ASPRID

Airport System PRotection from Intruding Drones

Summary of Scenarios Assessment

Deliverable ID:	**D1.5**
Document ID:	**ASPRID.WP1.D1.5.PU.V1.0.FINAL. Summary_of_Scenarios_Assessment**
Dissemination Level:	**PU**
Work Package:	**WP1**
Task:	**T1.4**
Project Acronym:	**ASPRID**
Grant:	**892036**
Call:	**H2020-SESAR-2019-2**
Topic:	**Innovation in Airport Operation**
Consortium Coordinator:	**INTA**
Edition date:	**29 September 2021**
Edition:	**00.01.01**
Template Edition:	**02.00.02**

Founding Members
EUROPEAN UNION EUROCONTROL
SESAR JOINT UNDERTAKING

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Domenico Pascarella / CIRA	WP1 Leader	27 September 2021
Gabriella Gigante / CIRA	WP1 Member	27 September 2021
Francesco Nebula / CIRA	WP1 Member	27 September 2021
Angela Vozella / CIRA	WP1 Member	27 September 2021

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
Edgar Martinavarro / INTA	Project Coordinator	29 September 2021
Michele Cioffi / ALI Scarl	WP2 Leader	30 September 2021
Maurizio Sodano / Soul Software	WP3 Leader	30 September 2021
Pierre Bieber / ONERA	WP4 Leader	30 September 2021
Francisco Jose Jiménez Roncero / ENAIRE	WP1 Member	29 September 2021
Pablo Lopez / AENA	WP5 Leader	29 September 2021

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Edgar Martinavarro / INTA	INTA Representative	30 September 2021
Angela Vozella / CIRA	CIRA Representative	30 September 2021
Michele Cioffi / ALI Scarl	ALI Scarl Representative	30 September 2021
Maurizio Sodano / Soul Software	Soul Software Representative	30 September 2021
Pierre Bieber / ONERA	ONERA Representative	30 September 2021
Francisco Jose Jiménez Roncero / ENAIRE	ENAIRE Representative	29 September 2021
Pablo Lopez / AENA	AENA Representative	29 September 2021

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
0.1	27 September 2021	DRAFT	Domenico Pascarella, Gabriella Gigante, Francesco Nebula, Angela Vozella	Creation
1.0	29 September 2021	FINAL	All	Internal review. First final version.
1.1	13 January 2022	FINAL	All	Section 1.1 update.

Copyright Statement

- This page is left intentionally blank -

ASPRID

AIRPORT SYSTEM PROTECTION FROM INTRUDING DRONES

This Project Deliverable is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 892036 under European Union's Horizon 2020 research and innovation programme.

Abstract

This document represents the deliverable "Summary of Scenarios Assessment" of ASPRID project.

The document aims at providing an overview of the results achieved by ASPRID project in regard to the following activities related to airport drone intrusions: threat analysis, identification of the operational scenarios, analysis of historical data of intrusions, operational vulnerability assessment, risk assessment of the threat scenarios, and preliminary design of a decision support system to cope with the selection of operational mitigation actions. Moreover, a methodological framework is described for the systematic execution of some of these activities.

The potential beneficiaries of the document, in addition to ASPRID consortium and the SESAR Joint Undertaking, are represented by European aviation organizations (i.e., airport operators and air navigation service providers) and European aviation authorities as well as technological companies or research institutions whose activity is related to Decision Support Systems development.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Term	Definition
ADS-B	Automatic Dependent Surveillance-Broadcast
ASPRID	Airport System Protection from Intruding Drones
ATC	Air Traffic Control
ATCO	Air Traffic Controller Officer
AVI	Airport Vulnerability Index
CoA	Course of Actions
COL	Critical Operation List
DSS	Decision Support System
EASA	European Union Aviation Safety Agency
ENAC	Ente Nazionale per l'Aviazione Civile
ETA	Event Tree Analysis
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
HTA	Hierarchical Task Analysis
ICAO	International Civil Aviation Organization
IE	Initiating Event
IPL	Independent Protection Layer
OLS	Obstacle Limitation Surface
OPL	Operational Protection Layer
OVA	Operational Vulnerability Assessment
OVI	Operational Vulnerability Index
PE	Pivotal Event
sUAS	small Unmanned Aerial System
TPL	Technological Protection Layer

Term	Definition
TVI	Task Vulnerability Index
UAS	Unmanned Aerial System
UK	United Kingdom
UKAB	UK Airprox Board
UTM	Unmanned Traffic Management

1 Introduction

1.1 Purpose

This document represents the deliverable D1.5 “Summary of scenarios assessment” of ASPRID (Airport System PRotection from Intruding Drones) project[1].

The document aims at disseminating ASPRID project objectives, tasks and results providing an overview of the results achieved by its Work Package 1 (WP1) “Scenarios and study cases definition”.

1.2 Scope

ASPRID project is the response to the request made from SESAR under the Exploratory Research view, in order to cope with the problem of protecting the airport operations from drone intrusion (careless or malicious) under a holistic and operationally oriented approach. The project proposes to investigate the vulnerability of an airport under the different types of threats and possible ways of response, as well as to study the interrelations between all those aspects, involving different scenarios. The risk analysis shall reveal and categorize the problem, from which an architecture will be developed, so as to cope with the different steps and elements that can impact on operations, establishing the adequate levels of alert, response and, if needed, neutralization.

The ASPRID work plan is comprised of the following six Work Packages:

- WP1: Scenarios and Study Cases Definition.
- WP2: System / Solution Definition.
- WP3: System Integration and Validation.
- WP4: Regulation Assessment.
- WP5: Communication, Exploitation and Dissemination.
- WP6: Management and Coordination.

[1] The opinions expressed herein reflect the authors’ view only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

The present document is the final report outcome of WP1. It collects inputs from all the task of WP1 as it is detailed in its Reference section. No new technical contents are presented behind those presented in previous WP1 deliverables.

The potential beneficiaries of the document, in addition to ASPRID consortium and the SESAR Joint Undertaking, are represented by European aviation organizations (i.e., airport operators and air navigation service providers) and European aviation authorities as well as technological companies or research institutions whose activity is related to Decision Support Systems development.

1.3 Structure

The document is structured in the following sections:

- Section 1, Introduction – It reports the introduction of the document, with information about the purpose, the scope and the structure.
- Section 2, Background – It reports background information, such as a short description of ASPRID project, the approach of WP1, and the introductory basic definitions for the remainder of the document.
- Section 3, Risk Assessment of Airport Drone Intrusions – It provides the description of the developed methodological framework for the risk assessment of airport drone intrusions.
- Section 4, Definition of Elements for Scenario Study (Actors, Activities and Threat Analysis) – It reports the results of task T1.1.
- Section 5, Analysis of Historical Data of Attacks– It reports the results of task T1.2.
- Section 6, Vulnerability Assessment of Operations (Runway and Ground) to Intruder Drones and Critical Operation List – It reports the results of task T1.3.
- Section 7, Risk Scenarios Definition – It reports the results of task T1.4.
- Section 8, Conclusions – It provided the conclusions of the document.
- Appendix A, Consistency Analysis with Threat-Assets-Control Relational Model – It provides the consistency analysis of the developed methodological framework with respect to the threat-assets-control relational model.

2 Background

This section reports the background information for the document.

In detail, the background information consists on the following sub-sections:

- a brief overview of ASPRID project;
- the description of the approach of WP1, with the related assumptions;
- the recap of some basic definitions, which are useful for the reference study.

2.1 ASPRID in Brief

ASPRID project assumes that the best way to protect airport operations from intruder drones is increasing awareness about such undesired events and setting-up procedures and protocols to manage them aiming at mitigating their effects on the operations.

All this can be achieved by a system of systems that detects, tracks and neutralizes the drone, eliminating or reducing the threat impact.

Then, it will be necessary to perform an *a priori* analysis of a set of critical operations regarding *safety* to intruders. All elements related with airport operations shall be analysed, as well as their interdependencies. Such analysis will exploit all the possible operations, in nominal and off-nominal situation, and their evolution to properly identify adequate responses. Additionally, intruder identification, monitoring, flight path prediction and artificial intelligence decision support will increase noticeably such a system efficiency. All the above require a true interdisciplinary approach to integrate all those elements in an efficient way, including the human factor, present in all phases from alert to decision making and countermeasures activation.

Many different considerations should be taken into account:

- Not all the intrusions are of the same nature: Drones may be introduced by mistake and there can be a cooperative way to solve the situation, or they may have malicious intentions and such a cooperation might not be possible. Moreover, intrusions may be isolated or multiple, organized as a group (swarm). Also, the physical features of the drones can be very diverse in terms of size, weight, speed, etc., being necessary different capacities to cope with them.
- The impact of the disturbance is not the same for all airport elements and functionalities.
- Not all airports have the same requirements.
- Not all stakeholders have to be involved in a determined situation or moment.

Thus, as the ASPRID project states, scenario definition and risk assessment are critical aspects to consider and should be the starting point to deliver a global scalable solution that responds particularly to each scenario and improve the current situation where the airport operation closure is the only way to prevent bigger damages.

In this way, the project will address these mainstreams:

- The identification of the problem: Threats, Airport assets to protect and Operations.
- Setting scenarios: Risk and vulnerability assessment, prioritization, selection, requirements.
- Definition of an airport protection from drone decision support architecture:
    - At managerial level: Alert system and levels, Communications, Decisions, Response.
    - At specific technology elements: Detection, Identification, Tracking, Neutralization.
- Concept Validation activities: HMI based solutions, sensitivity studies, integration of elements and subsystems.
- Concept Support activities: Review and assessment of regulations and procedures (normal and emergency).

Through the tools developed under ASPRID, the different options for mitigations of drone intrusions shall be analysed in terms of feasibility (according to time, space constraints, etc.) as the “danger weight” could depend on some physical, technological, operative requirements. This means that different areas, each of which correspond to a specific alert level, shall be identified. In particular, the thresholds of danger awareness shall be defined around a sensitive target to be protected. These thresholds will be used for detection, monitoring, identification, tracking & tracing target and classification of threats type, for a quick assessment of the threat and a prompt notification of warnings in order to be able to activate real-time relative countermeasures against potential unknown drones.

2.2 WP1: Scenarios and Study Cases Definition Approach

WP1 has been performed in accordance with ASPRID management plan [1] and ASPRID Grant Agreement [2].

The purpose of WP1 is to identify the operational scenarios, focusing on aircraft and airport operations, and perform their vulnerability assessment to intruder drones in order to define the risk scenarios and the list of critical operations. This analysis will enable in next steps the definition of protection issues for the critical operations preventing or mitigating the related risks. Moreover, WP1 is in charge of providing the definition and the preliminary design of a Decision Support System (DSS) to cope with the selection of operational mitigation actions, in order to manage the reference threat scenario.

The work of WP1 has been decomposed in the following sequential tasks:

- *Task T1.1 "Definition of elements for scenario study (actors, activities and threat analysis)"* – In this task, a detailed threat analysis has been performed by highlighting the different types of attacks and by providing a classification of the intruders based on their characteristics. A preliminary Event Tree Analysis (ETA) has been performed to determine the high-level off-nominal branches in the operations.

- *Task T1.2 "Analysis of historical data of attacks"* – This task has integrated the previous analysis by analyzing historical data regarding the presence of drones near airports, in order to complement the approach to define off-nominal scenarios in the project. Also, the task has provided some preliminary considerations for the possible definition of a vulnerability index of airports with respect to the reference threat, represented by unauthorized drone intrusions.

- *Task T1.3 "Vulnerability assessment of operations (runway and ground) to intruder drones and Critical Operation List"* – This task has provided the specification of a detailed Functional Description of the reference nominal airport operations, which represents the basic input for the risk assessment. Then, it has defined a task-based and performance-based methodology for the Operational Vulnerability Assessment of airport operations with respect to unauthorized drone intrusions. Lastly, it has defined a methodological concept of Event Tree Analysis for the risk assessment of drone intrusions in airport, by integrating the outcomes of the vulnerability assessment.

- *Task T1.4 "Risk scenarios definition"* – This task has assessed some specific risk scenarios, on the basis of the operational risk assessment provided by T1.3, for a given reference threat scenario about airport drone intrusions. Then, it has provided the definition and the preliminary design of a Decision Support System to cope with the selection of operational mitigation actions, in order to manage the reference threat scenario.

All the partners in the consortium have contributed to WP1, with different contributions according to the reference task.

2.2.1 Assumptions for the Proposed Approach

The following main assumptions have been adopted for the work in WP1, i.e.:

- Today, there is an ever-growing number of drones accessible to the public, based on a number of commercially available options and numerous drone do-it-yourself websites and forums. These drones vary greatly in type, size, mass and velocity. For ASPRID project, the design specifications of the intruding drones to be considered are limited to those that currently exist as commercially available, which include a mass limitation of less than 25 kg and a velocity limitation of less than 19 m/s, in accordance with EU regulation 2019/945.

- Airspace above all identified critical airport assets is considered restricted for all unauthorised drones. For this reason, a security cylinder should be utilized around each asset, rather than a semi-sphere *bubble*, which would allow flights above the asset at a particular altitude.

- Only the risk that the drone itself poses as a potential collision hazard to each of the airport assets is being considered at this time.
- The intent of the drone is not being considered for the risk analysis. Any unauthorized drone that enters restricted airspace is considered to be a threat.
- The Technological Protection Layer (TPL) and the Operational Protection Layer (OPL) represent two independent protection layers (i.e., countermeasures) for airport drone intrusions, so that the failure of the technological layer does not adversely affect the probability of failure of the operational layer. This implies that the OPL will go into action only in the case of a failure of the TPL.
- The Decision Support System (DSS) shall be an information system that supports the judgement and the sequence of actions or course of actions (i.e., short-term decisions) for the management of the operational mitigation of an airport with respect to drone intrusions. It shall not support the determination, i.e., the selection of strategic (long-term) decisions.
- The Decision Support System (DSS) shall be focused on the management of the short-term service disruptions related to airport drone intrusions, whereas it shall not consider long-term effects in regard to service disruptions of the ANS. Possible considerations about service continuity and about recovery to normal operation shall be always focused on a short-term management.

2.3 Basic Definitions

For the purposes of this document, the following basic definitions are introduced regarding the following aspects:

- vulnerability;
- threat;
- attack;
- threat analysis;
- security-based risk assessment;
- modelling formalisms for security risk assessment;
- risk scenario;
- threats-assets-controls relational model;
- vulnerability index;
- Hierarchical Task Analysis (HTA).

2.3.1 Vulnerability

A **vulnerability** is a weakness of a reference system (i.e. an infrastructure, an asset, a group of assets, an organization, etc.) that may be exploited for a temporary or permanent interruption of the system's operations.

2.3.2 Threat

A **threat** is anything that might exploit a vulnerability, for the temporary or permanent interruption of the system's operations. In general, a threat may be:

- *accidental*: unintentional;
- *malicious*: hostile and deliberate.

The former case refers to any accidental cause of the interruption of the system's operations. This type of threat is also named **safety threat** if the interruption of the system's operation exhibits a safety impact for the outcome (i.e., the reference system is a safety-critical system).

Instead, the latter case refers to a **security threat**, which represents any intentional cause of the interruption of the system's operations. Clearly, a security threat may also have a safety impact if the reference system is a safety-critical system. In the remainder of this document, unless otherwise specified, the term threat will be used to specify a **security threat**.

In case of a security threat, a **threat agent** is an entity (i.e., person, organization, system, etc.) that has the power to act, cause, carry, transmit or support the reference threat. Thus, a threat agent is the entity which has the **intention**, the **capacity** and the **opportunity** to exploit the vulnerabilities of the system.

2.3.3 Attack

An **attack** is the deliberate action carried out by a threat agent for the exploitation of vulnerabilities of the reference system. The threat agent is also named **attacker**. The **attack vector** is the method, or sequence of actions, applied by the attacker to exploit the vulnerabilities and to perform the attack. An **attack scenario** is the specification of:

- a reference system and its current operations;
- a threat and the related threat agent;
- the attack carried out, with the related attack vector;
- the sequence of events that are caused by the attack.

Generally speaking, an attack may be classified according to [7]:

- The **attack type**: the threat that is exploited for the attack.
- The **attacked asset**: the object or target of the attack and the related impact.

In detail, that attack type may be physical (in the case of physical threats) or cyber (in the case of cyber-threats). Also, the attacked asset may be physical (in the case of a physical impact of an attack) or cyber (in the case of a cyber impact of an attack). Thus, the following attack classes may be considered [7]:

- **Physical attack**: attack of a physical threat with a physical impact.
- **Cyber-physical attack**: attack of a physical threat with a cyber impact.
- **Cyber-physical threat**: attack of a cyber threat with a physical impact.
- **Cyber-attack**: attack of a cyber threat with a cyber impact.

Clearly, an attack scenario may be seen as an instance of the more generic risk scenario, which is described in section 2.3.7.

2.3.4 Threat Analysis

Threat analysis is a process by which potential threats are identified and assessed. Moreover, **threat assessment** is the part of threat analysis for the assessment of the identified threats, i.e. for the evaluation of the potential impact (seriousness or damage potential) and of the occurrence probability of the identified threats. Thus, threat assessment provides a mean to prioritize the threats and the related mitigations.

2.3.5 Security-Based Risk Assessment

The **security-based risk assessment** or **security risk assessment** of a system is the assessment of the security of the reference system against attacks. This assessment is a basic step of the **security risk management**, which is the process to ensure that the security controls for the system are fully commensurate with its security risks. Generally speaking, the security risk assessment consists of the evaluation of the vulnerabilities of the reference system and the evaluation of the occurrence probability of the potential impact of **security incidents**. The latter are off-nominal events in the system's operations that are caused by an attack of a threat agent.

In the remainder of the document, unless otherwise specified, the term risk assessment will be used to specify a security risk assessment.

