Cybersecurity risk assessment for Unmanned Aircraft Systems

Trung Duc Tran

THÈSE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE ALPES

Spécialité : **AUTOMATIQUE - PRODUCTIQUE**

Arrêté ministériel : 25 mai 2016

Présentée par

TRAN Trung Duc

Thèse co-dirigée par **Jean-Marc THIRIET**, Professeur, Université Grenoble Alpes
Nicolas MARCHAND, Directeur de recherche CNRS, GIPSA-lab
et **Amin EL MRABTI**, Société Sogilis

préparée au sein du
Laboratoire Grenoble Images Parole Signal Automatique (Gipsa-lab)
dans **l'École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS)**

Cybersecurity risk assessment for Unmanned Aircraft Systems

Thèse soutenue publiquement le **2 Février 2021**,
devant le jury composé de:

Marie-Laure POTET
Professeure, Université Grenoble Alpes, Présidente du jury
Mireille BAYART
Professeure, Université de Lille, Rapporteure
Frédéric KRATZ
Professeur, Institut National des Sciences Appliquées Centre Val de Loire, Rapporteur
Didier THEILLIOL
Professeur, Université de Lorraine, Examinateur
Guillaume HIET
Maître de conférences, Centrale Supelec, Examinateur
Eric GAILLARD
Responsable technique et opérationnel, Star Engineering, Examinateur
Amin EL MRABTI
Responsable recherche et développement, Sogilis, Encadrant de thèse
Nicolas MARCHAND
Directeur de Recherche, Centre National de la Recherche Scientifique, Directeur de thèse
Jean-Marc THIRIET
Professeur, Université Grenoble Alpes, Directeur de thèse

Résumé — Aujourd'hui, la croissance du nombre d'opérations de systèmes constitués de drones volants (Unmanned Aircraft System ou UAS) soulève des préoccupations de la part du public sur les questions de cybersécurité. Cet aspect doit donc être pris en compte, pour cela nous nous proposons de développer des méthodologies permettant de résoudre ces problèmes lors du développement de l'UAS. Ce sujet est au coeur de nos recherches. Cette thèse propose deux contributions importantes à cet égard. La première est une méthodologie centrée sur le système pour renforcer la cybersécurité d'un UAS existant (ou conçu). Cette méthodologie fournit à l'utilisateur un "workflow" pour analyser l'UAS, identifier les scénarios d'attaques possibles et les contre-mesures appropriées. Nous appelons cette méthodologie "Gestion des risques du système orientée cybersécurité". La seconde méthodologie est centrée sur les opérations, elle prend en compte les problèmes de cybersécurité dès la phase initiale de conception du système. Cette méthodologie a été conçue comme une version étendue de la méthodologie "Specific Operation Risk Assessment" (SORA). Ce choix s'explique par le fait que la SORA est une méthodologie de référence pour l'évaluation des risques des opérations dites "Spécifiques" d'UAS. La méthodologie SORA se concentrant uniquement sur la sûreté, et ignorant la cybersécurité, nos modules d'extension ont pour objectif de compenser ce manque. Notre méthodologie d'extension s'appelle "Evaluation des risques opérationnels spécifiques pour la sécurité et la cybersécurité" (en Anglais, SORA-C2S). Sur la base de cette méthodologie, nous avons construit un outil Web qui aide l'utilisateur à effectuer l'évaluation des risques de manière semi-automatique prenant en compte ces deux aspects de sûreté de fonctionnement et de cyber-sécurité. Cette thèse s'inscrit dans le cadre de la coopération entre la société Sogilis et le laboratoire Gipsa-lab.

Mots clés : Cybersécurité, évaluation des risques, système de drone, SORA, catégorie spécifique.

GIPSA-lab, 11 Rue des Mathématiques
38400, Saint-Martin-D'Hère, France

Abstract — Nowadays, the increasing number of Unmanned Aircraft System (UAS) operations raises public concerns on cybersecurity issues. Therefore, it requires methodologies to address these issues during the UAS development. It is the focal point of our research. This thesis has two significant contributions. Firstly, we propose a system-centric methodology to reinforce the cybersecurity of an existing (or designed) UAS. This methodology provides the user with a workflow to analyze the UAS, identify the possible attack scenarios, and identify suitable countermeasures. We call this methodology "System cybersecurity risk management". Secondly, we propose an operation-centric methodology that considers the cybersecurity issues in the early phase of the UAS development (before the UAS is designed). This methodology is an extended version of the Specific Operation Risk assessment methodology (SORA). The SORA is a wide-known methodology to assess the risks of UAS operations under the "Specific" category. However, the current stage of the SORA methodology focuses only on safety but ignore cybersecurity. Our extension modules fulfill this missing part. We call our extension methodology as Specific Operation Risk assessment for Safety and Cybersecurity (SORA-C2S). Based on this methodology, we built a web-based tool that helps the user to perform the risk assessment semi-automatically. This thesis is a part of the cooperation between the SOGILIS Company and the GIPSA lab.

Keywords: Cybersecurity, risk assessment, Unmanned Aircraft System, SORA, specific category.

GIPSA-lab, 11 Rue des Mathématiques
38400, Saint-Martin-D'Hère, France

Contents

List of Figures

List of Tables

List of Abbreviations

ARC	Air Risk Class
AT	Attack Tree
ATC	Air Traffic Controller
BVLOS	Beyond Visual Line of Sight
BT	Bow-tie
C2	Control and Command
CONOPS	Concept of Operations
CS	Cybersecurity
EASA	European Union Aviation Safety Agency
ESC	Electronic Speed Controller
ET	Event Tree
FT	Fault Tree
GCS	Ground Control Station
GRC	Ground Risk Class
GPS	Global Positioning System
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
INS	Inertial Navigation System
IE	Initial Event
IoT	Internet of Things
IT	Information Technology
JARUS	Joint Authorities for Rulermaking on Unmanned System
MEHARI	Method for Harmonized Analysis of Risk
OCSL	Operation cybersecurity susceptible level
OCSO	Operation cybersecurity objective
OSO	Operation safety objective
OT	Operational Technology

PMU	Power Management Unit
PRC	Privacy Risk Class
SAIL	Specific Assurance and Integrity Level
SAL	Security Assurance Level
SCADA	Supervisory control and data acquisition
SIL	Safety Integrity Level
SORA	Specific Operation Risk Assessment
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UE	Undesired Event
VLOS	Visual Line Of Sight

Introduction

An Unmanned Aircraft System or UAS was first used for military purposes but nowadays, this kind of system is more and more used for civil purposes. For the last few years, the civil UAS market has grown exponentially in terms of market size and application fields. The market size increased from $2 billion in 2016 to $14.1 billion in 2018 [1]. We can currently find many UAS applications in different economic sectors: photography, construction, mining, agriculture, site monitoring, logistics. UAS operators are continuing to explore and develop new UAS applications. It is expected that there will be more and more unmanned aircrafts operating above us, our home, cities, or industrial infrastructures. On the one hand, the popularization of this kind of system could bring new convenience and experience to our lives. On the other hand, it could also give us trouble. The malfunction or misuse of these systems, whether intentional or unintentional, could lead to severe consequences. For example, the UAS operation could intentionally or unintentionally violate people's privacy under flight; the unmanned aircraft could fall and hits people, infrastructures on the ground; or it could collide with a manned aircraft. The doubts prevent public acceptance and slow down the popularization of UAS. It attracts the concern of different stakeholders: operators, manufacturers, lawmakers.

Cybersecurity is one of the major problems preventing public acceptance of the UAS application. UAS is a cyber-physical system in which the digital components (sensor, software, communication, etc.) collaborate to control and monitor the physical parts (such as actuators, airframe). Like many other cyber-physical systems (industrial control system, automobile, etc.), the digital part of UAS always has vulnerabilities or flaws that could be exploited by attackers. In the literature, there are several reports on cybersecurity breaches: GPS jamming and spoofing [2], video interception [3], hijack attacks via communication [4], sensor spoofing [5]. By exploiting the digital part's vulnerabilities, the adversary could disturb the UAS's operation or take over control of the system for malicious objectives: injuring people on the ground, violating privacy, damaging infrastructure, etc. Therefore, the cybersecurity of UAS should be taken into consideration to prevent possible negative impacts and gain public acceptance. The cybersecurity of UAS is the main subject of this thesis.

Because of cybersecurity's importance in the UAS domain development, there are many research studies in this field. Observing the literature of UAS cybersecurity, we found two traditional research trends. One is to look for new vulnerabilities or new attack strategies. In other words, it is to answer the question: "How could we attack the system ?". The other one is to look for cybersecurity countermeasures against possible attacks. In other words, it is to answer the question: "How could we prevent the possible attack ?". Both cyber-attack and defense techniques evolve day by day. However, for a given UAS within a specific mission, taking into consideration all these possible cybersecurity attacks and implementing all corresponding countermeasures could be costly and unnecessary. Because depending on the

nature of the UAS and the mission, an attack's cost could be superior to the profit gained from the attacker's point of view. And in the point of view of the operator, a countermeasure cost could be superior to losses. Therefore, we should take into account the balance between lost-gain or cost-effectiveness when considering the cybersecurity issues of UASs. For that purpose, instead of the two traditional questions, we are interested in another question: "Which cyber-attack and countermeasure should be taken into account and in which priority order?".

To answer these questions, we need to perform a risk assessment. The risk assessment methodology provides a systematic and effective way to detect, analyze, evaluate possible security attacks, and select adequate countermeasures. Different risk assessment methodologies have been developed and used in the various industrial domains for a long time. The risk assessment methodologies have been first used to prevent potential accidents (safety). Since the computer is widely used in industry, risk assessment methodologies play an essential role in protecting the system against cyber-attack (cybersecurity). For example, we have MEHARI for IT systems, EVITA for automobile systems, IEC61508 for Industrial Automation and Control Systems, ED202A & ED203 for avionic systems. In the UAS domain, there is not much research in cybersecurity risk assessment for UASs. The most prevalent risk assessment methodology is the Specific Operation Risk Assessment (SORA). However, it currently focuses only on safety. Therefore, this thesis focuses on developing a cybersecurity risk assessment for UAS applications.

This dissertation is organized as follows. **Chapter 1** gives readers an overview of the unmanned aircraft systems, including UAS definition, general architecture, market, regulations, and cybersecurity vulnerabilities. **Chapter 2** compare safety vs. security/cybersecurity in different aspects: definition, risk concept, and the state of art of risk management. **Chapter 3** presents the first contribution - a methodology to reinforce the cybersecurity of an existing or pre-defined UAS. **Chapter 4** starts with explaining the SORA methodology and then presents our proposed solution to extend this methodology toward cybersecurity. **Chapter 5** illustrate the extended SORA methodology with different case studies and demonstrates how to use the assessment results within a development process. Finally, **Conclusion** sums up the outcome of our works and give some propositions for future works.

Chapter 1

Unmanned Aircraft System and related Cybersecurity issues

Contents

1.1 Definitions

According to International Civil Aviation Organization (ICAO)[6], An Unmanned Aerial Vehicle (UAV) or drone is an aircraft that could fly without a pilot on board and is either remotely or fully controlled from another place. However, a UAV cannot operate alone but needs to maintain the interaction with operators on the ground. Therefore, another term Unmanned Aerial System (UAS) has been introduced. That system contains the UAV and all necessary equipment, network, and persons to control an unmanned aircraft and fulfill a specific mission [6], [7], [8]. This kind of system has been firstly used in the military domain for dangerous missions. Nowadays, the progressive development of technology lowers the cost of accessing to this technology. That leads to a continuous increase of UAS applications in many civil domains such as goods transportation, agriculture, aerial photography [4].

1.2 System description

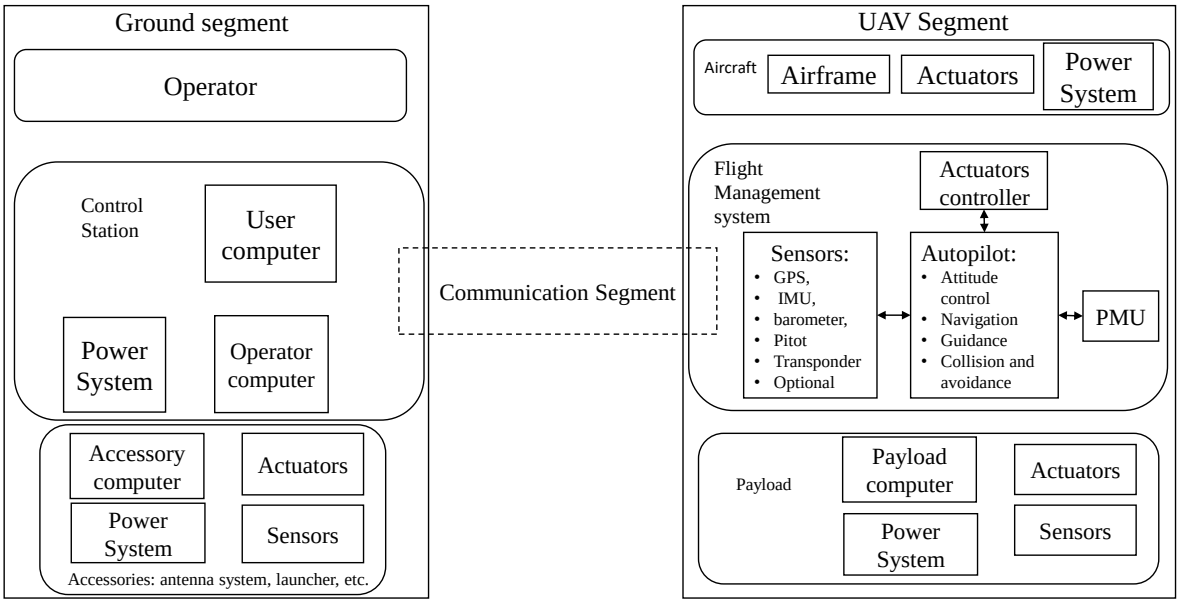


Figure 1.1: UAS architecture

Depending on the autonomous degree of the unmanned aircraft during the mission, the system complexity can vary [9]. For the lowest degree of autonomy, we could refer to the simple UAS for hobby purpose, which consists of a simple remotely controlled aircraft, a remote radio control and a pilot on the ground. Meanwhile for a higher degree of autonomy, a UAS could consist of a fleet of aircraft equipped with sophisticated sensors, processors, communication equipment, which allow the aircraft to fly beyond the visual range without the interaction of pilots. This part of the document brings out a generalized description of the UAS architecture. The components of a basic UAS can be grouped into three segments:

Unmanned Aerial Vehicle (UAV) Segment, Ground Segment, and Communication Segment [7], [8]. These segments could be described as shown in Figure 1.1, there are detailed and explained in the following section.

1.2.1 UAV segment

The UAV Segment consists of three main modules: Aircraft, Flight management system and Payload (see figure 1.1).

1.2.1.1 Aircraft

This module gathers Airframe, Actuators and Power system.

