical background

Bowtie analysis is a broadly used tool in risk management to identify root causes and consequences of hazards and show barriers that can prevent or mitigate the events to happen (for a review see Aust & Pons, 2019). The diagram is a combination of a fault tree analysis (FTA), event tree analysis (ETA), consequence analysis (CCA), and barrier analysis (BA). It simplifies FTA and ETA by removing complex symbols and merges them using the CCA approach, which focuses on single cause-consequence relationships.

Instead of using blocks, it introduces barriers placed on both ends of the diagram to prevent or lessen negative outcomes. The bowtie structure is laid out horizontally, forming its signature shape with a central knot, hence its name. The bowtie diagram includes hazard, top event, threats, consequences, barriers, as well as escalation factors and escalation factor barriers (see Figure 5 for a schematic overview[9]).

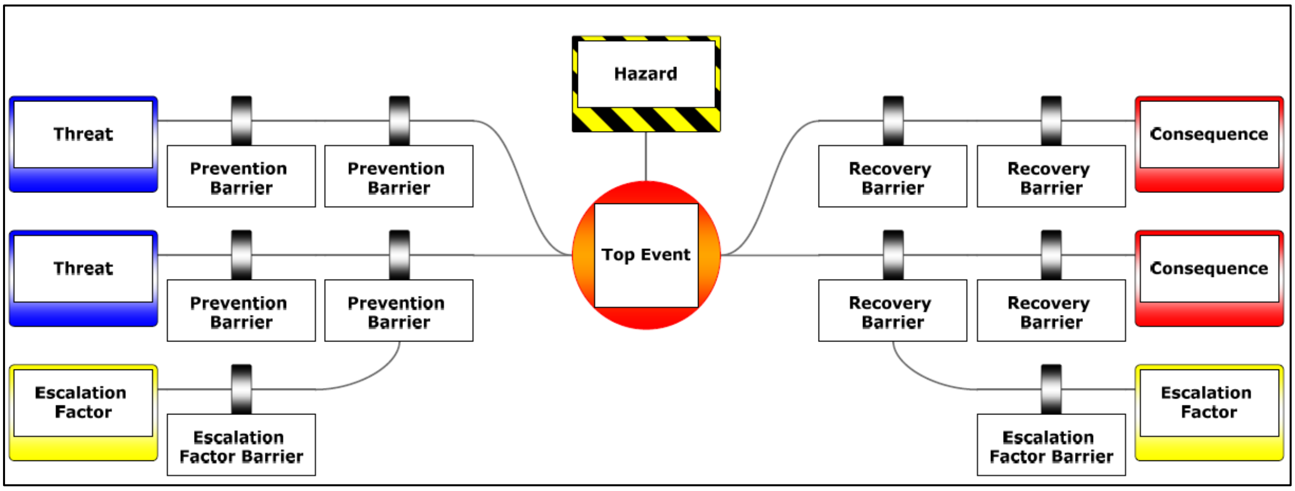


Figure 5 – Schematic bowtie diagram for risk management

A **hazard** is defined as condition (e.g. icing conditions), object (e.g. another vehicle), or activity (e.g. driving) that can potentially cause harm or damage, including injuries to personnel, damage to equipment, properties, or environment, or reduced ability to perform a prescribed function as intended.

Threats describe events that can potentially cause, through several pathways, the occurrence of the identified top event if all preventative controls (prevention barriers) fail. There can be one or multiple threats leading to the top event.

Prevention barriers are located on the left side of the Bowtie diagram, between the threat and top event. They prevent the hazard from being released by eliminating the threat entirely or preventing the top event from occurring. When the top event is reached, mitigation barriers become effective and reduce the likelihood of the consequences to occur, or limit the severity of the undesired consequences. These barriers are located between the top event and the consequences.

The conditions influencing the effectiveness are called **escalation factors**, and are depicted using branches from the main path barrier. Once the escalation factors are determined, the next step is to identify barriers that are in place to manage the escalation factors. Those barriers are called escalation factor barriers and are placed between the escalation factor and the affected barrier on the main threat path.

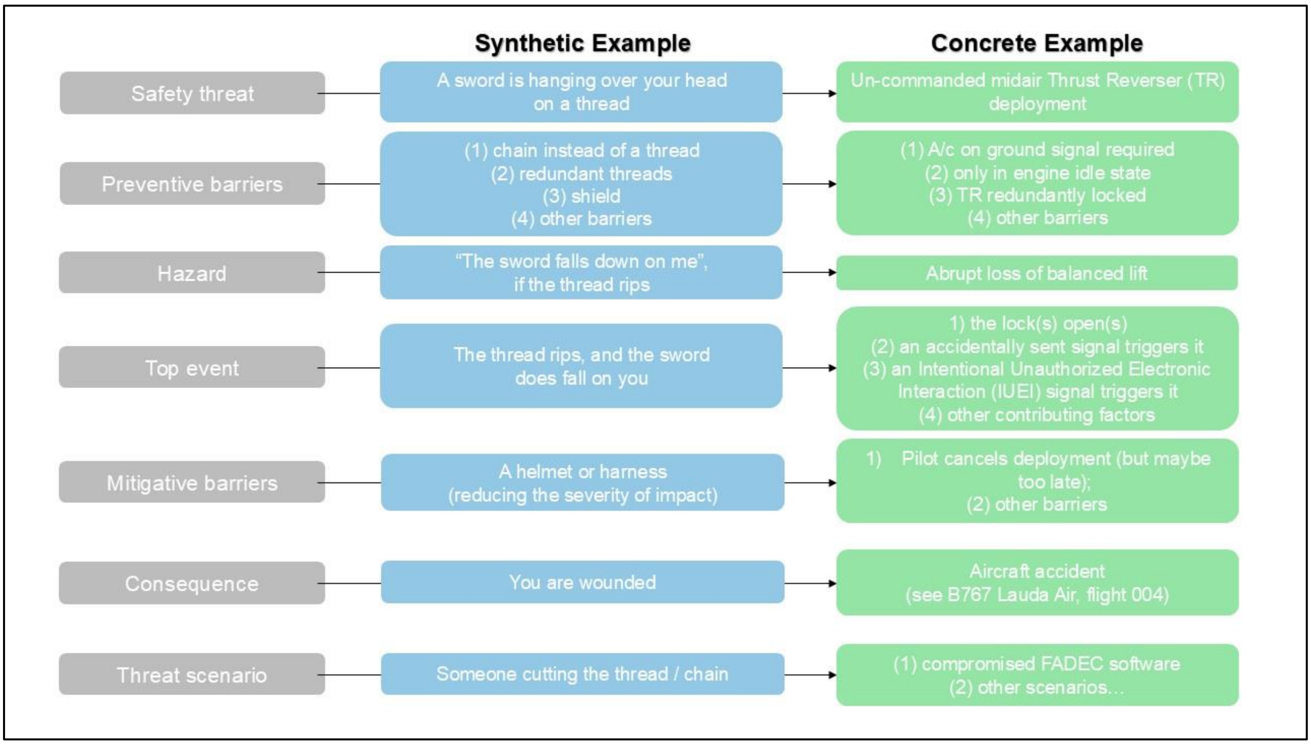
The **top event** is the point in time when the controlled state of a hazard is lost. It is yet to cause any damage or negative impact (unsafe state), but can lead to undesired outcomes if all prevention barriers fail. The term “top event” is derived from the fault tree analysis, where the critical event is on the top.

Recovery Barriers, which are also called controls or layers of protection, are measures that mitigate undesired outcomes. They can be categorised based on their location in the Bowtie diagram and their function.

[9] It should be mentioned that there is no standardised terminology for the different elements of a bowtie. The definitions in this document originate from UK CAA (https://www.caa.co.uk/safety-initiatives-and-resources/working-with-industry/bowtie/bowtie-elements/).

Consequences are potential outcomes or a chain of outcomes resulting from the release of the top event, directly resulting in loss of control or damage if mitigation barriers fail. Consequences are events not the actual loss or damage. The loss or damage is the 'outcome' against which severity is usually gauged.

Figure 6 below shows the flow in the bowtie analysis that could help in understanding the terms practically.



	Synthetic Example	Concrete Example
Safety threat	A sword is hanging over your head on a thread	Un-commanded midair Thrust Reverser (TR) deployment
Preventive barriers	(1) chain instead of a thread (2) redundant threads (3) shield (4) other barriers	(1) A/c on ground signal required (2) only in engine idle state (3) TR redundantly locked (4) other barriers
Hazard	"The sword falls down on me", if the thread rips	Abrupt loss of balanced lift
Top event	The thread rips, and the sword does fall on you	1) the lock(s) open(s) (2) an accidentally sent signal triggers it (3) an Intentional Unauthorized Electronic Interaction (IUEI) signal triggers it (4) other contributing factors
Mitigative barriers	A helmet or harness (reducing the severity of impact)	1) Pilot cancels deployment (but maybe too late); (2) other barriers
Consequence	You are wounded	Aircraft accident (see B767 Lauda Air, flight 004)
Threat scenario	Someone cutting the thread / chain	(1) compromised FADEC software (2) other scenarios…

Figure 6 – Flow of bowtie analysis

4.1.1.2. Use case: Security threat scenarios with aircraft design-based mitigations

The bowtie method has emerged as a powerful risk management tool in various industries including also aviation. For example, UK CAA created numerous bowties that are focused on aircraft operation and the "significant seven" top events that describe a range of significant safety accident scenarios . Hence, the bowtie method is widely known and used in the aviation safety domain, but it hasn't been yet well-established in security. In this study development of top events was based on Key Risk Areas defined in the Annex to the Regulation (EU) 2020/2034 (see 4.1.2).

For these reasons, some adaptations in the methodology were introduced. These were following a similar thinking process applicable to other risk analysis methods which are used by safety and security. An example of such adaptation is the safety term *hazard*, for which closest equivalence in the aviation security domain is the term *threat* (except for unintentional or intentional context). The ICAO Doc 9859 Safety Management Manual (SMM) defines hazard as *potential for harm which is present in one form or another within the system or its environment*. Threat is defined in the IATA Security Management System (SeMS) Manual as *a function of intention and capability to cause harm*. There is no definition of threat in ICAO documentation yet, however IATA definition of threat aligns with the understanding of it as explained in the Doc 8973 Chapter 9.[10]

In aviation safety, a hazard is typically defined as any factor, condition, or event that has the potential to compromise the safety of an aircraft, its occupants, or the surrounding environment. Hazards are identifiable

[10] Chapter 9, Threat and risk management describes that threat of the attack (meaning translating threat into plausible threat scenario) should be assessed from the perspective of intention and capability.

through recognition of failure conditions or threats (also called “safety event”)[11]. Safety events can arise from a variety of sources and may include adverse weather conditions, technical malfunctions, human error, operational challenges, or external factors such as air traffic congestion - all of them being unintentional. Still, safety threats are predominantly more foreseeable (due to the amount of data collected from safety reporting) and the exposure to them is better understood compared to security threats which produce low-frequency, high-impact deliberate (intentional) events.

Aviation security is of fundamental importance for preventing attacks with potentially catastrophic consequences in terms of human and economic losses. Although civil aviation as a whole is an attractive target, the aircraft itself stands out as the primary focus of attacks. One measure that airports take to prevent attacks against civil aviation are airport security controls to reduce the vulnerability against threats. In the implementation of security controls, different activities are undertaken - e.g. persons and their belongings / baggage are controlled for prohibited items (e.g. guns) before they are allowed to enter the security restricted areas of the airport and board an aircraft.

However, prohibited items (i.e. threats) might still be successfully brought on-board an aircraft (see Figure 7). Should this occur, mitigations can take place. These mitigations could be implemented through procedures, or actions based on training and experience. They may also originate from aircraft design requirements. The focus of this report is restricted to mitigations based on aircraft design requirements and therefore other mitigations remained out of scope.

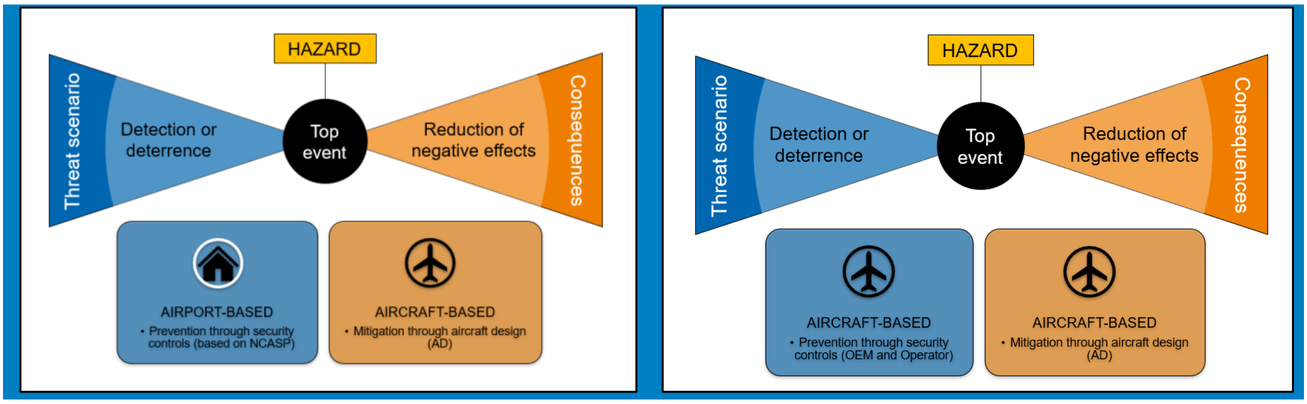

HAZARD
Threat scenario
Detection or deterrence
Top event
Reduction of negative effects
Consequences
AIRPORT-BASED
• Prevention through security controls (based on NCASP)
AIRCRAFT-BASED
• Mitigation through aircraft design (AD)
HAZARD
Threat scenario
Detection or deterrence
Top event
Reduction of negative effects
Consequences
AIRCRAFT-BASED
• Prevention through security controls (OEM and Operator)
AIRCRAFT-BASED
• Mitigation through aircraft design (AD)

Figure 7 – Schematic overviews for mitigating physical (left) and information security (right) threats using the bowtie method

As seen in Figure 8, the bowtie diagram for risk management can be adapted to include preventive security measures and mitigation measures as discussed earlier. The threat is a condition that could foreseeably cause or contribute to an aircraft incident / accident. A threat can be broken down to plausible threat scenarios (based on threats listed in D-2.1) that can lead to the top event. The consequence is an incident / accident scenario that results in death, injury, or damage to, or loss of equipment or property.