2.3.6 Modelling Formalisms for Security Risk Assessment

A proper security risk assessment generally employs a structured analysis approach, i.e. a sequential and explorative analysis for the systematic evaluation of the security-related behaviour of the reference system by considering all its significant elements. In detail, such a structured analysis may be effectively performed by means of a **model-based approach** within a **model-based security risk**

assessment. This applies modelling techniques for the unique specification of the reference aspects of the target system, such as: Failure-oriented behaviours, success-oriented behaviours, different views (i.e., functional, operational and organizational), etc. Clearly, these aspects shall be selected according to the scope of the analysis. This choice implies also the selection of the proper **modelling formalism**, supporting the specification of the chosen aspects themselves. Note that a model-based security risk assessment exhibits the following advantages:

- Improvement of the communication among stakeholders by means of well-known and unique modelling formalisms.
- Support of (possibly automated) *what-if* analyses for the computation of qualitative/quantitative values of interest about risk-related figures and performance metrics (i.e., probabilities, severities, tolerable failure rates, etc.).
- Possible reuse across multiple systems and objects, if the pattern-based modelling techniques are applied.

On the one hand, model-based security risk assessment clearly requires an analyser with some knowledge about the environment of the system. On the other hand, it requires an analyser with a knowledge about the target security domain of the system. In detail, the latter point implies the adoption of effective modelling formalisms for the specification and the description of security-related behaviours (e.g., in the form of sequence of events and/or decisions, course of actions, etc., with respect to attacks) within the reference system, in order to elicit security evaluations and also possible requirements for mitigation actions. Thus, these formalisms normally specify security-related behaviours by means of specific models, which may be analysed in depth for a qualitative / quantitative assessment of security properties.

The most used class of formalism is represented by the **logic trees**, which are any conceptual or mathematical model that describes scenarios of events and/or decisions in a tree-like structure [8]. They are an ideal tool for assessing risk (concerning both safety and security) since they manage the analysis of uncertain events, the characterisation of accidental or generally feared scenarios, the calculation of probability distributions, the evaluation of decision options, etc. In the next sections, we will discuss the following two instances of the logic tree class: **Attack Trees** and **Event Trees**. Indeed, these are the main options for the modelling of security-related behaviours. Moreover, also **FMECA** (**Failure Mode, Effects and Criticality Analysis**) is discussed.

2.3.6.1 Attack Trees

Attack Trees (also named **vulnerability trees** or **threat trees**) model the sequential actions of an attacker to defeat the defence (i.e., the security controls) of an asset [8], [9]. The attacker is generally represented by a rational adversary, that is to say, an attacker who does not attack if the attack is unprofitable and who chooses the most profitable way of attacking (maximum gain with the highest outcome or with the minimum cost) [10].

Attack Trees may be considered as a derivative of **Fault Trees**, since they apply the same logic mechanisms underlying the evaluation of the risks. Indeed, they both use a tree-based structure with

probabilistic estimations and Boolean-logic relationships. However, fault trees are used for safety risks since they analyse the failures of a system as a consequence of natural failures of its components. The basic events of the tree are the natural failures of components and their possible consequences; the top events of the tree are the feared events, intended as the failures of the system. Contrarily, Attack Trees are used for security risks since they analyse the failures of an asset as a consequence of malicious attacks. The basic events of the tree are the hostile actions of an attacker against the asset. The top events of the tree are the successful asset attacks.

Hence, Attack Trees may basically assess [9]:

- The set of attack vectors or threat vectors, i.e. the paths (intended as sequence of actions) by which an attacker may exploit the asset vulnerabilities and may achieve a successful attack.
- The likelihood of success of the attacks.

Moreover, they enable the identification and evaluation of attack vectors by combining several vulnerabilities in one analysis and identifying the most profitable attack vectors, which are the most convenient paths for the attacker.

Attack Trees are generally built according to a top-down and forward approach, by using a deductive analysis and backward logic (or backward chaining). Starting from the top event (i.e. the success of an attack), the modeller specifies the lower-level events (i.e. causes in terms of attack actions) and their logic interactions to achieve the top event. This process proceeds until the characterisation of a proper set of basic events. Thus, the adopted perspective is that of a deductive analysis: The modeller assumes that the erroneous behaviour (i.e. the successful attack) has been achieved and applies a deductive analysis and backward logic to look at the root causes (i.e. the possible attack vectors).

Some extensions of basic trees exist [9]. For example, there are countermeasure-centric extensions for the description of the interactions between attackers and defenders, such as **Attack–Defence Trees** or **Attack Countermeasure Trees**. Moreover, **Attack Graphs** are a variant to model the interdependency between vulnerabilities of the asset and its network topology, according to a graph-based data structure. They are an ideal solution for accurate and quantitative risk assessments since they may be used in conjunction with model checking techniques. However, Attack Graphs are more suitable for the analysis of cyber-security attacks.

2.3.6.2 Event Trees

Event Trees are logic trees for the modelling of the sequences of events [8]. Regarding risk assessment, they may be used both for safety risks and security risks. In the former case, they are used to identify and evaluate the sequence of events that lead to an accident. In the latter case, they are used to identify and evaluate the sequence of events that lead to an attack. In detail, an Event Tree is a logic tree model for illustrating the sequence of events and the possible outcomes which may be achieved after the occurrence of some initiating events. The initiating events are normally off-nominal events, such as the failure of single components for safety risk assessments and intrusions or vulnerability exploitations for security risk assessments.

As Fault Trees and Attack Trees, an Event Tree uses a tree-based structure with probabilistic estimations and Boolean-logic relationships. Indeed, an Event Tree specifies sequences of random events and each node represents a binary outcome in terms of occurrence or non-occurrence for an event in the sequence. Each sequence of events is modelled by a chain or path in the tree, which specify a particular scenario regarding the behaviour of the asset. Such a scenario is a failure scenario for safety risk assessments and an attack scenario for security risk assessments. Each scenario has a final event in the sequence, which represents the outcome of the scenario itself.

Hence, regarding security risks, an Event Tree may basically assess:

- The set of attack scenarios.
- The Likelihood of attack scenarios, given the likelihoods of the related initiating events.

The paths and the outcomes of the attack scenarios are determined by analysing how the scenario progression is influenced by intermediate events, i.e. the situations and conditions in the asset that may occur in responding to the initiating events (intrusions and vulnerability exploitations).

Moreover, note that Event Trees adopt a dual perspective with respect to Attack Trees (or Fault Trees). Indeed, Event Trees are built according to a backward approach, by using inductive analysis and forward logic (or forward chaining). Starting from the initiating event, the modeller specifies the possible consequences and their logic interactions to identify attack scenarios and the related outcomes by means of a *what-if* analysis. Thus, the adopted perspective is that of an inductive analysis: The modeller assumes that a vulnerability is present and exploited by an attacker and evaluates how such an exploitation may produce consequences and / or may manifest to achieve the outcome of a successful attack scenario.

2.3.6.3 Failure Mode and Effects and Criticality Analysis

The **FMEA** (**Failure Mode and Effect Analysis**) is a structured technique which investigates failure modes and their effects. It decomposes a system into its basic elements (components or functions) and, then, the failure modes of the single elements are examined for causes and effects. FMECA extends FMEA by adding a criticality evaluation of the failure modes.

Developed in the 1950s by the Us Department of Defence to improve the reliability of military equipment, FMEA was aimed at the assessment of reliability or safety of hardware [12].

2.3.7 Risk Scenario

A **risk scenario** or **mishap scenario** is a model of mishap process described by [13]:

- **perturbation events** and **pivotal events**;
- **causal relations** between the previous events;
- conclusions in terms of **undesired states**.

The concept of risk scenario is shown in Figure 1.

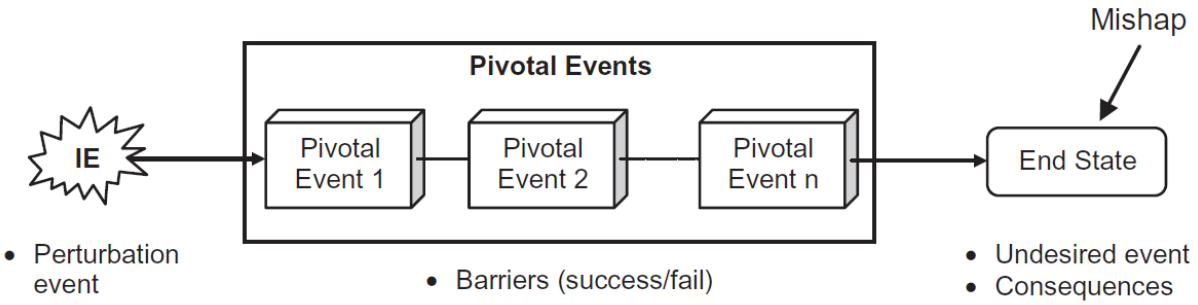

Figure 1. Risk scenario or mishap scenario [13].

In the scenario approach for risk analysis [13], the scenario begins with the **initiating event** (IE), which represents the perturbation event that fires the reference risk scenario. After the IE, some PEs occur according to specific causal orders, which provide different logical flows for the risk scenarios. The scenario ends with a list of possible risks or mishaps, which represent the possible **end states**. These provide the list of risks or mishaps, in terms of both undesired events and related consequences (e.g., impacts, damages, performance degradations, etc.).

Thus, risk scenarios are defined as:

- the possible logical flows, starting from the given IEs and considering the possible PEs, with their causal relationships;
- the list of possible end states or mishaps (undesired events and consequences), related to the logical flows.

Note that the concept of PE may include also the **barrier events** [13], i.e., events that are capable of preventing a scenario from proceeding to its undesired consequences, in order to prevent the occurrence of a mishap even though the occurrence of the IE and of previous undesired PEs.

Clearly, such scenario approach for risk analysis may be effectively managed by means of Event Tree Analysis (ETA) formalism.

2.3.8 Vulnerability Index

A **vulnerability index** is usually defined as a measure of the susceptibility of people, communities or regions to natural or technological hazards [14]. Thus, a vulnerability index represents a measure of the exposure of the system or the community under study with respect to the reference hazards.

A vulnerability index shall consider the versatile nature of vulnerability by a acknowledging its different dimensions [14]. Indeed, generally speaking, vulnerability is influenced by a set of conditions and processes resulting from physical, social, economic and environmental factors, which increase the susceptibility of a system or a community to the impact of hazards. Moreover, vulnerability encompasses the response and coping capability, being influenced also by the potential of the system

or of the community to mitigate and react with respect to the occurrence of a feared event. For all these reasons, a vulnerability index is an “umbrella”, i.e., it may be defined as a **composite indicator**, which is a “multidimensional” ensemble of multiple indicators. Such indicators combine the different dimensions of vulnerabilities and are combined in a single integrated framework to possibly:

- compare the vulnerability of different systems and communities;
- compare different policies or options of the same system;
- evaluate potential complications for recovery planning in case of occurrence of the feared event.

In particular, the ESPON Hazards project [14] acknowledges damage potential and coping capacity as the two main components of vulnerability. The project defines an approach for the measurement of the vulnerability of places as a combination of **hazard exposure** and **social response** within a specific geographic region. Furthermore, the project recognizes three different **vulnerability dimensions** to quantify hazard exposure and social response:

- **economic dimension**;
- **social dimension**;
- **ecological dimension**.

In general, an **environmental dimension** should be considered instead of the ecological one, to include more aspects (e.g., the impact of human activities in the natural world).

In the end, the hazard exposure may be represented as a combination of:

- **hazard likelihood**, i.e., the probability of the hazard event;
- **hazard mitigation**, i.e., the effectiveness of the measures to reduce the likelihood of the hazard or its impacts.

To measure vulnerability, the ESPON project used indicators that cover both damage potential and coping capacity, as well as the range of all three vulnerability dimensions. A weighted combination of the individual indicators created an **integrated vulnerability index.** In regard to the part for the hazard exposure, this is filtered by the components related to the different vulnerability dimensions, thus a specific place may have an **economic hazard exposure**, a **social hazard exposure** and an **ecological hazard exposure.**

Lastly, considering safety management, when analysing a potential hazard, it is taken into consideration the following variables:

- the probability that this hazard can occur;
- the severity, i.e., the impact of this hazard.

The combination of both variables provides the **hazard tolerability** or also **risk tolerability**.

2.3.9 Threat-Assets-Controls Relational Model

Reference [15] describes a model of the relationship between **threats**, **assets** and **controls**, named **threat-assets-controls relational model**. This model represents an applicable guidance material for the purposes of risk assessment in ASPRID project since it establishes a conceptual foundation of a **threat-driven approach**, which is a methodology and a set of practices with the primary purpose of enabling organizations to allocate the commensurate level of resources to defend their assets and components. Figure 2 illustrates such model.

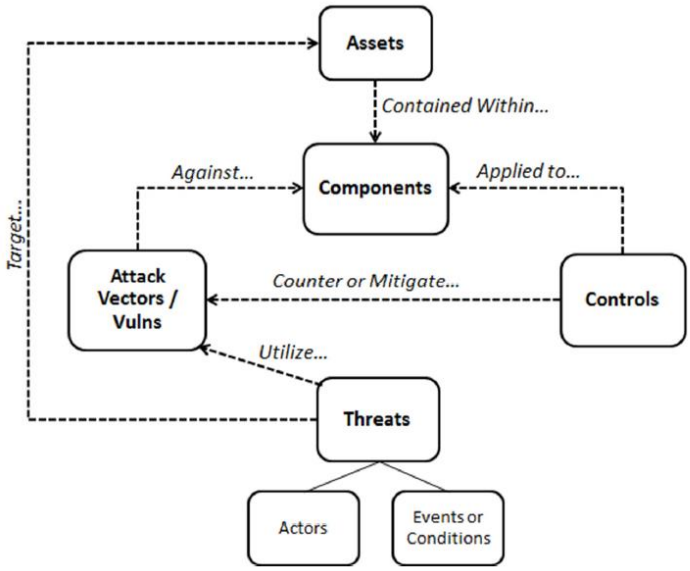

Figure 2. Threat-assets-controls relational model [15].

The following definitions are applied in [15]:

- **Asset –** any resource worth protecting (e.g., data, functionality, services, physical resources).
- **Attack surface –** the collection of components and interfaces that a threat actor could use to realize a threat against an asset.
- **Attack vector –** a specific sequence of exploits utilizing components within the attack surface to realize a threat against an asset.
- **Component –** any discrete element of a system (e.g., technology, processes, users, administrators).
- **Control –** a technology, process, or policy that removes, counters, or mitigates one or more threats, attack vectors or vulnerabilities.

- **Threat actor –** an entity that would attempt to impact an asset.
- **Vulnerability –** a specific weakness or flaw in a component or system that can be used to perform unintended actions.

This relationship model may be described as follows [15]:

- threats target assets, which are found in one or more components of the system;
- threat actor(s) gain access to the assets by exploiting components' vulnerabilities and by using attack vectors against components;
- security controls are applied to the components with the intent to counter or mitigate the vulnerabilities and/or attack vectors used by the threat actors.

Thus, according to this model, vulnerabilities and controls shall be defined with respect to components, which include the processes, i.e., the operations of the reference system.

Appendix A reports a consistency analysis of the developed risk assessment methodology for airport drone intrusions with respect to the threat-driven approach and the threat-assets-controls relational model.

2.3.10 Hierarchical Task Analysis

Hierarchical Task Analysis (**HTA**) is a process consisting in the decomposition of tasks into tasks to any desired level of detail [16]. Each subtask represents an operation, and is generally specified by:

- a goal;
- input conditions under which the goal is activated;
- the actions required to achieve the goal;
- the feedback related to goal achievement.

The relationship between a set of subtasks and the "parent" task is defined as a plan.

The main objective of HTA is to identify possible sources of performance failure and to study suitable mitigations, which may include the modification of task design.

3 Risk Assessment of Airport Drone Intrusions

This section describes the developed methodological framework for the risk assessment of airport drone intrusions.

3.1 Approach and Modelling Paradigm

The risk assessment carried on in this work is referred to the **baseline scenario**, i.e., without the implementation of the Decision Support System and of the drone detection and neutralization system. Future work in the WP3 of ASPRID project will assess the effects of the procedures changes and the drone detection and neutralization systems to evaluate their safety-based and security-based impact. Anyway, the Event Tree Analysis of this work already proposes some considerations for the efficiency (and the related success probability) of the technical capabilities of a system protecting the airport against drones, including mitigation aspects. Such considerations will be further analysed in WP3.

The following subsection reports a detailed analysis of the modelling formalisms for risk assessment (described in section 2.3.6) and provides the justification for the usage of Event Tree Analysis within the developed framework.

3.1.1 Analysis of Modelling Formalisms for Risk Assessment

For the purposes of ASPRID project, Event Trees have been used for the security risk assessment of airport operations against drone attacks. This choice may be motivated by the following aspects:

- The inductive analysis performed by means of Event Trees is more coherent with the ASPRID objectives with respect to the deductive analysis performed by means of Attack Trees. Indeed, when we apply the inductive analysis of Event Trees, we work according to the perspective that some vulnerabilities are present in the asset and have been identified. The objective of the analysis is to systematically evaluate all the possible consequences, in terms of sequences and scenarios, of the malicious exploitation of these vulnerabilities. This inductive perspective is suitable to elicit the requirements of security controls and mitigation actions for counter-measure systems and to design the test cases for such counter-measure systems. Clearly, such objectives are in line with the purpose of ASPRID project. On the contrary, the deductive analysis of Attack Trees is more suitable to investigate about the possible root causes of an observed attack. Thus, Attack Trees are an ideal tool for the refinement of counter-measure systems (e.g. with respect to experimented defects and attacks).

- Recent works specify also Attack Trees by means of a mixture of Fault Trees and Event Trees for a security bowtie analysis [8], [10], [11]. In detail, the Fault Tree portion identifies the cut sets for the triggering of attack scenarios, whereas the Event Tree portion specifies the inductive sequences of the possible consequences. However, Event Trees are a basic

requirement also for this extended formalism, which may be used for the advanced design and engineering of a counter-measure system.