Airframe is the mechanical structure of the vehicle excluding the propulsion system. The mechanical structures of UAV exist in various forms with different characteristics such as aerodynamic, size, mass, which are selected based on the requirement of the targeted operation. A UAV airframe basically falls into one of the following four categories: fixed-wing, rotary-wing (such as helicopter, multi copter), blimps and flapping-wing [8], [10] (see Figure 1.2). Besides the basic airframe, there are also hybrid ones that possess the characteristics of the basic airframes. For example, the tilt-rotor airframe is a combination of the fixed-wing airframe and the rotary airframe [11].

Figure 1.2: From the left to the right: fixed-wing, rotary-wing, blimp and flapping-wing airframes

Actuators are responsible for converting the control command to the physical movement of mechanical parts: propellers, flaps, rudder, spoilers, and parachute launcher. Hence the vehicle could change its attitude and altitude.

Power system is composed of electrical or mechanical components that are used to store, generate and distribute the energy. At the beginning, the mainstay for the power system was the internal combustion engine [12], which is suitable for big military UAVs. Nowadays, for lighter commercial UAVs, the electric power system become more popular with a lot of advanced technologies such as fuel cell [13], [14], solar cell [15], [16] and battery.

Open-source	Airframe	Hardware	Multi UAV	Flight plan	Geofencing	Collision Avoidance	Lasted release
Paparazzi	Fix-wing, rotary-wing	Varied	Yes	Yes	Yes	Yes	19-12-18
Pixhawk	Fix-wing, rotary-wing	Specific	Yes	Yes	Yes	Yes	21-04-20
Ardupilot	Fix-wing, rotary-wing	Varied	Yes	Yes	Yes	Under development	29-02-20
OpenPilot	Fix-wing, rotary-wing	Specific	None	Yes	N/A	No	18-07-15
AeroQuad	Rotary-wing	Varied	None	No	N/A	No	31-01-13
Commercial							
Picollo	Fix-wing, rotary-wing	Specific	Yes	Yes	Yes	Yes	N/A
MicroPilot	Fix-wing, rotary-wing, Blimp	Specific	Yes	Yes	Yes	Yes	N/A
Veronte	Fix-wing, rotary-wing, Blimp	Specific	Under development	Yes	Yes	Yes	N/A

Table 1.1: Comparison of the popular open-source and commercial autopilots [17]

1.2.1.2 Flight Management System

The Flight Management System is a set of all avionic components that observe behaviors of vehicle and control actuators/engines to perform a safe and automatic flight. The key elements of this module are autopilot, elementary sensors, power management unit, actuator controller and the on-board communication modules.

Autopilot referring both hardware and software aspects. It is the center of the Flight Management System (FMS) and it communicates with other components of the FMS (sensor, actuator, communication, power management unit (PMU)). The basic role of this component is to estimate the state of the aircraft and navigate the aircraft following the command of the pilot on the ground or the programmed flight plan. Following the progressive increase of the number of UAVs, there has been an exponential increase in the hardware and software of autopilots under either the open-source form or commercial form. A brief comparison of the popular current open-source and commercial autopilots is shown in Table 1.1.

Sensors are on-board sensors allowing the aircraft to navigation. Traditionally, the main core sensors of a UAV are Global Navigation Satellite System (such as Global Position System - GPS) and Inertial Measurement Unit (IMU). Because of their complementary nature (e.g accuracy but low data rate for GPS; high data rate but error accumulation for IMU [18]), GPS and IMU sensors are the preferred sensor couple for the majority of flight management systems [19]. The outputs of these sensors are integrated by the autopilot to estimate the behavior of the aircraft. There are many developed algorithms for GPS/IMU integration such as uncoupled integration, loosely coupled integration, tightly coupled integration, and deeply coupled integration [20]. Besides the traditional GPS/IMU couple, the research have also investigated on other sensor combinations such as GPS/vision-computer couple [21], IMU/vision-computer couple [22]. To enhance the aircraft state estimation, the UAV could be equipped with several

kinds of supplemental sensors such as a barometer or a magnetometer.

Actuator controllers are electronic components that convert autopilot command into control-signals which then are sent to actuators. One of typical actuator controllers is the Electronic Speed Controller (ESC) that adjusts speed of the electrical motor.

PMU is composed of electronic components that are responsible for measuring and managing the energy of the vehicle.

1.2.1.3 Payloads

Payloads are components unnecessary for the flight of the UAV but necessary to fulfill a specific objective of the operation. For safety and security, payloads should be equipped with their own power system isolated from the main power system of aircraft and they should not be connected directly to the autopilot or the other critical systems [7]. Therefore, a payload system could have its own sensors, actuators, peripherals, and processors. Depending on applications, an unmanned aerial vehicle could be equipped with various types of payload components. The most popular payload component is the camera. This component is widely used for many UAS applications related to the audio-visual production, the monitoring application or the inspection of large infrastructures such as bridges, windmills, or power lines [23], [24], [25]. The LIDAR is another popular sensor payload which attracts a lot of research related to the UAS. The LIDAR allows to measure distance with high accuracy, so it could be used to make high-resolution maps [26], [27]. Following the increase of numbers of UAS applications, nowadays, more and more equipment could fit to a UAV as payloads such as the spraying system for precision agriculture [28], [29], or the cargo for good transportation.

1.2.2 Ground segment

The Ground segment (see Figure 1.1) includes all elements which are not parts of the vehicle itself but required for a flight. The main elements of this segment are: Operator, Control Station and Accessories (see figure 1.1).

1.2.2.1 Operator

According to the definition of the International Civil Aviation Organization (ICAO) [6], an operator is a person, an organization or an enterprise engaged in or offering to engage in an aircraft operation. Depending on the complexity of the UAS operation or application, the size of operator could vary. For example, for the most simple UAS operations, an operator could be only a pilot who flies manually the remote control aircraft. Meanwhile, in more complex UAS operations, an operator could be a structured organization consisting of many persons

such as pilots (or crew members), maintenance staffs, managers. The roles of each operator member should be defined by a local civil aviation authority.

1.2.2.2 Control Station

The Control Station consists of hardware and software on the ground used as Human-Machine Interfaces (HMI) to control/observe the vehicle and the payload. Depending on the purpose of the UAS application, the UAS could have more than one control station [7]. For instance, in order to observe an industrial site, a UAS could be deployed with two control stations. The first one is placed far away from the industrial site and is used by pilots to full control both the vehicle and the payloads. The second one is a mobile station (such as a tablet, a smartphone). This mobile station is used by a person inside the industrial site and is able to access to payload data only such as camera data.

1.2.2.3 Accessories

Accessories are devices which are not directly involved in a UAS operation but needed to perform it such as antenna/camera tracking system, UAV catapult launcher, battery charger, or transport case.

1.2.3 Communication Segment

The communication segment (see Figure 1.1) is vital for any kind of UAS applications. This segment includes different communication systems which provide the UAS with ability of remote control and remote data acquisition [30]. During the operation, the communication systems could convey various kinds of data. The essential one for most UAS is the Control and Command (C2) including telemetry data, flight control data, flight configuration data. This kind of data is exchanged between the aircraft and the pilots to conduct a safety flight. The other kind of data is Payload data including the data to control the payload and the data generated by payload such as video data. This kind of data this not vital for the flight but is important to fulfill the operation objective (such as video data for the monitoring application) [31]. Besides these two kinds of data, the communication systems could also convey the traffic data. This kind of data is exchanged between the aircraft, ground control stations, and air traffic controller (ATC) to maintain the airspace safe and efficient. With a larger number of UASs in the future, this kind of data and the related technologies are essential factors to integrate successfully the UAS in the national airspace systems [30] [32].

Based on the need of connectivity of the intended operation (e.g range, bandwidth), the complexity of the communication systems could vary a lot. For a simple operation, the communication system could provide only the connection between the aircraft and the Ground Control Station (GCS). For a more complex operation, the communication systems could

connect an unmanned aircraft to others to build a swarm of UAV or connect GCS with ATC to share the information on the traffic.

1.3 UAS market and Application

The history of UASs started in the early 1900s when they were first used as targets for military practices [33]. From that moment, the market of UAS was steps by steps shaped. For the last century, the market focused on only the military applications such as reconnaissance/combat mission while the civil application of UAS was not recognized. From the 2000s, the UAS market for the civil application started to grow up. At the beginning, in the civilian context, the unmanned aircraft were used as toys for individual entertainment purposes. Then, the development of technology (such as miniaturizing component, increasing computing power, improving sensor and battery capacity) make UAS smaller and more attractive for professional and commercial uses in many sectors of the economy such as:

- **Photography and media sector:** Before the emergence of the UAS technology, to take photos or make a film shot from the air, photographers and film-makers have no choice but to use helicopters or planes which is costly and not flexible. Nowadays this task could be alternatively realized by using a UAV equipped with a high quality camera. With the decrease of the price, this kind of UAV becomes more and more popular in this sector. In fact the product and the service related to UAS in this sector generate most of the revenue in the civil drone industry in 2016 (60 - 70% of the total [34], [1]).

- **Agriculture sector:** This sector profits also the emergence of the UAS technology to lower the operation cost. Instead of the plane or the satellite, the farmers could use the UAS to spray pesticide, collect and analyse data of their fields (such as strength of nutrient uptake of the field [35], stress in a plant several days before it becomes discernible [36],...). According to the *Agricultural Robots and Drones 2017-2027: Technologies, Markets, Players* [37], the UAS application for the agriculture will be a major market and reach over $470 million in 2027.

- **Energy sector:** The UAS is also attractive for companies in the energy sector. This sector focuses on using the UAS for maintenance and inspection to reduce a variety of risks related to infrastructures and staffs performing hazardous tasks. According to a survey realized in 2019 [38], more than two-thirds of the energy companies (over 247 companies took part in the survey) are currently using UAS for their activity. However, most UAS operations are still in the area of POC-Proof of Concepts or R&D of UAS application. The most required features of this sector for the UAS application, which need to be improved in the future are endurance, flexibility and reliability of the flights.

- **Logistic and transport sector:** The UAS is expected to be a part of the logistic and transportation system in the future. The unmanned aircraft system could be used to deliver small packets with the greatest competitive advantage in dense (sub-)urban areas. This kind of application attracts a lot of consideration of the big companies in the

field of e-commerce such as Amazon, UPS, FedEx. According to a forecast of SESAR Joint Undertaking (public-private partnership responsible for the modernization of the European air traffic management), the size of the fleet of UAV for this application could reach 70000 in 2035 [32]. However, at this moment, UASs for good delivery are still not widely deployed and accepted, most flights in this sector are still realized for concept validation purposes. One of the most important enabler factors for this kind of application is the regulation which is not fully defined [32].

For the last decade, we recognized an explosion of the civil UAS market. From 2012 to 2019, over $3 billions were invested in this domain, and the market size grows from $2 billions in 2016 [1] to $14.1 billions in 2018 [39]. Meanwhile the market of military UAS is always dominated by the companies that have strong positions in the industry such as Boeing, Lockheed Martin, Airbus, the market of civil UAS is almost dominated by the new players or start ups [33]. The best examples for this trend are the cases of the Chinese company DJI and the French company Parrot which are the most successful UAS manufacturers in the market. The market explosion brings opportunities not only to the manufacturers but also the other players in this field to develop their business. They are the companies who provide the industry services (monitoring, observing, inspecting...by drone), training programs and the software solutions to analyze the huge data collected by drones [33].

Looking forward the future of the civil UASs, many organizations and market research companies present market forecasts. SEAR Joint Undertaking predicts that there will be around 400,000 commercial drones flying over the sky of Europe (excluding 7 millions of leisure drones) in 2050 [32]. According to Market Research Future, the size of the civil drone market will be $70 billions of valuation in 2027 [40]. The Drone Industry Insights predicts that the civil drone market will reach $ 43.1 billions in 2024 [1]. Interact Analysis company forecasts $15 billions as the value of the market in 2022 [41]. Although these numbers are only predictions which could be more or less accurate, they are all optimistic. In other words, these numbers reflect the confidence in the growth of the civilian drone market in the near future.

1.4 UAS integration into the airspace

The airspace is organized and maintained basically based on complex systems of regulations and standards to ensure that all flights operate in a safe and efficient manner. These regulations and standards cover many aspects of the aviation industry from the aircraft design to the operation. For example, a manned aircraft has to be certified, registered, maintained according to a program; the crew has to have a license and the operator has to be certified [42]. Additionally, the aircraft is required to exchange with the Air Traffic Controller to avoid the collision. However the current regulation system has been designed to fit to the manned aircraft rather than the unmanned aircraft.

In fact, there are a lot of challenges to integrate safely and efficiently the UAS into the airspace [43]. One of these challenges is that the current regulations for manned aircraft are not suitable for unmanned aircraft systems [42]. Different from the manned aircraft market, the UAS market is dominated by a large quantity of low-cost UASs with a short cycle-life (about thirty months [44]). Therefore, designing, certifying, operating the UAS based on costly processes used for the manned aircraft does not make sense. The other challenge is how to maintain the safe operation of the airspace with both unmanned aircraft and manned aircraft. To avoid the air collisions, the manned aircraft is generally equipped with several equipment allowing to communicate with Air Traffic Controller and other aircraft, to receive clearances and emergency warnings such as radio communication, transponder. It seem to be burdensome for all drone operators to comply with the requirements [42]. Moreover, because of its small size and the high flexibility of operations, unmanned aircraft could takeoff/land anywhere and does not fly following the fixed and named way-points as the manned aircraft [45], [42]. That makes air traffic control with both manned and unmanned aircraft a complex task.