[11] Guidance on Hazards Identification, Safety Management System and Safety Culture Working Group, 2009 - https://www.easa.europa.eu/en/downloads/24190/en

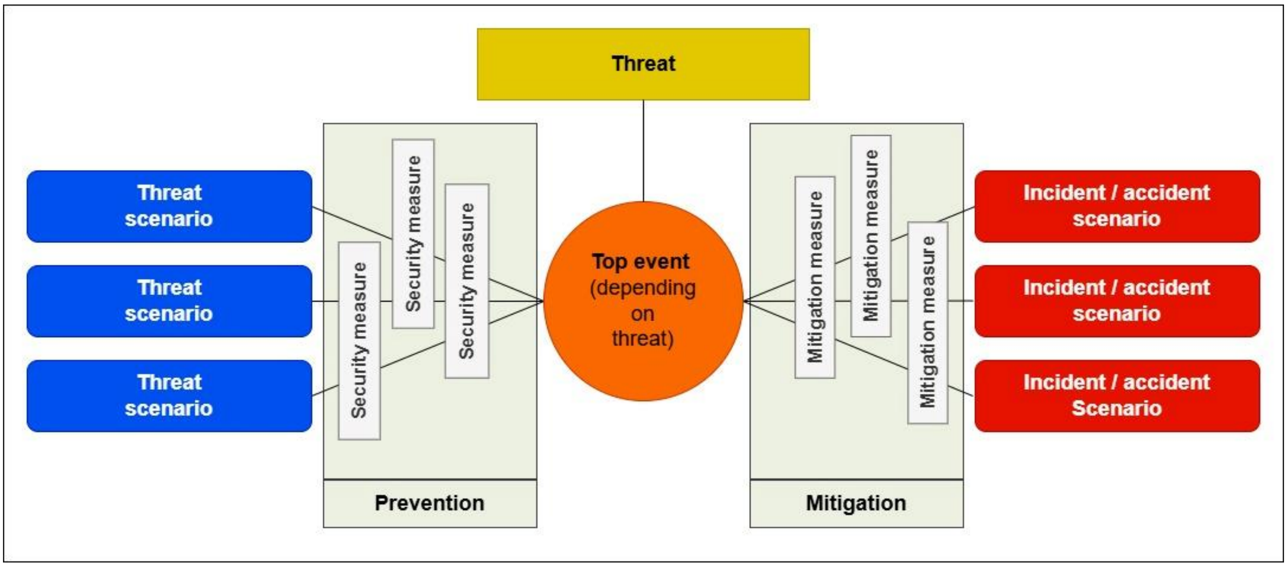


Figure 8 – Generic bowtie model for mitigating physical and information security threats

A threat scenario is defined by ICAO AVSEC Global RCS as "*the identification and description of a plausible act of unlawful interference comprising a target, the means and methods of an attack (modus operandi), and the adversary*". Table 2 shows how threat scenarios were defined for the purpose of this report.

Table 2: Threat scenario

	Target WHAT	Adversary WHO	Modus operandi HOW
Question	What is the target?	Who is attempting to conduct the attack?	Threat item/tool – how does the adversary instigate the attack? Concealment/transmission method – how does the adversary get the threat to the target?
Output for this analysis	Large aeroplanes	Passenger, insider (aviation employees), NTP	Threat item – prohibited article, malicious component affecting availability or integrity of data or systems Concealment/ transmission method – on body (person-borne) or in hold / cabin baggage, mail / cargo / in-flight supplies, or by digital or physical means against software and hardware for information security related threat scenarios

With this in mind, a bowtie per threat building one or more threat scenarios can be developed (see Figure 9 for a generic example).

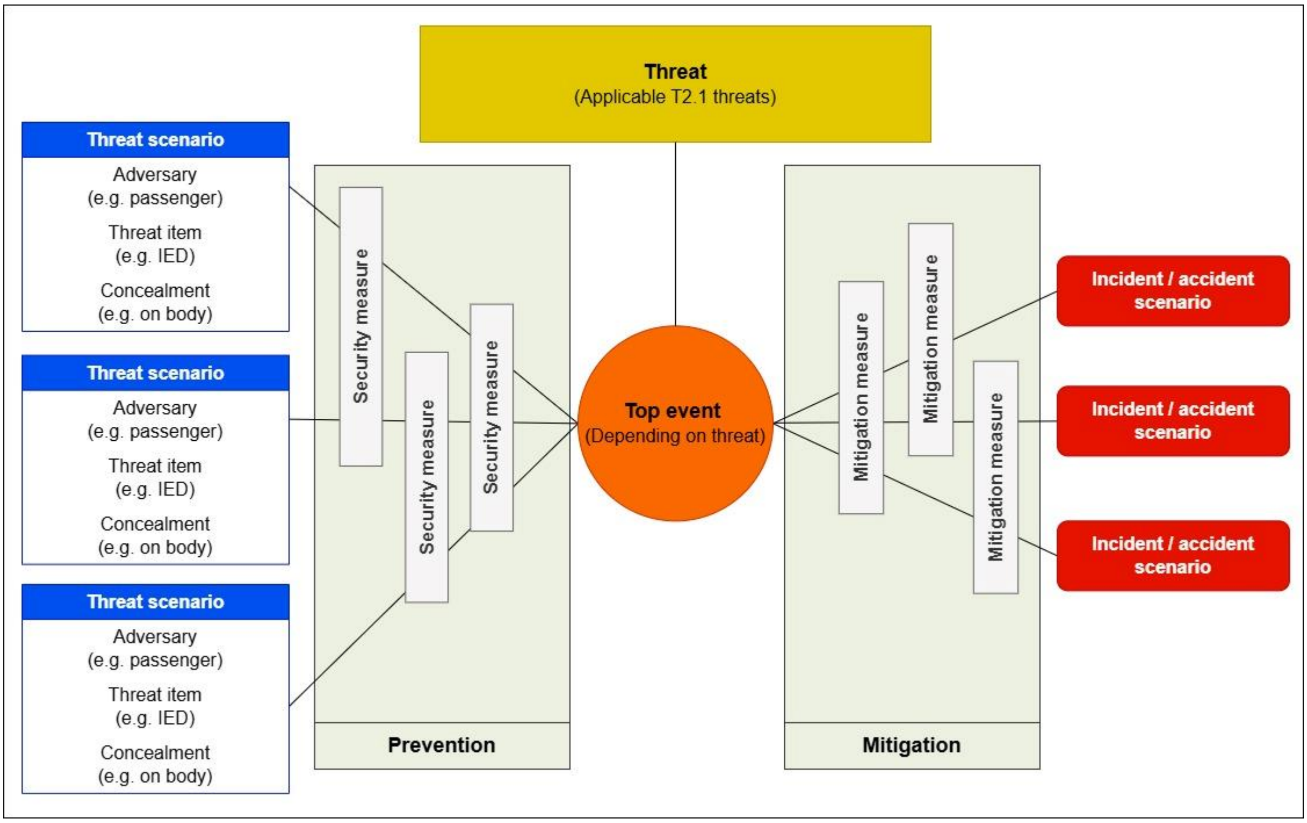


Figure 9 – Generic bowtie model for mitigating physical & information security threats using threat scenarios

In the scope of information security threats, scenarios listed in 4.2.1.4 refer to system functions rather than system names. This approach is consistent with industry stakeholders' approach and reflective of FHA and DAL processes. In this context threats scenarios refer to system functions with DAL severity levels where failure may lead to catastrophic, hazardous or major effects[12].

Below are non-exhaustive examples of system functions in terms of their DAL levels:

- DAL A – Flight Control, Autopilot, Engine and Thrust Control, Navigation and Guidance, Landing Gear and Breaking
- DAL B – Secondary Flight Controls, Fuel Management, Thrust Reverser Control, Environmental Control, Primary Electric Power Distribution
- DAL C – Passenger Address and Interphone, Flight Data Recording.

Some of identified threat scenarios in this context may include:

- Corrupted flight plan update data sent via ACARS
- Uploading of corrupted database into the FMS
- Denial of Service attack on FMS[13]

[12] For details see CS-25 Amendment 28, AMC 25.1309 System design and analysis

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

4.1.2. Top safety events

Following the identification of threats and threat scenarios, the research team looked into the taxonomy of top events as a next step. Top event in the bowtie methodology is typically explained as the "*critical moment when control is lost over a hazard*". It means the situation is yet to cause critical damage or actual harm, but it is this stage when protective barriers fail.

The following top event types are used for the purpose of further assessments[14]:

- **Airborne collision** - a collision between aircraft while both aircraft are airborne; or between aircraft and other airborne objects (excluding birds and wildlife);
- **Aircraft upset** - an undesired aircraft state characterised by divergences from parameters normally experienced during operations, which might ultimately lead to Loss of Control (LoC) an uncontrolled impact with terrain;
- **Collision on airside** - a collision between an aircraft and another object (other aircraft, vehicles, etc.) or person caused by this object or person that occurs on an aerodrome;
- **Fire, smoke and pressurisation** - an occurrence involving cases of fire, smoke, fumes or pressurisation situations (including explosive decompression) that may create conditions (e.g. structural damages) incompatible with human life. This includes occurrences involving fire, smoke or fumes affecting any part of an aircraft, in flight or on the ground;
- **Ground damage** - damage to aircraft on ground on any other ground area than a runway or predesignated landing area, as well as damage during maintenance;
- **Obstacle collision in flight** - collision between an airborne aircraft and obstacles rising from the surface of the earth. Obstacles include tall buildings, trees, power cables, telegraph wires and antennae as well as tethered objects;
- **Terrain collision** - an occurrence where an airborne aircraft collides with terrain, without indication that the flight crew was unable to control the aircraft. It includes instances when the flight crew is affected by visual illusions or degraded visual environment;
- **Other injuries** - an occurrence where fatal or non-fatal injuries have been inflicted, which cannot be attributed to any other key risk area.

4.2. Physical and information security threats and their preventive security measures

The first step of this study was to narrow down the focus of physical and information security threats which are related directly to the aircraft safety and survivability, and loss of lives (of passengers and crew) for the analysis. Landside threats to airport terminal or attacks against Air Traffic Control (ATC) infrastructure are determined out of scope. This step allowed to focus on aircraft design standards which play a role in mitigating security threats. The following section describes process based on which relevant security threats were ultimately selected (Section 4.2.1) and their corresponding preventive measures (Section 4.2.2).

[14] The research team noted one of the Key Risk Areas "security". It was however determined as unsuitable for the analysis. Risk areas listed in the Annex to the Regulation (EU) 2020/2034 are defined by the actual event or occurrence and its consequence, when the last one is indicated as "security" and defined as an act of unlawful interference and further "includes all incidents and breaches". This category does not define any actual event, moreover it seems to suggest grouping all security related events in one category which would make any further analysis impractical.

4.2.1. List of security threats

4.2.1.1. Affected operational areas

Aircraft safety was defined in D-2.1 as "*perimeter encompassing all contributors that might lead to a serious incident or an accident*". Given the focus of the report D-3.1.1 and D-3.1.3 out of the entire list red indicates out of scope areas and green initial identification of the in-scope area. This area has been overlaid by reverse engineering process identifying threats which have aircraft design-based mitigations (design and certification related elements only).

Hence, the following elements are considered in and out of scope for analysis:

In Scope	Out of scope
• AAE (Aircraft & Aircraft Equipment): Aircraft itself, its components, design, certification, and maintenance procedures	• ATM & ATS (Air Traffic Management & Air Traffic Services) • AO (Airport Operations) related to screening • GO (Ground Operations): refueling / de-icing, aircraft load, handling of baggage and passengers • AO (Air Operations) • Off-Airport Operations

4.2.1.2. Threat type

To further align with the report D-2.1 analysis of the "Type of threat" component was performed as defined in D-2.1 from the perspective of where it could occur (i.e. air- or landside, IUEI). Following the same methodology as described in Section 4.2.1.1 specific airside, landside and information security threats were selected and considered for this report. Consequently, considering the focus of the report D-3.1.1 and D-3.1.3 the list of threats was narrowed down to those that affect an aircraft directly and could be analysed for the presence of aircraft design-based mitigations.

Hence, the following elements are considered in and out of scope:

In Scope	Out of scope
• Airside: Passengers and baggage screening as well as baggage handling / (un-)loading • Landside: Airports surroundings such as the infrastructure / activity in the immediate vicinity • IUEI: targeting DAL A - B system functions	• Airside: Refuelling, de-icing, aircraft cleaning, catering (un-) loading, line maintenance activities, passenger handling (dis-embarking) • Landside: Fuel supply, air cargo and catering supply, maintenance, Continuous Airworthiness Management Organisations, airport remote infrastructure (such as VOR, ILS, communications antenna, approach control room etc.) • IUEI: all others • Airport systems (screening equipment & critical infrastructure) • Data providers

4.2.1.3. Adversary

According to the D-2.1 report "*defining the perpetrator type within each threat scenario facilitates a more comprehensive understanding of potential threat origins*". Three distinct categories of perpetrators *(also called "threat actors")* were therefore identified in D-2.1: insider, passengers, and non-travelling persons

The following elements are considered in scope for the analysis:

- Passenger and insider (airside)
- Non-travelling persons (landside)

For the purposes of this report, the same approach is followed. It has been considered helpful in identifying various threat scenarios, and their escalating factors together with corresponding preventive and mitigation measures applicable for different threat scenarios.