- Regarding FMEA and FMECA, some works propose to apply them also for security evaluations [12]. The idea is to apply a combined approach for safety and security assessment by specifying cause-effect chains, which are triggered by a single failure mode of a single basic element. Each failure mode has a failure cause and each failure effect is associated with a failure mode that causes the effect. However, in regard to the ASPRID project, the proposed analysis shall not be focused on the failure modes of basic elements, also due to the fact that only the failure modes and the probabilities for hardware components are normally well known, whereas the failure modes of complex systems (including software parts and human beings) may be coupled with a high degree of uncertainty. Moreover, the security-related extension of FMEA includes also a cause-effect chain analysis starting from an attack. However, the purpose of this additive analysis is deemed to be equivalent to that built-in the ETA.

3.2 Methodological Framework for Risk Assessment of Airport Drone Intrusions

This section describes the developed **methodological framework** for the **risk assessment of airport drone intrusion**. Such methodological framework consists in a set of principles and tools and in a detailed workflow for the systematic execution of the risk assessment of airport drone intrusions.

In detail, Figure 3 illustrates the developed methodological framework. The figure highlights both the activity flow and the related interfaces by reporting:

- input data (yellow blocks);
- activities (green blocks);
- outcomes (blue blocks), in terms of both intermediate and final outcomes.

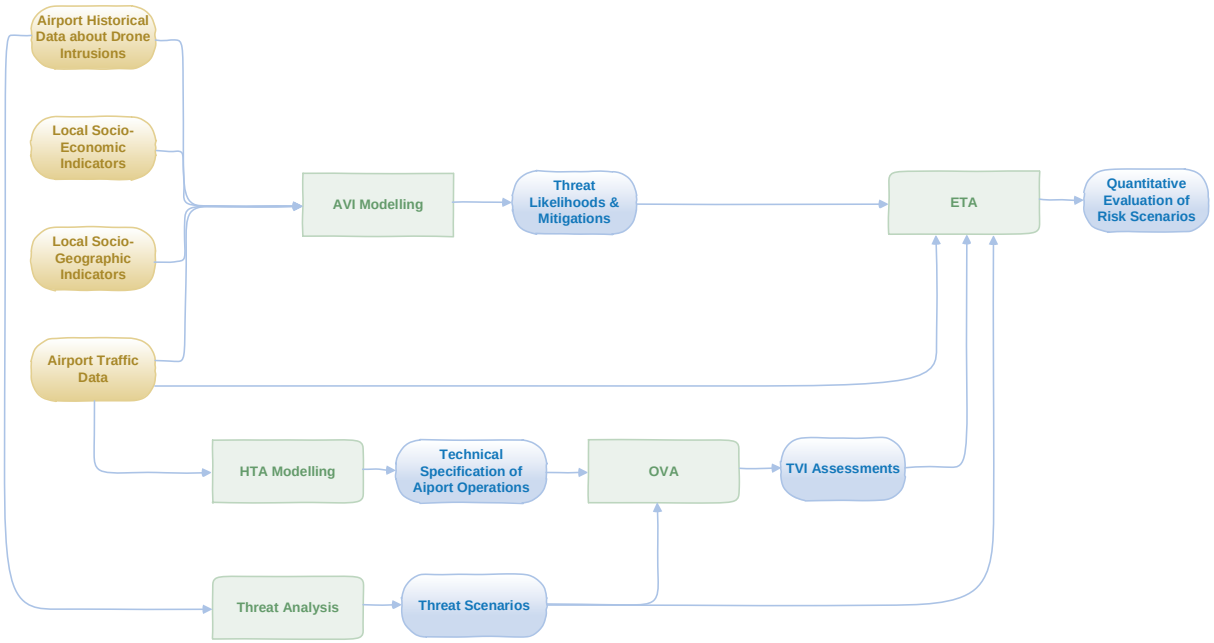

Figure 3. Developed methodological framework for the risk assessment of airport drone intrusions.

The developed framework prescribes the following activities:

- **Threat Analysis** – It identifies the possible threat scenarios about airport drone intrusions. It is possibly fed by historical data and is generally performed by also exploiting a detailed analysis of the features of the intruder drones and of the reference airport.
- **AVI Modelling** – It estimates the Airport Vulnerability Index with respect to drone intrusions, by assessing both a threat likelihood and a threat mitigation (even if, considering the available data, only the threat likelihood has been discussed). Different inputs may be used for the AVI model, such as: historical data about airport drone intrusions; socio-economic and socio-geographical indicators; airport traffic data; etc.
- **HTA Modelling** – It provides a technical specification of airport nominal operations by using a specific formalism, based on Hierarchical Task Analysis. The technical specification reports a detailed characterization of the operations in terms of phases and tasks. Different attributes are identified for each task, including actors, resources, durations, preconditions and postconditions.
- **OVA** – It provides the estimation of the Task Vulnerability Index of each task (as specified in the HTA Modelling), according to a functional-based and performance-based strategy.
- **ETA** – It provides the Event Tree Analysis for the quantitative evaluation of the risk scenarios.

The following list provides a mapping between the previous activities and WP1 tasks (mentioned in section 2.2 and further described in the following chapters):

- Threat Analysis has been analysed in T1.1 (deliverable D1.1 [3]) and in T1.3 (deliverable D1.3 [5]).
- AVI Modelling has been analysed in T1.2 (deliverable D1.2 [4]) and in T1.4 (deliverable D1.4 [6]).
- HTA Modelling has been analysed in T1.3 (deliverable D1.3 [5]).
- OVA has been analysed in T1.2 (deliverable D1.2 [4]).
- ETA has been analysed in T1.1 (deliverable D1.1 [3]), in T1.3 (deliverable D1.3 [5]) and in T1.4 (deliverable D1.4 [6]).

Lastly, Figure 4 shows the relationships with external activities of the developed methodological framework. In detail, the highlighted external activities are: the design of the detection and the neutralization system; the operational mitigation design, with the related Decision Support System; the safety and security assessment review, for the updates of risk assessment models.

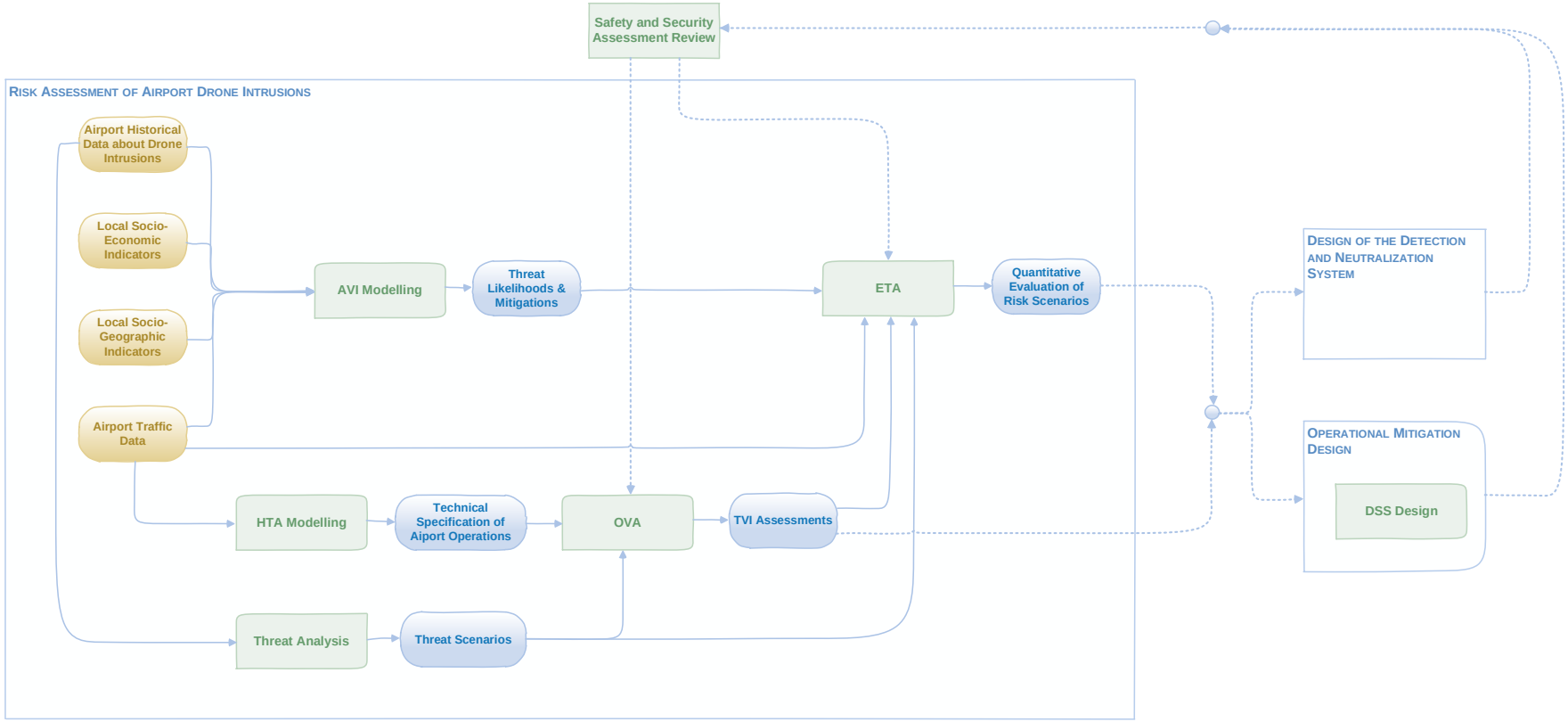

Figure 4. Relationships with external activities of the developed methodological framework for the risk assessment of airport drone intrusions.

4 Definition of Elements for Scenario Study (Actors, Activities and Threat Analysis)

This section reports the main results achieved by task T1.1 “Definition of elements for scenario study (actors, activities and threat analysis)”.

The detailed description of the results is available in deliverable D1.1 [3], which is confidential. More information is accessible on request on website https://www.asprid.eu/.

4.1 Threat Analysis of Airport Drone Intrusions

A high-level classification of drones and threat types, upon the drone’s flying principle, could be:

- *Fixed-Wing*: Powered by generally one electric or reciprocating engine and less often by jet engines, they fly at higher speeds, with more endurance and range. However, hovering is not possible as the wing always needs an air current in order to produce lift. In this type of drones, the threat to Critical Assets is mainly related to fly-by or collision.
- *Multi-Rotor*: Powered by four or more electric motors, they are much more manoeuvrable, showing vertical take-off and landing (VTOL) and hovering capabilities. However, the speed, endurance and range are more limited. In this type of drones, the threat to Critical Assets is mainly related to fly-by, whereas collision could pose a smaller threat due to the lower speeds.
- *Fixed-Wing - VTOL*: They are able to take-off and land vertically or horizontally, showing a mixture of the performances of the pure-type drones. This type could pose the worst threat, whereas it is not very commercially available nowadays. It can be assumed they pose the same threats than those of Fixed-Wing type.

Table 1 reports a common classification of drone categories.

Table 1. Drone categories.

Designation	Weight range	Flight range
Micro and mini drones close range	W ≤ 5 kg	25 km ≤ R ≤ 40 km
Lightweight drones small range	5 kg < W ≤ 50 kg	10 km ≤ R ≤ 70 km
Lightweight drones medium range	50 kg < W ≤ 100 kg	70 km ≤ R ≤ 250 km
Medium heavy drones	300 kg < W ≤ 500 kg	70 km ≤ R ≤ 300 km
Heavy medium range drones	500 kg ≤ W	70 km ≤ R ≤ 300 km
Heavy drones large endurance	1500 kg ≤ W	R ≤ 1500 km
Unmanned combat aircraft	500 kg < W	R ≤ 1500 km
Average drones	100 kg < W ≤ 300 kg	150 km ≤ R ≤ 1000 km

A number of actors present in the great majority of the considered intrusions may include:

- *Drone*: Its systems usually include external references for trajectory navigation such as GPS or even visual navigation.
- *Pilot & Ground Control Station* (drone-pilot interface): The *Telemetry* and *Tele-command* of the drone are carried out through this interface, sometimes referred as GCS, that ranges from an all-terrain truck to a mobile phone or tablet. This element allows for a remote control of the drone, even in BVLOS conditions.
- *Communication link*: Provides the communication with the drone, from the GCS. The *Uplink* and the *Downlink* refer to, respectively, the Tele-command and the Telemetry. A *Silent Mode* can also be established, in which an automated or semi-automated flight may be carried out, without continuous human intervention (*Autopilot*).
- *Payload*: Nowadays, drones are capable of carrying any number of payloads that range from simple cameras to jamming electronics or a full array of weapons (missiles, chemical weapons, warheads, etc.).

4.2 Threat Identification

The different threats a drone can pose are mainly:

- **fly-by** or drone flying too close to an asset;
- **collision**;
- **jamming**;
- **radio interference** on airport communications (by sole drone or by payload);
- **weapon firing**.

As for the ASPRID project scope, the considered threats are fly-by and collision.

4.2.1 Intrusion Types of Non-Authorized Drones

A **drone intrusion** indicates any unexpected and unauthorized physical intrusion of a drone into a reference airspace or infrastructure. More generally, a **drone system intrusion** may be considered to include also the cases of intrusions by **teams** or **swarms** of drones. However, in the remainder of this document, unless otherwise specified, the term drone intrusion will be used also to indicate intrusions of swarms and teams of drones.

The reference intrusion may be either:

- **Malicious**: hostile and deliberate drone intrusion.
- **Accidental** or **negligent**: unintentional drone intrusion.

A malicious drone intrusion is also named **attack** or **drone attack.** For example, a malicious drone intrusion in an airport may be deliberate so as to damage an airport's asset, to interfere with airport's operations, etc. Moreover, an intrusion of a swarm or a team is hardly negligent, so this type of intrusion should be always considered as a malicious intrusion, that is to say, an attack.

Contrarily, an accidental intrusion may be due to human errors, drone failures, etc.

With reference to the basic definitions given in section 2.3.3, note that a malicious drone intrusion (or drone attack) represents an attack due to a security threat, whereas the reference drone is the threat agent[2] or attacker. Contrarily, an accidental drone intrusion is not formally an attack, but it is a safety threat. However, for the purposes of this document and of ASPRID project, both types of intrusions have been considered as a reference for the threat analysis of airport drone intrusions.

With reference to the classification of attacks in section 2.3.3, being drones a physical threat, their attacks may be:

- A physical attack: malicious collision with a physical asset.
- A cyber-physical attack: a drone with radio signal jamming or spoofing, for instance.
- An interference: a drone data link interferes the communications of the target system, for example.

Also, note that a drone may be the target of a cyber-physical threat (e.g., ADS-B spoofing to attack a drone, manipulation of sensor data, hijacking of the telemetry link and/or the command & control link, etc.). Instead, cyber-attacks (e.g. malware insertions, network analysis, data corruption, etc.) do not generally involve drones.

4.3 Critical Asset Identification and Assessment

As shown in Figure 5, **critical assets** of an airport are those that are deemed to be both **necessary** to the nominal airport operations and **vulnerable**, i.e., being capable of interrupting or halting the airport operations as a result of a drone collision or a drone flying too close.

[3] In general, the drone system, including the pilot, is the threat agent.

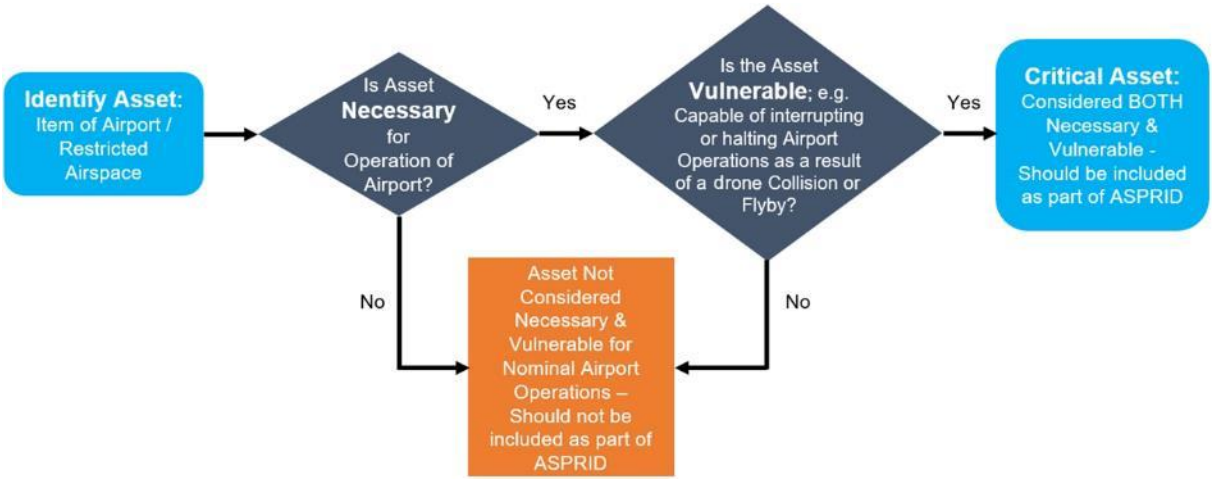

Figure 5. Block diagram for critical asset identification.

The necessary assets are the following:

- Runway(s) and its Associated Restricted Areas and Aids.
- Taxiway(s) and Associated Visual Aids (marking, lights, signs, markers).
- Apron(s) and Associated Visual Aids (marking, lights, signs, markers).
- Runway Associated Restricted Airspace and OLS (Obstacle Limitation Surface).
- Air Traffic Control Tower(s).
- Aircraft: Parked, Started-Up, Taxiing, Taking Off or Landing.
- Aircraft Hangar(s).
- Communication / Navigation / Surveillance System(s).
- Precision Approach Lighting System(s), Visual Slope and Runway Illumination System(s).
- Aviation Terminal(s).
- Fire Station(s) and Emergency Access Roads.
- Passenger Transportation System(s).
- Border Fence(s).
- Fuel Depot(s).

- Power Station(s).
- Auxiliary Buildings and Facilities.
- Freight Warehouse(s).
- Automated Meteorological Systems: RVR, WDI, Ceilometer, Observation Emplacement, Meteorological Data Collection Sensors: Pressure, temperature, humidity, visibility, wind direction and speed.
- Sentry Boxes.
- Ground Personnel and Pedestrians.