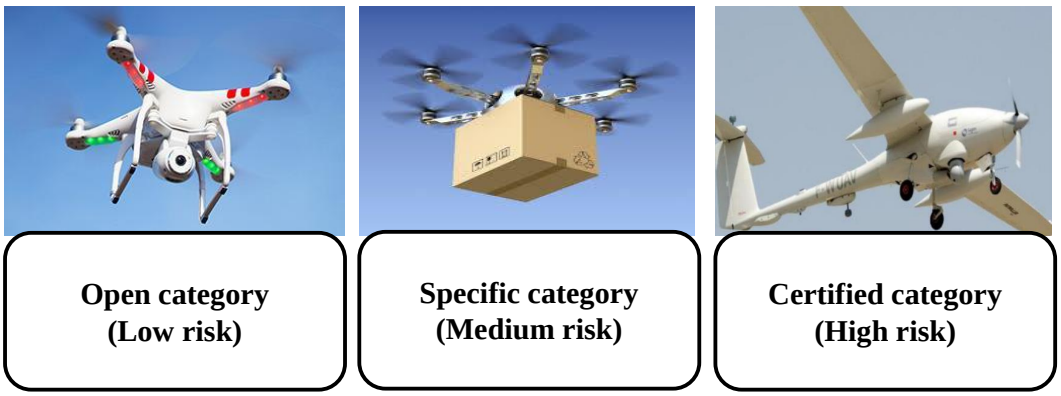


Figure 1.3: Three categories of UAS operations

1.4.1 Regulations

To integrate UAS into the airspace, the European Commission started to consider this vehicle in 2008 by issuing the regulation EC2008/216. This regulation is the first law document dedicated to UAS operations. However, this document detailed the rules for only UAS operations with aircraft of more than 150kg. The rules for operations with aircraft of fewer than 150kg were the charge of each member state. It means European countries had their own rules for this kind of process. This diversity leads to the UAS market's segmentation and could prevent some UAS operations (e.g., cross border flight). Therefore, it needed EU-level regulations that consider all UAS operations to amend the EC2008/216 regulation. In 2015, the European Commission tasked the European Union Aviation Safety Agency (EASA) to develop a regulatory framework and regulation proposals. Then in 2015 and 2017, EASA releases two documents: NPA2015-10 [46] and NPA2017-05 [44]. The principle of these proposals could be resumed as follows:

- The new regulations consider all kinds of UAS. It means that the 150kg limitation should be removed.
- This regulatory framework is operational centric. It means that the regulation is organized based on the operations' risks. It should set up three categories of operations from low to high risk:
  - **Open Category:** consists of low-risk operations, such as most leisure flights and some professional activities. Operations under this category do not require the explicit authorization from civil aviation authorities. For these operations, the safety is ensured by strict operation limitation (e.g no proximity to people, traffic, infrastructure, no dangerous items, no item dropping, only one UAS per pilot).
  - **Specific Category:** regroups medium-risk operations, such as operation beyond visual line of sight (i.e., no visual contact between pilot and UAV during flight). For the operations in this category, it is required to perform a risk assessment.
  - **Certified Category:** consists of operations that have risk equivalent to manned aircraft operations. The requirements for these operations are comparable to manned aviation requirements, for example the certification of the UAS, a licensed remote pilot and an operator approved by the competent authority.
- The regulations should address different safety risks: mid-air collision with manned aircraft, harm to people, and property damage.
- The requirements should proportionate to the operation's risk.
- Security and privacy should be considered. Security is not limited to overflight of sensitive areas. Cybersecurity is also an issue for drones

In 2019, based on the proposals above, the European Commission issued Commission Delegated Regulation (EU) 2019/945 and Commission Implementing Regulation (EU) 2019/947. Commission Delegated Regulation (EU) 2019/945 defines certification requirements, including CE marking & third-country operators. Commission Implementing Regulation (EU) 2019/947 defines requirements for operation and registration. In the 2019/947 regulation, the boundaries of three operation categories are defined as follows:

- **Open Category:** UAS operations are always considered to be in the this category when:
  - The maximum takeoff mass is fewer than 25kg.
  - The aircraft does not carry dangerous goods.
  - The aircraft does not drop any material.
  - The remote pilot age is equal to or more than 16.
  - The pilot keeps the aircraft in her/his visual range at all times (Visual Line Of Sight operation).

  - The aircraft does not fly over assemblies of people.
  - The maximum altitude above the ground level is 120m.

- **Specific Category:** UAS operations are always considered to be in the this category when there is one of Open Category conditions is not met
- **Certified Category:** UAS operations are always considered to be in the this category when:
  - The aircraft flies over assemblies of people with dimensions exceeding 3m; or
  - transports of people; or
  - carries of dangerous goods.

It is expected that most UAS operations will operate under the Specific category. For this category, the operator must perform and submit a risk assessment according to the SORA methodology. But the operator could skip a full risk assessment in some cases:

- The operation complies with the Standard Scenarios (STS-01 and STS-02) predefined in the 2019/947 regulation.
- The operation meets the operational characterization described in the Predefined Risk Assessment described in the guidance document of Commission Implementing Regulation (EU) 2019/947.

1.4.2 U-space concept

Besides regulatory proposals, another effort of EASA for the UAS integration is the proposal of “U-Space" concept. Not as its name, this concept does not refer to the new volume of airspace allocated to UAS operation, but it refers to a set of new technical services supporting the UAS operation. These services are or will be developed to enable complex UAS operations with the high autonomous degree in all operational environments including urban, suburban, rural [47]. The U-space concept proposes four blocks of services with the increase of the connectivity and automation level of drones:

- **Fundamental services (U1)** consists of e-registration, e-identification and geofencing services. These services helps the authority identify the drone and support the security and safety requirements.
- **Initial services (U2)** support the management of drone operations and may include flight planning, flight approval, tracking, airspace dynamic information, and procedural interfaces with air traffic control.
- **Advance services (U3)** provide drones the capacity to detect and avoid automatically the conflict with others when they fly in a dense area.

Figure 1.4: U-space illustration [47]

- **Full service (U4)** offer integrated interfaces with manned aviation, support the full operational capability of U-space and will rely on very high level of automation, connectivity and digitalization for both the drone and the U-space system.

Since the standard and technologies related to U-space are simultaneously developed by many public organisations and private companies, many services of this concept are available today. However, that not means that U-space could be immediately implemented because of the fragmentary of such development and lack of real test within real condition [42].

1.5 Cybersecurity issues

1.5.1 GPS

As mentioned in 1.2.1.2, the GPS receiver is an essential component of the UAV, especially when the UAV can fly in auto mode. This component provides the raw information on the

position of the vehicle based on the satellite signals. These signals come from GPS satellites locating 1300 miles away from the earth and has to travel through the atmosphere of the planet. They are extremely weak when reaching the receptor on the UAV. That makes the GPS receiver vulnerable to a jamming attack (GPS jamming) in which attackers could interface original GPS signals by higher power ones. This kind of attack could be conducted using low-cost equipment available on the market [48] and does not require any specialized knowledge. Moreover, the GPS data for civil utilization is not encrypted. That makes the GPS receptor vulnerable to spoofing attacks (GPS spoofing). In this attack, the attacker could deceive the GPS receptor with fake GPS signals containing incorrect position information. In reality, there are several UAV incidences suspected to result from GPS spoofing attacks such as the crash of the S-100 Camcopter UAV, the capture of the military UAS RQ-170 [2]. In the research, the possibility of GPS spoofing has been illustrated by the attack experiment in many works. For example, in July 2012, the UT Austin's Radio Navigation Lab conducted a GPS spoofing attack against a small UAV in controlled conditions, which result in a commanded dive [49]. Another experiment was conducted by Seo et al. [50], which forces the drone to land in an incorrect location by using the GPS spoofing technique. To perform a successful GPS spoofing attack requires complex equipment and GPS knowledge compared to a GPS jamming attack. The consequence of a GPS spoofing could be more brutal than a GPS-jamming attack. Because in the case of the GPS jamming, the attack could be detected and considered a failure of a GPS component (loss of GPS signal). The most commercial UAVs have fail-safe mechanics to handle this situation (such as safe-landing based on other sensors). Meanwhile, in the case of GPS spoofing, the attacker could take over control of the UAV's flight path without the pilot's awareness. Different countermeasures against GPS spoofing were proposed in the literature (see more in Annexe D).

1.5.2 IMU

The Inertial Measure Unit (IMU) is another fundamental component of a UAV. This component provides the UAV with a capacity to sense the movements without the need for external references (e.g., GPS uses satellite signal as an external reference). A simple IMU consists of a gyroscope (sensing angular rate) and an accelerometer. These sensors measure the movements of the UAV based on the displacement of sensing mass. Due to the limitation of the size, power, and cost, most small/commercial UAVs are equipped with low-cost IMUs which are unshielded. That makes the IMU vulnerable to acoustical interference. Although there are no reports about the cyber attack via the IMU, several works are done to present the possibility of this kind of attack. Yunmok et al. [51] experimented a denial of service attack against the gyroscope of a UAV by the intentional acoustic interference at the close resonate frequency of the sensor. Meanwhile, Lu et al. [52] demonstrated an approach to fully control over the gyroscope's output signals by the intentional acoustic interference based on the short-time Fourier analysis. The same attack on accelerometers is illustrated by Trippel et al. [53]. Besides attack techniques related to IMU, different defense approaches are also researched. The common approach coming to mind is the sensor redundancy. However, it requires additional sensors. Tu et al. [54] propose a method for IMU attack detection and fault-tolerant

without addition sensor. If the IMU is under attack, the attitude data is estimated based on only position data and heading data. Crispoltoni et al. [55] propose a data-based approach to detect anomalies within IMU data. Yaseen et al. [56] offer a Generalized Predictive Controller along with a fault detection mechanism. This mechanism could be used as a countermeasure to detect the compromised IMU data.

1.5.3 Communication

Depending on the communication requirements (range, bandwidth, cost, etc.), the communication technologies used for UASs could vary, such as WiFi, RF, 4G/LTE, satellite, etc. Because these technologies are used for general purposes, not only the UAS application, many works are introduced to secure such technologies. For the small/commercial UASs, due to the limitation of resources or the misconfiguration, the security of the communication could not be at the right level. Several works in the literature were done to illustrate the possibility of the cyber attacks on UASs via the communication system. Vattapparamban et al. [4] experimented with a de-authentication attack on different low-cost UASs by exploiting the vulnerabilities of WiFi. For the same communication technology, Fournier et al. [57] succeeded in taking over control of a drone in the DroneJack project.

Many commercial UASs use the open-source MAVLink protocol on the top layer of communication systems to transmit the UAV and GCS messages. However, the original version of the Mavlink protocol (version 1.0) does not provide any mechanisms to protect exchanged messages (confidentiality, availability, authentication). With this version, the security of the communication channel is totally based on the lower communication layers. For example, if the WiFi communication is compromised, the MAVlink could not provide any protection.The limitation of the autopilot resource could hinder the implementation of robust encryption for the MAVlink protocol. [58]. The encrypted MAVlink protocol is discussed in the thesis of Marty [59].

1.5.4 Autopilot & GCS

Autopilot is sometimes connected with external devices for many purposes, such as downloading flight data, getting update-package, or re-configuring. That makes autopilot vulnerable to the infection of viruses or unauthorized access. In these kinds of attacks, attackers could maliciously change the flight parameters to alter the behavior/control laws of the system [60]. For the most commercial UAS, the GCS is usually built on general-purpose computers (laptop, desktop, smart-phone) with GCS software. Therefore, like other applications based on these devices, GCS could be an initial target for cyber attacks. For example, the attacker could maliciously modify the data stored on GCSs (such as flight parameters, flight plan, map) to deceive the pilot [60]. Heiges et al. [61] experimented an attack scenario in which the GCS software was compromised and displayed erroneous information to hinder the other attacks on the autopilot.

1.6 Conclusion

This section provides readers an overview of the Unmanned Aircraft System. Thanks to the development of technology, this system's price have decreased quickly for the last decade. It leads to that this system becomes more and more popular, and is used for many economic sectors: agriculture, construction, photography, etc. The fast growth of the number of unmanned aircraft in the airspace requires actions to keep the airspace, the people's lives, and property on the ground in safety. For this need, the European Commission and the European Union Aviation Safety Agency (EASA) developed the UAS operations regulations. Besides the new regulation, the EASA introduced the "U-space" concept to organize the UAS operation efficiently within the airspace, especially in the urban zone. The UAS is a combination of digital components and mechanical components. Besides safety, cybersecurity is also an issue for unmanned aircraft systems. There are many security problems reported in the literature.

Chapter 2

Comparison between Safety and Security/Cybersecurity

Contents

2.1 Introduction

In the previous chapter, we introduced the Unmanned Aircraft System's general concept and the public concern on its safety and security/cybersecurity. Because both safety and security refer to humans and assets' protection, they are sometimes used interchangeably in language's daily use [62]. That could lead to some confusion. Therefore, in this chapter, we first provide our definitions for these terms, emphasizing the differences between them. Then we discuss the similar aspects between safety and security. This chapter also reviews how safety and security/cybersecurity issues are addressed in both industry and academics.

2.2 Definitions

There are many different ways to define two terms: Safety and Security. These could vary from an expert to another, from a technical community to another [63]. For example, in the aerospace industry, safety could be defined as *"the state which the risk of harm to persons or property is reduced to an acceptable level"* [64] while for Industrial Control System (ICS) it could be defined as *"This state is freedom from "something" that could have negative consequences, such as harm to humans or animals, economic loss, or any other form of damage or loss"* [65]. For the information system, the security could be interpreted as *"a process involving the protection of information from a wide range of threats in order to ensure business continuity and minimize business risk"* [66], while for an embedded system, this term could be defined as *"Security is the ability of an entity to protect resources for which it bears the protection responsibility"* [67]. There are not absolute definitions for both terms: Safety and Security [68]. That sometimes leads to the ambiguity in using these terms. Moreover, both Safety and Security refer to risks and some kinds of protection, therefore, in some cases, these terms are used interchangeably such as in [69].

However, Safety and Security are still two different terms which should have different meanings. Several works in the literature are presented to show the differences between these terms. For example, based on the review of the definitions in 86 official documents (international, national standards/regulations in different sectors), Pièrre-Cambacédès et al. [70] proposed two principal distinctions between the Safety and Security definitions. The first one is Malicious vs. Accidental (M-A) distinction. The Security addresses to the undesired risks originating from malicious action meanwhile the Safety addresses the ones originating from accidental/non-intentional event. This distinction seems to be widely accepted in the literature [68], [71], [72], [73], [74]. The second distinction is called Environment-System (E-S) origin distinction. The security is concerned with the risks originating from the environment (every other thing around the considered system) and potentially impacting the system. Meanwhile, the safety deals with the risks arising from the considered system and potentially impacting the environment. This distinction is also accepted in some other researches such as [68]. However, in our opinion, the second distinction is not very clear. For example, related to the security of a plane, we could consider scenarios arising from malicious actions and impacting not only

the plane but also the life of passengers, the finance of the company, etc. Meanwhile, related to the safety of a plane, we could concern unsafely scenarios arising from adversarial weather conditions.

Based on the short analysis above, we adopt the following definitions:

- Security is a state that the system is protected against the risks originating from the malicious intent. The Cyber-security is a sub-term of Security relating to only the digital world.

  Note: In the context of our research, the term security refers in fact to the cybersecurity in most cases, except when explicitly stated.

- Safety is a state that the system is protected against the risk originating from an accident or an unintentional event.

The two definitions above should not be considered as absolute definitions. Our purpose in adopting these definitions is to avoid the misunderstanding in our context research and the remaining of the document. Moreover, in our opinion, understanding the nature of Safety and Security is more interesting than creating a short phrase to describe these terms. Therefore, in the next of this section, we analyse profoundly the similarities and differences between safety and security in different aspects.

2.3 Different aspects of Safety and Security

2.3.1 Risk concept

Safety and security have a common point which is the term "risk". In both fields, the risk is widely used by the practicals and researchers as a fundamental concept to drive activities to protect the system or the operation under consideration. The definition of this term could vary a little between different technical communities as shown in Table 2.1. Despite having a little difference between different communities, the risk term could always be expressed as the combination of two measurements (or estimation): "how bad an incident could be ?" and "how often it could happen?" or expressed by a simple formula: risk = likelihood x severity of consequence.