4.2.1.4. Final list of threat and threat scenarios for this report

The goal for the research in this stage of the project was to identify **threats which both have a direct impact on aircraft** safety and survivability, and can result in catastrophic consequences such as loss of lives (passengers and crew) as an outcome of damaging or destroying aircraft structure. Also, only threats that **can potentially be mitigated by aircraft design standards are considered. As a result, these threats are investigated and analysis visualised** through adapted bowties (see 5.1).

An initial list of threats compiled has been further consulted with stakeholders by means of a workshop, a survey and semi-structured interviews[15]. Based on inputs and to support further assessment these threats listed in 2.1 were aggregated so they reflect more accurately the intention of this report and focus on aircraft design standards (numbers in brackets correspond to Table 1 in section 3.2.1):

- IED in passenger cabin (#1, #4)
- IED in the hold/cargo compartment (#2, #3)
- Impact of an object (in the air) (#5, #6, #7, #8)
- Impact of an object (on the ground) (#5, #6, #9, #10, #11)
- CBR threats (#13, #14)
- Aircraft used as a weapon (#15)
- Conventional hijack (#16)
- Other threat items in the cabin (#17, #18)
- Sabotage (#23, #24)
- IUEI against DAL A and B system functions (#32, #33)

Table 3 therefore shows which threats from D-2.1 remain for the analysis for this report[16].

Table 3: Final list of threats and threat scenarios for analysis. I = Insider, P = Passenger, NTP =Non-Travelling Person.

#	Threat	Adversary	Threat type
Threat type I: IED in passenger cabin			
1	IED on body (person-borne IED, PBIED) IED in cabin baggage	I / P	Airside
4	IED in services and flight supplies	I / NTP	Airside
Threat type II: IED in hold / cargo department			
2	IED in cargo IED in mail	I / NTP	Airside
3	IED in hold baggage	I / P	Airside
Threat type III: Impact of an object (in the air)			
5	RPAS (inside conflict zone)	NTP	Landside

[15] Details of the validation process for threats will be covered in D-3.1.4 report.

[16] Details on examples of reasoning will be in covered in D-3.1.4 report.

#	Threat	Adversary	Threat type
6	RPAS (outside conflict zone)	NTP	Landside
7	MANPADS (inside conflict zone)	NTP	Landside
8	MANPADS (outside conflict zone)	NTP	Landside
Threat type IV: Impact of an object (on the ground)			
5	RPAS (inside conflict zone)	NTP	Landside
6	RPAS (outside conflict zone)	NTP	Landside
9	IED (vehicle-born)	I	Airside
10	Vehicle attack	I	Airside
11	IED (UGV-borne)	I	Airside
Threat type V: CBR threats			
13	Chemical attack	I / P	Airside
14	Biological & radiological attack	I / P	Airside
Threat type VI: Aircraft used as a weapon			
15	Aircraft used as weapon	I / P	Airside
Threat type VII: Conventional hijack			
16	Conventional hijack (taking hostages and making demands)	I / P	Airside
Threat type VIII: Other threat items in the cabin			
17	Prohibited article onboard by NTP	I	Airside
18	Attack with improvised weapon	I / P	Airside
Threat type IX: Sabotage			
23	Intentional placement of FOD	I	Airside
24	Sabotage	I	Airside
Threat type X: IUEI against aircraft system functions			
32	DAL A or B system functions not available	I / P / NTP	Cyber
33	DAL A or B system functions data tampered	I / P / NTP	Cyber

4.2.2. List of preventive security measures

Regulation (EC) No 300/2008 lays down common rules in the field of civil aviation security. Aviation security is defined in Article 3 as: "*the combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference that jeopardize the security of civil aviation.*" Civil aviation is defined as: "*any air operation carried out by civil aircraft, excluding operations carried out by State aircraft referred to in Article 3 of the Chicago Convention on International Civil Aviation.*"

Commission Implementing Regulation (EU) 2015/1998 lays down detailed measures for the implementation of the common basic standards on aviation security. Annex 1 lays down the following set of preventive measures which were taken into consideration:

- Access control
- Screening of persons other than passengers
- Examination of vehicles
- Items carried by persons other than passengers
- Surveillance, patrols and other physical controls
- Identification and protection of civil aviation critical information and communication technology systems and data from cyber threats
- Aircraft security search

- Protection of aircraft
- Screening of passengers and cabin baggage
- Screening of hold baggage
- Protection of hold baggage
- Cargo (and mail) screening
- Protection of cargo and mail
- Air carrier mail and air carrier materials screening
- Security controls for in-flight supplies
- Screening of in-flight supplies
- In-flight security measures

In case of several types of threat scenarios preventive security measures in Regulation (EU) 2015/1998 did not provide sufficient input to the study. This has been the case for threats related to:

- Remotely Piloted Aircraft System (RPAS)
- Man Portable Air Defence System (MANPADS)
- Intentional Unauthorized Electronic Interaction (IUEI)

In these instances, the research explored other sources of regulations, standards and recommendations to provide information on existing preventive measures. Also, in these instances preventive measures are presented in descriptive form rather than focused of listing specific, individual security controls.

Specifically, for information security scope, the research recognized the risk-based approach in terms of aircraft system architecture and system security measures described in CS 25.1319 which states "*Protection must be ensured by showing that the* ***security risks have been identified, assessed and mitigated as necessary***". In this context the research referred to additional guidance and industry best practices[17]. As such rather than listing specific security measures a reference is made to Security Assurance Levels (SAL) required depending on the DAL level criticality. As described in the DO-356 / ED-203A document relevant SAL is defined for functions with assigned DAL as design objectives for the system development. Entities applying risk-based security controls (e.g. based on NIST 800-53 or ED-204/ED-205) would be required to provide for certification objective coverage relevant for specific SAL level required[18].

4.3. Current aircraft design standards

The safety of modern civil aircraft operations depends, amongst other factors, on the aircraft design. From the safety perspective, the aircraft design needs to consider the aircraft itself as well as the safety of passengers and crew.

In reality, the design and development of an aircraft is a long and complex process which needs to consider different, sometime conflicting factors (Bond & Ricci, 1992; Nicolai & Carichner, 2010). The basic properties of traditional aircraft design are obviously the four forces which make an aircraft fly: lift, drag, thrust and weight (Torenbeek, 2013). The historical aircraft designs were performed manually, and moving forward as technology progressed was supported by Computer Aided Design (CAD). On one hand, this allowed to include more factors into the design process, on the other, this approach and data-analytics enhanced awareness of certain risks. Therefore, as described by Torenbeek (2013) "*a certain amount of conservatism is inherent in the development of civil aircraft design*".

[17] Annex I to ED Decision 2020/006/R – AMC Amendment 18, and related European Organisation for Civil Aviation Equipment (EUROCAE) and Radio Technical Commission for Aeronautics (RTCA) documents: EUROCAE ED-202B / RTCA DO-326A; and ED-203A /RTCA DO-356

[18] Several industry documents provide for possible security controls to handle the threat of IUEI. Two organizations, EUROCAE and RTCA coordinate publication and issue equivalent guidance which are recognized as AMCs. These include: ED-202B (Airworthiness Security Process Specification) / RTCA-326A, ED-203A (Airworthiness Security Methods and Considerations) / RTCA-356A, ED-204A (Information Security Guidance for Continuing Airworthiness) / RTCA-355A.

Extensive literature describes the stages of aircraft design. As it is not the purpose of this report to describe in detail the design process, it is illustrated here only in general terms and to provide for the context for further analysis. It is evident that every airplane is designed for a determined purpose which generally for civil large airplanes will be to transport passengers and cargo.

- Product design
  - Conceptual design – refers to definition of aircraft mission requirements (range, payload, speed, capacity), top level requirements (TLR) and market analysis (demand)
  - Preliminary design – refers to detailed modelling of aerodynamics, propulsion, structures and systems
  - Detailed design – refers to specification of dimensions, materials, and components. It includes analysis of the airframe, integration of avionics, electrical, hydraulic and other systems. Manufacturing process is also designed in this phase
- Manufacturing – aircraft components are built according to specification. This stage includes testing for materials, processes and subsystems to assess performance and reliability
- Testing phase – evaluation of performance, safety and compliance through the testing program

To illustrate and help to understand the timeframe of full commercial aircraft design, Torenbeek (2013) uses the example of Boeing 777. The project go-ahead was given before the aircraft entered the detailed design stage between 1990 and 1991. Typically, between 9 to 12 months is needed for preceding the conceptual design and between 12 and 16 months for the preliminary design phase. Given the certification of this aircraft happened in 1995, it needs to be noted that the full process can take between 5 to 7 years for a large commercial aircraft.

The basic principles of aircraft design include the estimation of weights, determination of flight envelope, structural loads, aerodynamics, and controls. Design should optimise the aircraft in terms of performance, efficiency, reliability, and safety. In terms of safety and security, it is necessary to indicate that the aircraft design process assumes the aircraft will operate in the environment which displays an acceptable level of safety and security. In other words, the aircraft is not designed in the vacuum. Quite contrary, when the aircraft is designed, it is assumed that other stakeholders can create an acceptable environment to ensure the relevant level of safety and security, similarly to expectations on the operational side.

Large aircraft are mostly used by air operators granted the right to conduct commercial flights based on the Air Operator Certificate (AOC). The AOC is evidence that the operator is able to conduct safe operations using an airworthy aircraft. Airworthiness is related to system reliability. The reliability of a function can be improved with redundancy and dissimilarity of systems (but consequences need to be kept in mind). A reliable aircraft is one of the objectives identified early in the design stage. An aircraft is granted permission to be operated after being issued with the Type Certificate. Since 2003, EASA is responsible for the certification of aircraft in the EU and for some European non-EU countries and issues the Type Certificates accordingly. This certificate testifies that the type of aircraft meets the safety requirements set by the European Union. EASA describes four steps of the type-certification process which include:

- Technical familiarisation and certification basis
- Establishment of the certification programme
- Compliance demonstration
- Technical closure and issue of approval[19]

In terms of regulatory/certification environment, the design requirements referred to here are EASA CS-25 which are issued in accordance with the article 76(3) of the Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a

[19] https://www.easa.europa.eu/en/domains/aircraft-products/aircraft-certification

European Union Aviation Safety Agency: *"The Agency shall, in accordance with Article 115 and with the applicable delegated and implementing acts adopted on the basis of this Regulation, issue certification specifications and other detailed specifications, acceptable means of compliance and guidance material for the application of this Regulation and of the delegated and implementing acts adopted on the basis thereof"* and article 104(3) (a) of the above-mentioned regulation.

The Airworthiness codes i.e. certification specifications (CS) and the associated acceptable means of compliance (AMCs) are established by regulatory authorities (i.e. EASA and FAA) and contain a series of design requirements including:

- Strength of structures
- Flight qualities
- Performance
- Criteria for good design practice
- Systems
- Necessary tests
- Flight and maintenance manual content
- Airworthiness requirements-structure
    - Subpart A – general
    - Subpart B – flight
    - Subpart C – structure
    - Subpart D – design and construction
    - Subpart E – powerplant
    - Subpart F – equipment
    - Subpart G – operating limitations and information
    - Subpart H – electrical wiring interconnection system
    - Subpart J – auxiliary power unit installations

Hence, the following elements are considered in and out of scope:

In Scope	Out of scope
• **Aircraft:** Large aeroplanes[20] • **Requirements:** security and safety directly related to security as described in CS-25	• **Aircraft:** Other types of flying vehicles • **Requirements:** not related to security or not described in CS-25

Given the nature of the project, three groups of CS-25 requirements were identified (see Table 4). It is important to indicate ADRs are only part of the overall mitigations. This research does not analyse other mitigations which can be in form of procedures, trainings, and communication within the crew. It also does not account for actions from other entities involved in handling an emergency situation (e.g. ATC).

During the consultations in the scope of physical aviation security, stakeholders emphasized reliance on ground-based preventive security measures when developing assumptions in the aircraft design process. A main one is that the aircraft operates within a secure environment, with necessary preventive measures established through National Civil Aviation Security Programs effectively protecting it during operations.

This assumption appeared to be supported by the overall compliance level among EU Member States with the aviation security regulatory framework, as highlighted in the European Commission's 2022 Annual Report on the implementation of Regulation (EC) 300/2008 concerning civil aviation security rules.[21] The report indicates

[20] Large aeroplanes generally refer to those with maximum take-off weight (MTOW) of more than 5,700 kg (12,566 lbs). These aircraft are typically used for commercial air transport, such as passenger and cargo services.

[21] COM(2024) 107 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0107

a stable compliance rate of around 80%, even as aviation security requirements have become more stringent over time.

However, a less optimistic picture emerges when considering security implementation on a global scale. In the absence of specific worldwide data, the research team used ICAO's Global Aviation Security Plan (GASeP) as a reference.

GASeP's first iteration in 2017 set an aspirational target for 100% of states to achieve over 90% effective implementation of the Annex 17 global aviation security framework. However, the updated version (2024) revises this goal to "80% of states reach or surpass 75% effective implementation." Even accounting for the increased robustness of security measures in Annex 17 between the 2017 and 2024 versions, the global compliance level with basic measures remains far from the ideal, potentially challenging the assumption made during the design process. The research could not confirm whether entities responsible for aircraft design and regulators are fully aware of the global implementation status of Annex 17.

The aircraft design should in these circumstances, to the extent practical, consider physical security threats such as terrorism, hijacking, and sabotage. Measures like systems separation, secure cockpit doors, or the Least Risk Bomb Location (LRBL) are practical example of addressing the issue. As there is no general safety requirement which addresses failure of aviation security to protect the aircraft from physical security threats it remains critically important that preventive security measures are fully implemented on the ground and in processes surrounding the aircraft during its operations. Aircraft based security measures are developed based on the CS-25.795 and related AMC and GM[22].

From the information security perspective there is a broad recognition of the need for preventive security measures at the aircraft design stage. It is confirmed by clear indication of security risks and the necessity of protection against *intentional unauthorised electronic interference*.[23] In this context the aircraft design shall also consider information security threats and develop protections based on identified risks.