Categorization of each necessary asset was conducted in terms of being vulnerable to a drone intrusion. Results of the categorization are that the vulnerability of each of the previously identified necessary assets has been found to be capable of interrupting or halting airport operations under drone Collision and/or drone Fly-By intrusion scenarios. Therefore, every asset previously listed can be categorized as critical.

To assess the criticality of an asset, the developed analysis has evaluated how close could a rogue drone approach the asset before interrupting or halting its functionality, considering the applicable threat scenarios (fly-by and collision). This value is herein referred to as the **safety radius of the critical asset**. The general airspace to be considered for the protection of an asset will be a security cylinder with a certain safety radius, as shown in Figure 6.

Figure 6. Critical assets and safety radii.

If an intruding drone enters restricted airspace, the effect could result in various levels of interruption to the airport as a whole. Table 2 reports a possible classification of these levels of severity.

Table 2. Severity of outcomes.

Level	Description
1	Death or Permanent/Severe Loss of all Airport Operations > 1 Day
2	6 Hours < Severe Injuries / Airport Loss of Operation < 1 Day
3	1 Hour < Light Injuries / Airport Loss of Operation < 6 Hours
4	Personal Distress / Small Interruption to Airport Operation < 1 Hour
5	No Effect to Airport Operations

Reference [3] provides the detailed results of the assessment and some additional considerations for:

- The intrusion of multiple drones and / or swarms.
- The nature (negligent or malicious) of the intrusions and intention prediction.
- The intrusion of non-standard drones (commercial or not).
- The interaction with U-Space and UTM.

5 Analysis of Historical Data of Attacks

This section reports the main results achieved by task T1.2 “Analysis of historical data of attacks”.

The detailed description of the results is available in deliverable D1.2 [4], which is confidential. More information is accessible on request on website https://www.asprid.eu/.

5.1 Assessment of Public Record Databases

Some databases are publicly available to report data about drone sightings, especially (but not only) near airports. The following are the public databases that have been considered for the purposes of the analysis in ASPRID project:

- **FAA UAS Sighting Reports** [17];
- **UKAB (UK Airprox Board) sUAS Reports** [18].

Table 3 reports some examples of FAA UAS Sighting Reports, whereas Table 3 shows some examples of UKAB sUAS Reports. In detail, the UKAB risk level is expressed according the ratings provided in Table 5.

Table 3. Examples of FAA UAS Sighting Reports [19].

Day of Sighting	State	City	Summary
01/04/2020	MINNESOTA	MINNEAPOLIS	PRELIM INFO FROM FAA OPS: MINNEAPOLIS, MN/UAS INCIDENT/1400C/C-ROC ADVISED MSP - CVG, REPORTED UAS WHILE ESE BOUND AT 3,300 FEET 2 ESE MSP. NO EVASIVE ACTION TAKEN. LEO NOTIFICATION NOT REPORTED.
01/04/2020	GEORGIA	ATLANTA	PRELIM INFO FROM FAA OPS: ATLANTA, GA/UAS INCIDENT/2005E/ATLANTA TRACON ADVISED CESSNA C150, REPORTED BLUE AND GREEN UAS 300 FEET BELOW ACFT AT THE 12 O'CLOCK POSITION WHILE W BOUND AT 4,300 FEET 23 N ATL. NO EVASIVE ACTION TAKEN. FULTON COUNTY PD NOTIFIED.
02/04/2020	TEXAS	DALLAS	PRELIM INFO FROM FAA OPS: DALLAS, TX/UAS INCIDENT/2258C/ADDISON ATCT ADVISED CESSNA C172, REPORTED A UAS AT 2,000 FEET 10 E OF ADDISON ARPT. NO EVASIVE ACTION REPORTED. LOCAL LAW ENFORCEMENT NOTIFIED.
03/04/2020	MONTANA	HELENA	PRELIM INFO FROM FAA OPS: HELENA, MT/UAS INCIDENT/1644M/HELENA ATCT ADVISED H60,

Day of Sighting	State	City	Summary
			REPORTED A UAS AT 450 FEET. NO EVASIVE ACTION REPORTED. LEO NOTIFICATION NOT REPORTED.

Table 4. Examples of UKAB sUAS Sighting Reports [20].

Airprox No	Date	Year	Aircraft	Object	Latitude	Longitude	Alt	Reported Location	Risk
2020135	24/08/2020	2020	A321	Drone	N5127	W0004	04500	London TMA	C
2020140	25/09/2020	2020	Tutor	Drone	N5100	W00221	02000	London FIR	C
2020142	16/09/2020	2020	Hawk	Model Aircraft	N5028	W00413	00300	London FIR	C
2020144	11/10/2020	2020	Cirrus 22T	Drone	N5118	E00001	01600	London FIR	C
2020148	10/10/2020	2020	C150	Unknown	N5129	E00035	4000	London TMA	C
2020150	16/10/2020	2020	A321	Unknown	N5128	W00024	01700	London CTR	A
2020155	16/10/2020	2020	PA31	Drone	N5127	W00023	02000	London CTR	B

Table 5. UKAB risk ratings [21].

Risk	Meaning
A	Risk of Collision: aircraft proximity in which serious risk of collision has existed.
B	Safety not assured: aircraft proximity in which the safety of the aircraft may have been compromised.
C	No risk of collision: aircraft proximity in which no risk of collision has existed or risk was averted.
D	Risk not determined: aircraft proximity in which insufficient information was available to determine the risk involved, or inconclusive or conflicting evidence precluded such determination.
E	Met the criteria for reporting but, by analysis, it was determined that normal procedures, safety standards and parameters pertained.

Several references already provide an analysis of FAA UAS sighting reports (such as [22], [23], [24]). Such references are mostly focused on the past years and do not provide a review of 2020. For the purposes of the analysis in ASPRID project, the developed assessment is focused on FAA UAS sighting reports in 2020. A detailed processing has been performed by assessing temporal and by-State evolutions, especially for altitude and airport distances of the sightings. The assessment has also considered the fact that the year 2020 is not fully representative for the air transport sector compared to previous years, due to the pandemic of coronavirus disease 2019 (COVID-19).

Moreover, UKAB already provides a processing of their reported data about sUAS sightings [20]. However, for the purposes of the analysis in ASPRID project, an additional processing and assessment have been performed to focus on the sightings in the vicinity of airports or affecting airport operations, whereas the available UKAB's processing refer to all the sightings.

The analysis has been performed by means of Microsoft Excel and MATLAB.

Even if with some specific differences (e.g., regarding the occurrences of drone sightings), there are some similarities between the assessment of FAA UAS sighting reports and the assessment UKAB sUAS sighting reports. These especially concern the evolutions of airport distances and sighting altitudes, which exhibit traits in common, such as the followings:

- most of sightings occur when the aircraft are near to airports, also because these areas have more control and monitoring (for example, see Figure 7);
- altitudes have more an extended distribution on different scales (for example, see Figure 8);
- the scatter plots of airport distances and altitudes have similar clustering patterns (for example, see Figure 9).

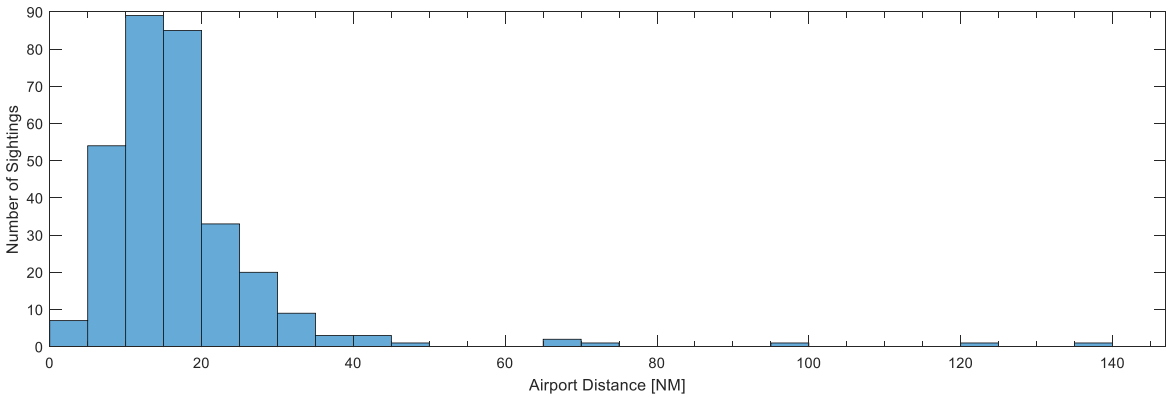

Figure 7. By-distance distributions in UKAB sUAS sighting reports affecting airports.

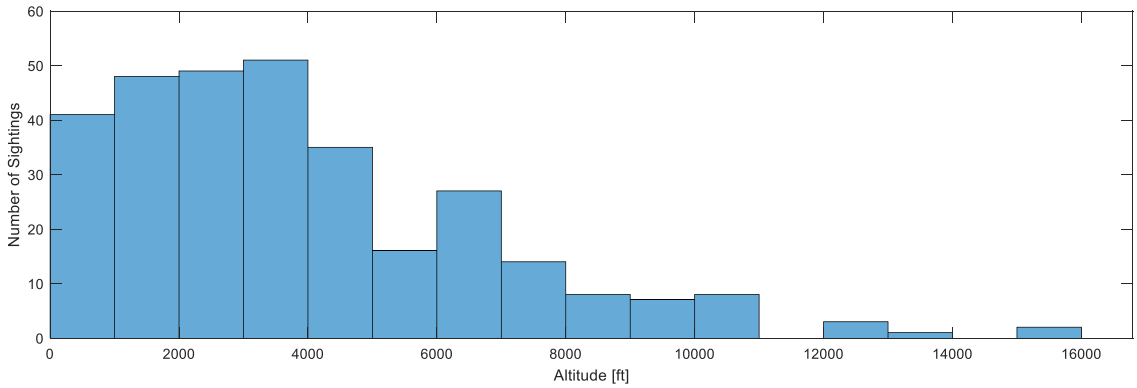

Figure 8. By-altitude distributions in UKAB sUAS sighting reports affecting airports.

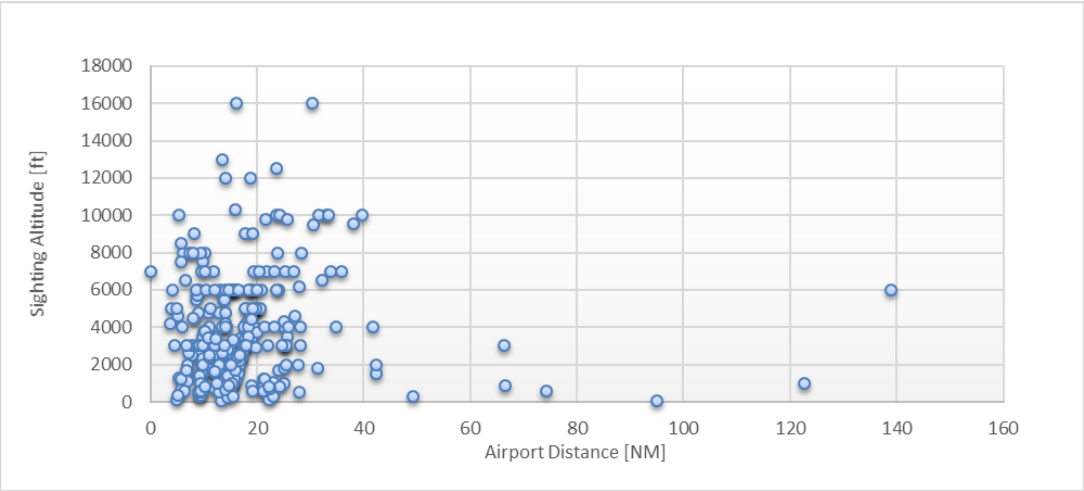

Figure 9. Scatter plot of the airport distance and the sighting location altitudes in UKAB sUAS sighting reports affecting airports.

The deviations regarding the sighting occurrences may be attributed to the characteristic contexts (e.g., to the socio-economic contexts), as further explained in the vulnerability index study in section 5.3.

5.2 Feature Modelling

Starting from the assessment results of FAA UAS Sighting Reports and UKAB sUAS Sighting Reports, some models have been built with the following objectives:

- to fit **probability distributions** to the historical features of the phenomenon of unauthorized drone intrusions in airports;
- to draw inferences from data and to check the feasibility of building **classification/predictive models** for the features of the phenomenon of unauthorized drone intrusions in airports.

Clearly, such results are specific for the adopted records of FAA and UKAB, even if some similarities may arise, also in regard to other distributions for different contexts (i.e., different airports in different countries).

The outcomes of the modelling may have a double value:

- for the purposes of ASPRID project, they may provide some useful considerations for:
    - risk assessment, to better tune some features of its (vulnerability assessment, risk scenarios, etc.) with respect to the predicted features of the phenomenon of unauthorized drone intrusions in airports;
    - the validation activities, to better tune the validation scenarios with respect to the predicted features of the phenomenon of unauthorized drone intrusions in airports;

- for more general purposes, they may provide some preliminary considerations to arrange a systematic process for the inclusion of historical features and predictive models in the safety and security risk assessment of unauthorized drone intrusions in airports.

For the sake of brevity, this document reports some results for the modelling of UKAB data. Detailed results are available in [4].

5.2.1 Probability Distributions

Given the nature and the structure of the available data, the following modelling objective has been pursued: to fit probability distributions to the historical features of the phenomenon of unauthorized drone intrusions in airports, related to the occurrences of:

- the sighting altitude;
- the distance of the nearby airport with respect of the intrusion location.

In detail, a **Rayleigh** model and a **Weibull** model [25] have been designed to compare their accuracies. For example, Figure 10 reports a comparison of the sample data and the distribution models in terms of probability distribution. It shows how the Weibull distribution turns out to be more accurate to fit the distribution of the occurrences of the altitude locations.

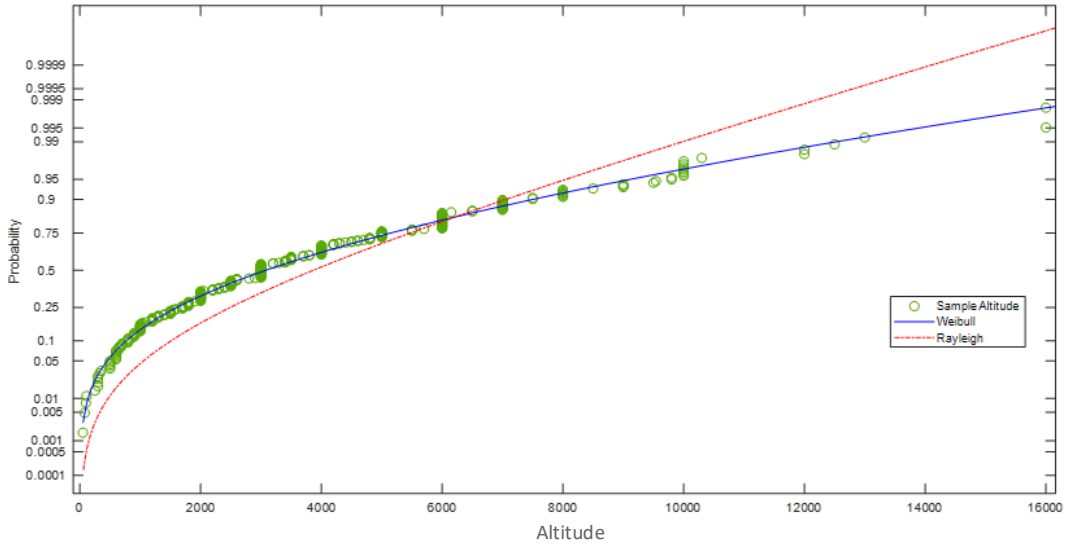

Figure 10. Probability distribution of the sample data and of the models for altitude locations in UKAB sUAS sighting reports affecting airports.

In regard to the distribution of the airport distances, a **Burr** model [26] has been used. Figure 11 reports a comparison of the sample data and the Burr distribution model in terms of probability density.

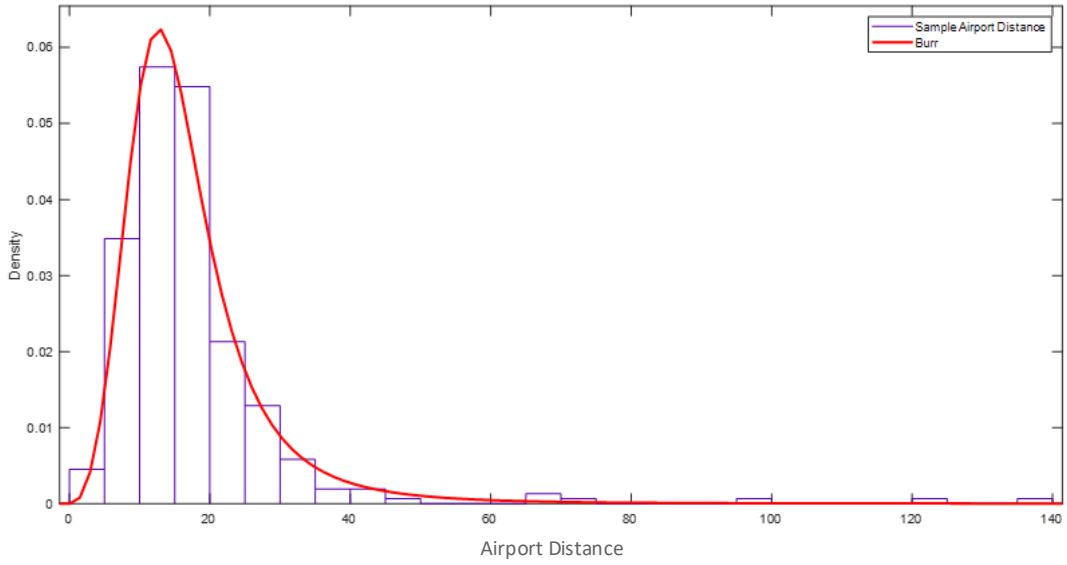

Figure 11. Probability density of the sample data and of the Burr model for airport distances in UKAB sUAS sighting reports affecting airports.