2.3.2 Risk management

Generally, people in charge of the safety risk or the security risk have to answer some questions such as "have all incidents been identified ?", "are the implemented protections all adequate or necessary", etc. To answer these questions, risks are usually dealt with risk management. Risk management provides a systematical and effective way to detect, analyze,

Community and source	Risk definition
Safety	
Nuclear (IAEA Glossary[69])	A multi-attribute quantity expressing hazard, danger, or chance of harmful or injurious consequences associated with actual or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences.
Aeronautics (ARP4754a[75])	The combination of the frequency (probability) of an occurrence and its associated level of severity.
Chemicals (CCPS Glossary[76])	The measure of human injury, environmental damage, or economic loss in terms of the incident likelihood and the magnitude of the loss or injury
Medical device (ISO 14971[77])	combination of the probability of occurrence of harm and the severity of that harm
Security	
Oil & gas (OLF-104[78])	The combination of the probability of an event and its consequences
General IT (NIST SP800-53[79])	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Information System (ISO 27000[80])	Risk is often expressed in term of a combination of the consequence of an event and the associated "likelihood" of occurrence
Internet (IETF RFC 4949[81]	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result

Table 2.1: Risk definition in different communities

evaluate possible incidents, and select adequate countermeasures. Moreover, the risk management helps balance the operation vs. the economic cost of implementing countermeasures [82]. Most of the risk management includes risk assessment. The risk assessment is the "key component", which provides sufficient knowledge, awareness, and understanding of the risks for justifying security measures to reduce the risks [83] in the risk management process. The risk assessment consists of the risk identification step, the risk analysis step, and the risk evaluation steps:

- **Risk identification** (see Figure 2.1) aims to identify the risk scenarios that could happen and have an undesired impact. For this step, the different risk management methods could propose different strategies. Some methods simplify this step by proposing the user a list of basic scenarios (e.g the MEHARI method (see 2.4.2) for the security of the information system and the SORA methodology (2.4.1) for the safety of the UAS operation). Other methods provide tools or models to help users reason the possible scenarios. Such methods could follow either a deductive or an inductive approach [84]. The inductive approach focuses on answering the questions "how could a given consequence occur?" or "what is the cause of a given consequence?". The good examples for this case are the Fault Tree method and the Attack Tree method. Meanwhile, the deductive approach starts with an initial event (component failure or error) and tries to answer the question "what is the consequence of a dangerous event?". Good examples for this approach are the HAZOP method and the FMEA method. All these methods are described in the following parts.

Likelihood	Frequent	Low	Medium	High	High	High
	Probable	Low	Medium	Medium	High	High
	Occasional	Low	Low	Medium	Medium	High
	Remote	Low	Low	Low	Medium	Medium
	Improbable	Low	Low	Low	Low	Medium
		Negligible	Minor	Serious	Major	Critical
		Severity				

Table 2.2: Risk estimation matrix in ISO14971-Risk Management to medical devices

- **Risk analysis** (see Figure 2.1) is the activity to comprehend the nature of risk related to the scenarios identified in the risk identification. As aforementioned, the risk is the combination of the likelihood and the severity of consequences; therefore the risk analysis involves the estimation of these factors [85]. The estimation of the likelihood and the severity could be either qualitative or quantitative. For safety, according to the observation of Khan et al. [86], the quantitative approach and the hybrid approach are more and more considered than the qualitative technique. Meanwhile, for security, the qualitative approach is the most preferable [87]. The reason for these phenomena could be the availability of the data. In safety, the data on component failures or accidents are usually accessible (e.g by testing, we can estimate the life cycle of a mechanic/electronic component) and the information on safety accidents could be collected in public (news-

paper, reports, etc.). Therefore the likelihood factor of risk related to safety could be estimated by using mathematical tools such as statistic and probability. While for security, the information on security incidents is usually not all accessible [68]. Moreover, the likelihood of a successful attack is strongly dependent on a lot of uncertain factors such as the capacity, the motivation of attackers, and the attack technique which evolves day by day. That makes quantitative estimation difficult in the security discipline. After being estimated, the likelihood and the severity are combined into a risk level. Usually, the combination could be done by using a risk estimation table. (e.g Table 2.2)

- In **risk evaluation**, based on the result of the risk analysis, the decision-maker decides which risks could be ignored, which risks should be treated. The highest risks will be treated first with the highest priority and the lower risks will be ignored or be treated later.

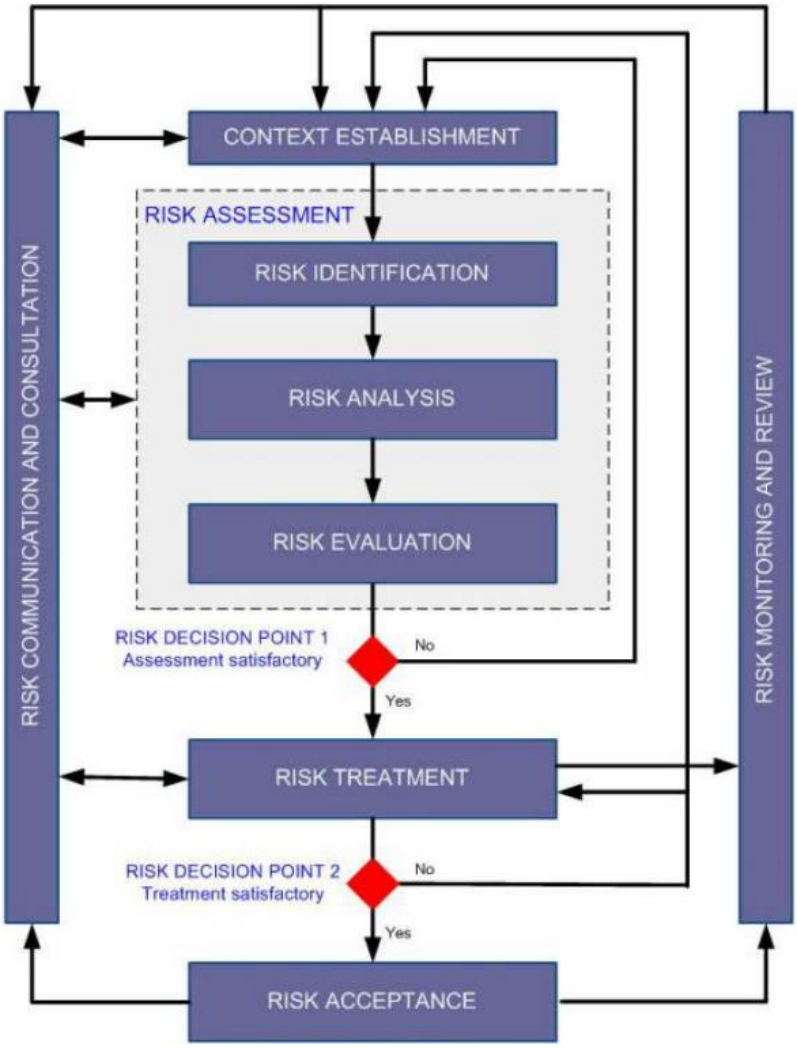


Figure 2.1: ISO 27005 risk management framework

Besides the risk assessment, the risk management could include other activities: the context

establishment, the risk treatment, the risk communication. The context establishment aims to prepare all necessary input information (such as information on the operation, system, setting risk evaluation criteria, risk acceptance criteria, etc.) for the risk assessment (see Figure 2.1). The context establishment is considered a critical activity influencing the final result [83], [88]. **Risk treatment** refers to reduce the risks after the risk assessment by implementing different treating options. Traditionally, there are four categories of treating options: risk avoidance, risk reduction (or mitigation), risk acceptance, and risk transfer [68]. The **risk communication** is an activity to exchange and share information on risks between security managers and other stakeholders such as developer, client, supplier [89], [90]. Figure 2.1 presents a complete framework of risk management proposed by the ISO 27005 Standard on security information risk management. This framework is consistent with the one proposed in another guide of the same organization on general risk management - ISO 31000:2009 [91].

2.3.3 System design process

Both safety and security have major influences on the system design. They are considered not only supplements of a system design but also one of the most important objectives that derive the system design [68]. For example, safety requirements, like the single-failure criterion in the nuclear industry, lead to redundancies, the diversification, and the physical separation of sub-systems or components [92]. As another example, in IT systems, the security requirements lead to the need for the segmentation of the network, in which components are virtually separated based on their functions and security risks. The implementation of these measures or strategies have huge impact on the architecture of the system. Therefore, the sooner safety and security requirements are considered in the design process, the more effective and financially efficient their implementations are [68], [93]. This idea is adopted for designing critical systems such as an airplane. In the aeronautic industry, the design of a product is unfolded according to the V-cycle process that covers the functionality requirements identification, requirement implementation, and the requirement validation. To take into account safety issues in each step of the design process, the standard ARP4754 proposes a second V-cycle process which cover safety requirement identification, implementation, and validation (the ARP4754 standard is widely used in aeronautic as a development guide). Two processes are unfolded in parallel as shown in Figure 2.2. Then, when the cyber-security becomes an important concern in the aeronautics, this industry adopts the third V-cycle process related to cyber-security assessment, which is proposed in the standard ED-202A / DO-326A [94]. The cyber-security process is conducted in the same time as two other ones.

2.3.4 Operation and Human factor

Both safety and security should be considered not only in the system development but also in operation. The risks related to safety and security could be reduced through “non-development” activities such as maintenance, inspection, monitoring. The maintenance, regular inspection, change record, and activity log play an important role to keep the system

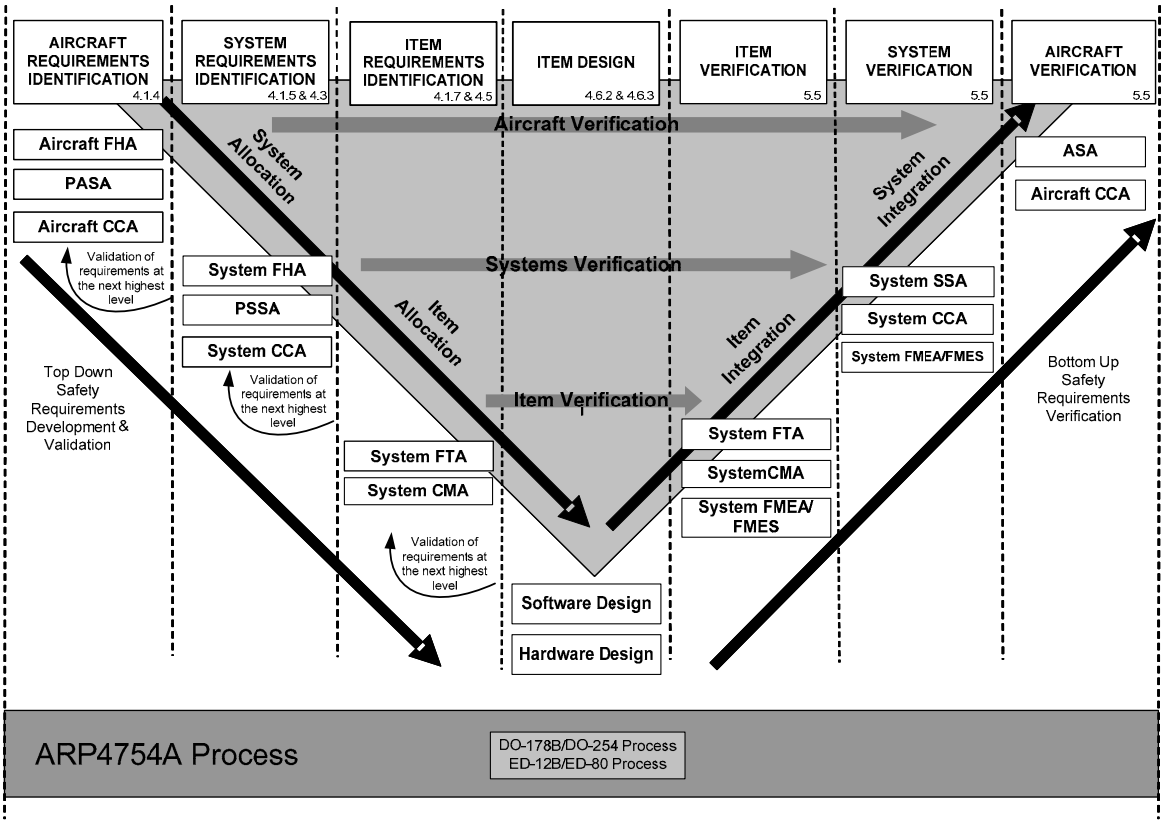


Figure 2.2: Double V-cycle process in the standard ARP4754 [75]

operation in safety [95] and security [96]. On one hand, these activities are considered as preventive measures to reduce risks. On the other hand, these activities help generate the operating feedbacks to develop new technique measures or updates. Besides these activities, staff training, emergency plan establishment, and regular testing exercises are other activities to assure both the safety and the security of the system in operation [97], [98], [92]. These activities deal with the human factor in the operation which is considered as an important source of security and safety incidents. In safety, the Three Mile Island event is a typical nuclear accident caused by the fault of the operator, which attracted the concern on the human factor [68]. The role of the human factor in security (cyber-security) is acknowledged later at the beginning of the 1990s after the social engineering attacks realized by the hacker Mitnick [99].

2.4 Standards and methodologies for the risk management

2.4.1 Safety

IEC 61508 is a safety standard developed by the International Electrotechnical Commission (IEC) for electrical/electronic/programmable electronic (E/E/PE) safety-related systems.

This standard has been developed since the computer-based system was increasingly used within the industry in the 1980s. On one hand, the adoption of the computer-based system proposes many safety advantages as well as functional improvements and economic benefits. On the other hand, this adoption makes the system complexity arise and creates a challenge in designing these systems in such a way as to prevent dangerous failures [100]. The IEC 61508 guides to minimize these failures in all E/E/PE safety-related systems. This standard helps to establish the requirements to ensure that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL) [101].

ARP4754, ARP4761 constitute guidance for safety analysis and development of the avionic system. Among them, the ARP4754 standard guides the process of airworthiness certification in a highly integrated avionic system. The detailed development process for hardware and software is deal within respectively the DO-254 standard and the DO-178C standard. The interface between the DO-254 and DO-178 standards and the ARP4754 standard is Development Assurance Level (DAL). The DAL is assigned to software/hardware system by the process mentioned in the ARP4754 and is implemented in detail by the processes mentioned in the DO-254 and DO-178C. Accompanying the 4754 standards, the ARP4761 standard provides a depth guidance in terms of risk assessment technique to conduct the process indicated in the ARP4754 standard. To conduct risk assessment processes, different techniques such as Fault Tree Analysis, Markov Analysis, Fault Mode Effect Analysis, are used in combination [102].

Specific Operation Risk Assessment (SORA) is a risk assessment methodology dedicated to drone operations. This methodology is endorsed by the European Aviation Safety Agency (EASA) as a means to fulfill the EU requirements. On one hand, this methodology provides both the UAS operator and the aviation authority with a communication tool in the context of administrative processes (such as operation validation) [103]. On the other hand, this methodology provides drone constructors, hardware/software manufacturers with a tool to anticipate the necessary requirements related to the safety in early phase of the development [103]. Nowadays, the SORA methodology focuses on the safety aspect but ignores the security aspect. More detailed description of this methodology is presented in [104].

2.4.2 Security

ISO 27005 standard This standard is partly explained in 2.3.2. We remind that it is a guidance to implement the information security risk management in an organization. This standard does not provide a specific risk management method, but, rather constitutes a framework for risk management process [90]. The framework consists of six activities: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring/review. Beyond the information security in an organization, ISO/IEC 27005 is also referred as a guidance to ensure cybersecurity in cyber-physical systems, in which the IT part and the physical part exist simultaneously and interact with each other.