Table 4: List of CS-25 requirements in relation to security

[22] See please references in AMC 25.795, CS-25.795 Amendment 28

[23] Certification Specifications and Acceptable Means of Compliance for Large Airplanes, CS-25.1319

Specific security requirements	Requirements indirectly related to security		Security non-related requirements
• CS-25.795 • CS-25.1319, and Appendix H25.6	• CS-25.21 • CS-25.305 • CS-25.307 • CS-25.365 • CS-25.561 • CS-25.562 • CS-25.563 • CS-25.603 • CS-25.783 • CS-25.820 • CS-25.831 • CS-25.841 • CS-25.851 • CS-25.853 (and Appendix F) • CS-25.854 • CS-25.857	• CS-25.863 • CS-25.865 • CS-25.963 • CS-25.1091 • CS-25.1302 • CS-25.1303 • CS-25.1309 • CS-25.1317 • CS-25.1322 • CS-25.1326 • CS-25.1327 • CS-25.1329 • CS-25.1331 • CS-25.1333 • CS-25.1351 • CS-25.1352 • CS-25.1385 • CS-25.1387	• Other general, performance, controllability and manoeuvrability, trim, stability, stalls, lightning protection, etc.

5. Assessment of aircraft design specifications and their relevance for mitigating physical and information security threats

This chapter provides the analysis in form of bowtie analysis (Section 5.1) and a gap analysis (Section 5.2).

Table 5 combines all information from previous chapters and is used for the analysis with bowties and the gap analysis.

Table 5: Relevant threat scenarios (including threat, adversary, concealment), threat type, security measures, top event, and mitigation measures.

#	Threat scenario	Security measures	Threat escalating factors	Threat escalating factor barriers	Top event	Mitigation measures – CS.25 reference
Threat type I: IED in passenger cabin						
1	• **1.1** IED carried in cabin baggage or in personal items • **1.2** IED carried on person (PBIED)	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Vehicles examination • Screening of passengers • Screening of cabin baggage and items carried • Access control	• IED not assembled • Sophisticated concealment • Non-organic explosive material • Insider (airport worker or crew) • Human factor (screeners performance)	• Training of screeners (CBT/ image analysis) • Training of screeners (search techniques) • New screening technology • Enhanced background checks • Surveillance, patrols • Aircraft protection • Aircraft check/search • Security culture (reporting) • Image analysis CBT • Work motivation (and other Human factor elements)	• Fire, smoke & pressurisation	• Least Risk Bomb Location - 25.795 (c) (1) • Flight deck smoke protection - 25.795 (b) (1) • Passenger cabin smoke protection – 25.795 (b) (2) • Survivability of systems – 25.795 (c) (2) • Chemical oxygen generators – 25.795 (d) • Interior design facilitating search – 25.795 (c) (3) • Lavatory door unlockable from the outside – 25.820 • Compartment ventilation – 25.831 (b) • Controls of cabin pressure – 25.841 (b) • Fire extinguishers – 25.851 (a) • Fire protection (lavatories, flight controls, other flight structures) – 25.865 • Materials used in compartment – 25.853 (a) (c) • Flight crew alerting system – 25.1322
4	• **1.3** IED introduced in services and flight supplies	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Security controls for in-flight supplies • Screening of in-flight supplies • Protection of in-flight supplies • Access control	• IED not assembled • Sophisticated concealment • Non-organic explosive material • Insider • Human factor (screeners performance)	• Training of screeners (CBT/ image analysis) • New screening technology • Enhanced background checks • Surveillance, patrols • Aircraft protection • Aircraft check/search • Security culture/ reporting • Work motivation	• Fire, smoke & pressurisation	• Least Risk Bomb Location – 25.795 (c) (1) • Flight deck smoke protection – 25.795 (b) (1) • Passenger cabin smoke protection – 25.795 (b) (2) • Survivability of systems – 25.795 (c) (2) • Chemical oxygen generators – 25.795 (d) • Interior design facilitating search – 25.795 (c) (3) • Lavatory door unlockable from the outside – 25.820 • Compartment ventilation – 25.831 (b) • Controls of cabin pressure – 25.841 (b) • Fire extinguishers – 25.851 (a) • Fire protection (lavatories, flight controls, other flight structures) – 25.865 • Materials used in compartment – 25.853 (a) (c) • Flight crew alerting system 25.1322
Threat type II: IED in hold / cargo compartment						
2	• **2.1** IED in cargo (mail)	• Screening of cargo • Protection of cargo	• Sophisticated concealment • Non-organic explosive material • Insider	• Training of screeners (CBT/ image analysis)	• Fire, smoke & pressurisation	• Cargo compartment fire suppression – 25.795 (b) (3) • Survivability of systems – 25.795 (c) (2)

#	Threat scenario	Security measures	Threat escalating factors	Threat escalating factor barriers	Top event	Mitigation measures – CS.25 reference
		• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Access control	• Human factor	• Training of screeners (search techniques) • New screening technology • Enhanced background checks • Surveillance, patrols • Security culture (reporting) • Work motivation		• Cargo compartment fire and smoke detection – 25.857 • Fire protection (lavatories, flight controls, other flight structures) – 25.865
3	• **2.3** IED in hold baggage	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Screening of hold baggage • Protection of hold baggage • Access control	• Sophisticated concealment • Non-organic explosive material • Insider • Human factor	• Training of screeners (CBT/ image analysis) • Training of screeners (search techniques) • New screening technology • Enhanced background checks • Surveillance, patrols • Security culture(reporting) • Work motivation	• Fire, smoke & pressuri-sation	• Cargo compartment fire suppression – 25.795 (b) (3) • Survivability of systems – 25.795 (c) (2) • Cargo compartment fire and smoke detection – 25.857 • Fire protection (lavatories, flight controls, other flight structures) – 25.865
Threat type III: Impact of an object (in the air)						
5	• RPAS	• Registration of UAS operator • Registration of UAS (Certified Category) • Operational declarations by the UAS operators • Accreditation to use*) • Zonal restrictions and prohibitions to use UAS *) *) as no standards exist in the Reg 1998/2015 these are based on Regulation (EU) 2019/947 and ICAO Guidance (8973 and Protection of Civil Aviation Infrastructure against Unmanned Aircraft)	• Militarized drones • Conflict zones • GNSS jamming/spoofing	• Risk Assessments**) • EASA Conflict Zone Alerting System**) • Conflict Zones Information Bulletin **) **) there are no standards in the Reg 1998/2015 however preventive barriers can be build based on risk assessments carried by organisations based on these elements and following the Integrated European Aviation Security Risk Assessment Group methodology and information sharing	• Aircraft upset (Loss of Control)	• Fuel tank inerting system – 25.975 • Design for emergency landing – 25.561 (a) (b) (c) (d) • Design for emergency landing – 25.562 (a) (b)
7	• MANPADS	• *) no specific standards exist however Annex 17 4.3.6 requires States to implement measures on the ground or operational procedures in accordance with the risk assessment	Conflict zones	Same as above	• Aircraft upset (Loss of Control)	• Fuel tank inerting system – 25.975 • Design for emergency landing – 25.561 (a) (b) (c) (d) • Design for emergency landing – 25.562 (a) (b)

#	Threat scenario	Security measures	Threat escalating factors	Threat escalating factor barriers	Top event	Mitigation measures – CS.25 reference
Threat type IV: Impact of an object (on the ground)						
5	• RPAS	• Registration of UAS operator • Registration of UAS (Certified category) • Operational declarations by the UAS operators • Accreditation to use • Zonal restrictions and prohibitions to use UAS *) these are based on ICAO Guidance (8973 and Protection of Civil Aviation Infrastructure against Unmanned Aircraft)			• Ground damage	
9	• Vehicle-borne IED	• Access control • Examination of vehicles • Screening of persons other than passengers • Screening of items carried by persons other than passengers	• Insider • Human factor (screener performance)	• Enhanced background checks • Surveillance, patrols • Security culture(reporting) • Work motivation	• Ground damage	• Fuel tank inerting system – 25.975
10	• Vehicle attack	• Access control • Examination of vehicles	• Insider • Human factor (screener performance)	• Enhanced background checks • Surveillance, patrols • Security culture(reporting) • Work motivation	• Ground damage	• Fuel tank inerting system – 25.975
11	• IED, UGV-borne	• Access control	• Insider	• Enhanced background checks • Surveillance, patrols • Security culture(reporting)	• Ground damage	• Fuel tank inerting system – 25.975
Threat type V: CBR threats						
13 14	• Chemical Biological or Radiological attack	• *) no specific standards exist however these are Dangerous Goods and transport of them shall be prevented and measures below may contribute: • Screening of persons other than passengers • Screening of items carried by persons other than passengers • Screening of passengers • Screening of cabin baggage	• Equipment detection limitations • Similarity to harmless objects	• Training of screeners (search techniques)	• Other injuries	• Compartment ventilation – 25.831 (b)
Threat type VI: Aircraft used as a weapon						

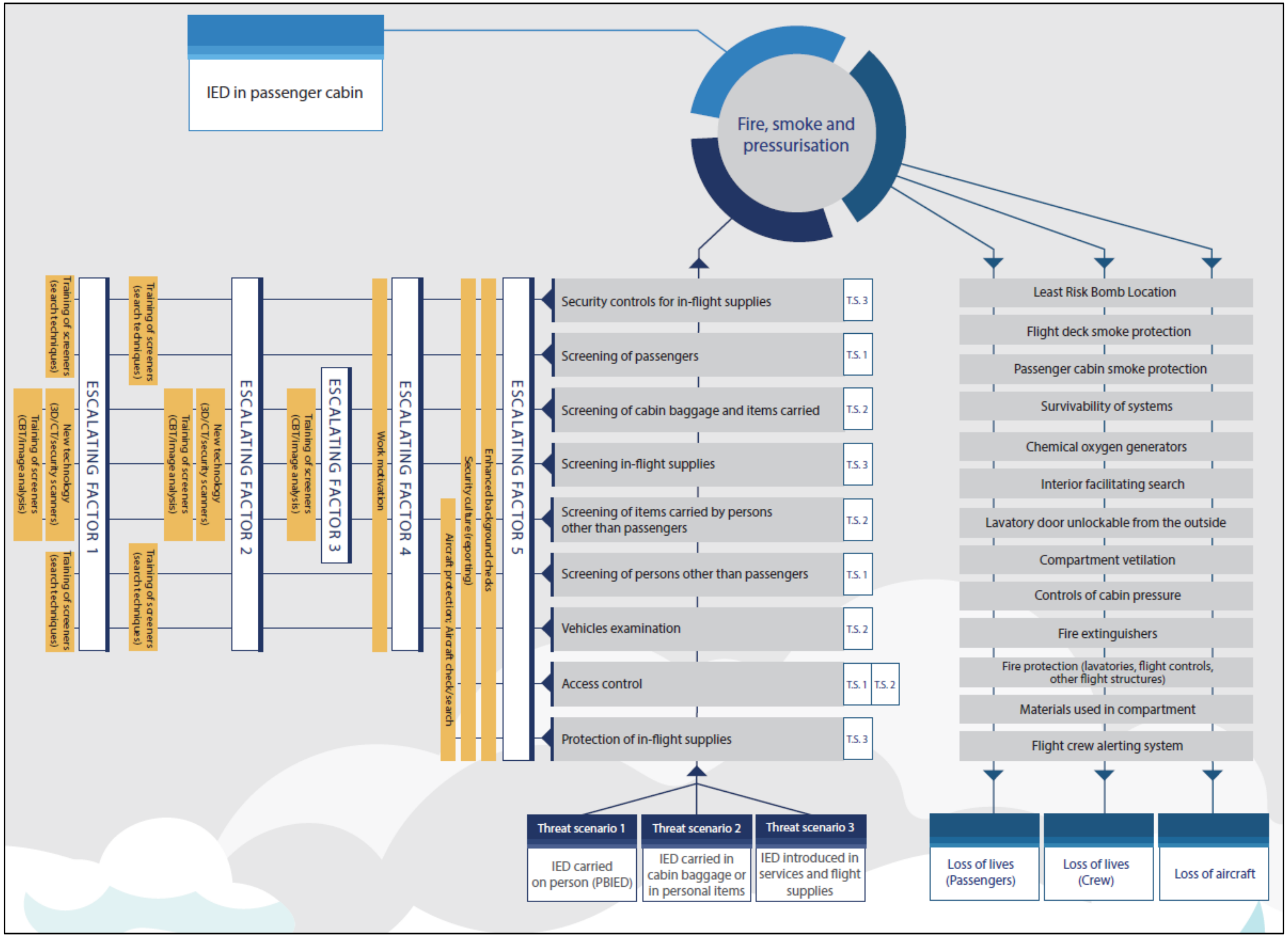
#	Threat scenario	Security measures	Threat escalating factors	Threat escalating factor barriers	Top event	Mitigation measures – CS.25 reference
15	• Aircraft used as weapon	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Screening of passengers • Screening of cabin baggage In-flight security officers	• Insider	• Enhanced background checks • Security culture(reporting)	• Obstacle collision in flight	• Secure flight deck door – 25.795 (a) • Design facilitating search – 25.795 (c) (3)
Threat type VII: Conventional hijack						
16	• Conventional hijack (taking hostages and making demands)	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Screening of passengers • Screening of cabin baggage In-flight security officers	• Insider	• Enhanced background checks • Security culture(reporting)	• Other injuries	• Secure flight deck door – 25.795 (a) • Design facilitating search – 25.795 (c) (3) • Precautions to intentional opening the door during flight – 25.783 (b)
Threat type: VIII: Other threat items in the cabin						
17	• Prohibited article onboard	• Screening of persons other than passengers • Screening of items carried by persons other than passengers • Aircraft check/search	• Insider	• Enhanced background checks • Security culture(reporting)	• Other injuries	• Chemical oxygen generators – 25.795 (d) • Opening in pressurised compartment – 25.365 (e) (f) • Secure flight deck door – 25.795 (a)
18	• Attack with improvised weapon	• In-flight security officers			• Other injuries	• Chemical oxygen generators – 25.795 (d) • Opening in pressurised compartment – 25.365 (e) (f) • Secure flight deck door – 25.795 (a)
Threat type IX: Sabotage						
23	• Intentional placement of FOD by insider	• Surveillance and patrols			• Aircraft upset	• Air intake – 25.1091
24	• Damage or destruction of aircraft part/system	• Enhanced background checks • Security culture (reporting)			• Aircraft upset	• Crew alerting system – 25.1322
Threat type X: IUEI against aircraft system functions						
33	• DAL A and B system functions s not available (controllable or responding)	• Risk-based measures meeting relevant SAL Objectives based on CS-25.1319 with security controls developed based on e.g.	• Insider • Human factor • Compromising systems in flight • System interfaces	• Cyber hygiene • Cybersecurity culture • Awareness • Training • Enhanced background checks	• Aircraft upset	• Installed systems and equipment – 25.1302 • Flight and navigation instruments – 25.1303 • Equipment, systems and installations – 25.1309 • Equipment, systems and network information protection – 25.1319