5.2.2 Classification Model of the Risk Level

An additional modelling objective has been the following: to build a predictive model for the classification (i.e., estimation) of the risk level of the intrusion according to the other sighting data. Such objective may be useful to verify the possibility of:

- estimating (according to a model-based approach) the risk of drone intrusions when such information is not explicitly provided or assessed by the sighting sources;
- monitoring (according to a model-based approach) the temporal evolutions and trends of the risks of drone intrusions, even for databases lacking of risk information.

The modelling has been performed by means MATLAB (Statistics and Machine Learning Toolbox).

The model has been built for the classification of the risk level of a drone unauthorized intrusion (according to the criteria provided in Table 5) as a function of the following features (i.e., inputs):

- the sighting altitude;
- the distance of the nearby airport with respect of the intrusion location;
- the affected airport.

Thus, the proposed target function represents a **risk classification function**, working on the previous features as inputs. This function may be useful to verify the possibility of estimating the risks of drone intrusions, even starting from databases lacking of an explicit risk information.

The available UKAB reports about airports, in number of 310 reports, have been used for the training of the classification model, which has to estimate the risk level by using the previous features as inputs.

In detail, a **Fine Gaussian Support Vector Machine** (SVM) [27] has been designed according to a **supervised learning** approach for machine learning. Indeed, supervised learning prescribes the machine learning of a classification function by means of known input-output pairs, which represent the set of training data. Thus, the training data are "labelled" since the output label (i.e., the classification) is provided for the available training inputs. In this case, the label is specified by means of the risk level estimated by the sources of the sighting and indicated in the UKAB sighting reports. The adopted algorithm for the supervised learning analyses the training data and infers the risk classification function, which can be used for mapping new examples without labels (i.e., without the explicit risk levels, as in sighting records that do not report this information).

As an example, Figure 12 reports the achieved predictions as a function of the airports and the airport distances. The different colours of the points represent the different risk levels estimated by the classifier. Given that the model has been designed in order to provide a feasibility check, a detailed validation (e.g., by means of cross-validation to analyse overfitting problems) has not been performed.

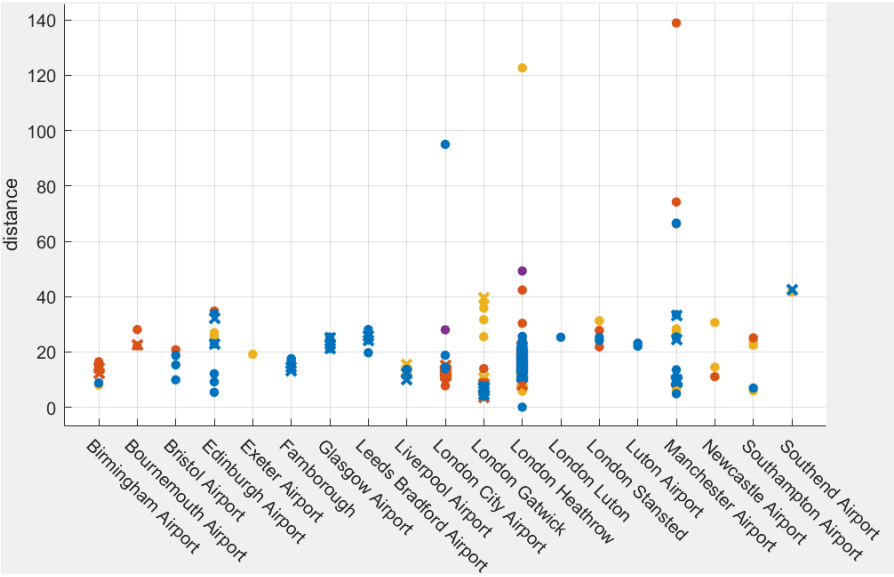

Figure 12. Scatter plot of the predictions of the risk classification model for UKAB sighting reports affecting airports ("o" for correct and "x" for wrong).

Clearly, the developed model is just an example for the possibility of building predictive for the features of the phenomenon of unauthorized drone intrusions in airport. Greater accuracies are expected by:

- using more training data (i.e., more labelled sighting reports with the risk levels);
- using other inputs for the classification (e.g., the time of the day, meteorological conditions, etc.).

5.3 Vulnerability Index Study

A vulnerability index study has been performed in the form of a preliminary analysis. Such analysis has the following objectives:

- to verify the possibility of defining an **Airport Vulnerability Index** (**AVI**) to quantify the exposure or susceptibility of an airport with respect to unauthorized drone intrusions, coherently with the basic definitions in section 2.3.8;
- to provide some preliminary considerations about the definition of such index;
- to highlight possible additional data that would provide an added value for the identification of a complete "operational picture" underlying the processing of the airport vulnerability index.

With respect to the basic definitions in section 2.3.8, a tailoring has been performed in order to adapt the definitions and practices of a generic vulnerability index to the context of the proposed analysis, i.e., to the phenomenon of unauthorized drone intrusions in airports. In detail, for the sake of this analysis, the target is represented by the **threat** of unauthorized drone intrusions in airport, which replaces the hazard concept in section 2.3.8.

Thus, an exhaustive definition of the AVI shall address the quantification of a **threat exposure** or **susceptibility** (instead of the hazard exposure, wherein the threat is represented by the unauthorized drone intrusions in airports), by breaking it down into the following components:

- the **threat likelihood** (instead of the hazard likelihood);
- the **threat mitigation** (instead of the hazard mitigation).

The following relationship holds:

$$\mathrm{AVI}_{\mathrm{drone}} = f\big(P(\mathrm{drone}), M(\mathrm{drone})\big),$$

wherein $P(\mathrm{drone})$ is the likelihood function of a drone intrusion in the reference airport for the AVI, $M(\mathrm{drone})$ is the mitigation function of a drone intrusion in the reference airport, and $f(\cdot)$ is the combination function of the threat likelihood and the threat mitigation for the definition of the threat exposure (i.e., the AVI). *This function quantifies the exposure or the susceptibility of an airport in regard to unauthorized drone intrusions*.

Given that the definition of a vulnerability index has to address the different vulnerability dimensions (as described in section 2.3.8), both $P(\mathrm{drone})$ and $M(\mathrm{drone})$ may generically expressed as a multidimensional combination of different functions, each one related to a single dimension. For example:

$$P(\mathrm{drone}) = g\big(d_{\mathrm{social}}(\cdot) + d_{\mathrm{economic}}(\cdot) + d_{\mathrm{ecological}}(\cdot) + \cdots\big).$$

The functions $d_{\text{social}}(\cdot)$, $d_{\text{economic}}(\cdot)$, $d_{\text{ecological}}(\cdot)$, etc., represent multiple quantitative indicators to be used as **dimensional influence variables** for the AVI, *each of which quantifies the influence of a given dimension of the airport's context (e.g., social, economic, etc.) on the exposure or susceptibility of the airport in regard to unauthorized drone intrusions*.

In order to preliminarily verify the potential of the definition of the AVI index, an analysis has been performed starting from the available public record databases. As indicated by $P(\text{drone})$ expression in the last equation, such analysis requires also some additional data to be used as dimensional influence variables, i.e., the economic-dimension influence, the social-dimension influence, etc. Given the preliminary nature of the analysis, only the following public socio-economic data have been found to be useful for the proposed activity in regard to FAA reports:

- the population of the States in the USA;
- the number of registered drones for each State in the USA.

To the contrary, equivalent data have not been found for the UK in regard to UKAB reports. Thus, these reports have not been considered for this analysis.

Given the available inputs for the analysis, the analysis itself has aimed at the following objectives:

1. *Providing an estimator of the* $\mathrm{P}(\text{drone})$ *function in the case of all the FAA airports in a given State and in a given year*
    - Only the likelihood function $\mathrm{P}(\text{drone})$, and not the mitigation function $M(\text{drone})$, has been studied since the available FAA reports directly show only information about the occurrences of drone sightings, whereas they do not show information about the impacts and the mitigation actions in regard to the airports.
    - Formally, the term *estimator* is used since it represents an estimation (i.e., a prediction) of the real value of $\mathrm{P}(\text{drone})$. Clearly, such estimation is an approximation, e.g., due to the unavailability of all the possible inputs related to influence variables, due to modelling errors, etc. The *accuracy of the estimation* may be measured by comparing the real number of drone intrusion occurrences (as reported in FAA data) and the predicted number of drone intrusion occurrences according to the developed estimator.
    - The analysis has been performed at an aggregated State-level (and not at a local level for the single airports) since the available socio-economic indicators (population and number of registered drones) refer to a geographical State-scale. Note that an individual analysis for the single airports (even if theoretically valuable) has not been performed since it requires local data about the regions, i.e., the proximity socio-economic information with respect to the reference airport.
    - The analysis has been performed on a yearly time horizon, i.e., to develop a predictor of the number of drone intrusions in a given year. The choice is also due to the application of the FAA data in section 5.1, which refer to a single year. Clearly, the

same approach may be applied also for different time horizons (e.g., seasons, months, etc.).

2. *Characterizing the estimator of the* $\mathrm{P}(\mathrm{drone})$ *function as a function of socio-economic data*

    - This choice is strictly related to the nature of the available inputs (population and number of registered drones for each State), which represent socio-economic indicators.

Thus, the proposed analysis may provide some preliminary considerations for the definition of an ***estimator*** *of an Airport Vulnerability Index as a* ***function of socio-economic indicators*** (e.g., population, number of registered drones, etc.).

Fitting model with a quadratic-polynomial structure have been developed for the estimator $\hat{P}(\mathrm{drone})$ of the yearly number of unauthorized drone intrusions in a given State. For example, Figure 13 reports the correlation fitting model between the population and the number of drone sightings (2016-2020) for by-State FAA airports. The accuracies of the developed fitting models for the estimator have been evaluated by means of the coefficient of determination R^2. In detail, this is 0.8724 for the model in Figure 13, which means that the achieved estimator explains about the 87% of the variance in the correlation between the input variable (State population) and the estimated variable (the yearly number of drone sightings in a State). Thus, the population density determines an **Airport Socio-Geographical Vulnerability Index** for the unauthorized drone intrusions in airports.

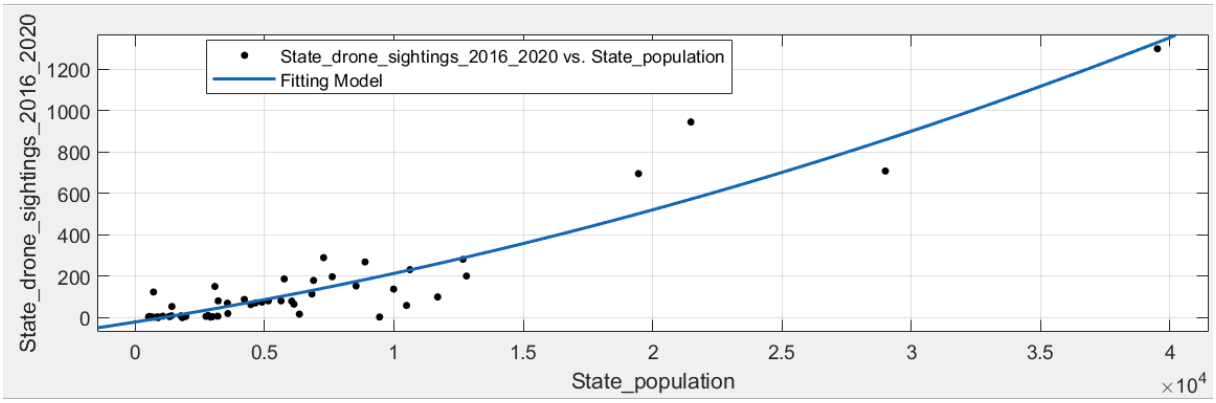

Figure 13. Correlation fitting model between the population and the number of drone sightings (2016-2020) for by-State FAA airports.

Clearly, a greater collection of data could validate the above considerations, leading to the definition of a sound model for the AVI. In general, other data (so, other dimension-related indicators for vulnerability) are expected to influence an airport's exposure to drone intrusions, such as the followings:

- the type of airport;
- the airport's traffic or number of airport operations;

- the unmanned traffic (if any);
- the season;
- meteorological conditions;
- the actual number of purchased drones in the proximity region of the airport;
- the counter-UAS solutions in the airport;
- the legal framework for drones in the country of the airport;
- etc.

6 Vulnerability Assessment of Operations (Runway and Ground) to Intruder Drones and Critical Operation List

This section reports the main results achieved by task T1.3 “Vulnerability assessment of operations (runway and ground) to intruder drones and Critical Operation List”.

The detailed description of the results is available in deliverable D1.3 [5], which is confidential. More information is accessible on request on website https://www.asprid.eu/.

6.1 Detailed Functional Description of Nominal Airport Operations

The reference airport operations have been modelled by breaking down the operations themselves in a structured and hierarchical set of **phases** and **tasks**. In detail, an HTA-based approach has been applied, wherein:

- phases represent the first level of the operational hierarchy and are a coherent grouping of actions for a specific goal;
- tasks represent the last level of the operational hierarchy and they belong to a given phase, thus, they are the elementary actions to achieve the goal of the reference phase.

Each phase may be represented in terms of the following attributes:

- *identifier* – unique numerical identifier of the phase;
- *name* – a descriptive label of the phase.

Each task may be represented in terms of the following attributes:

- *identifier* – unique numerical identifier of the task;
- *name* – a descriptive label of the task;
- *action description* – a descriptive summary of the action related to the task;
- *type* – the class of the action related to the task;
- *actor* – the actor responsible for the execution of the action related to the task;
- *location* – the physical location (e.g., airport’s asset) wherein the action is performed;
- *resource* – the physical resource(s) required for the execution of the action;

- *duration* – the time duration generally (i.e., on average) required for the execution of the action;
- *input* – the input(s) required for the execution of the action;
- *output* – the output(s) delivered by the execution of the action;
- *precondition* – logical condition(s) or event(s) that have to be satisfied before the execution of the action;
- *postcondition* – logical condition(s) or event(s) that will be satisfied after the execution of the action.

In regard to the type of task, the following classification is currently adopted:

- *sequential* – a task which cannot be performed in parallel with other tasks;
- *parallel* – a task which may be performed in parallel with other tasks.

For example, Table 6 reports a summary technical specification of the approach phase. The detailed technical specification is available in [5].

Table 6. Summary technical specification of the approach phase.

Phase	Task	Action Description	Actor	Location	Resource
Approach	**Runway Clear**	Verify no aircraft, vehicles, people or FOD on the runway prior its use	ATCO	Runway	*Radio communication (ATC instructions)* *Surveillance system (radar display system)*
	ATC clearance	Approach is approved by the TWR control service	ATCO	OLS Runway	*Radio communication (ATC instructions)* *Navigation systems (VOR, DVOR, ILS, NDB…)* *Surveillance system (radar display system)* *Standard instrument arrivals Carts (STAR)* *Approach and Runway lighting* *Radio failure procedure*
	Precision approach (CAT I, II or III)	Final approach segment: to the RWY (from 6NM to the RWY threshold) following a usually 6% slope of descent	Pilot	OLS Runway	*Radio communication (ATC instructions)* *Navigation systems (VOR, DVOR, ILS, NDB…)* *Surveillance system (radar display system)* *Standard instrument arrivals Carts (STAR)* *Approach and Runway lighting* *Radio failure procedure*

	Non-precision approach	Final approach to the RWY (from 6NM to the RWY threshold) freely flown to a predefined level	Pilot	OLS Runway	*Radio communication (ATC instructions)* *Navigation systems (VOR, DVOR, ILS, NDB…)* *Surveillance system (radar display system)* *Standard instrument arrivals Carts (STAR)* *Approach and Runway lighting* *Radio failure procedure*
	VFR approach	Final approach to the RWY, by joining defined access points to enter the ATZ and proceed to fly the airport pattern	Pilot	OLS Runway	*Radio communication (ATC instructions)* *Visual Approach Cart (VAC)* *Radio failure procedure*
	Missed approach	Final approach cannot be continued to a successful landing. Aircraft would follow ATC instruction. Usually it will re-join the aerodrome circuit and proceed to try to approach.	Pilot ATCO	OLS Runway	*Radio communication (ATC instructions)* *Missed approach procedures* *Radio failure procedure*

6.2 Operational Vulnerability Assessment

The **Operational Vulnerability Assessment** (**OVA**) is the assessment of the weaknesses of the operations of the reference system, which may be exploited by one or more threats in several threat scenarios. The framework developed in ASPRID project prescribes a quantitative evaluation for such assessment, by assigning an **Operational Vulnerability Index** (**OVI**) to the airport operations in a given threat scenario. In other words, the OVI represent an indicator of the vulnerability (i.e., weakness) of an operation with respect to a specific threat scenario. In general, the one and same operation will exhibit different OVI values for different threat scenarios.

In ASPRID, the proposed strategy for the OVA is:

- **task-based**, since it is performed on a task basis, i.e., by assigning an OVI to each task within the reference operations/phases in a specific threat scenario;
- **functional-based**, since the evaluation of the OVI takes into account the impact of the threat scenario on the functional behaviour of the tasks;
- **performance-based**, since the evaluation of the OVI takes into account the impact of the threat scenario on the operations along different performance dimensions, and not just the safety performance.

The OVI assigned to each task is also named **Task Vulnerability Index** (**TVI**). This represents an indicator of the vulnerability (i.e., weakness) of a task with respect to a specific threat scenario. This indicator

has been evaluated by considering the impact of a threat scenario on each task in terms of both functional aspects and performance aspects.

The **Critical Operation List** (**COL**) is defined for a given threat scenario as the ranking of the tasks according to their TVI values.

In the end, for the purposes of the analysis of this document, the OVA for the threat scenarios provide:

- an evaluation of the vulnerability of tasks of the system without protections or mitigations against the threats (i.e., the unauthorized intrusions of drones in the airport);
- an evaluation of safety performance degradations and task vulnerabilities according to the principle of **worst-case scenario**;
- an assessment of the **non-cascading effects** or **first-level effects** of the threat scenarios on the operations.