IEC 62443 is an industrial standard for risk management to secure the Industrial Automation and Control System (IACS). This standard provides processes and best practices to develop, integrate, and assess components about the cybersecurity threat. The IEC 62443 is built on the concept of ISO 27005 series and refines them to adapt the differences between the Operational Technology (OT) and the Information Technology (IT) [83]. However, the integration of Internet of Thing (IoT) devices into IACS has accelerated the convergence of OT and IT and resulted in new cyber-security threats for IACS. Hence, Leander et al. [105] argued that at some points, the current IEC62443 standard is not sufficient to deal with the new security threat brought by IoT devices into IACS such as handling of cross-zone communication and software updates.

ED202A/DO326 is a guidance for the airworthiness security process, which is developed by two industrial committees Radio Technical Commission for Aeronautics (RTCA) and European Organisation for Civil Aviation Equipment (EUROCAE). The objective of this document is to add new processes to handle the threat of intentional unauthorized electronic to the current process of aircraft development and certification defined in the APR4754 standard. The airworthiness security process consists of three main parts: (1) Certification activity, (2) risk assessment related activities (equivalent to context establishment and risk assessment activities in the ISO/IEC 27005 standard) and (3) security development activities (equivalent to treatment activities in the ISO/IEC 27005 standard) [106]. The ED202A standard is followed by ED203 that explains with more details the activities.

Method for Harmonized Analysis of Risk (MEHARI) is an open-source information risk management methodology. It has been developed and maintained by CLUSIF (CLUB for Security of Information in France) – an association of companies and experts in the information security since the mid-1990s. This methodology is designed to implement risk management according to ISO/IEC 27005 [107]. The newest version of MEHARI provides not only detailed definitions, processes with specific examples according to activities in ISO/IEC 27005 but also a database of knowledge in vulnerabilities, security incidences and security solutions; a questionnaire for evaluating security service quality. Because the original applicative domain of MEHARI is "information security in an organization", the existing database and the supporting tool is suitable for this domain. However, CLUSIF provides also guidance to establish a new knowledge database to adapt MEHARI to other specific systems such as Industrial Automation and Control System (IACS), Supervisory control and data acquisition (SCADA), etc. [108].

E-safety Vehicle Intrusion proTected Applications (EVITA) [109] [110] is a research program funded by the European Commission and a consortium consisting of car manufacturers, automotive suppliers, security experts, hardware/software experts. The objective of this project is to design, verify, prototype a modular, cost-efficient security solution to protect sensitive data for automobile on-board network comprising of electronic control units (ECUs), electronic sensors, and electronic actuators. For this purpose, this project presented a methodology for security requirement analysis. Although compliance with the ISO/IEC

27005 standard is not mentioned and is not an objective, the methodology could cover some important activities of ISO 27005 framework such as the context establishment, the risk assessment and treatment activities.

2.5 Safety analysis techniques

2.5.1 HAZOP

HAzard and OPeration (HAZOP) is a systematic and structural technique used worldwide to identify the hazard of a system and its operation problem. In other words, this method aims to identify risk scenarios related to a given system. The method is based on an important argument that the risk scenarios are caused by the deviation of the system from the intended design [111]. Therefore, to identify the scenario, HAZOP focuses on looking for deviations (status, behavior,...) and deducing the consequence of these deviations. The deviation identification process relies on using guide words (less, more, late, early, faster, slower, etc.) combining with process parameters (e.g., temperature, flow, pressure) [112]. Based on these words, the people in charge brainstorm together different deviations such as "the motors run faster than design intent". Because of focusing only on the malfunctions of equipment and process parameters, this method does not consider the scenarios related to the human factor. HAZOP analysis first appeared in the 1960s to identify possible hazards present in chemical facilities to Eliminate any source leading to major accidents, such as toxic releases, explosions, and fires. Over several decades, HAZOP is extended to other types of facilities. CHAZOP (computer Hazard and operability Study) is a derived version of the HAZOP technique but is specialized for control and safety systems (PLC, I/O card, circuit breakers, actuators, local control panel,...) [113]. This version proposes new guide words and parameters such as no signal, out of range signal, no power, no communication, I/O card failure, software programming, incorrect/inadequate and cyber-attack [113]. EHAZOP (Electrical hazard and operability study) is another extrapolated version of the HAZOP technique but it is dedicated to electrical systems (power generation, transformation, transmission and distribution...). This version proposes also new guide words such as power surges, 24 VDC supply failure, flashover, transformer incident substation bus bar failure, lack of maintenance, etc.

2.5.2 SIL analysis

Safety Integrity Level (SIL) presents the required performance level of safety measures to achieve an acceptable level of risk for an industrial process. The required safety performance is measured in terms of the probability of failure on demand (PFD). The term SIL is used worldwide and is standardized in the IEC 61508 which provides guidelines for the design, installation, operation, maintenance, and test of Safety Instrument System [114]. This standard proposes 4 levels of SIL with different values of PDF as shown in Table 2.3. In the safety process, the SIL is assigned to safety measures based on the amount of risk reduction which

Solicitation	Low Demand	High Demand
SIL	PDF Average	Failure/hour
1	$[10^{-2}, 10^{-1}]$	$[10^{-6}, 10^{-5}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-7}, 10^{-6}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-8}, 10^{-7}]$
4	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

Table 2.3: SIL value in IEC61508 [114]

is necessary to keep the system in safety. According to the works of Summers [115], there are several basic techniques for SIL assignments as follows:

- **Modified HAZOP** is an extension of HAZOP analysis. It is a subjective assignment based on the team's qualitative understanding of severity and likelihood. Therefore, it depends heavily on the experience of team members. Because this approach is very subjective, it requires that the team member know not only the system under consideration but also the acceptable risk tolerance of the company. Moreover, it needs some consistency between the personnel on the SIL assignment teams from project to project.

SIL	Consequence
4	Potential for fatalities in the community
3	Potential for multiple fatalities
2	Potential for major serious injuries or one fatality
1	Potential for minor injuries

Table 2.4: SIL assignment based on Consequence [115]

- **Consequence-only evaluation** is a SIL assignment technique based on only the severity of consequence while the likelihood of risk scenario is ignored. As a result, all scenarios resulting in possible fatalities would be assigned the same SIL without considering their likelihood. It is the simplest technique because the likelihood is often difficult to estimate. This technique is appreciated when historical data is limited [115]. An example of a table decision for SIL assignment is shown in Table 2.4.

- **Risk matrix** is one of the most common techniques, among refining, chemical and petrochemical companies [115]. Different from Consequence Only, this technique is based on the correlation of the severity and the likelihood of the risk scenario to SIL. To apply successfully this technique, the process, system, and associated risk must be well understood so that the qualitative estimation of the likelihood and severity can be made. An example of a risk matrix for SIL assignment is shown in Figure 2.3

- **Risk graph** is a qualitative technique for SIL. In this technique, the SIL is commonly assigned based on four factors: consequence or severity consequence (C); frequency and

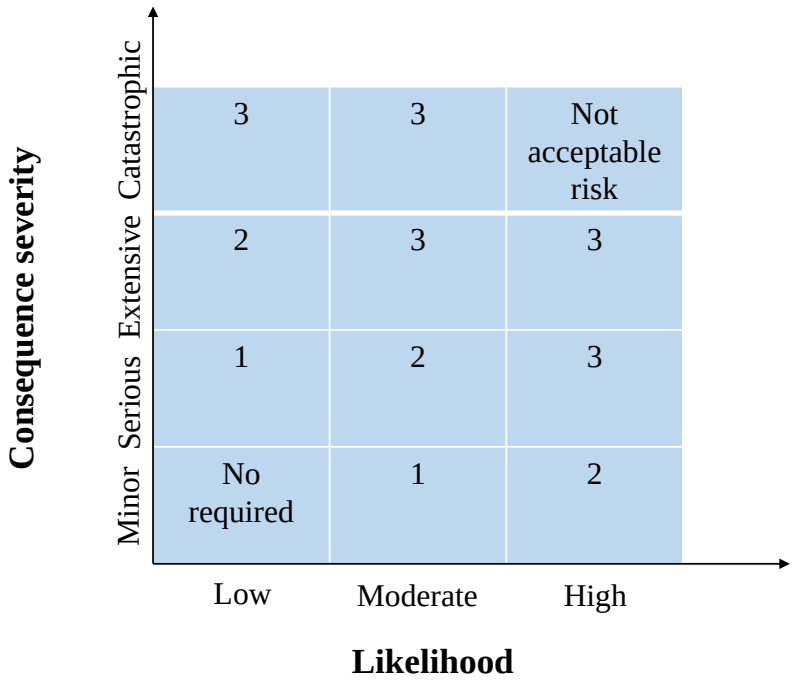


Figure 2.3: Risk matrix for the SIL assignment in the ANSI/ISA 84.00.01 standard

exposure time (F); possibility of avoiding the hazardous event (P); and probability of the unwanted occurrence (W) [114] as shown in Figure 2.4. The combination of the three last factors: F, P, W represents the likelihood of a risk scenario. In other words, the SIL is always assigned based on the nature of the risk: consequence and likelihood, however, the likelihood is replaced by its contributor parameters (F, P, W).

- **Quantitative assessment**: In this technique, the SIL for safety measures is determined based on a quantitative estimation of the likelihood of the associated incident. The method requires a thorough understanding of the potential causes of the incident and an estimated probability of each potential cause. Therefore, this method is suitable for the case that there is very limited historical information about incidents, so that the qualitative determination of likelihood is extremely difficult [115]. To determine the required SIL, the accepted or tolerable risk probability is divided by the calculated process demand as follows:

$$\text{Probability of failure on demand} = \frac{\text{Tolerable risk probability}}{\text{Process Demand}}$$

At this point, we can find that the SIL is quite similar to the risk level mentioned in 2.3.2. Both terms correlate with the severity and the likelihood of the incident or the risk scenario and could be used in risk assessment activity. However, these are still two different things. The risk level is the combination of likelihood and severity and represents the nature of the system or process. When a safety measure is implemented, the risk level could be changed (we hope that it reduces to the acceptable level). Meanwhile, the SIL represents the performance

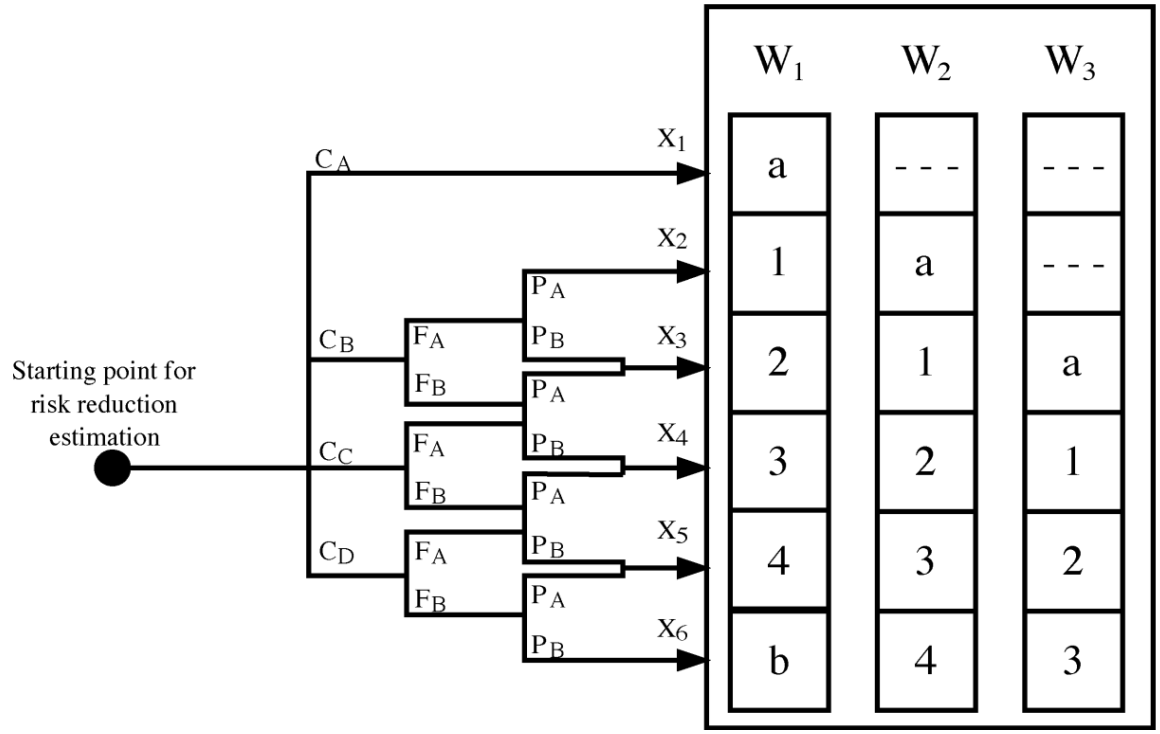


Figure 2.4: Risk graph for SIL assignment [114]

target for safety measures. When a safety measure is chosen to implement, the SIL doesn't change but a question is raised: "does the chosen measure satisfy the required SIL ?".

2.5.3 Fault Tree Analysis

The Fault Tree Analysis (FTA) is a graph-based analysis technique for system safety. It was first developed and applied by the Bell company for aerospace applications in the 1960s [86], then it becomes popular and widely used in other critical systems such as the nuclear power, automotive, medical systems [116]. This technique helps the analyst to evaluate a given system and to understand and prevent associated risks. By applying FTA, the analyst could create a visual model illustrating how equipment failures and human errors could contribute to an accident event. Based on this model, the analyst could identify the riskiest conditions and place safety measures or recommendations. Therefore, the FTA is commonly performed during the system development and its result influences the design by predicting and preventing future problems [93].

The FTA process concludes two steps. The first step is to show how different components failures or certain environmental conditions can combine to cause a given system failure. This step is started by choosing an undesired event (UE) as the top node of the graph. The UE is

any event that is identified as objectionable and unwanted. Then, by reasoning deductively, the intermediate events that contribute to the UE are identified and placed into the graph as the branch nodes. The branch nodes and top nodes are connected by different logic gates such as OR, AND, XOR as shown in Figure 2.5. The deductive reasoning process is repeated to identify the cause of identified intermediate events until reaching the basic events which could not be decomposed into smaller events. After constructing the tree graph, boolean algebra is applied to identify cut-sets which are the smallest combinations of basic events necessary and sufficient to cause the UE. The second step is to calculate the probability of the UE based on the probability of basic events in Cut-sets. The result of this step helps analysts to recognize not only the likelihood global of the UE but also the significance for all the events in the fault tree in terms of their contributions to the UE probability.

Although the conventional Fault Tree is highly successful and widely used, it have also limitations. The conventional FTA is the inability to model the time sequence of the events during constructing the tree graph. For example, if we have a system including two components A and B with two assumed situations: "if component A fails before B fails the system will not fail" and "if component B fails before A fails the system will not fail"; the FTA could not distinguish these situations. To overcome this limitation, different approaches are proposed to create a dynamic fault tree analysis such as new logic gates [117], Bayesian Networks based approaches [118], new algebra frameworks [119], Monte Carlo based approaches [120]. As another limitation, the conventional FTA is the inability to overcome the uncertainty on the failure data of basic events. For many complex and large systems, it is often difficult to determine precisely the probability of all basic events. That leads to an unreliable result. To overcome this limitation, Tanaka et al. [121] proposed to use the fuzzy theory in FTA. Then, this idea is adopted by other researchers to develop further the Fuzzy Fault Tree Analysis (FFTA) [122] [123], [124].