#	Threat scenario	Security measures	Threat escalating factors	Threat escalating factor barriers	Top event	Mitigation measures – CS.25 reference
		NIST 800-53, ED-204, including but not limited to: • Administrative controls • Logical or technical controls • Physical controls • Quality control		• Separation on domains • Supply chain information security		• Flight Crew Alerting – 25.1322 • Flight Instruments external probes heating system alert – 25.1326 • Direction indicator – 25.1327 • Flight Guidance System 25.1329 • Instruments using power supply – 25.1331 • Instruments system – 25.1333 • Electrical systems, equipment and installations – 25.1351, 25.1353 • Operating procedures - 25.1585 • Performance information – 25.1587
33	• DAL A and B systems' data integrity tampered	• Risk-based measures meeting relevant SAL Objectives based on CS-25.1319 with security controls developed based on e.g. NIST 800-53, ED-204, including but not limited to: • Administrative controls • Logical or technical controls • Physical controls • Quality control	• Insider • Human factor • Compromising systems in flight • System interfaces	• Cyber hygiene • Cybersecurity culture • Awareness • Training • Enhanced background checks • Separation on domains • Supply chain information security	• Aircraft upset	• Installed systems and equipment – 25.1302 • Flight and navigation instruments – 25.1303 • Equipment, systems and installations – 25.1309 • Equipment, systems and network information protection – 25.1319 • Flight Crew Alerting – 25.1322 • Flight Instruments external probes heating system alert – 25.1326 • Direction indicator – 25.1327 • Flight Guidance System 25.1329 • Instruments using power supply – 25.1331 • Instruments system – 25.1333 • Electrical systems, equipment and installations – 25.1351, 25.1353 • Operating procedures - 25.1585 Performance information – 25.1587 Appendix H25.6

5.1. Bowtie analysis

In this section, the bowties for the chosen threats and threat scenarios (see again Table 5) are presented. Next to each diagram, the escalating factors (EFs) are described.

5.1.1. Threat type I


IED in passenger cabin
Fire, smoke and pressurisation
Security controls for in-flight supplies
T.S. 3
Screening of passengers
T.S. 1
Screening of cabin baggage and items carried
T.S. 2
Screening in-flight supplies
T.S. 3
Screening of items carried by persons other than passengers
T.S. 2
Screening of persons other than passengers
T.S. 1
Vehicles examination
T.S. 2
Access control
T.S. 1
T.S. 2
Protection of in-flight supplies
T.S. 3
Threat scenario 1
IED carried on person (PBIED)
Threat scenario 2
IED carried in cabin baggage or in personal items
Threat scenario 3
IED introduced in services and flight supplies
Least Risk Bomb Location
Flight deck smoke protection
Passenger cabin smoke protection
Survivability of systems
Chemical oxygen generators
Interior facilitating search
Lavatory door unlockable from the outside
Compartment vetilation
Controls of cabin pressure
Fire extinguishers
Fire protection (lavatories, flight controls, other flight structures)
Materials used in compartment
Flight crew alerting system
Loss of lives (Passengers)
Loss of lives (Crew)
Loss of aircraft
ESCALATING FACTOR 1
Training of screeners (search techniques)
New technology (3D/CT/security scanners)
Training of screeners (CBT/image analysis)
Training of screeners (search techniques)
ESCALATING FACTOR 2
Training of screeners (search techniques)
New technology (3D/CT/security scanners)
Training of screeners (CBT/image analysis)
Training of screeners (search techniques)
ESCALATING FACTOR 3
Training of screeners (CBT/image analysis)
ESCALATING FACTOR 4
Work motivation
ESCALATING FACTOR 5
Enhanced background checks
Security culture (reporting)
Aircraft protection; Aircraft check/search

Escalating Factors (EF) description:

EF 1: IED not assembled

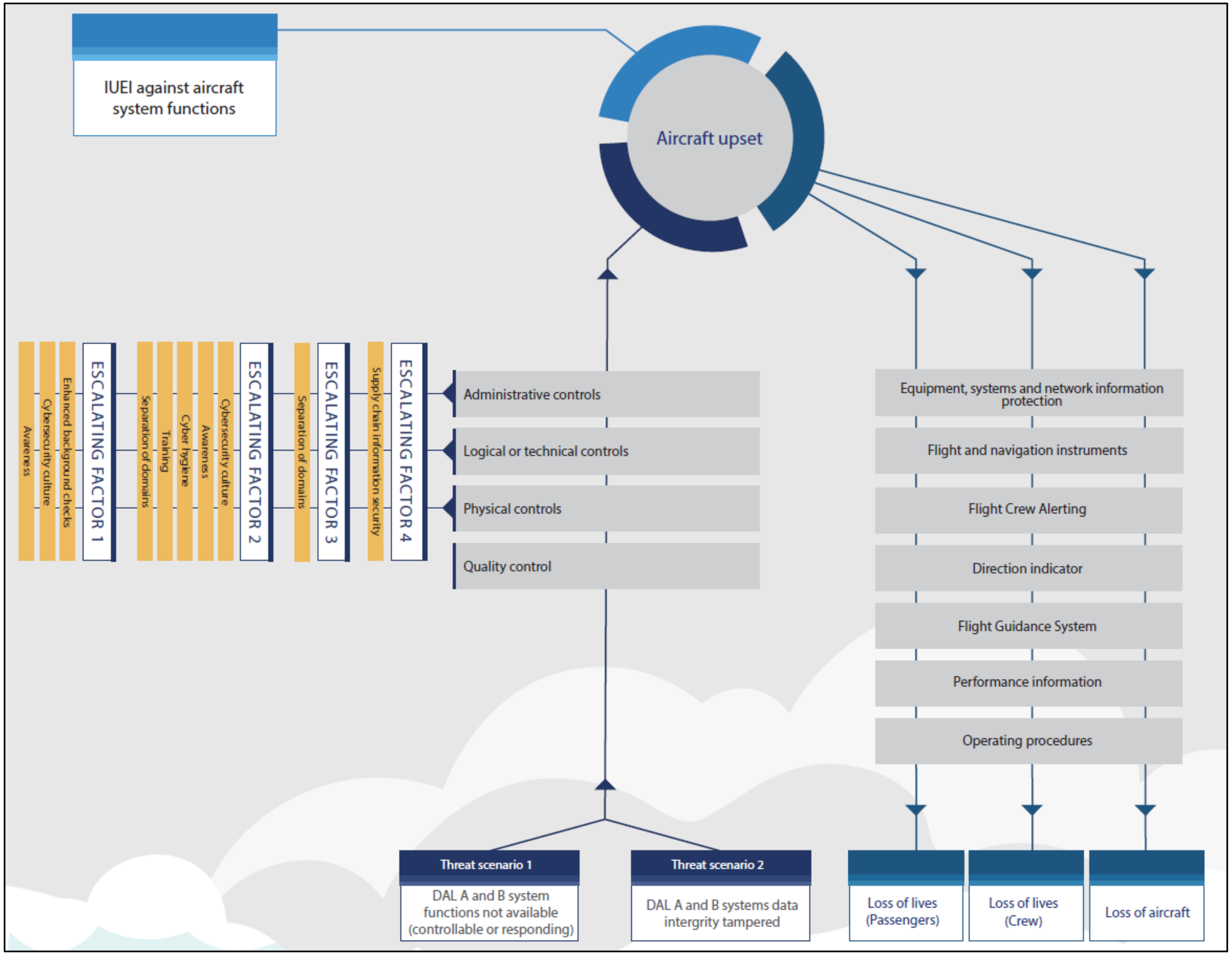
EF 2: Sophisticated concealment

EF 3: Non-organic materials

EF 4: Human factors (screener performance)

EF 5: Insider

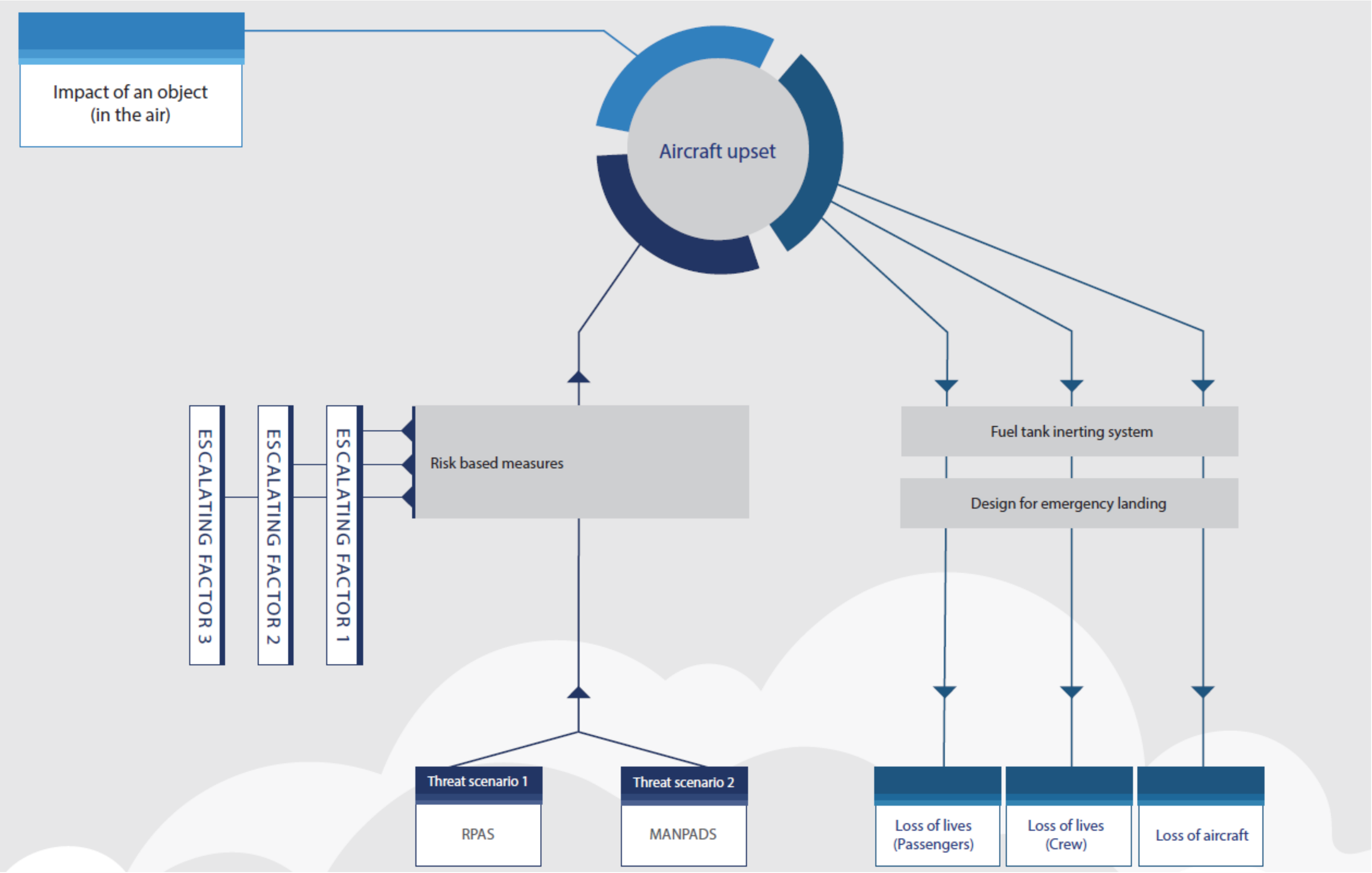
5.1.2. Threat type II



Escalating Factors (EF) description:

EF 1: Sophisticated concealment
EF 2: Non-organic materials
EF 3: Human factors (screener performance)
EF 4: Insider