In particular, the choice for the latter bullet is justified by the intention of consolidating and illustrating the proposed basic approach for the OVA of airport drone intrusions. This implies the reporting of just the tasks for the operations/phases that are directly impacted by the threat scenario.

For the functional part, a **functional effect** is defined as the impact of a threat scenario on a task considering the function that the task has to perform.

6.2.1 Task Functional Effect and Task Functional State

The operational effect is assessed by evaluating the **functional state** of the task in the threat scenario, that is the execution mode of the task induced by the occurrence of the threat scenario.

Table 7 reports the possible values for the functional state of a task in a threat scenario.

Table 7. Classification of the functional states of a task in a threat scenario.

Functional State	Description
Normal	It is the functional state of a task whose execution is not altered by the occurrence of the reference threat scenario. In this state, the task functioning is as intended and its execution goes on as in the nominal case from a functional point of view.
Degraded Mode	It is the functional state of a task whose execution is performed in a degraded mode due to the occurrence of a threat scenario. The execution in a degraded mode consists in a reduced level of service for the task, by maintaining service continuity. This state is normally related to a performance degradation of the task.

Functional State	Description
Loss	It is the functional state of a task whose execution fails due to the occurrence of the reference threat scenario. The failure consists in the loss of the service for the task.

6.2.2 Task Performance Effect and Task Performance Degradation

Concerning performance, a **performance effect** is defined as the impact of a threat scenario on a task from a performance point of view. The performance effect is assessed by evaluating the **performance degradation**, that is the reduction of the performance levels achieved by the task due to the occurrence of the threat scenario. Clearly, a performance degradation generally occurs only for tasks which exhibit a "degraded behaviour" in the threat scenario, i.e., which enter a functional state that is *Degraded Mode* (see Table 7).

For the purposes of the analysis in ASPRID, the performance degradation of a task has been evaluated along the following performance dimensions: **safety**, **time**, **workload**, **passenger satisfaction**.

Reference [5] presents a possible approach the classification of performance degradations, but it should be considered as an example. Indeed, the level of detail and the complexity of tables for risk classification should be adapted to the needs and complexities of each airport. As an instance, Table 8 reports the possible values for the time performance degradation in a threat scenario.

Table 8. Classification of the time performance degradation of a task in a threat scenario.

Time Performance Degradation	Description
High	Level of time performance degradation of a task in a threat scenario with one of the following conditions: • major or significant delay in completing the task.
Medium	Level of time performance degradation of a task in a threat scenario with one of the following conditions: • moderate delay in completing the task.
Low	Level of time performance degradation of a task in a threat scenario with one of the following conditions: • negligible or minor delay in completing the task.

6.2.3 Task Vulnerability Index

A possible classification of the TVI levels is reported in Table 9. The strategy is to extend the global outcome categorization of a threat scenario in an airport by considering the functional-based and the performance-based views for the operational vulnerability assessment on a task basis.

Table 9. Classification of the Task Vulnerability Index of a Task in a threat scenario.

Task Vulnerability Index	Description
1	The threat scenario causes an off-nominal behaviour of the task, which is represented by a functional state that is *Degraded Mode* or *Loss*. The off-nominal behaviour of the task in the threat scenario causes deaths or a or a severe interruption to airport operations. For this vulnerability value, the followings are the typical maximum levels of task performance degradation: • safety performance degradation: *Catastrophic*; • time performance degradation: *High*; • workload performance degradation: *High*; • passenger satisfaction degradation: *High*.
2	The threat scenario causes an off-nominal behaviour of the task, which is represented by a functional state that is *Degraded Mode* or *Loss*. The off-nominal behaviour of the task in the threat scenario causes severe injuries or a or a major interruption to airport operations. For this vulnerability value, the followings are the typical maximum levels of task performance degradation: • safety performance degradation: *Hazardous*; • time performance degradation: *High*; • workload performance degradation: *High*; • passenger satisfaction degradation: *High*.
3	The threat scenario causes an off-nominal behaviour of the task, which is represented by a functional state that is *Degraded Mode* or *Loss*. The off-nominal behaviour of the task in the threat scenario causes light injuries or a or a moderate interruption to airport operations. For this vulnerability value, the followings are the typical maximum levels of task performance degradation: • safety performance degradation: *Major*; • time performance degradation: *Medium*; • workload performance degradation: *High*; • passenger satisfaction degradation: *High*.

Task Vulnerability Index	Description
4	The threat scenario causes an off-nominal behaviour of the task, which is represented by a functional state that is *Degraded Mode* or *Loss*. The off-nominal behaviour of the task in the threat scenario causes personal distress or a small interruption to airport operations. For this vulnerability value, the followings are the typical maximum levels of task performance degradation: • safety performance degradation: *Minor*; • time performance degradation: *Medium*; • workload performance degradation: *Medium*; • passenger satisfaction degradation: *Medium*.
5	The threat scenario does not cause a real off-nominal behaviour of the task, which is represented by a functional state that is *Normal* or *Degraded Mode*. The behaviour of the task in the threat scenario does not affect the airport operations. For this vulnerability value, the followings are the typical maximum levels of task performance degradation: • safety performance degradation: *Negligible*; • time performance degradation: *Low*; • workload performance degradation: *Low*; • passenger satisfaction degradation: *Low*.

In the same way of the approach for performance degradation classification in section 6.2.2, the proposed approach for the quantification of TVI represents an example and it may be customized according to the needs and complexities of the specific airport.

6.2.4 Assessment Results

The following threat scenarios are considered in this work as reference examples of the proposed approach for the OVA:

- **Threat scenario #1** – *Unauthorized operations of a drone in the arrival path of the runway*.
- **Threat scenario #2** – *Unauthorized operations of a drone in the departure path of the runway*.
- **Threat scenario #3** – *Unauthorized operations in proximity of boarding/de-boarding passengers*.

These scenarios have been employed since they impact on different operations, phases, actors and locations, according to the technical specification.

In regard to a generic airport, reference [5] provides the detailed results of the assessment in terms of:

- the detailed description of the impacted features of nominal airport operations;
- the OVA of each threat scenario;
- the COL for each threat scenario.

As an example, in regard to for threat scenario #1, Figure 14 and Table 10 respectively report the OVA results (for the Approach phase) and the COL.

			Unauthorized Operations of a Drone in the Arrival Path of the Runway						Description
			Operational State	Safety Performance Degradation	Time Performance Degradation	Workload Performance Degradation	Passenger Satisfaction Degradation	Vulnerability	
Operation	Approach								
Phase	Phase Id	Phase Name							
	1	Final Approach							
Tasks	Task Id	Task Name							
	1.1	Runway Clear	Degraded Mode	Negligible	Medium	High	Low	3	A high increment of the workload of ATCO and of the task time are expected without supports systems for the identification and tracking of the intruder drone.
	1.2	ATC clearance	Degraded Mode	Negligible	Medium	High	Low	3	A high increment of the workload of ATCO and of the task time are expected without supports systems for the identification and tracking of the intruder drone.
	1.3	Precision approach (CAT I, II or III)	Degraded Mode	Negligible	Low	Medium	Low	4	For the interaction with ATCO, a medium increment of the workload of the pilot is expected for approaching aircraft.
	1.4	Non-precision approach	Degraded Mode	Negligible	Low	Medium	Low	4	For the interaction with ATCO, a medium increment of the workload of the pilot is expected for approaching aircraft.
	1.5	VFR approach	Degraded Mode	Negligible	Low	Medium	Low	4	For the interaction with ATCO, a medium increment of the workload of the pilot is expected for approaching aircraft.
	1.4	Missed approach	NA	NA	NA	NA	NA	NA	Off-nominal tasks are not considered.

Figure 14. Operational vulnerability assessment for threat scenario #1 (Approach phase).

Table 10. Critical operation list for threat scenario #1.

Task		TVI
Task Id	Task Name	
2.1	*Landing*	2
1.1	*Runway Clear*	3
1.2	*ATC Clearance*	3
2.2	*Runway Taxiing*	3
7.4	*Runway Clear*	3
1.3	*Precision approach (CAT I, II or III)*	4
1.4	*Non-precision approach*	4
1.5	*VFR Approach*	4
2.3	*Runway clearance by rapid exist taxiway*	4
2.4	*Runway clearance by taxiway at the runway end*	4
2.5	*Runway clearance by using the runway turn pad*	4
2.6	*Runway Clear*	4

6.3 Event Tree Analysis

In the context of ASPRID, the Event Tree Analysis (ETA) helps to assess the acceptability of a risk related with drone intrusion in or near the airport. An illustration of an Event Tree is provided in Figure 15, according to the Event Sequence Diagram notation used by the CATS tool developed by NLR [28].

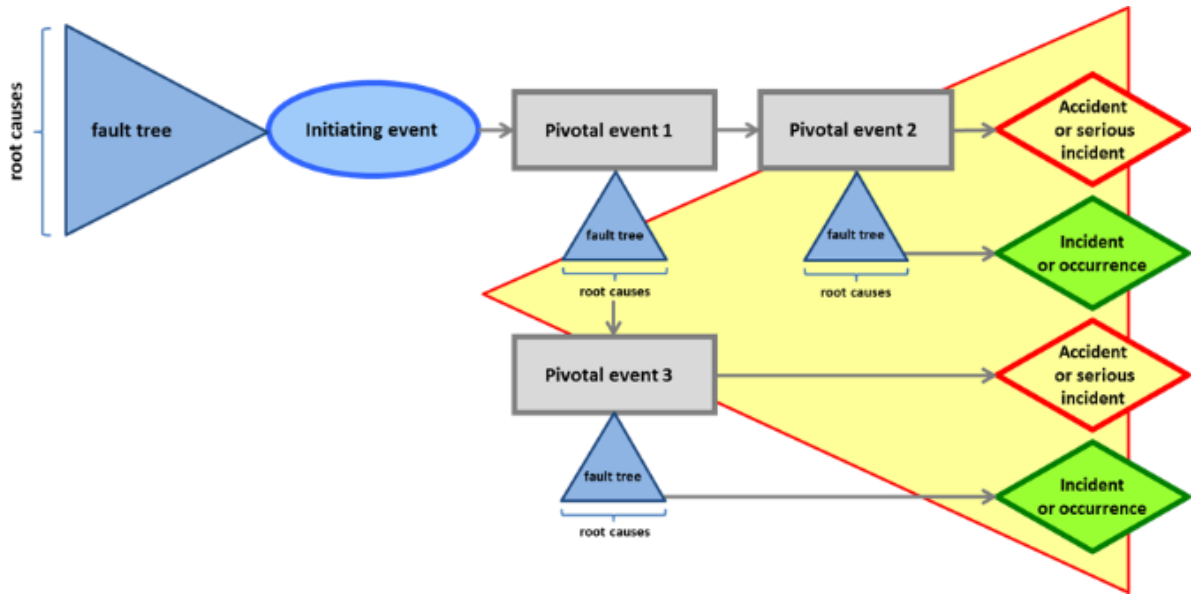

Figure 15. Illustration of an Event Tree.

The Event Tree describes in a graphical way sequence of events leading to various safety outcomes that could include no safety effect, Incident, serious Incident or Accident. The first event of the sequence is called the initiating event, the next events in the sequence (also called Branch) are called pivotal events. These events have generally two outgoing arrows to be followed whether the pivotal occurs or not. In the previous figure, the outgoing horizontal arrow is followed when the pivotal event occurs and the vertical arrow is followed when the pivotal event does not occur. So, in this Event Tree, a sequence starting with the initiating event followed by Pivotal events 1 and 2 would lead to an Accident or serious Incident whereas the sequence where Pivotal event 1 occurs but events 2 does not occur would only lead to an Incident.

A major benefit of an Event Tree is that it provides a graphical synthesis of all possible safety outcomes of the sequences of events considered. But, as you should consider for each pivotal event whether it occurred or not, the Event Tree size rapidly grows with the number of pivotal events considered. In practice, one should limit the number of pivotal events in order to obtain a useful Event Tree. As the previous figure shows it, a Fault Tree could be attached to each event in the Event Tree. This helps to limit the number of pivotal events. The Fault Tree can be used to describe how combinations of events that we do not want to consider as pivotal event lead to a pivotal event.

We have developed a **Generic Event Tree** that would be applicable to analyse various types of threats and that is a part of the developed methodological framework for risk assessment of airport drone intrusions. Figure 16 shows the structure of such Generic Event Tree. We used 3 pivotal events that are directly linked with the main technical capabilities of a system protecting the airport against drones following EUROCAE ED-286 [29]:

- Detect: capability to detect, identify and track a drone.
- Decide: capability to assess whether a detected drone could cause a risk and decide the best mitigations to be undertaken for the next step of the current operation.
- Mitigate: capability to reduce the severity of a drone threat. This capability includes technical means to neutralize of the drone or means to send alarms to a remote pilot but it does not include operational mitigations of airport tasks.

Event Tree : Intrusion of [TYPE] drone in [LOCATION] when [OPERATION] is occurring									Op. Outcome (TVI)					
Bid	Threat Scenario	IProba	Detect	EProba	Decide	EProba	Mitigate	EProba	BProba	Task1	Task2	Task3	Task4	Task5	Acceptable ?
1	Intrusion of [TYPE] drone in [LOCATION] when [OPERATION] is occurring	1,0E-02	ok: The intruder drone is efficiently detected by technical means.	0,5	ok: the threat is efficiently assessed by technical means.	0,5	ok: Technical mitigation means are efficiently.	0,5	**1,3E-03**	4	4	4	4	4	yes
2							nok: Technical mitigation means are not efficient.	0,5	**1,3E-03**	3	3	4	4	4	yes
3					nok: the threat is not efficiently assessed by technical means.	0,5	ok	0,6	**1,5E-03**	3	3	4	4	4	yes
4							nok	0,4	**1,0E-03**	2	3	3	4	4	no
5			nok: The intruder drone is not efficiently detected by technical means.	0,5	ok	0,6	ok	0,7	**2,1E-03**	3	3	4	4	4	yes
6							nok	0,3	**9,0E-04**	2	3	3	4	4	no
7					nok	0,4	ok	0,9	**1,8E-03**	2	3	3	4	4	no
8							nok	0,1	**2,0E-04**	2	2	3	4	4	no

Figure 16. Generic Event Tree for the developed methodological framework of risk assessment of airport drone intrusions.

First of all, the initiating event is a threat scenario of the form "*Intrusion of [TYPE] drone in [LOCATION] when [OPERATION] is occurring*". Then, the column labelled "Acceptable?" gives the yes/no answer to the following question: is the computed probability of the branch smaller than the target probability of its operational outcome? In the case of a non-acceptable branch then certainly operational mitigations (such as aborting or delaying tasks) should be considered in order to modify the TVI of the tasks and consequently reduce the severity of the operational outcome of this branch. In the generic

tree we have used the following target values: 5.10^{-2} for a branch whose most severe task is TVI 4, 5.10^{-3} for a branch whose most severe task has TVI 3 and 5.10^{-4} for a branch whose most severe task has TVI 2.

In the Generic Event Tree, the threat scenario includes a description of the type of the drone. This may be related also to UTM scenarios, such as:

- Off-nominal cooperative drone: The drone is authorized to operate near the airport but it is not following its agreed flight plan yet it is a cooperative drone broadcasting its e-identification.
- Off-nominal in category Open C0: This type of drone does not need an authorization to be operated outside of the airport and it does not need to broadcast its e-identification. It is a low risk drone that flies away from its authorized flight zone.

Finally, we could also consider the situation where there is no drone intruding the airport. This situation would be used to assess false-alarm scenarios, where the "Detect" capability would incorrectly detect an intruding drone potentially leading to the spurious activation of mitigations that could have an operational effect on the airport operations.

Another extension with respect to classical Event Tree is that we directly use the result of the Operational Vulnerability Assessment in order to describe the outcome of a sequence of events on the airport operations. In the Generic Event Tree described in the previous figure, the columns under the label "Operational Outcome (TVI)" give the Task Vulnerability Index (TVI) for each task in the operation considered by the threat scenario.

For example, the last branch of the Event Tree (the one with Branch identifier Bid=8) is the worst-case scenario where all technical protection means are not efficient. Only non-technical means could be used to protect the airport against drones. As this is the worst-case scenario, the TVI is directly extracted from the Operational Vulnerability Assessment result presented in the previous sections.

For other branches representing less severe scenarios we included improved TVI because the impact on airport tasks would be less severe. Branch 1 represent the best-case scenario where all technical means are efficient in that case we would apply maximal improvement of TVI for all airport tasks. For less degraded scenarios such as branches 2, 3 and 5 that include the loss of efficiency of only one capability we consider a moderate improved TVI. Finally, the remaining branches represent severely degraded scenarios where two out of the three capabilities are not efficient. We consider in that case a very limited improvement of the TVI.

Detailed results about the Event Tree implementation for a generic airport are available in [5].

7 Risk Scenarios Definition

This section reports the main results achieved by task T1.4 “Risk scenarios definition”.

The detailed description of the results is available in deliverable D1.4 [6], which is confidential. More information is accessible on request on website https://www.asprid.eu/.

7.1 Reference Scenario

Task T1.4 has further developed the methodological framework of risk assessment by adapting it to a specific reference scenario, which is a set of:

- a reference airport;
- a reference threat scenario.

Milan Malpensa Airport (IATA: MXP / ICAO: LIMC) has been chosen as a reference airport for the evaluation of threat scenarios. The airport is located 49 kilometres from central Milan, has two passenger terminals as well as a dedicated cargo terminal. It presents two runways in a parallel configuration, as shown in Figure 17, with various taxiways connecting these with the aforementioned terminals and other airside areas.

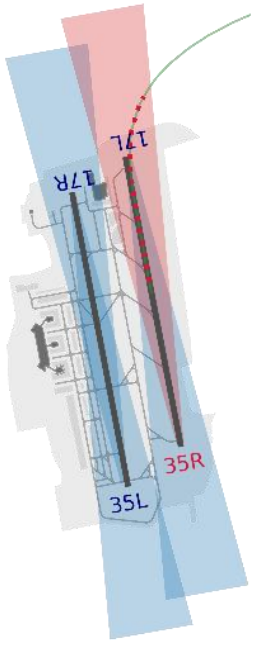

Figure 17. Milan Malpensa (LIMC) runways and departure paths.