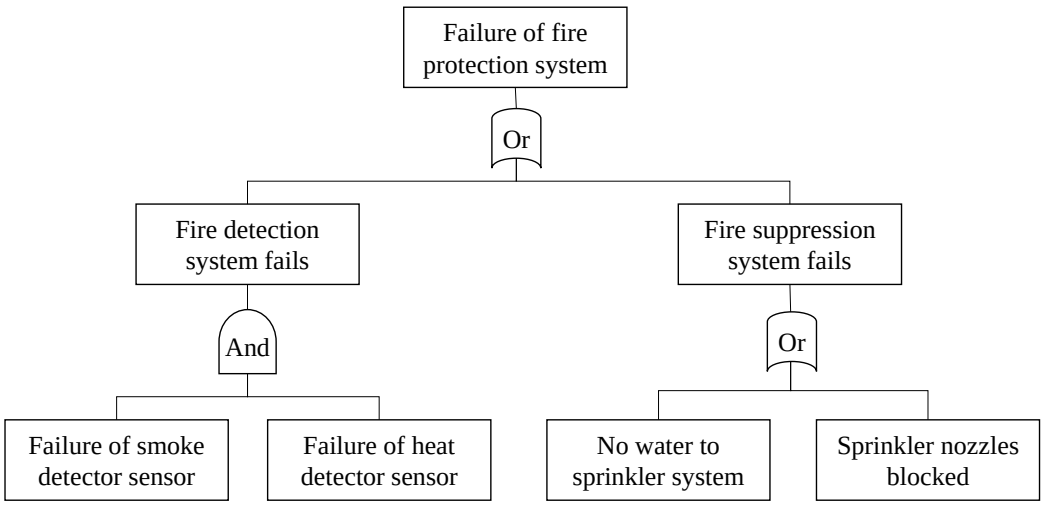


Figure 2.5: Example of Fault Tree Analysis [125]

2.5.4 Event tree

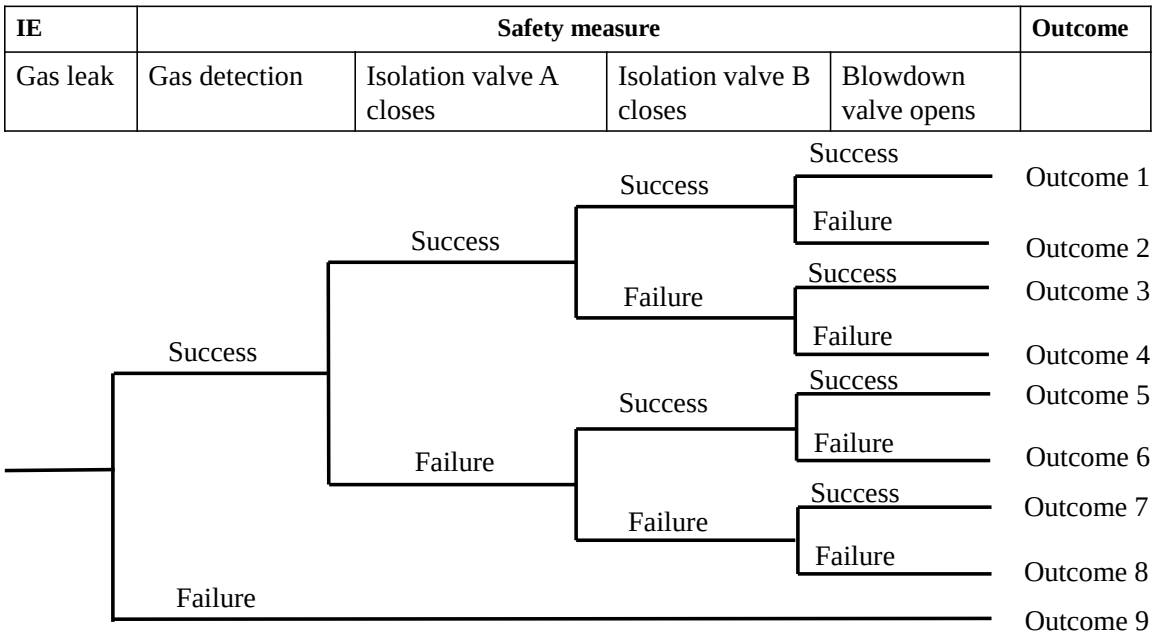
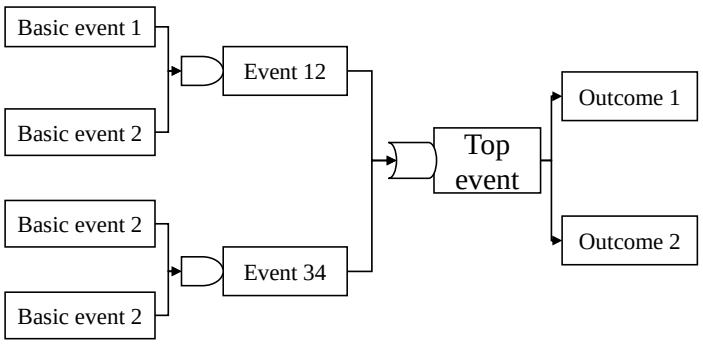


Figure 2.6: Example of event tree graph [126]

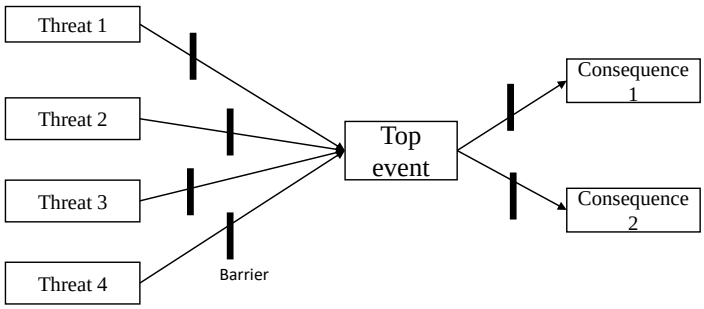
Event tree analysis is another graph-based analysis technique introduced in nuclear reactor programs in the 1970s [127] and then adopted by other industries such as aeronautic, chemistry. This technique is generally applied in the early phase of system design and development to identify safety issues and design safety measures rather than take corrective actions after tests or accidents [93]. It helps to identify inductively and evaluate qualitatively sequences of events (or risk scenarios) in a potential accident started by an initial event (IE). Based on the graphic approach, this approach focuses on illustrating the relation between an accident resulting from an IE and the failure of associated safety measure in term of logic and probability. In the even tree graphic, accident scenarios (or risk scenarios) are modeled by three elements: an Initial Event (IE), Pivot events, and Outcome. An IE is on the top of the graphic and represents a perturbation in the system (such as fire, gas leakage, pressure lost) that requires the response of an operator or the response of the safety system to avoid undesired consequences. Pivot events are immediate points that follow the IE in the graphic tree branch (sometimes called branch points). The pivot events represent successes or failures of safety systems on responding to the initial event. The Outcomes are the endpoint of the tree graphic, which represents losses of some kinds such as Loss of life or injury/illness to personnel, Damage to or loss of equipment or property, Failure of the mission, which could range from minor to major consequences. An example of event tree is shown in Figure 2.6. The event tree graph gives a short and simple description of possible outcomes and provides a tool to estimate their frequency/probability. The probability of initial event and pivot events could be revealed from the historical data or the result of other analyses such as Fault tree analysis [126]. The probability of Outcome is calculated by multiplying the ones of IE and pivot events.

2.5.5 Bow-tie analysis

The Bow-tie analysis is a graph-based technique for safety risk assessment, which has become popular and used in high hazard industries such as oil & gas, aviation, mining [128]. This technique model safety accidents by a graph in the shape of a bow-tie. The principal elements of this graph include a Top Event, Threats, Consequences, and Barriers. The Top event is the central point of a bow-tie, which is usually defined as some kind of loss such as "loss of containment" in oil and gas and "loss of separation" in aviation [128]. The threats locate on the left of the Top event and represent the causes of the Top event, while the consequences locate on the right side of the Top event and represent the consequences of the Top Event or the outcomes of the accident. Each bow-tie graph has only one Top Even which is caused by multi-threats and leads to multi-consequences. The Barriers are on both sides of the Top event. They illustrate different measures planned to prevent, control, or mitigate accidents [129].



(a) FT-ET bow-tie



(b) Shell bow-tie

Figure 2.7: Bow-tie graph example [128]

Although the bow-tie has been popular, it lacks of a consistent approach [128]. At least, we can recognize at least two approaches named also "bow-tie analysis" which are different in terms of graph structure, purpose, risk quantification. The first approach is a combination of Fault-tree and Event-Tree as shown in Figure 2.7a. In this approach, the bow-tie graph starts with a fault tree, converges in a top event, then it diverges using an event tree. Barriers in this approach are usually not indicated directly in the graph but rather under forms "fail/successful

event" of safety measure. Taking advantage of both the Fault tree and the Event tree analyses, this approach allows the analyst to break down and analyze the possible accidents in detail. Therefore, this approach is used to calculate the probability of consequence [130], [131]. In the work of Salvi et al. [132], the quantitative result of this approach is used to justify the performance requirement of safety measures under Safety Integrity Level (SIL). On the other hand, this approach has the same difficulties than conventional FT and ET such as data uncertainty [133], non-dynamic model [134], model uncertainties [135]. The second approach is the Shell bow-tie. Instead of a combination of FT and ET, this approach provides a simple bow-tie graph as shown in Figure 2.7b. The left side of the graph includes multi-threats which could cause the top event by themselves without any intermediate events. The top event then causes single consequences on the left. In this approach, barrier elements are directly presented on both the left side and the right side of the graph. In comparison with FT-ET based graphs, the shell bow-tie graph has a higher abstraction level and less specific information so it is less powerful to calculate the probability of consequences. However, the shell bow-tie is much simpler to understand. It has less symbol and illustrates more clearly the safety barrier than FT-ET based graphs. That makes the shell bow-tie a good tool to communicate [128], [136] (e.g operations, users, administrators) and "ensure that there is a barrier or control for each failure pathway" [137].

2.5.6 Markov Analysis

Markov Analysis or Markov process is a graph-based technique for modeling state-transitions of system and calculating (failure) state occurrences. System states are a combination of (working/failure) states of subsystems or components. For example, a system has two components A and B; there are different system states such as (A-working, B-working), (A-failure, B-working), (A-working, B-failure), (A-failure, B-failure). In Markov Analysis, it's assumed that the system state changes continuously from one state to another over the time and the future system state depends on only the current state. These state transitions are modeled by a State Transition Diagram. This diagram shows different states of a system, transition directions accompanied by transition rates as shown in Figure 2.8. The State Transition Diagram is used to establish a set of first-order differential equations, which represent the relationship between the probability of different states over time. By resolving this set of equations, we have the probability of failure states.

Comparing with other techniques, the Markov analysis has both advantages and disadvantages. Its strong point is that it could take into account some aspects which are impossible for other techniques such as timing, repairing activity, fault-tolerant [93]. Therefore, it is a powerful tool to conduct a precise quantitative analysis [138]. However, this technique is quite complex to learn and requires the analysts to have a good knowledge of mathematics. Moreover, the graphs could be large, difficult to read and trace when the system under consideration becomes large [93]. For these reasons, in 2003, Bouissou et al. [139] proposed the Boolean Driven Markov Process (BDMP) - a combination of the Fault Tree analysis and Markov analysis. This technique takes the advantages of both origins: (1) easy to understand,

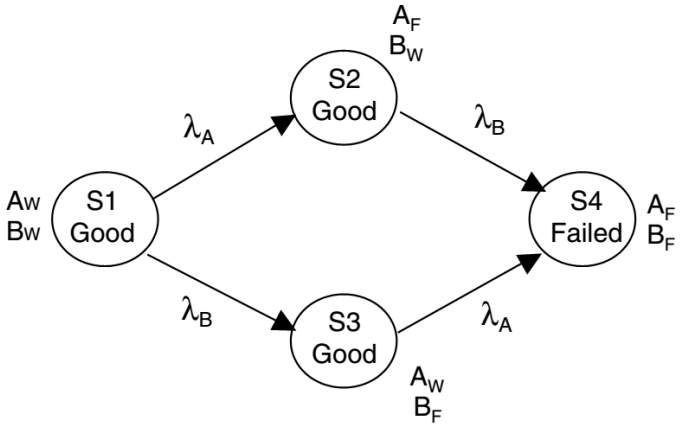


Figure 2.8: State Transition Diagram [93]

create and trace (Fault Tree), (2) precise quantification (Markov analysis).

2.5.7 Petri Net

Petri Net (PN) is an analysis technique to identify hazards or accident scenarios but not to calculate quantitative probabilities. To identify hazards, the PN analysis provides a tool to model graphically a system at a wide range of abstract levels. Like the Markov model, the PN models could also illustrate different system states (including failure states) and deal with the timing, state transitions, repair activities. The strength point of these models is that they could illustrate the links between hardware, software, and human elements in the system. However, the PN analysis is not as widely used for system safety analysis as other techniques such as Faul tree or Event tree because of its complexity. The PN model quickly becomes large and complex as the system size increases [93]. Therefore its use has rarely been applied to large systems and has been limited to the examination of software control systems.

2.5.8 FMEA

The Failure Mode and Effect Analysis (FMEA) is a bottom-up technique to analyze the safety of systems and prioritize actions to reduce the risk. It was first introduced in 1949 by the US Army, then has been used extensively to analyze safety in a wide range of industries such as aerospace, automotive, nuclear, mechanical, and medical industries [140]. In FMEA, the analysis focuses on examining/identifying all component failures and their effects on operations, systems, the environment. Then the combination of the component failure rate and the severity of effect interprets the risk of component failure and indicates the priority for the associate risk reduction action. Pierre et al. [141] propose a solution to generate automatically a FMEA analysis from a system design written in UML/SysML. This solution helps improve the interaction between the system design and analysis processes. In the more detail version of FMEA known as Failure Mode, Effects and Criticality Analysis (FMECA), the information

on the capacity to detect the component failure is also taken into account to evaluate the risk. As the information on components (such as failure mode, failure rate) is required, the FMEA is generally performed when the detailed design of a system is available or new detailed design is changed. The strong point of this technique is that it is relatively easily understood, inexpensive to perform, and provides meaningful results [93]. However, it has also a weak point. The first one is that the analysis quality depends on the user's experience, so the result could be subjective and not robust [142], [138]. The second one is that the FMEA could not identify all risk scenarios. Because the technique looks at a single component failure while an accident could result from a combination of component failures [93].