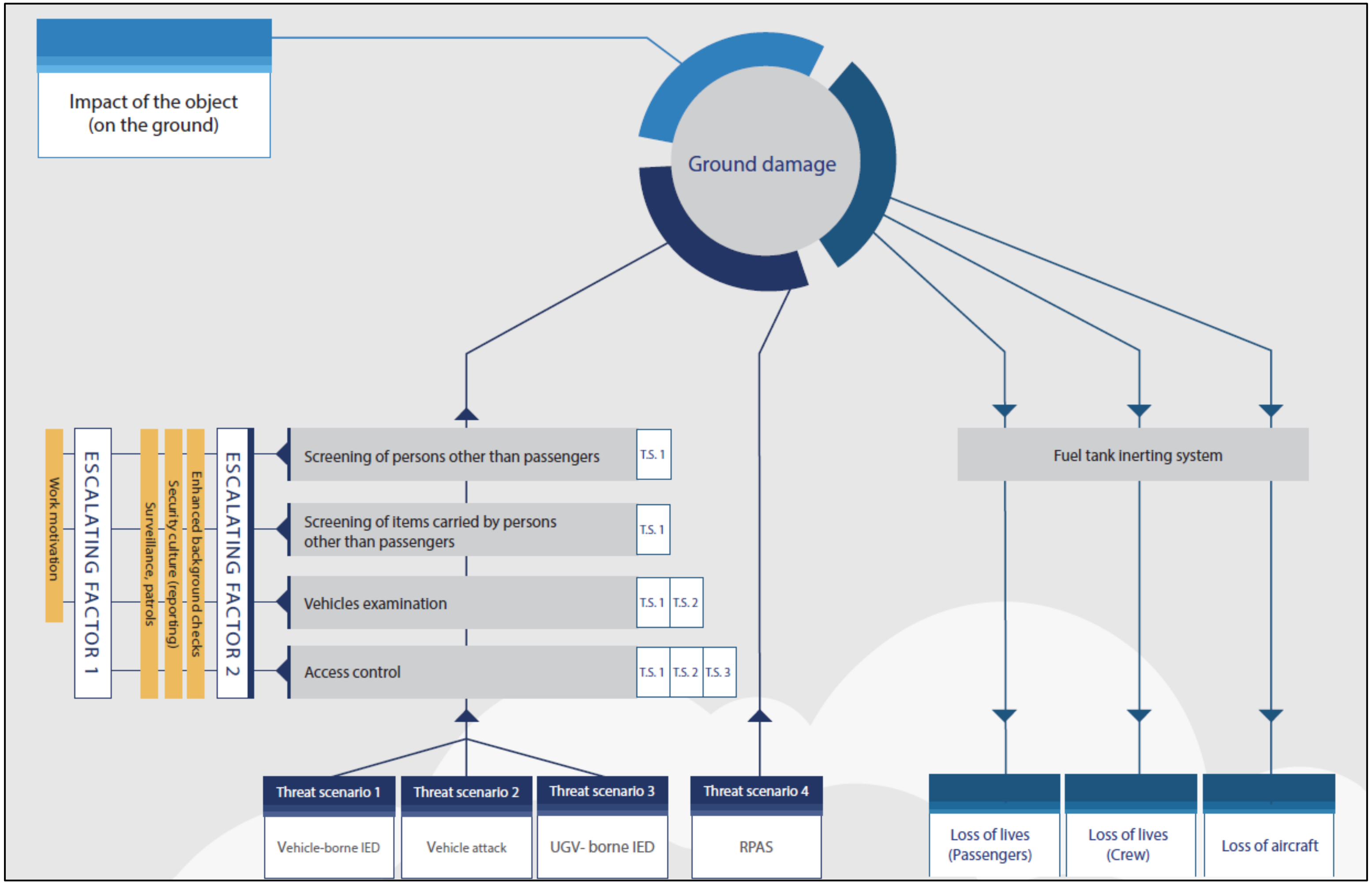
5.1.3. Threat type III



Escalating Factors (EF) description:

EF 1: Conflict zones
EF 2: Weaponized drones
EF 3: GNSS spoofing / jamming

5.1.4. Threat type IV

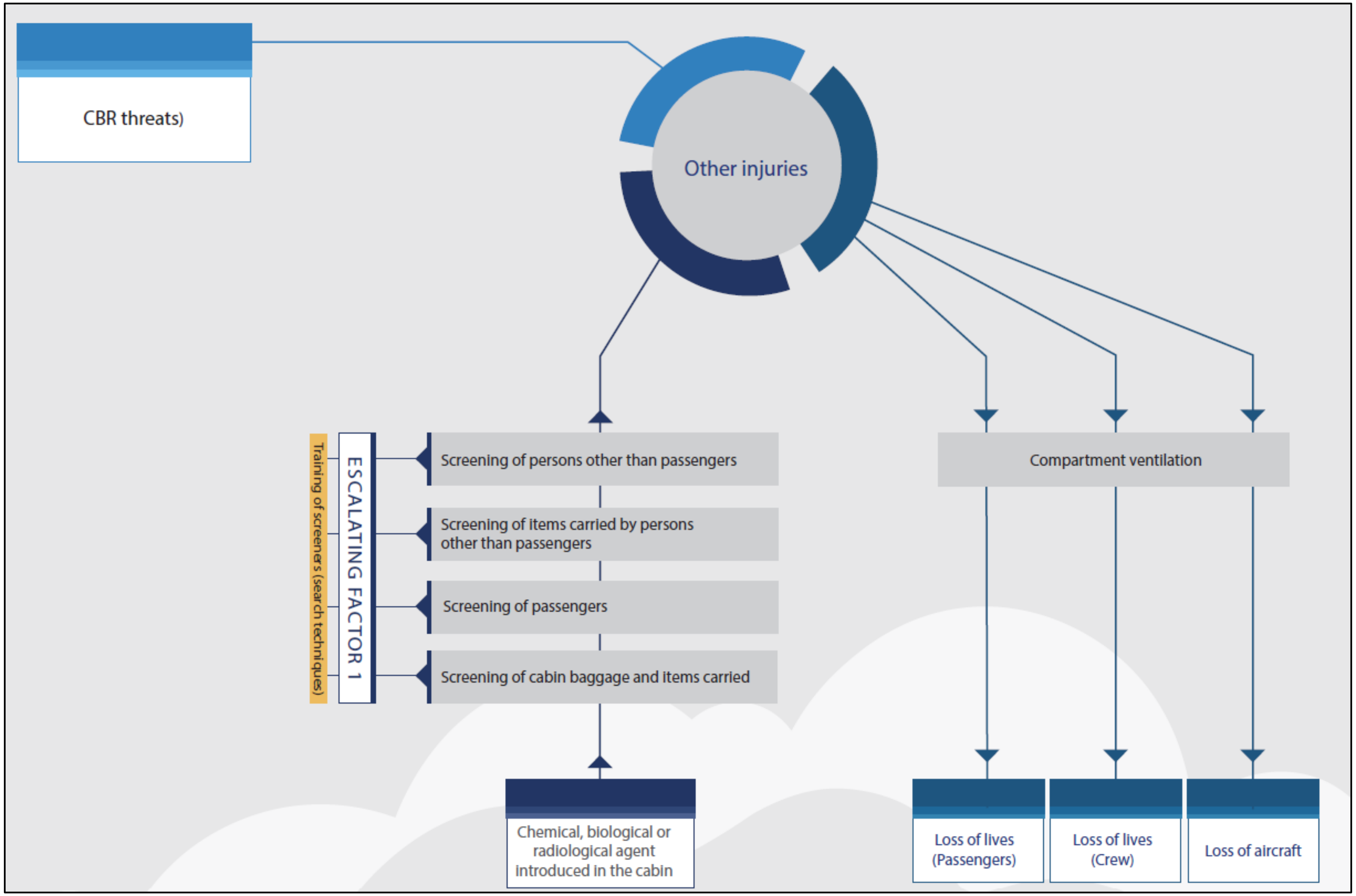


Escalating Factors (EF) description:

EF 1: Human factors (screener performance)

EF 2: Insider

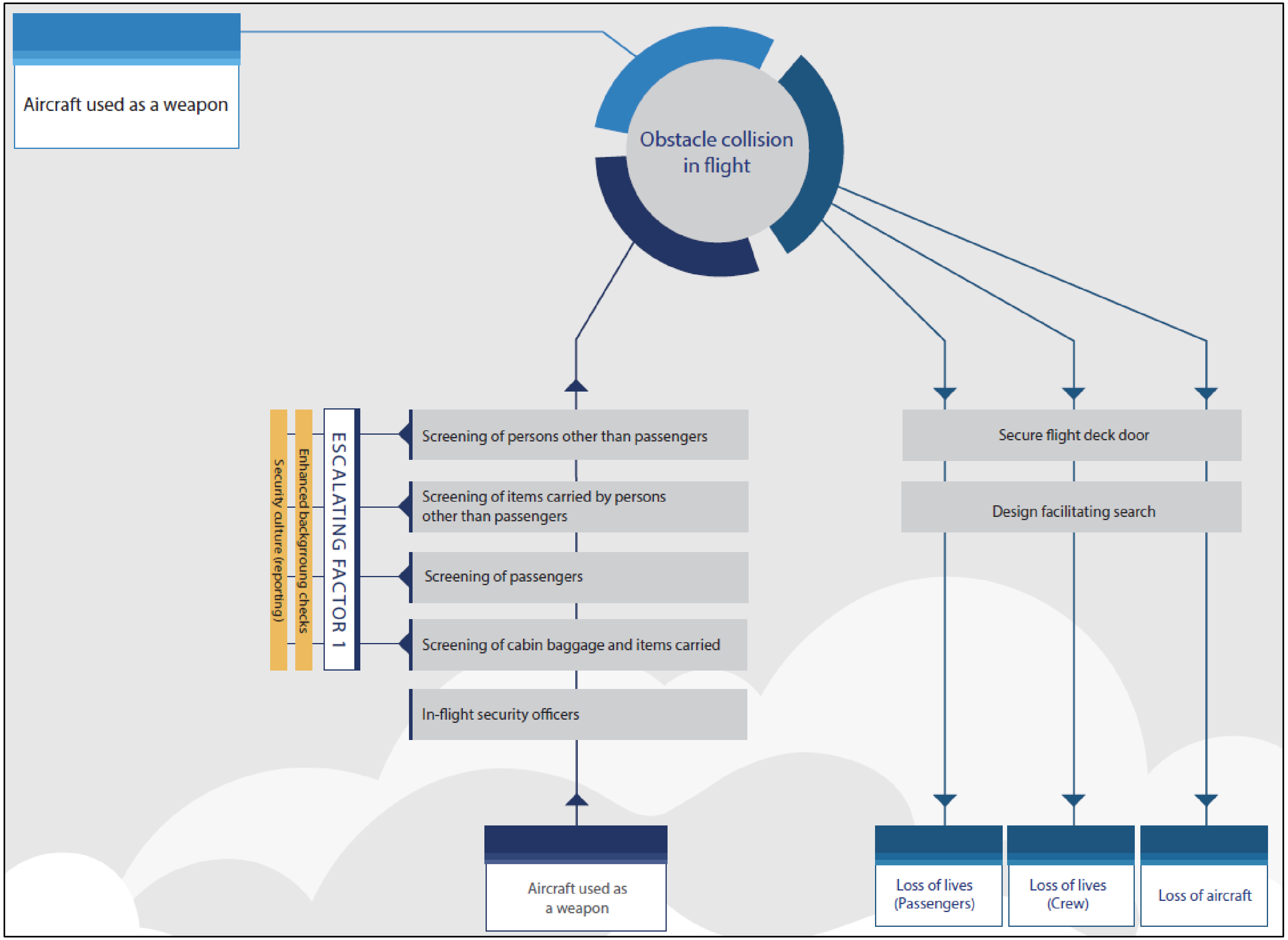
5.1.5. Threat type V


CBR threats)
Other injuries
Training of screeners (search techniques)
ESCALATING FACTOR 1
Screening of persons other than passengers
Screening of items carried by persons other than passengers
Screening of passengers
Screening of cabin baggage and items carried
Compartment ventilation
Chemical, biological or radiological agent introduced in the cabin
Loss of lives (Passengers)
Loss of lives (Crew)
Loss of aircraft

Escalating Factors (EF) description:

EF 1: Equipment detection limitations

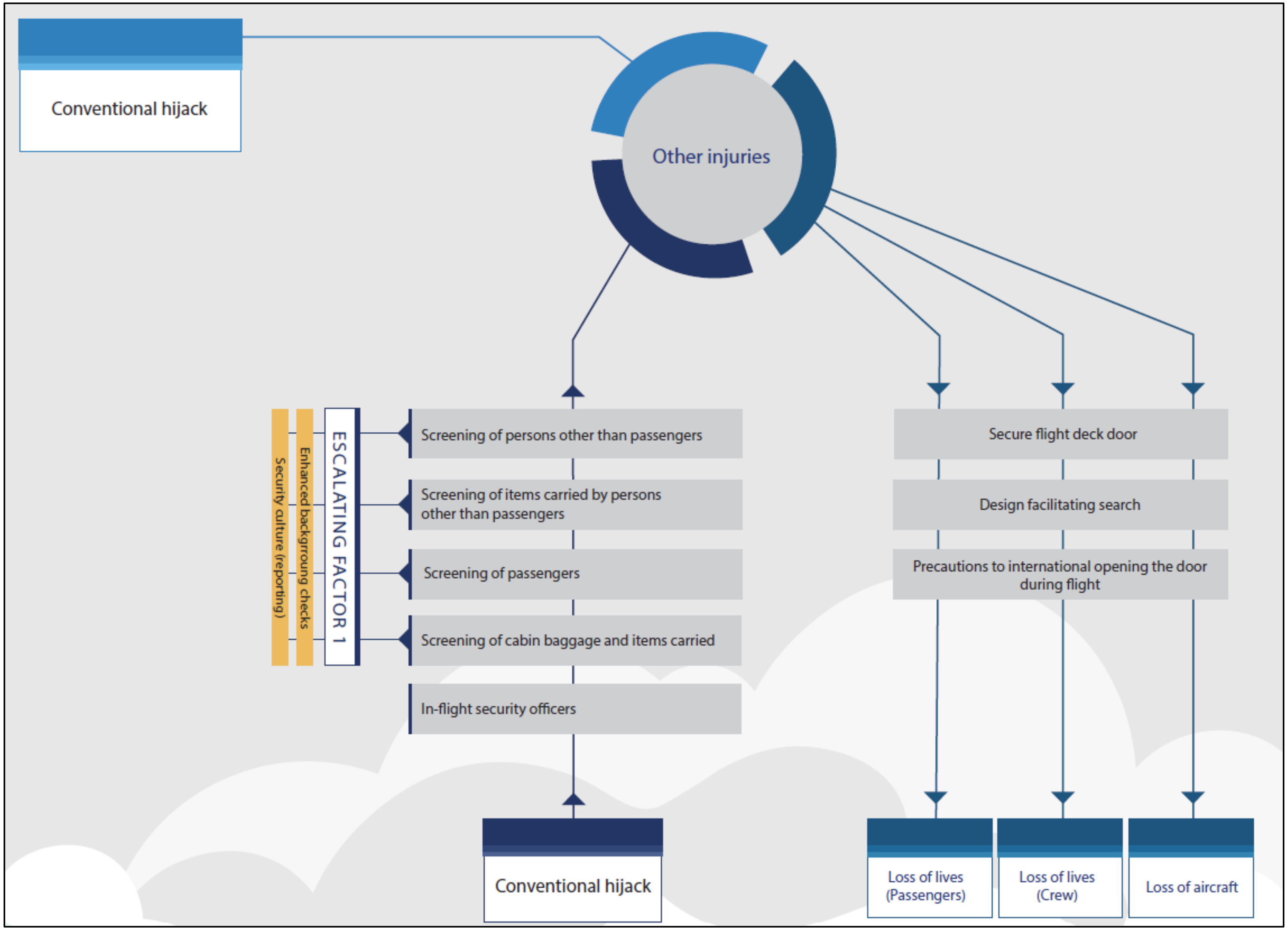
5.1.6. Threat type VI


Aircraft used as a weapon
Obstacle collision in flight
ESCALATING FACTOR 1
Enhanced backgroung checks
Security culture (reporting)
Screening of persons other than passengers
Screening of items carried by persons other than passengers
Screening of passengers
Screening of cabin baggage and items carried
In-flight security officers
Aircraft used as a weapon
Secure flight deck door
Design facilitating search
Loss of lives (Passengers)
Loss of lives (Crew)
Loss of aircraft