In 2019, Milan Malpensa handled 28.846.299 passengers and was the 20th busiest airport in Europe and the 2nd busiest airport in Italy in terms of passengers. In terms of cargo and freight, in 2019, it was the 6th busiest airport in Europe and 1st in Italy.

It has been be considered a good reference airport for this study because it is of medium complexity regarding the other European airports, but nonetheless handles a great number of passengers, so an UAS threat could cause great safety issues and economical losses.

Instead, the reference threat scenario is the threat scenario #2 in section 6.2.4, i.e.:

- *Unauthorized operations of a drone in the departure path of the runway*.

The selected threat scenario is relevant also from the point of view of guidance material and historical data. For example, several FAA reports analysed in D1.2 [4] highlight an impact on departing aircraft by drone intrusions, even if they do not provide an explicit indication about the exact position of the intruder drone with respect to the airport.

7.2 Assessment Results

This section reports a summary of the results for the risk assessment of the reference scenario. The detailed results are available in [6].

The threat analysis, the functional description of nominal airport operations and the OVA are the same as in the "basic" methodology framework, which are respectively described in section 4.1, in section 6.1 and in section 6.2.

7.2.1 Airport Vulnerability Index

The AVI has been adapted to the reference scenario, on the basis of the data provided by courtesy courtesy of the Italian Aviation Authority, ENAC (Ente Nazionale per l'Aviazione Civile). In detail, the yearly data of airport drone intrusions in Italy (2015-2020) and the total number of registered drone operators in Italy have been used as significant inputs to infer an AVI model for the reference scenario.

In this specific case, a linear structure has been applied for the model of the AVI within Italian airports, which is two-dimensional with the following expression:

$$\hat{P}(\text{drone},year) = p_{10} \cdot n_{\text{drones}}(year) + p_{01} \cdot n_{\text{airport\_movements}}(year) + p_{00},$$

wherein p_{10}, p_{01} and p_{00} are the fitting real coefficients.

The achieved coefficient of determination R^2 for this model is equal to 0.9365. Thus, the designed estimator explains about the 93.7% of the variance in the correlation between the input variables (the yearly number of drones and the yearly number of airport movements in Italy) and the estimated variable (the yearly number of airport drone intrusions in Italy). Such analysis suggests that the number

of drones and the number of airport movements determines an effective **Airport Socio-Economic Index** to quantify airport vulnerabilities with respect to drone intrusions.

An alternative model may be developed without considering the data of 2020, which should present anomalies due to the influence of COVID-19 pandemic. However, the magnitude order of the provided vulnerability estimations should not change due to the normalization with respect to airport movement data. Moreover, the influence of the pandemic is still on-going also in 2021 and may be evaluated in future ASPRID activities.

Based on the results for the definition of an AVI model in Italy, a possible estimation in 2021 has been derived for Milan Malpensa airport. The inputs for the estimation have been represented by:

- *Number of drones in Italy in 2021* – For this input, the current number has been kept.
- *Number of movements of Italian airport in 2021* – This input has been evaluated by using the current EUROCONTROL's measurement of traffic variation for Italian airports between 2020 and 2021 [30]. In particular, EUROCONTROL comprehensive assessment reports a variation of +29% in regard to the traffic level of Italy. Thus, the number of movements in 2021 has been predicted starting from the available data about number of movements in 2020[3] (703751) and by applying a growth factor of 29%.

Moreover, the following parameters have been estimated:

- *Number of drones influencing Milan Malpensa airport in 2021* – This input has been evaluated by assuming that the number of drone operators and the number of drones in a region are proportional to the population of the region.
- *Number of movements of Milan Malpensa airport in 2021* – This input has been evaluated by using the ratio between the number of movements of Milan Malpensa and the total number of airport movements in Italy in 2020[3].

By using these inputs, the fraction of $\hat{P}(\text{drone},2021)$ related to Milan Malpensa has been computed by using the previous percentages. The detailed results are available in [6].

7.2.2 Event Tree Analysis

Several detailed event trees have been developed for the reference scenario. Some aspects are similar for all the detailed event trees:

[3] https://assaeroporti.com/wp-content/plugins/multipage_xls_reader/pdf_file/2020.pdf, last accessed on July 14th, 2021.

- The Operational outcome has been updated with the result of the OVA for the take-off operation.
- We used the following target values: 10^{-2} for a branch whose most severe task is TVI 4, 10^{-3} for a branch whose most severe task has TVI 3 and 10^{-4} for a branch whose most severe task has TVI 2. These targets should be improved in the future with the analysis of historical data related with weather events and with drone incident.
- The probabilities of the pivotal events are related to the efficiency of the barriers (Detection, Decision, Mitigation) and have been quantified by partially considering some data provided by ENAIRE and AENA in regard to testing results of the efficiency of various Counter-UAS technical means.

Moreover, we have used EUROCONTROL Airport Corner website[4] to retrieve more precise information related with runway occupancy. It gives the maximum operations at peak hour by runway configurations. It also provides a frequency of runway configuration usage. This information is useful to quantify the probabilities of the initiating event related to the impacted runway by drone intrusion. For example, the maximum departure rate (40 departures/hour) is obtained with the configuration that allows to use both runways 35L and 35R for take-offs.

Collected ADS-B (Automatic Dependent Surveillance-Broadcast) data also provide another source of information in order to determine the runways used for take-off/landing at Milan Malpensa airport (LIMC). Most commercial flights operating on Milan Malpensa airport broadcast their positions through ADS-B technology. We used data from the OpenSky Network[5], a non-profit association based in Switzerland, providing the public (essentially researchers) with a large historical database of traffic data, collected through the multitude of sensors of OpenSky Network stakeholders. ADS-B data can be downloaded and processed with the Open Source Python library traffic[6].

We focused on flights from or to Milan Malpensa airport during a given timeframe. For instance, through the traffic library, we requested trajectories of all flights landing in LIMC during a month, limiting the part of each trajectory to the Milan Terminal Maneuvering Area (TMA). Once trajectories near airport have been filtered and resampled, it is possible to determine the runway used by the aircraft through additional functions provided by the traffic library. Basically, polygons are created around each runway and all the segments of the trajectory that intersect with these polygons are added to determine the runway that was probably used (with most segments). The collected data can provide very fine-grained statistics of runway occupancy for a given period of interest such as a day,

[4] https://ext.eurocontrol.int/airport_corner_public/.

[5] https://opensky-network.org/.

[6] https://traffic-viz.github.io/.

month, etc. When coupled with meteorological data such as wind strength and direction it can also provide a way to predict what is the runway configuration that is the most likely to be used.

Two Event Trees were developed for departure path of runways 35R or 35L: one for intrusion taking place at less from one km from the airport and the second one for intrusion taking place at a larger distance. For both of the event trees the probability of the threat scenario (in the cell "Threat Scenario") is computed using the Airport Vulnerability Index for Malpensa airport (addressed in section 7.2.1.) and the frequency of the runway configurations with departures on runways 35R or 35L.

The final Event Trees are available in [6]. As an example, Figure 18 reports the hypothetic assessment for an UTM scenario (intrusion of authorized off-nominal cooperative drone).

	Event Tree : Intrusion of **authorized off-nominal cooperative** drone in **LIMC 35 departure path** when **take-off** is occurring					**Op. Outcome (TVI)**							
Bid	**Threat Sc.**	**Detect**	**Decide**	**Mitigate**	**BProba**	**8.3 Take-off rotation**	**8.4 Take-off transition**	**8.6 Take-off path**	**1.1 Runway Clear**	**7.4 Runway Clear**	**8.1 ATC clearance**	**8.2 Take-off ground run**	**Acceptable ?**
1	3,9E-03	0,99	0,7	0,7	**1,9E-03**	4	4	4	4	4	4	4	VRAI
2				0,3	**8,0E-04**	3	3	4	4	4	4	4	VRAI
3			0,3	0,7	**8,0E-04**	3	3	4	4	4	4	4	VRAI
4				0,3	**3,4E-04**	2	2	3	4	4	4	4	FAUX
5		0,01	0,6	0,7	**1,6E-05**	3	3	4	4	4	4	4	VRAI
6				0,3	**6,9E-06**	2	2	3	4	4	4	4	VRAI
7			0,4	0,7	**1,1E-05**	2	2	3	4	4	4	4	VRAI
8				0,3	**4,6E-06**	2	2	2	3	3	3	3	VRAI

Figure 18. Event Tree for Intrusion of authorized off-nominal cooperative drone in LIMC 35 departure path when take-off is occurring.

7.3 Decision Support System for Operational Mitigation

Task T1.4 has also addressed the preliminary design of a **Decision Support System** (**DSS**) for the management of **operational mitigation actions** in regard to airport drone intrusions.

In detail, Figure 19 shows the relation between the Generic Event Tree and the operational mitigation strategy in the developed methodological framework. Such figure highlights the flows of the event tree that shall be managed by means of operational mitigation. However, Figure 19 is just qualitative.

Indeed, from a quantitative point of view, the operational mitigations will be effectively triggered when the risk level of a flow of the event tree exceeds the target level of acceptability for the risk, as described in section 7.2.2.

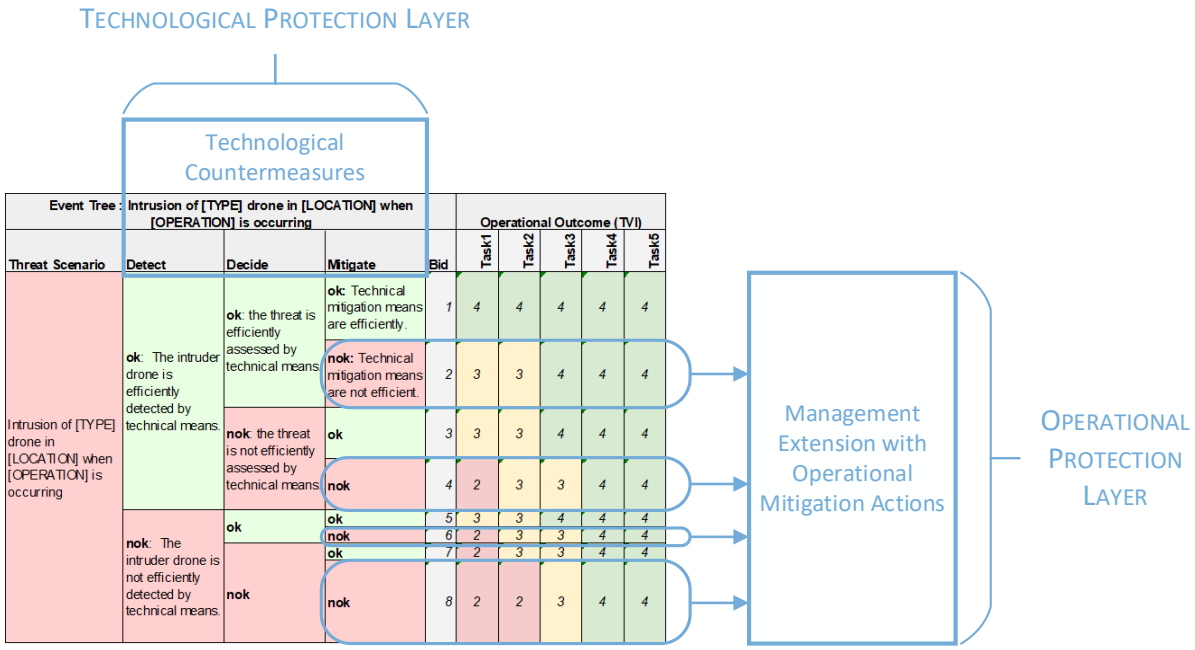

Figure 19. Relation between the Generic Event Tree and operational mitigation actions in ASPRID methodology.

Thus, technological countermeasures and operational countermeasures represent two different IPLs, named respectively **Technological Protection Layer** (**TPL**) and **Operational Protection Layer** (**OPL**). The OPL represents the reference of the DSS.

Generally speaking, a DSS is an information system that aids a decision-making process requiring:

- **judgment**, i.e., the evaluation of the context and of the situation (i.e., the situational awareness);
- **determination**, i.e., the selection of strategic decisions (e.g., long-term decisions);
- **sequence of actions** or **course of actions**, i.e., the selection of tactical decisions (e.g., short-term decisions) and the execution of the related actions.

A DSS may support some or all of the previous activities within a decision-making process, according to the high-level functional flow shown in Figure 20.

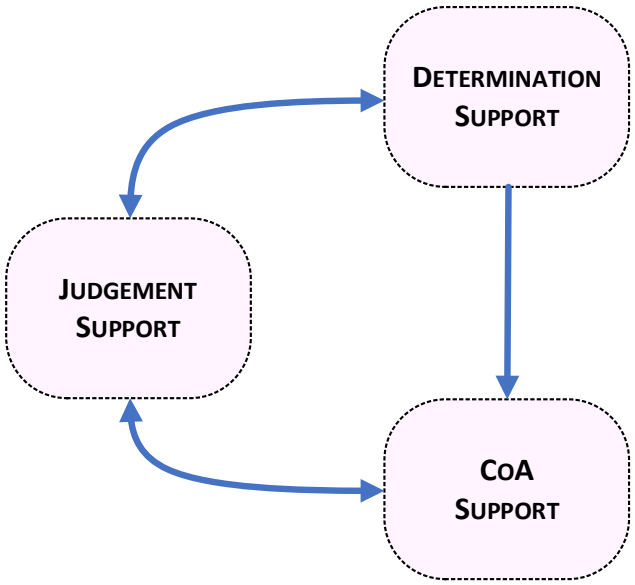

Figure 20. High-level functional flow of a generic DSS.

*The reference DSS shall be an information system that supports the **judgement** and the **sequence of actions** (or **Course of Actions**, **CoA**) for the management of the operational mitigation of an airport with respect to different threat scenarios related to drone intrusions*. In detail:

- For the judgement, the DSS shall support the **evaluation of the hazardous situation** and the **classification of the risk level** of the occurring threat scenario related to the current airport drone intrusion. The term hazardous situation is used since a situational awareness is required according to several inputs, not only in regard to the features of the intrusion, but also in regard to the background situation of the airport, i.e., for the on-going tasks and for the expected tasks within nominal operations.

- For the sequence of actions, the DSS shall support the execution of **contingency procedures** (or **emergency procedures** or **backup procedures**) by evaluating the best mitigation actions. In particular, a contingency procedure may be defined as *a contingency plan or a set of contingency plans, completed with type of actions, resources and evaluation rules*.

Moreover, such a DSS may be considered as *an information system which will implement an automated support for:*

- *the classification of the hazardous situation, by evaluating the risk level of the occurring threat scenario in regard to airport drone intrusions*;

- *the execution of the contingency procedures, by suggesting the proper sequence of actions to the reference end-users.*

The target end-users of this DSS are the following:

- Supervisor ASPRID Operator, for the Judgement Support;
- ATCOs, for both Judgement Support and CoA Support.

Based on the previous considerations, Figure 21 shows the high-level functional flow of the reference DSS, to be used as a starting modelling framework for the preliminary design.

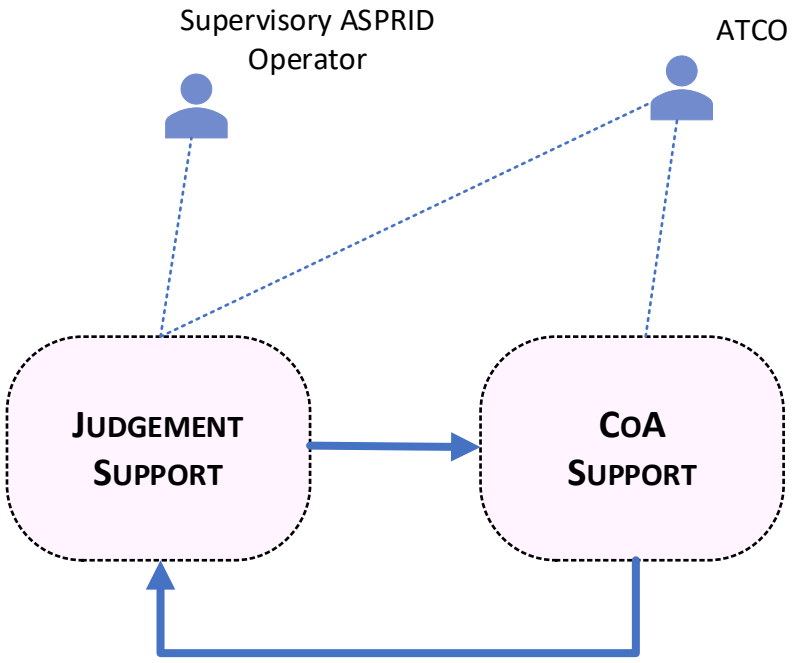

Figure 21. High-level functional flow of the reference DSS.

Clearly, EUROCONTROL's guidelines for contingency planning [31] have been considered for the definition the modelling paradigm in regard to the specification of the contingency procedures.

Figure 22 reports the preliminary architecture of the reference DSS. The figure highlights the **functional blocks** or **functional modules** required for the implementation of the DSS and their **functional interfaces**.