2.5.9 Summary

Technique	**Risk assessment**		
	Risk identification	Risk analysis	Risk evaluation
HAZOP	Based on guide words Table form Causal-Hazard-Consequence	X (from other source)	Compare with criteria Identify Risk level
SIL analysis	X (not focus)	X (from other source)	Multi approach Identify targeted performance of measures
Fault Tree	Deductive reasoning, Graph model Basic event-Top event	Quantitative Probability propagation	X (not focus)
Event Tree	Inductive reasoning Graph model Top event-Outcome	Quantitative Probability progation	X (not focus)
Bow-tie	Combination of FT, ET Illustrate safety barriers.	Combination of FT, ET	X (not focus)
Markov Process	X (not focus)	Quantitative System state probability	X (not focus)
Petri-net	X (not focus)	Quantitative System state probability	X (not focus)
FMEA	Inductive reasoning Table form Failure mode - Effect	X (from other source)	Compare with criteria Identify risk level

Table 2.5: Risk assessment techniques comparison

Above, we introduced eight basic techniques widely-used for the risk assessment. Each of them focuses on some tasks of a risk assessment (see Table 2.5). For the risk identification task, we can use HAZOP, Fault Tree, Event Tree, Bow-tie, and FMEA. For the risk analysis task, Fault Tree, Event Tree, Bow-tie, Markov Process, Petri-net could provide accurate qualitative results. For the risk evaluation task, Hazop, SIL analysis, and FMEA give more detailed instructions than other techniques. Moreover, each technique has strong points in different aspects, such as communication, reasoning, documentation. Therefore, in a risk assessment for a critical system, various techniques could be used in combination. For example, the FMEA, Fault Tree, Hazop could be used to conduct a Preliminary System Safety Assessment (PSSA)

- defined in the ARP 4761 standard for avionic systems [143]

2.6 Security analysis techniques

2.6.1 From SIL levels to SAL levels

Similar to the safety discipline, the security discipline involves designing, implementing, and verifying some kind of protection. Therefore, the SIL concept could be useful in the security discipline. However, The original SIL analysis has a limitation as applied to the security discipline [144], [145]. SIL factor represents only the targeted performance in terms of failure rate on demand, while the security requires usually the resiliency to network-based attacks and exploitable software or hardware conditions. Based on the SIL concept, Kube et al. [144] propose a basic concept of Security Assurance Level (SAL), which represents targeted component resiliency against a compromise of security controls or designed functions. The concept of SAL is adopted and further developed in the ISA99/IEC62443 [145], [87] standards which deal with the cybersecurity of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. These standards use Security Assurance Levels (SALs) to describe the protection needed to ensure the security of a system. The security protection is described by seven foundation requirements: (1) Access control, (2) Use control, (3) Data integrity, (4) Data confidentiality, (5) Restrict data flow, (6) Timely response to an event, and (7) Resource availability. The SAL is defined in terms of 4 different levels (1, 2, 3, 4) with the increasing of the rigor of the foundation requirements as resumed in Table 2.6.

SAL	**DESCRIPTION**
SAL 1	**Protection against causal or coincidental violations** Causal or coincidental violations are usually caused by the lax application of security policies
SAL 2	**Protection against intentional violation using simple means** That means the attacker does not need detailed knowledge of security, the domain, or the particular system under attack
SAL 3	**Protection against intentional violation using sophisticated means** Attackers are required to have advantage knowledge on security and domain operation of the targeted system to conduct this kind of violation
SAL 4	**Protection against intentional violation using sophisticated means with extended resources** Similar to SAL 3, but attackers have extended resources such as high-performance computers, extended periods of time

Table 2.6: SALs in IAS99/IEC62443 [145]

2.6.2 HAZOP in security

As aforementioned, the fundamental of HAzard and OPeration (HAZOP) is that the unsafe situation is caused by the behavior deviation of the system. To adapt this technique to the security discipline, it requires some modifications. Winther et al. [146] propose a HAZOP-based technique to identify different security threats related to a given Critical System. The security threats are identified based on the combination of the new guide-words and the negative of security attributes such as disclosure, manipulation, denial. Wei et al.[147] propose another HAZOP-based approach dedicated to embedded systems. This approach uses the attack taxonomy proposed by the Computer Emergency Response Team (CERT) as new guide-words and model system behaviors by sequence diagrams. Instead of modifying or changing the original guide-words, Srivatanakul et al. [148] and Daruwala et al. [149] propose to use the original HAZOP and Use-case model to carry out security analysis of software and hardware. In this approach, the means of guide-words should be understood broader and the user is required to be more creative. The use of the HAZOP-based concept forces the analyst to consider unusual scenarios. However, the abstraction level related to a predefined list of guide-words could also hide risks that will not be considered [68].

2.6.3 From Fault Trees to Attack Trees

The Attack Tree (FT) analysis is a tree-graph based technique to identify feasible attacks against a given system and prioritize security countermeasure. This technique is considered an adaptation of the safety technique Fault Tree analysis (FT) for the security discipline[148] [68]. The concept of AT analysis is quite similar to the one of FT analysis. The attack tree illustrates the goal of an attack as a top node of the tree. The intermediate goal which the attackers need to achieve to reach the goal of the attack is represented by the intermediate nodes of the graph. The graph ends with different leaf nodes representing basic attack actions. The nodes are connected by only two logic gates (AND/OR) instead of at least four in FT analysis. The concept of AT analysis is firstly presented by Schneier [150] in 1999 and illustrated in the context of the payment system, [68], [151]. In this work, the author evaluates the risk and prioritizes the countermeasures based on the cost of attack which is qualitatively estimated. Since the first presentation, the AT tree has been adopted and further extended. This method is commonly used in many different applications or industrial domains such as automobile [152], smart health [153], industrial control system [154], online-banking [155]. Ekstedt et al.[156], Kordy et al [157] extend the conventional attack-tree graph to the attack-defense tree to model security countermeasures. Regarding countermeasure and risk evaluation, Jürgenson et al. [158] propose to use different parameters such as cost, the feasibility of the attack, and skill level required by the attacker. The fuzzy theory [159], game theory [160] are also proposed to improve the analysis.

2.6.4 FMEA-based technique

The Failure Mode Effect Analysis is a safety analysis technique to identify and understand the effect of feasible failure mode. Because of being systematic, easy to understand and "self-documented", this technique has inspired the works in the security discipline. Several works are presented in the literature to adopt FMEA to security with some modifications. For example, Aagedal et al. [161] used FMEV in a security context within the CORAS European project; Gorbenko et al. [162] proposed Intrusion Modes and Effects Analysis (IMEA) for Web service analysis; Schmittner et al. [163] used FMEA for automobile security; Bowles et al. [164] proposed Threat Effect Analysis (TEA) for software analysis. The principle of these works is that instead of failure modes, they focus on examining feasible threat/attack modes and their effects on a given system and operation. The threat/attack modes are usually related to and reasoned from the loss of security attributes (Confidentiality, Integrity and Availability). Toward a systematic co-analysis approach (both safety and security), Schmittner et al. [73] proposed Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) technique. The authors provide a visual model for security-safety risk scenario and a detailed process to conduct the FMEA for the security and safety analysis.

2.6.5 Bow-tie analysis for security

Bow-tie (BT) analysis is a powerful tool to model visually the risk scenario and to communicate between different stakeholders. Therefore, it could be interesting to adopt this technique for security analysis. A report of the SANS Institute company [165] argues that the BT analysis could be conducted for the security analysis in the same manner for the safety analysis without any notion changes. The US Coastguard has also published a guideline on how to apply the BT technique to identify and respond to cyber attacks against maritime transportation systems [166]. In this guideline, cyber-attacks are mentioned with a high level of abstraction such as hacktivists, insider threats. For the cybersecurity of the software system, Harry [167] from PI Square use Shell bow-tie to model visually attack paths and defense measures. However, comparing to other safety analysis techniques, the adaptation of bow-tie analysis for the security discipline is quite limited, especially in the academic field. By using the Google Scholar tool, we find out very few works conducted for this subject. The most significant works related to this subject are done by Abdo et al. and Bernsmed et al.[168]. Abdo et al. [169] combined the FT-ET bow-tie with the AT to conduct a Safety-Security co-analysis for Industrial Control System. The strength point of this approach is that it allows considering risk scenarios caused by the coupling between security issues and safety issues. Bernsmed et al.[168] visualized malicious activities, random failures, security countermeasures, and safety barriers by using a common Shell BT graph. The authors proposed also a method for quantifying risks based on threat likelihood and consequence severity.

2.6.6 Markov process for security

The Markov Processes (BDMP) is a precise risk quantification tool used in the safety discipline. This technique is used also in the security discipline. Ye et al. [170] used the Markov process to observe and analyze the cyber-security risk of a computer and network system. The result of this work is used to build a real-time cyber-attack detection system. Xiaolin et al. [171] proposed a Markov Game Theory-based Risk Assessment Model for Network Information System. This model includes two Markov chains. One is to model the threat propagation and discover the hidden risk, and another is to model the repair process implemented by the system Administrator. The result of this assessment is used to build an automatic tool generating defense scheme. The coupling between the Markov process and game theory is also adopted by Lakhno et al [172] to examine the cybersecurity of the Smart City concept. Like in the Safety discipline, the limitation of the Markov process is the difficulty to read, trace, and model a complex system. For these reasons, Pièvre-Cambacédès et al. [173] adapted the Boolean logic Driven Markov Process (BDMP) concept from the safety domain to the security domain. Instead of Fault Tree, the BDMP for security combines the Markov process with Attack Tree. Attack trees are inherently static and can only examine independent events without time-consideration, whereas BDMP is dynamic and can examine simple dependencies. BDMP allows the modeling of attack sequences, but also of security countermeasures such as attack detections [174].

2.6.7 Petri-net for security

The application of Petri-net for the security analysis was first introduced by McDermott in [175]. In this work, the author proposes to use to model cybersecurity risk in the context of penetration testing and arguments that Petri nets can model sophisticated attacks combining several flaws which is difficult for other graph-based techniques such as Attack Tree. After the work of McDermott, the Petri-net based technique for the security discipline is developed further in many directions and various industrial domains. To diminish the disadvantage of Petri net in the complexity and time consumption, Zhou et al. [176] propose an approach to cover the attack tree to Petri net in the context of Internet intrusion analysis. This approach allows taking advantage of both the attack tree technique (reducing the cost of modeling) and the Petri net technique (allowing model security measures). Fu et al. [177] propose to combine Petri Net and big data analysis to evaluate the cyber security of the cyber-physical system. However, due to the complexity, this approach still requires the participation of experts in data mining to improve the accuracy of the evaluation. Jianfeng et al. [178] propose a Petri net based approach to analyze the cybersecurity in the context of the chemical process. In this approach, the Petri net technique is extended to examine also the attack time (e.g., moment, duration).

2.7 Integrated approach for safety and security

As mentioned in the previous sections, safety and security have many interactions. Firstly, the definitions of these terms are very close. Both of them refer to the protections of the system. A loss of security protection could lead to a loss of safety. Lisova et al. [179] argued that "A connected safety-critical system is not safe if it is not secure". Secondly, the safety and security domains share the same concepts about risk, risk assessment, risk management. Many security assessment techniques are origin from the ones used in the safety domain. Finally, both safety and security are essential concerns in the development and the operation of systems. Therefore, it comes naturally to integrate safety and security aspects into one integrated approach of risk assessment. In academia, there are some works related to this subject. For example, Reichenbach et al. [180] introduced an integrated methodology based on threat vulnerability and risk assessment (TVRA) technique with safety integrity levels (SILs). This methodology allows to address the influences of security issues on safety. Plósz et al. [181] proposed a method combining the FMEA technique with the STRIDE model - a security threat classification (Spoofing, Tampering, Repudiation, data leak, Denial of service, Elevation of privilege). This integrated method allows reducing time and effort by considering the commonalities of safety assessment and security risk assessment at once. Fovino et al. [182] proposed to combine the attack tree and fault tree within a risk assessment approach. For this purpose, the authors proposed a technique to integrate attack trees into pre-build fault trees to extend the usability of the results of traditional risk analysis with the consideration of potentially malicious attacks. With the same ideal, Abdo [169] use the attack-fault trees to co-analyze safety and security. However, the author argued that the safety scenario and the security scenario should not be treated based on the same scale of probability. Because the decision-maker could not know if the unacceptable risk is generated from safety-related causes or security-related causes. Therefore, the author proposes to evaluate the risk level based on two-terms likelihood parts: one for safety and one for security. Puys et al. [183] propose an approach to assess the cybersecurity of Industrial Control Systems based on the safety risk assessment. In this approach, the safety risk assessment provides the feature to model the cybersecurity attack scenarios. This approach takes advantage of the fact that industrial systems are usually well analyzed in terms of safety.

In the industry, the safety and security integrated approaches only start to attract consideration. For example, the DO-326 standard was developed in 2015 to extend the safety based process defined in the ARP4761 standard toward cybersecurity. Another example is the evolution of the IEC 61508 - the IEC 63187 standard, which is being developed to adapt better the current technology development and take into account the cybersecurity aspect.

2.8 Conclusion

This chapter discusses two different terms: safety and security/cybersecurity. Safety refers to an accidental event, while security/cybersecurity refers to an attack (malicious intention). To

address safety and security in system design or operation, practitioners and researchers usually use a fundamental concept: risk - a combination of likelihood and severity of a scenario. We found different methodologies for assessing the risk related to safety and security in the literature. In the past, safety and security were taken into account by separated methodologies. The safety methodologies have been developed since the beginning of the last century. The security (cybersecurity) methodologies have been developed since the 1980s when computers and networks became more popular. Many security/cybersecurity methodologies were developed based on the existing ones in the field of safety. Due to the interactions between safety and security, the integrated approach is currently an interesting subject. For our focused application - Unmanned Aircraft System (UAS), both safety and cybersecurity are now considered by the public. It exists a risk assessment methodology dedicated to this application: Specific Operation Risk Assessment. However, this risk assessment methodology considers only safety but not the cybersecurity aspects. In the aerospace industry, the security risk assessment methodology is mentioned in the DO-326A standard. However, this methodology seems to be too large and costly to be applied for commercial UAS. Therefore, this thesis aims to develop the security risk assessment methodologies dedicated to UAS. Chapter 3 introduces our system-based security risk management. Chapter 4 introduces our operation-based security risk assessment.