Escalating Factors (EF) description:

EF 1: Insider

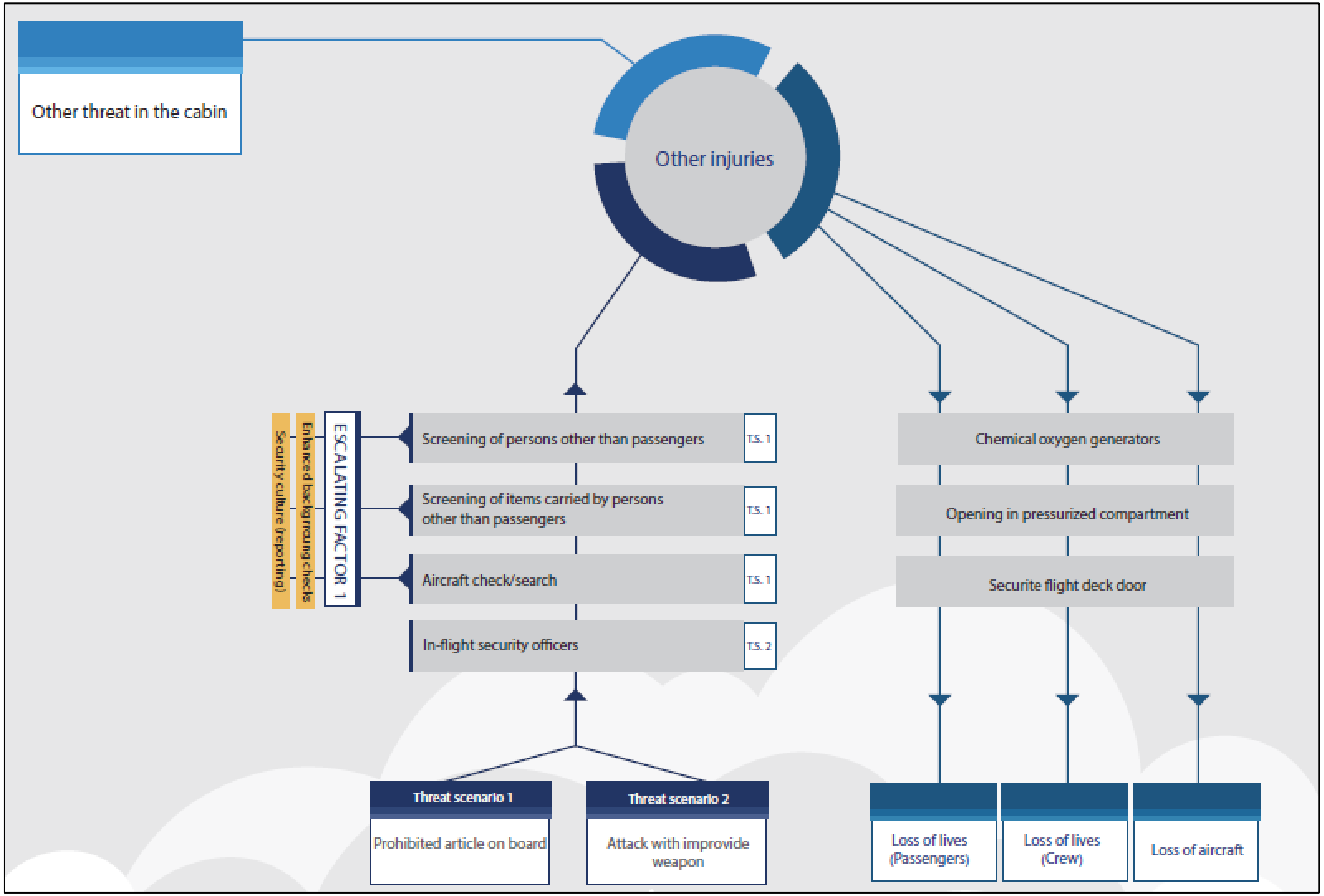
5.1.7. Threat type VII


Conventional hijack
Other injuries
ESCALATING FACTOR 1
Enhanced backgroung checks
Security culture (reporting)
Screening of persons other than passengers
Screening of items carried by persons other than passengers
Screening of passengers
Screening of cabin baggage and items carried
In-flight security officers
Secure flight deck door
Design facilitating search
Precautions to international opening the door during flight
Conventional hijack
Loss of lives (Passengers)
Loss of lives (Crew)
Loss of aircraft

Escalating Factors (EF) description:

EF 1: Insider

5.1.8. Threat type VIII

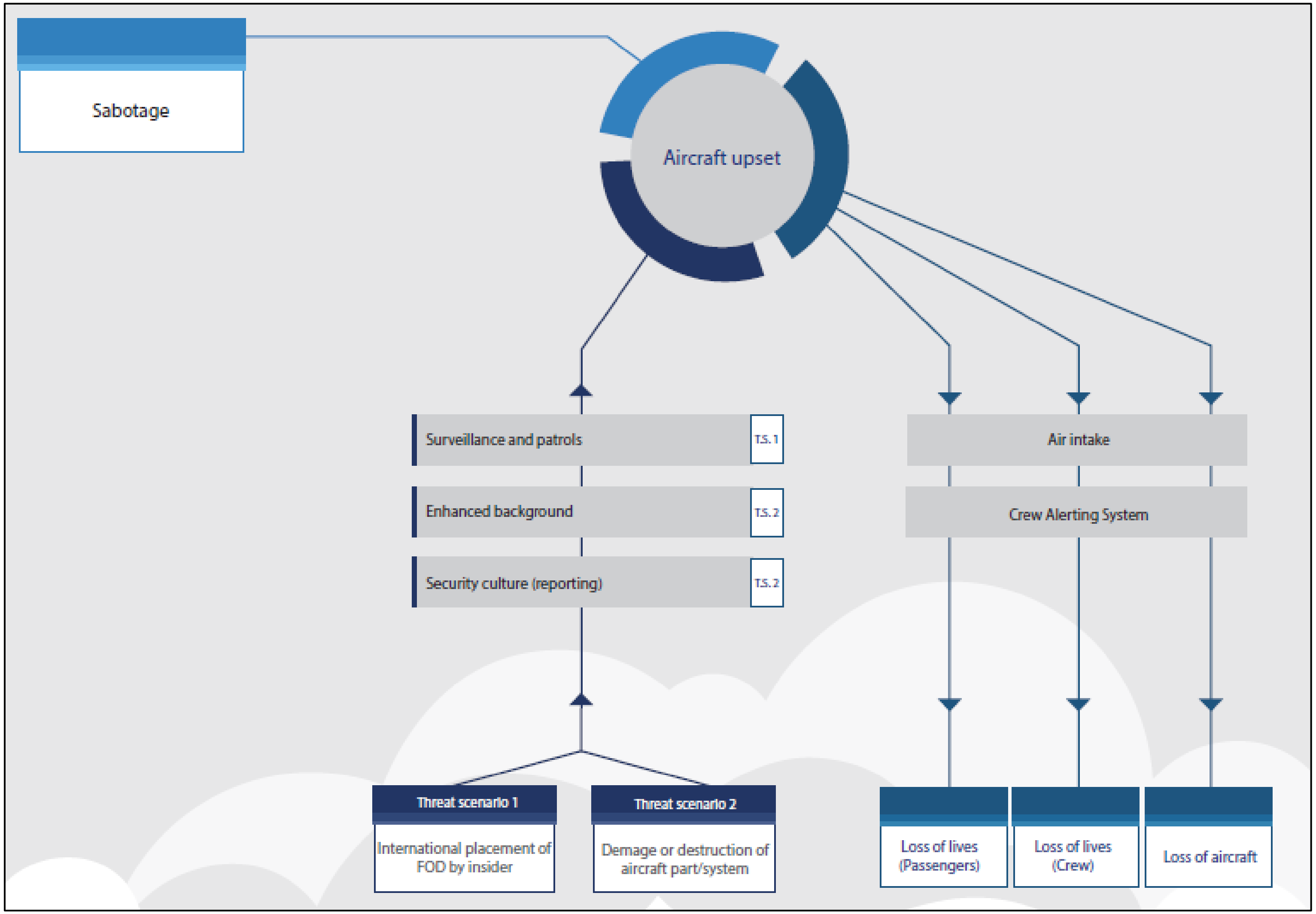


Other threat in the cabin
Other injuries
Security culture (reporting)
Enhanced background checks
ESCALATING FACTOR 1
Screening of persons other than passengers
T.S. 1
Screening of items carried by persons other than passengers
T.S. 1
Aircraft check/search
T.S. 1
In-flight security officers
T.S. 2
Chemical oxygen generators
Opening in pressurized compartment
Securite flight deck door
Threat scenario 1
Prohibited article on board
Threat scenario 2
Attack with improvide weapon
Loss of lives (Passengers)
Loss of lives (Crew)
Loss of aircraft

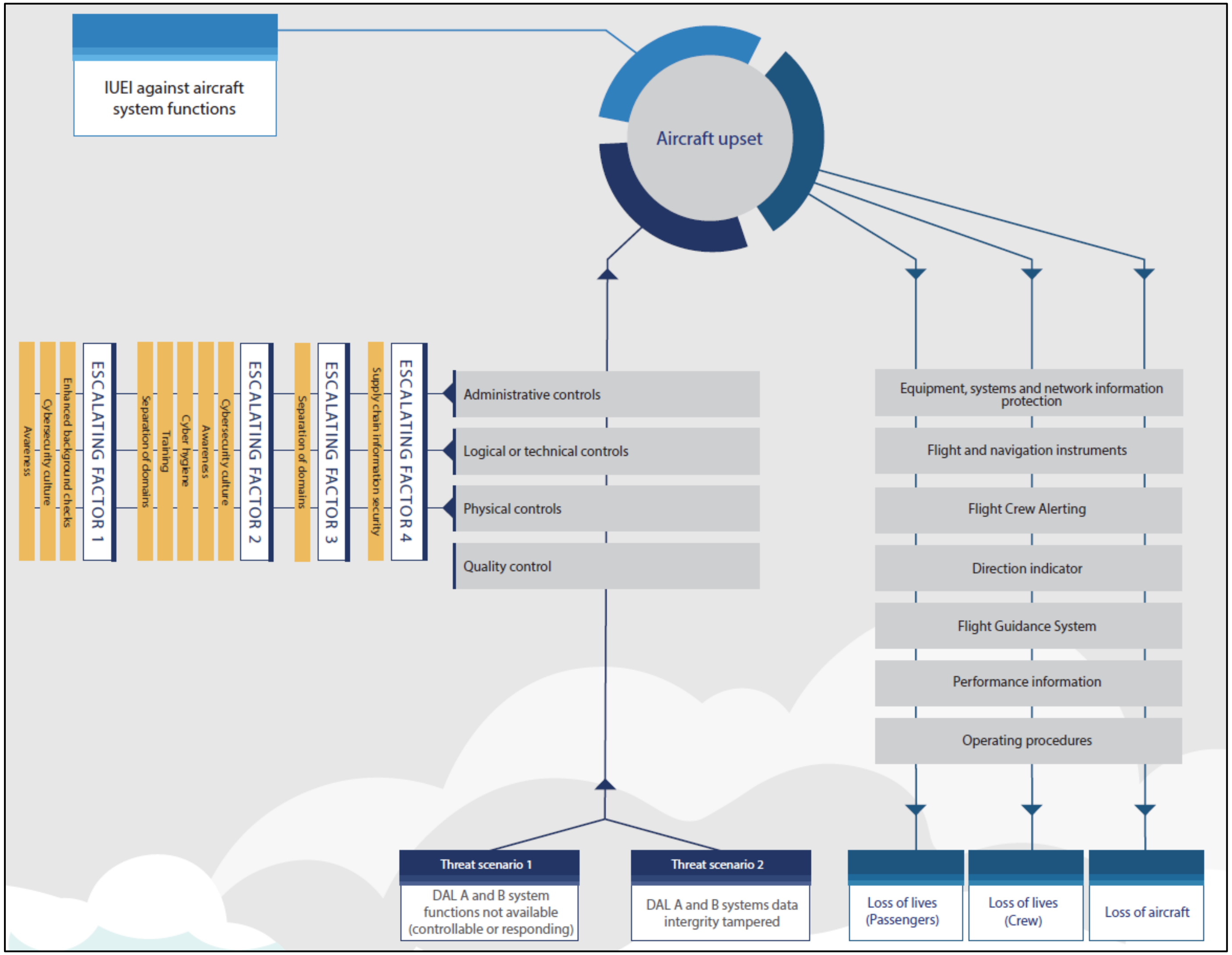
Escalating Factors (EF) description:

EF 1: Insider

5.1.9. Threat type IX



5.1.10. Threat type X



Escalating Factors (EF) description:

EF 1: Insider

EF 2: Human factor

EF 3: Compromising systems in-flight

EF 4: System interfaces

5.2. Relevance of aircraft design requirements

This section summarizes the analysis of aircraft design requirements from the perspective of their relevance in mitigating physical and information security threats. It also investigates if it is possible to conduct a gap analysis in that scope and to what degree it could cover aircraft design standards. The input to this section was based on:

- Analytical work described in the previous section
- Consultation with stakeholders
- Interviews with subject matter experts

Initially the desire has been to focus only on gaps related to aircraft design standards. Consultation with stakeholders described in section 5.2.1 and analysis of preventive security measures in combination with aircraft design specifications indicated however, this may not be the most practical and supported approach as the aircraft design may not necessarily be most relevant placeholder to address specific issues.