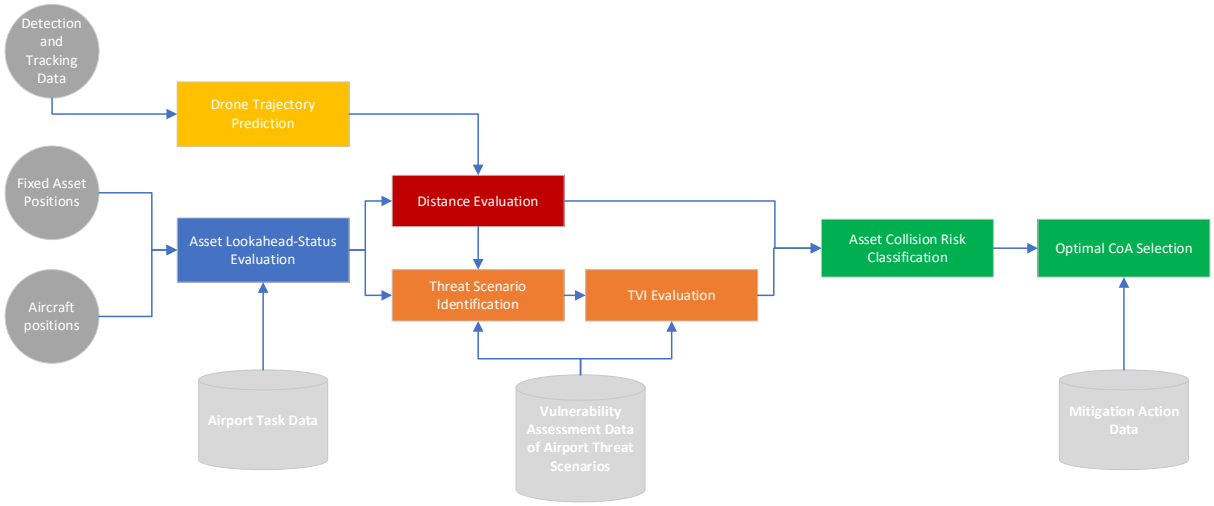

Figure 22. Preliminary architecture of the reference DSS.

The prescribed functional modules of the reference DSS are the following:

- **Drone Trajectory Prediction** – This module computes a prediction of the trajectory of the intruder drone in a given lookahead window, which is a time parameter. The prediction shall be driven by the outcomes of the Detection, Tracking and Identification system. Indeed, the features of the intrusion (e.g., the past trajectory of the drone, its type, its current speed and position, etc.) will be used for the prediction. The estimations shall be based on probability distributions, where available.

- **Asset Lookahead-Status Evaluation** – This module determines the future status of all the critical assets involved in airport operations, including both fixed assets and mobile assets (i.e., aircraft). The prediction starts from the current status. For fixed assets, the status is simply the static position of the asset with its safety radius. For mobile assets, the status is the combination of their position and their task, jointly with the safety radius. The lookahead window for the status evaluation shall be the same of the drone trajectory prediction.

- **Distance Evaluation** – This module estimates the physical distance between the predicted position of the drone and each asset with respect to the safety radius in its lookahead-status evaluation, when applicable. The estimations shall be based on probability distributions, if available in the Drone Trajectory Prediction. Such estimations will represent the **likelihood** component for risk classification.

- **Threat Scenario Identification** – This module identifies the occurring threat scenario related to the drone intrusion, based on the values provided by the Distance Evaluation module.

- **TVI Evaluation** – This module provides the TVIs for all the airport tasks included in the lookahead window (i.e., the ones available in Asset Lookahead-Status Evaluation) for the identified threat scenario. The TVI Evaluation shall be based on the classification criteria

provided in [5]. Jointly with the Threat Scenario Identification, this module provides the **severity** component for risk classification.

- **Asset Collision Risk Evaluation** – This module provides a classification of the **collision risk level** for each asset. The probability part of the risk shall be based on the outcomes of the Distance Evaluation block. The severity part of the risk shall be based on the outcomes of the TVI Evaluation block.

- **Optimal CoA Selection** – This module provides a support for the selection of the optimal course of actions within operational mitigation, based on the estimations of asset collision risks. The optimality shall be intended in terms of performance impact of the mitigations. In particular, the optimal CoA shall be the one minimizing the performance degradations of airport operations.

More detailed results about the preliminary design of the reference DSS and about the proposed operational mitigation procedures are available in [6], which defines also a contingency procedure to be performed by the Supervisory ASPRID Operator.

8 Conclusions

This document represents the deliverable D1.5 “Summary of scenarios assessment” of ASPRID project. It is the final report outcome of WP1.

The present document disseminates the following results by means of the execution of ASPRID WP1:

- a new methodological framework for the risk assessment of airport drone intrusions;
- threat analysis of drones in regard to their possible intrusions in airports, highlighting their main features (types and classification);
- threat analysis of drones in regard to their possible intrusions in airports, highlighting their additional features in terms of teams, swarms, U-Space, UTM, customization and types of intrusion;
- threat assessment of airport drone intrusions;
- processing of the public records of drone sightings, by providing an assessment and a filtering in terms of several attributes;
- some preliminary models of some reference features for the phenomenon of unauthorized drone intrusions in airports in order to check the feasibility of:
    - fitting probability distributions to the historical features of the phenomenon of unauthorized drone intrusions in airports;
    - drawing inferences from and building classification models for the features of the phenomenon of unauthorized drone intrusions in airports.
- the definition of an Airport Vulnerability Index to quantify the threat exposure of an airport with respect to unauthorized drone intrusions, by including different vulnerability dimensions, e.g., socio-economic and socio-geographical indicators;
- the definition of a modelling approach for the functional description of nominal airport operations, based on Hierarchical Task Analysis;
- the detailed technical specification of nominal airport operations;
- the definition of a task-based, functional-based and performance-based modelling approach for the Operational Vulnerability Assessment of airport operations with respect to unauthorized drone intrusions;
- the methodological concept of Event Tree Analysis (the Generic Event Tree) for the risk assessment of unauthorized drone intrusions in airports, by considering also the operational analysis;

- the analysis of Italian data about airport drone intrusions, which have been provided by courtesy of the Italian Aviation Authority, ENAC (Ente Nazionale per l'Aviazione Civile);
- the preliminary analysis for the definition of an Airport Vulnerability Index and its detailed estimation for aggregated Italian airports and for Milan Malpensa airport;
- the detailed results of Event Tree Analysis for the reference scenario and the related risk scenarios;
- the preliminary design of a Decision Support System to cope with the selection of operational mitigation actions, in order to manage the reference threat scenario, considering both Judgement Support and Course-of-Action Support for ATCOs;
- the definition of contingency procedure to be performed by the Supervisory ASPRID Operator.

In regards of some of the results presented, ASPIRD project future work is the following:

- deepening the design of the Decision Support System for operational mitigations;
- update of the risk assessment models, considering the solution design and possibly analysing cascading effects;
- update of the proposed AVI models with new available data (if any).

9 References

[1] Martinavarro, E., Remiro, A., Lopez, P., and Sodano, M. (2020). Project Management Plan. ASPRID Project, EU Contract No 892036, Deliverable D6.1, Edition 1.0, ASPRID.WP6.D6.1.CO.V1.0.FINAL.

[2] ASPRID Grant Agreement 892036 – Annex 1.

[3] Guerra, M., Hughes, Z.W., Pascarella, D., Sodano, M., Cioffi, M., Dubot, T., Roncero, F.J., and Redondo de la Mata, E. (2021). Definition of Elements for Scenario Study. ASPRID Project, EU Contract No 892036, Deliverable D1.1, Edition 1.0, ASPRID.WP1.D1.1.CO.V1.0.FINAL.

[4] Pascarella, D., Gigante, G., Nebula, F., Redondo de la Mata, E., Roncero, F.J., and Olmo Criado, M. (2021). Analysis of Historical Data of Attacks. ASPRID Project, EU Contract No 892036, Deliverable D1.2, Edition 1.0, ASPRID.WP1.D1.2.CO.V1.0.FINAL.

[5] Pascarella, D., Gigante, G., Vozella, A., Redondo de la Mata, E., Bieber, P., and Dubot, T. (2021). Vulnerability Assessment of Operations and Critical Operation List. ASPRID Project, EU Contract No 892036, Deliverable D1.3, Edition 00.01.00, ASPRID.WP1.D1.3.CO.V1.0.FINAL.

[6] Pascarella, D., Gigante, G., Vozella, A., Redondo de la Mata, E., Pidre Cidras, R., Guerra, M., Hughes, Z., Bieber, P., Dubot, T., Sodano, M., and Ippolito, M. (2021). Risk Scenarios Definition. ASPRID Project, EU Contract No 892036, Deliverable D1.4, Edition 00.01.00, ASPRID.WP1.D1.4.C0.V1.0.FINAL.

[7] Sampigethaya, K., Kopardekar, P., and Davis, J. (2018). Cyber Security of Unmanned Aircraft System Traffic Management (UTM). 2018 Integrated Communications, Navigation and Surveillance Conference (ICNS). IEEE. 1C1-1. DOI: 10.1109/ICNSURV.2018.8384832.

[8] Dillon-Merrill, R.L., Parnell, G.S., and Buckshaw, D.L. (2008). Logic trees: Fault, success, attack, event, probability, and decision trees. Wiley Handbook of Science and Technology for Homeland Security. 1-22. DOI:10.1002/9780470087923.hhs004.

[9] Hutle, M., Hansch, G., and Fitzgerald, W. (2015). D2.2 Threat and Risk Assessment Methodology. SPARKS (Smart grid Protection Against cybeR attacKS). Contract No 608224.

[10] Buldas, A., Laud, P., Priisalu, J., Saarepera, M., and Willemson J. (2006). Rational choice of security measures via multi-parameter attack trees. International Workshop on Critical Information Infrastructures Security. (2006). Springer, Berlin, Heidelberg. 235-248. DOI: 10.1007/11962977_19.

[11] EASA (2021). Drone Incident Management at Aerodromes. Part 3: Resources and practical tools. European Union Aviation Safety Agency, Cologne, Germany, 8 March 2021.

[12]Schmittner, C., Gruber, T., Puschner, P., and Schoitsch, E. (2014). Security Application of Failure Mode and Effect Analysis (FMEA). International Conference on Computer Safety, Reliability and Security. Springer, Cham. 310-325. DOI: 10.1007/978-3-319-10506-2_21.

[13]Ericson, C. A. (2011). Concise encyclopedia of system safety: Definition of terms and concepts. John Wiley & Sons.

[14]Kumpulainen, S. (2006). Vulnerability concepts in hazard and risk assessment. Natural and Technological Hazards and Risks Affecting the Spatial Development of European Regions, Philipp Schmidt-Thomé (ed.). Geological Survey of Finland, Special Paper 42, pp. 65–74.

[15]Muckin, M., and Fitch, S.C. (2014). A threat-driven approach to cyber security. Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization. Lockheed Martin Corporation.

[16]Annett, J. (2003). Hierarchical task analysis. Handbook of cognitive task design, 2, pp. 17-35.

[17]https://www.faa.gov/uas/resources/public_records/uas_sightings_report/, last accessed March 18, 2021.

[18]https://www.airproxboard.org.uk/Topical-issues-and-themes/Drones/, last accessed March 18, 2021.

[19]FY2020_Q3_UAS_Sightings, Reported UAS Sightings (April 2020-June 2020), https://www.faa.gov/uas/resources/public_records/uas_sightings_report/media/FY2020_Q3_UAS_Sightings.xlsx, last accessed March 18, 2021.

[20]Current Drone Airprox Count and Information, https://www.airproxboard.org.uk/uploadedFiles/Content/Standard_content/Topical_Issues_and_Themes/Current%20Drone%20Airprox%20Count%20and%20Information.xlsx, last accessed March 18, 2021.

[21]https://www.airproxboard.org.uk/Learn-more/Contributory-factors-and-risk-ratings/, last accessed March 18, 2021.

[22]Pyrgies, J. (2019). The UAVs threat to airport security: risk analysis and mitigation. Journal of Airline and Airport Management, 9(2), 63-96. DOI: 10.3926/jairm.127.

[23]Wang, C. (2020). Investigating the Threats of Unmanned Aircraft Systems (UAS) at Airports (Doctoral dissertation, Purdue University Graduate School).

[24]Gettinger, D., and Michel, A. (2015). Drone Sightings and Close Encounters: An Analysis. Center for the Study of the Drone at Bard College.

[25]Merovci, F., and Elbatal, I. (2015). Weibull-Rayleigh distribution: theory and applications. Appl. Math. Inf. Sci, 9(5), 1-11.

[26]Rodriguez, R. N. (1977). A guide to Burr Type XII distributions. Biometrika, 64(1), pp. 129–134. DOI: 10.1093/biomet/64.1.129.

[27]Fischetti, M. (2016). Fast training of support vector machines with Gaussian kernel. Discrete Optimization, 22, pp. 183-194. DOI: 10.1016/j.disopt.2015.03.002.

[28]CATS Team Project (2009), Causal Model for Air Transport Safety, Final report, 2 March 2009.

[29]EUROCAE (2021). ED-286, Operational Services and Environment Definition for Counter-UAS in Controlled Airspace. March 2021.

[30]EUROCONTROL (2021). EUROCONTROL Comprehensive Assessment for Thursday, 8th July 2021, Covid 19 Impact on European Aviation. [Online] https://www.eurocontrol.int/sites/default/files/2021-07/covid19-eurocontrol-comprehensive-air-traffic-assessment-08072021.pdf, last accessed on 14th July 2021.

[31]EUROCONTROL (2009). EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services (including Service Continuity). Edition 2.0, April 2009.

Appendix A Consistency Analysis with Threat-Assets-Control Relational Model

This annex discusses the consistency of the developed methodological framework with respect to the threat-driven approach and the threat-assets-controls relational model, which is discussed in section 2.3.9. This model represents a proper applicable guidance material for the purposes of the definition of a risk assessment methodology in ASPRID project since it establishes a conceptual foundation of a threat-driven approach.

Figure 23 illustrates the mapping of the outcomes of task T1.1 [3] with respect to the threat-assets-controls relational model. Such figure highlights that this task has provided a full characterization of the framework in regard to:

- assets, by means of:
    - critical assets identification;
    - vulnerability analysis of assets;
    - ranking of critical assets;
- threats, by means of a threat analysis of airport drone intrusions in terms of:
    - drone characterization;
    - identification and assessment of drone intrusions;
    - evaluation of drone physical attacks (fly-by/collisions).

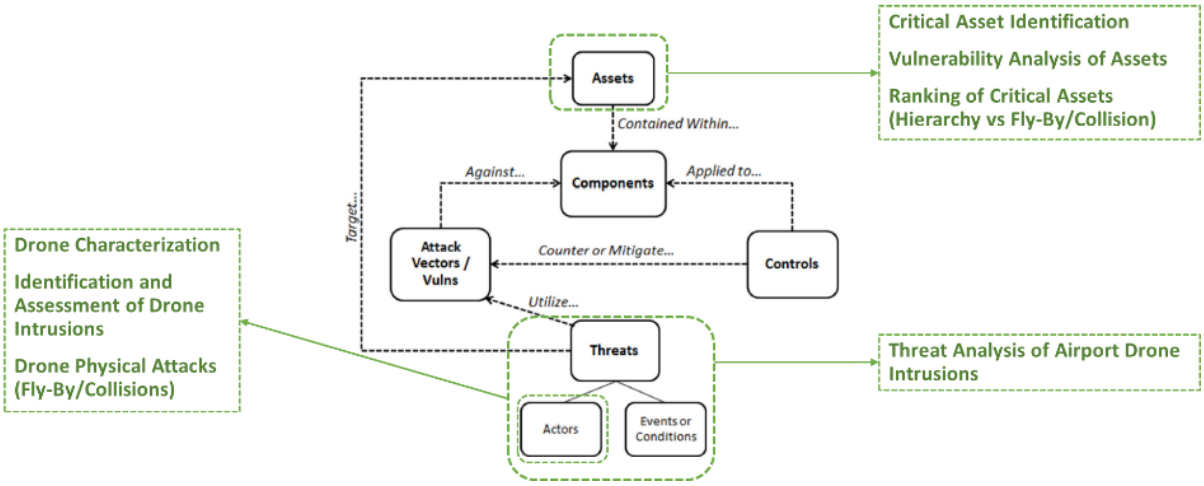

Figure 23. Mapping of T1.1's outcomes [3] with respect to the threat-assets-controls relational model.

Also, task T1.2 [4] has provided a more complete characterization of the threats by means of the analysis of historical data and by means of the definition of the Airport Vulnerability Index.

Task T1.3 [5] has integrated T1.1 with the required operational perspective, as illustrated in Figure 24. Indeed, it completes the methodological framework in regard to:

- components, by providing a detailed functional description of nominal airport operations in a systematic and structured notation;
- vulnerabilities, by means of:
    - the OVA;
    - the COL for the reference threat scenarios;
    - the ETA integration with the operational perspective.

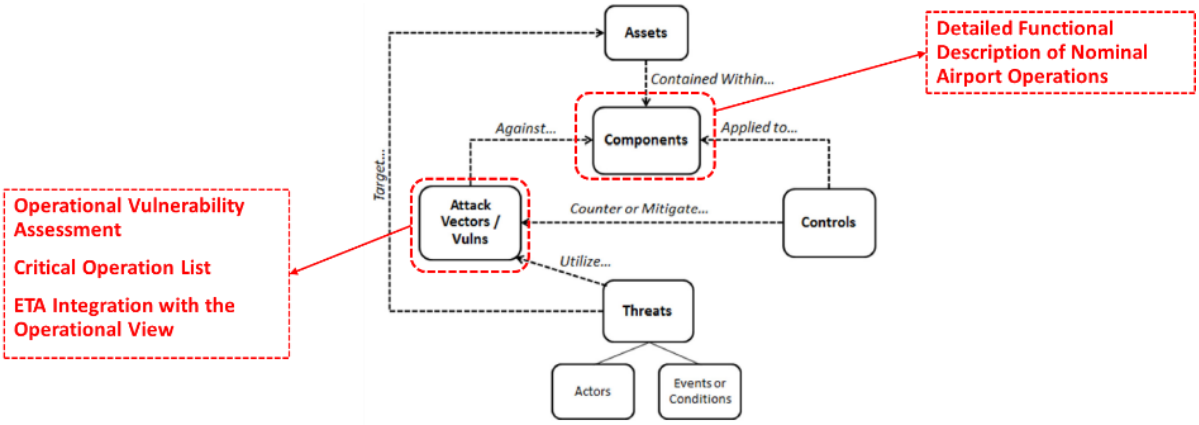

Figure 24. Mapping of outcomes of T1.3's [5] outcomes with respect to the threat-assets-controls relational model.

In the end, task T1.4 [6] has contributed to the definition of controls by addressing the operational counter-measures for airport protection against drone intrusions (i.e., the operational mitigation actions in regard to the task affected by threat scenarios).

- END OF THE DOCUMENT -