5.2.1. Input collection (stakeholders' consultation) related to relevance and gaps

Stakeholders' engagement in the scope of this task included surveys, workshops and dedicated interview sessions. In terms of situational security assessment, participants were asked to rate the degree of confidence in the system given existing security measures (preventions) and aircraft design-based mitigations.

The research used the list of types of threats from Table 3 as a reference for the survey. Main conclusions from consulting stakeholders were:

- There is a high level of recognition of risks embedded in the aviation sector as system was assessed vulnerable (with gaps of different degree) in case of every threat. The percentage of respondents who replied that some gaps exist in relation to threat types ranged between 32% and 79%
- Major gaps were less often indicated for traditional and known threats especially if they have a larger catalogue of preventive security measures compared to rather novel threats with less developed catalogue of preventive security measures. In this context threat types I, II, IV, VI, VII and VIII were assessed through the survey less often as having major gaps compared to threat types III, V, and X where replies indicating major gaps ranged between 29 and 55%.

Also, an overwhelming majority agreed with the following statements:

- The aircraft shall not be considered the "first line of defence" in preventing security threats (almost 80% of respondents agreed with this statement)
- Security measures should be primary implemented "on the ground" not in the aircraft (over 90% respondents agreed with this statement)

The survey also showed that although there was no evident correlation between indicated level of perceived gap for particular threat types and a number of applicable aircraft-design standards directly or indirectly related to security, stakeholders recognized interdependencies between safety and security evidence. The vast majority of them actually agreed with the following statements:

- Some aircraft design requirements, even if not directly required due to security reasons can help in handling the situation caused by the threat (over 90% of respondents agreed with this statement)
- Aircraft design requirements introduced due to safety reasons can contribute to mitigate security threats (almost 90% of respondents agreed with this statement)

5.2.2. Relevance assessment and gap analysis

The research team investigated further the consideration that aircraft should be more "beneficiary" of the secure environment rather than "contributor".

One of the main reasons according to consulted entities seem to be related to the general concept of the design process of the aircraft and how this process needs to account for many different factors and still deliver the aircraft according to its mission requirements.

Security threats are analysed and monitored by aircraft manufacturers and adequate solutions are designed either in accordance with provided AMCs or in an alternative method providing for the equivalent level of security, however:

- 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. It is also in line with the philosophy that "security is everyone's responsibility" and applying preventions on the ground may be more efficient than designing measures in the aircraft.
- Security spreads throughout the entire system so in most cases preventions should be implemented in the surrounding of an aircraft. This is also related to the duration of the aircraft design process itself, and the fact that any retrofitting for aircraft already in operations would have much bigger impact compared to implementation of measures on the ground.[24]Aircraft design alone will not achieve the goal of improved security system if existing procedural aspects are not taken into consideration as preventions and/or mitigations by aircraft operators. In this context an example could be the of *Interior design to facilitate searches* (CS-25.795 (c) 3). Design itself is only a baseline element, which needs to be followed by properly designed aircraft operator procedures indicating areas requiring search supported by robust training which will equip personnel implementing that procedure with necessary knowledge and competences.
- In terms of information security threats security measures are implemented as an outcome of the risk assessment and relevant continuous airworthiness instructions are provided to operators[25]. Relevant security measures shall be considered throughout the entire chain as barriers will only be as effective as the weakest link in the system. An example of this is loadable software procedure and protections applied for the servers where updates might be stored between the point in time they are provided by the aircraft manufacturer and uploaded onto the aircraft.

Research did not identify specific gaps in the aircraft design requirements specifically, therefore the research adopted a more holistic approach and investigated gaps in overall aviation security related to certain threat types. The focus has been on threat types I, II, III, V and X due to their critical impact on aircraft structure or its occupants.

Table 6 therefore contains results of this analysis.

[24] According to the Federal Aviation Administration (FAA) the retrofitting cost per aircraft for reinforced cockpit door after 9-11 attacks ranged between 12,000 and 17,000 USD, covering door reinforcement and integration with cockpit security protocols. The total expense for the U.S. fleet alone was projected to reach between 92.3 and 120.7 million USD over a decade, including installation and minor increases in fuel consumption due to the added weight of the reinforced doors, https://en.wikipedia.org/wiki/Airport_security_repercussions_due_to_the_September_11_attacks

[25] Airbus provides Security Handbook and Boeing provides Airplane Network Security Operator Guidance (ANSOG)

Table 6: Gap analysis of security landscape related to certain threat types

Threat type	Current state	Gap(s)	Relevance of existing aircraft design requirements	Further recommendations on future state
Threat type I	Preventive security measures in place allow to detect threats through application of: - access control - screening of passengers and cabin baggage - screening of staff and items carried - vehicles examination	Certain threats have lower chance of being detected due to: - limitations of the equipment - screeners performance - insiders There is a potential of using non-prohibited articles which are Dangerous Goods to cause safety threatening situation during the flight in the passenger cabin	Design of aircraft assumes appropriate security level is ensured by application of measures on the ground. Specifications related to LRBL and physical separation of systems are designed to limit the effects of an explosive or incendiary device and provide for survivability of systems necessary for safe flight and landing. They are supported by additional specifications relevant in case of smoke, fumes or decompression.	Additional design standards in that scope would be considered disproportionate. Moreover, any additional security specifications should be considered through perspective of potential detrimental effect on safety. Instead consideration should be to reinforce: - competencies of screeners in detecting threats - prevention of insiders - prevention of transport of undeclared or misdeclared Dangerous Goods - detection technology development to support screeners' decision-making process
Threat type II	Preventive security measures in place allow to detect threats through application of: - access control - screening of hold baggage and cargo - screening of staff and items carried - protection of hold baggage and cargo	Certain threats have lower chance of being detected due to: - limitations of the equipment - screeners performance - insiders There is a potential of using non-prohibited articles which are Dangerous Goods to cause safety threatening situation during the flight especially, if insider exploits Regulated Agent security controls	Design of aircraft assumes appropriate security level is ensured by application of measures on the ground. Specifications related to cargo compartment fire suppression systems and physical separation of systems are designed to limit the effects of an explosive or incendiary device and provide for survivability of systems necessary for safe flight and landing.	Additional design standards in that scope would be considered disproportionate. Moreover, any additional security specifications should be considered through perspective of potential detrimental effect on safety. Instead consideration should be to reinforce: - competencies of screeners in detecting threats - prevention of insiders - prevention of transport of undeclared or misdeclared Dangerous Goods - detection technology development to support screeners' decision-making process

Threat type	Current state	Gap(s)	Relevance of existing aircraft design requirements	Further recommendations on future state
Threat type III	In terms of UAS there is a system of authorizations, registration and accreditation supported by risk-based measures implemented depending on the risk assessment. Prevention of MANPADS is related to international and national enforcement of arm-controls	There is a deficit of preventive measures in case UAS are intentionally used to cause harm or endanger safety (e.g. weaponized civil drones). Additionally, there is an increased exposure of aircraft to the risk of weaponized or military UAS and MANPAD in case of operations in or near conflict zones.	Certain design specifications can help to mitigate effects of collision between the UAS and the aircraft or MANPAD launched projectile hitting the aircraft but only to the certain degree.	Additional design standards in that scope would be considered disproportionate. It is recommended instead to focus on continuous risk assessment related to operations over zones of military conflicts and in relation to critical phases of flight and implementation of preventive measures on the ground against MANPAD and UAS.
Threat type V	Existing preventive measures related to screening are not targeting these particular threat scenarios.	Increased exposure of passengers and crew to the risk of chemical, biological or radiological agents in the cabin due to equipment	Only aircraft design specification which relates to ensuring that crew and passenger compartment air must be free from harmful or hazardous concentrations of gases or vapours however it refers to carbon monoxide concentrations and as such is related to smoke and fumes in the cabin.	Additional design standards in that scope would be considered disproportionate. It is recommended instead on risk-based measures which can help to prevent intentional introduction of undeclared or misdeclared Class 6 or 7 substances.
Threat type X	Existing measures are risk-based and applicable in the design stage as well as part of continuous airworthiness. They include solutions covering: secondary systems, domain segregation, least-privilege access rights, limiting access points, using	Increased exposure for attacks performed by insiders or targeting data integrity if interfaces and third parties do not apply equally robust security measures (e.g. for temporary storage of software updates between	Risk-based measures implemented follow identification of vulnerable areas within the scope the manufacturer is responsible for. Additionally, manufacturers address the challenge of “supply chain” implementing assurance processes for hardware and	Implementation of new information security regulation (Part-IS) will strengthen information security posture of all stakeholders enforcing introduction of systemic solutions and implementation of relevant security measures. Compliance burden could be eased by developing conformity matrix between different regulations helping to avoid duplicated efforts or contradictions. Entities involved

Threat type	Current state	Gap(s)	Relevance of existing aircraft design requirements	Further recommendations on future state
	several technology concepts for duplicated systems. Aircraft manufacturers provide relevant documentation to aircraft operators.	distribution by the manufacturers and uploading to the aircraft). Generally higher level of risk if the attack materialises in-flight. Acceleration of speed between the breach and the negative effect.	software suppliers and provide guidance to operators.	should proactively identify threats to account for its evolution and speed between breach and reaching vulnerable point of the system. Exchange of expertise through building teams of mixed expertise: safety, security, airworthiness and cyber experts to increase situational awareness and capacity

6. Conclusion

This report investigates the critical interdependencies among physical security, information security, and aviation safety, particularly in relation to aircraft design standards.

The report explains how critical the role of robust preventive security measures safeguarding both aircraft operations and passengers is and how measures considered during the aircraft design process contribute to either prevention or mitigation of threat scenarios.

The analysis included the feasibility of conducting a gap analysis of aircraft design specifications in this context. It relied on analytical work, consultations with stakeholders, and expert interviews which suggested that addressing issues solely through design may not be the most relevant or effective approach. Although interdependencies between design, safety, and security exist, elements such as procedures, training, or communication—outside the project's scope—should also be evaluated for their potential to enhance mitigations. Importantly, the research did not identify any substantial aircraft design specification gaps requiring intervention within this framework.

Each of these domains—security, information security, safety, and design—evolves at its own pace, shaped by distinct factors. For example, aircraft systems have transitioned from isolated, single-purpose components to interconnected, multi-functional systems with extensive internal and external interfaces in a relative short time. This evolution adds complexity to cross-domain coordination and up-to-date knowledge sharing across safety and security domains. At the same time safety benefits from this interconnectivity. Enhanced safety levels, for instance, are supported by faster access to data, allowing for more timely analyses. Also, improvements in aviation security have reduced the urge for major safety-related modifications to aircraft, with only two elements added for last over 20 years – chemical oxygen generators specifications and secondary cockpit barrier[26].

On the threat landscape, both information security and traditional aviation security face the challenge of uncertain threat actor capabilities and intentions, further complicated by geopolitical influences and, in some cases, the involvement of state actors. This underscores the importance of continuous vulnerability assessment in information security, particularly to anticipate and address "unknown-unknowns" before they materialise as threats. However, this should take into account the duration of design and certification process and challenges, any modifications, to once agreed specifications, can trigger (necessity to re-evaluate, including the impact of security solutions on safety).

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.

Physical security threats also demand ongoing dialogue about system vulnerabilities and how aircraft design can enhance mitigation strategies. Evidence of manufacturers' responsiveness includes the adoption of oxygen generator requirements to address specific security risks. To facilitate cross-domain learning and maintain situational awareness, channels of communication must remain open between aviation security, safety, aircraft

[26] The latter is required only by the FAA

design, and airworthiness stakeholders. 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.

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 "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.

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. For instance, implementing security measures such as reinforced cockpit doors must consider potential safety impacts, like pressurization hazards, to ensure that security enhancements do not inadvertently introduce new safety risks.

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 and improve communication with industry stakeholders, including operators, airports, and CAMO.

This report aims to highlight the interconnected nature of security and safety within aviation, prompting further examination to identify opportunities for comprehensive risk management in air operations. By fostering an integrated approach, the aviation industry can better manage embedded risks, ensuring safe and secure air travel in a rapidly changing threat environment.

BIBLIOGRAPHY

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.

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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R2034&qid=1717162856354

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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1998&qid=1717163035532

European Commission (2011). Flightpath 2050 – Europe’s Vision for Aviation. Available at: https://www.arcs.aero/sites/default/files/downloads/Bericht_Flightpath_2050.pdf

ICAO Annex 17 Security, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, July 2022. https://www.icao.int/Security/SFP/Pages/Annex17.aspx

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

EASA CS-25 Easy Access Rules for Large Aeroplanes. https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-large-aeroplanes-cs-25

AMC-20 Amendment 18 https://www.easa.europa.eu/en/document-library/certification-specifications/amc-20-amendment-18

ICAO Doc 9859 - Safety Management Manual (SMM) https://www.icao.int/SAM/Documents/2017-SSP-GUY/Doc%209859%20SMM%20Third%20edition%20en.pdf

IATA Security Management System (SeMS) Manual. https://www.iata.org/en/publications/store/security-management-system-manual/?utm_source=google&utm_medium=cpc&utm_campaign=pubs-evergreen-search-b&utm_content=se-brand&utm_content=se-sems-iata-manual&gad_source=1&gclid=EAIaIQobChMIuZPC4IO4hgMVvIfCCB1A0Tk-EAAYASAAEgK5f_D_BwE

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

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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0300&qid=1717163073940

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. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1139&qid=1717163117431

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

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

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

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

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union