Chapter 3

System Cybersecurity risk management

Contents

3.1 Introduction

As mentioned in Chapter 2, cybersecurity plays a critical role in the system development process. For that reason, many risk management methodologies have been introduced in both academics and industry. However, there is no adequate methodology for the UAS sector, which is overgrowing. That is one of our motivations to develop and introduce a cybersecurity risk management methodology dedicated to an Unmanned Aircraft System (UAS). Moreover, through this study, we aim to add the cyber-security aspect to the development process of the SOGILIS company - our industrial partner. The output of the risk management is used as the input of the development process as shown in Figure 3.1

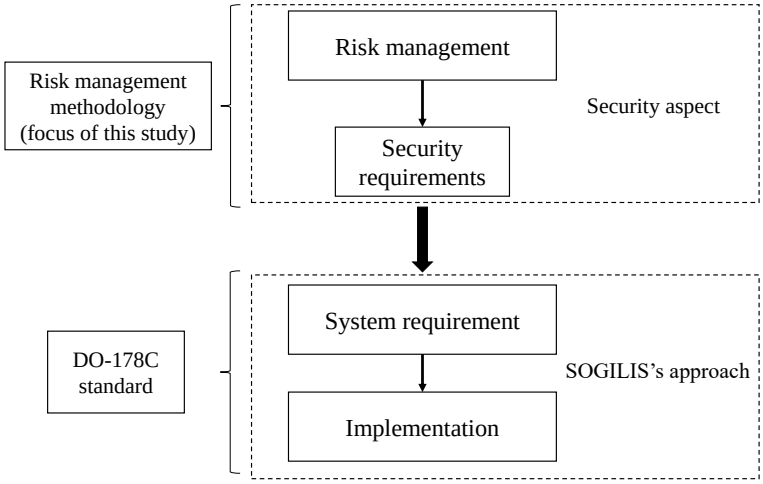


Figure 3.1: General approach

3.2 Proposed methodology

By inspiring risk management methodologies existing in other domains, we developed a simple methodology including four principal activities. They are "Context establishment", "Risk identification", "Risk analysis and evaluation", and "Treatment" as shown in Figure 3.2. In the Context of establishment activity, we propose a method to collect and arrange all the information on the protected system's situation, defining risk management's scope. For the Risk identification activity, we propose a method to identify the possible security risks based on the attack tree method and the malfunction analysis. The Risk analysis and evaluation activity is to define the priority of each defined risk. The risk with the highest priority needs to be treated first with robust solutions. In the last one - Treatment activity, we define the security requirements, which are used to design, verify security solutions. These activities are described in more detail in the remaining of this section.

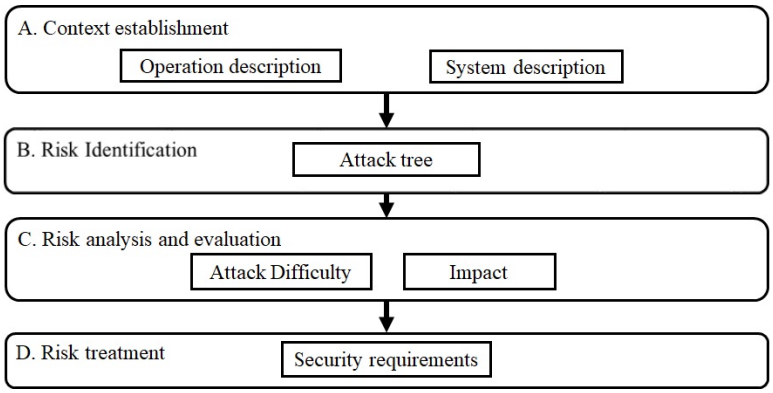


Figure 3.2: Work-flow of the proposed methodology

3.2.1 Context establishment

In this methodology, the context establishment (activity A) aims to prepare for the other risk assessment activities. This activity includes the following steps:

- Operation description
- System under consideration description

3.2.1.1 Operation description

This step aims to describe as detailed as possible the objective and process which the deployed system needs to achieve in the point of view of operators. For this purpose, we utilize the guideline of JARUS-SORA [184] for collecting and presenting operation information as follows:

- Detailed description containing all information to get understanding of how, where, and under which limitations or conditions the drone is deployed.
- Detailed description of the operation type (such as Visual Line Of Sight or Beyond Visual Line Of Sight), operator's involvement, and the system's automation level during the flight.
- Detailed description about the processes of system deployment and maintenance as well as the people involved in these processes
- Detailed description of contingency procedures in place (e.g.when running out of battery, loss of connection).
- Several cyber-security assumptions about the system under consideration, the environment that allows to reduce the scope of analysis and neglect several kinds of attacks, for instance, "all staff are trusted so that all attacks launched intentionally by internal staff are neglected".

Note 1: From this description, we could extract further information such as functions that the system needs to perform (e.g., following a specific trajectory, sending video back to the Ground Control Station - GCS), reference factors used to analyze the severity of impact (e.g., number of deaths in case of the operation that a drone flies over a crowd, financial loss in case of an operation that a drone transports goods).

Note 2: The cyber-security assumptions need to be identified carefully; if not, potential attacks could be neglected.

3.2.1.2 System under consideration description

The purpose of this step is to obtain the necessary knowledge about the protected system. This step focuses on collecting several kinds of information: architecture, cyber-security environment, interfaces, functions.

- **Architecture**: a system could be decomposed into sub systems. They includes basic sub-systems (autopilot, ESC, etc.) and additional sub-systems (camera, payload, etc.)). These elements and their interconnections should be identified.
- **Environment**: all people, external systems that could interact with the system under consideration. For instance, a UAS's environment could consist of maintenance personnel, manufacture, Internet, operators, etc. For each element of the environment, their capabilities of access and roles need to be detailed.
- **Interface**: all entry points that elements of the environment could interact with the system. For example, in the case of a drone, the ground control station sends command data to the drone via RF communication. Therefore the RF communication is an interface of the drone.
- **Functions**: all discrete actions (described by action verbs) necessary to achieve the system's objectives. The information on **system functions** could be deduced from the system operation information presented in the architecture description. For example, the system function could be following a pre-determined trajectory, recording, and transmitting video back to the ground station. In the function description, it should also detail the requirements for this function. For example, for "sending video back to the ground station" function, it should detail the video's intended quality, video data confidentiality, etc.

Each component or sub-systems also has its own architecture, function, interface, environment. Therefore, all the mentioned information should be collected in many abstract levels. For example, besides architecture, interface, function, cyber-security environment of the UAS, we need to know the ones of autopilot, RF module, camera, etc.

Note: Depending on the development process (design, test, documentation) and the status of the system (under development or ready to use), this information could exist (documented)

or not. In case they do not exist, they should be deduced from existing information in a way that ensures information completeness

3.2.2 Risk identification

In the risk identification step, we aim to achieve three objectives. The first objective is to identify as exhaustively as possible risks. The second one is to light the nature of the risks and their evolution (including basic action of attackers, malfunctions in components at different abstract levels, and a malfunction at the system level). The last one is to facilitate security requirement selection. For this purpose, this methodology adopts a new version of the attack tree for this step. The process for building attack trees is shown in Figure 3.3.

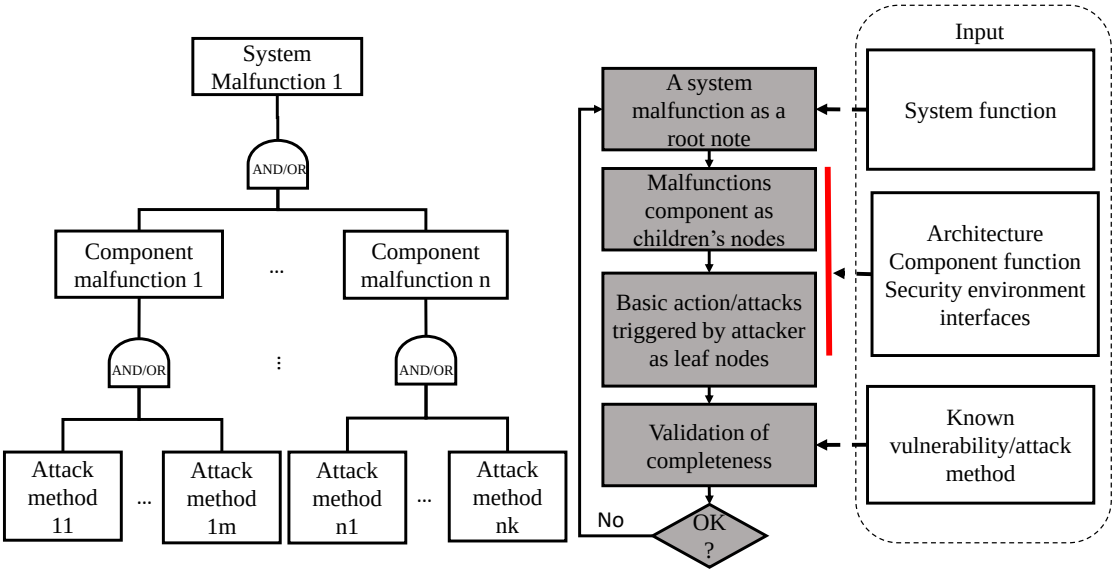


Figure 3.3: Attack tree construction work-flow

Firstly, each attack tree starts with a malfunction of the system at the highest abstract level, as a root node that presents the goal of attack (for example, "drone crashes" or "the video is disclosed"). These malfunctions could be directly deduced from the desired functions of the system identified in the context establishment. Each malfunction is considered as the loss of one of three security attributes (Confidentiality, Integrity, Availability) see Table 3.1.

For example, if a drone flies automatically following a pre-determined trajectory, we could consider "fly and follow a pre-determined trajectory" as a system function. We could determine two related malfunctions of the drone: (1) "crash" (loss of availability) and (2) "divergence from pre-determined trajectory - following the trajectory defined by attackers" (loss of integrity).

Next, malfunctions in components contributing to root malfunction are deduced and expressed as child nodes of the attack tree (e.g., the autopilot provides an incorrect command to the motors). To infer the malfunction of components, we use lists of component functions

Table 3.1: Malfunctions due to loss of security attributes

Security attributes	Malfunction description
Availability	Malfunction presenting the denial of access to the function
Integrity	Malfunction presenting the misuse or the in-correction of the function
Confidentiality	Malfunction presenting the disclosure of information/data

and architectures as inputs.

For example, we consider the "crash of drone" malfunction as a root node. This system malfunction is related to the "fly following a pre-determined trajectory" system function mention in the previous example. This function is achieved based on the cooperation of different components. They are :

- *Autopilot, which estimates flight status and provides motor command*
- *GPS, which provides position data*
- *Inertial measurement unit (IMU), which provides attitude data.*

We determine its possible malfunctions for each component and above using the three cybersecurity attribute keywords (Confidentiality, Integrity, Availability). They could be "GPS provides incorrect position data", "GPS is unable to provide position data", "autopilot is unable to control aircraft", etc. We added these malfunctions to the attack tree as child nodes.

We then repeat this process to identify the components' causes (considered as sub-system) until reaching the lowest level elements (where information is not available for further analysis). Lastly, the attack tree ends with leaf nodes expressing malicious actions or attack methods that could be launched by an attacker for triggering attacks. We could deduce these malicious actions from information about the UAS's environment.

The attack trees give us a visual presentation about the risks related to a system function after being finished. Each path from the leaf node to the root node expresses an attack scenario that attackers could carry out. Each attack scenario is a cyber-security risk which we need to be evaluated in the next steps. Because the process of building attack trees is deductive, the result is more or less influenced by the capacity of the person who performs the analysis. Therefore, at the end, the completeness of the result needs to be verified by checking if all documented attack methods have been identified in the attack trees.

Note: During the deduction process, however, some malfunctions/vulnerabilities are considered as very difficult to occur. They should be kept on the attack tree if the link between them and higher malfunctions/ malicious action is logical. For example, "flashing GPS with

malware via its USB port" is difficult to occur but could happen so that it needs to be shown in the attack tree.

3.2.3 Risk analysis and evaluation

This step aims to determine which attack scenario needs to be considered and which one could be neglected. This step's basic idea is similar to the one in safety analysis, where the level risk is characterized by two factors: the likelihood and the severity of impact. However, the likelihood of an attack is difficult to determine due to the lack of feedback. Instead of likelihood, we evaluate the difficulty of attack (DOA). The DOA expresses the total effort which an attacker needs to carry out a successful attack. The attacks easy to perform but could have a significant impact should be treated first. The attacks that are difficult to perform could have a minor impact and could be neglected or treated with low priority. Table 3.2 shows the mechanics used to decide the risk level of each attack scenario (L, M, H denote representatively Low, Medium and High risk level).

DOA	None	L	M	M	H	H
	Basic	L	L	M	M	H
	Moderate	L	L	L	M	M
	High	L	L	L	L	M
	Very High	L	L	L	L	L
		No Impact	Low	Medium	High	Very High
	Severity of attack					

Table 3.2: Risk level

In this methodology, the difficulty of an attack and its severity is evaluated qualitatively by more than one person. The severity of attack could be reasoned from operation information collected in the context establishment activity. An attack's difficulty could be evaluated based on the nature of necessary equipment (e.g., cheap or expensive, famous or not), the required knowledge of attack techniques and systems to carry out the attack.

We adopt the guidelines proposed in the ED202A/DO326 standard - cybersecurity for the manned aircraft for the difficulty level. In this standard, the difficulty of each scenario is determined based on three criteria: "Preparation Means", "Execution Means" and "Windows of Opportunity". The "Preparation Means" expresses the difficulty in terms of resources, time, and knowledge to prepare the attack (e.g., finding the vulnerability and discovering the target characteristics). The "Execution Mean" represents the required resource, time, and knowledge to execute an attack (e.g., amount of time to break the encryption algorithm). The "Windows of Opportunity" represents the difficulty related to the moment of attack (e.g., it is difficult to mount an attack if possible only during the system reboot). These criteria are evaluated using the scales provided in the ED202A/DO326 standard (see Table 3.3, Table 3.4, and Table 3.5). The sum of the points assigned to these criteria is the total difficulty point of the scenario. This point is then matched with one of 5 difficulty levels (None, Basic, Moderate, High, and

Very High), as shown in Table 3.6.

	Knowledge		
Equipment	None/Public information and no preparation time	Uncontrolled information and no signification preparation time	Insider Knowledge or Significant preparation time
None/Standard[1]	0	2	6
Special COTS[2]	0	2	6
Special[3]	N/A	4	6
Bespoke[4]	N/A	5	6

Table 3.3: Preparation means

Points	Description
0	The attack can be carried out at any time
1	The attack can be carried out during regular cruise flight.
2	The attack vector is available while the aircraft is on the ground.
3	Maximum effectiveness for mandatory operational procedures limiting the window of opportunity.
6	The attack vector is only available in a restricted time phase, e.g. on the ground in maintenance mode
8	The attack can only be carried out during a very restricted time slot independent from the flight phase (e.g. during system reboot).

Table 3.4: Windows of opportunity

	Expertise				
Equipment		Layman	Proficient	Expert	Multi Expert
	None/Standard	0	4	6	10
	Special COTS	4	4	6	10
	Special	N/A	6	8	12
	Bespoke	N/A	N/A	10	12

Table 3.5: Execution means

From 0 to 6	From 7 to 12	From 13 to 18	From 19 to 24	More than 24
None	Basic	Moderate	High	Very High

Table 3.6: Difficulty of Attack scale

[1] No equipment or something commonly already found
[2] Something which can be readily bought, but which is usually not yet in the possession of an average person
[3] Something which cannot be readily bought, but which needs to be assembled/built
[4] Special equipment which requires a bit amount of resources to assemble

3.2.4 Treatment

For each threat scenario selected for treating in the previous step, a set of cyber-security requirements should be established. A cyber-security requirement is not a specific security measure, but it is only a security objective that needs to be fulfilled to ensure the system's cyber-security. For each cyber-security requirement, one or more security measures could be considered. They need to be tested/simulated and evaluated (cost, effectiveness) before being selected for wiring down system requirements.

In this methodology, we adopt the classification of security requirement mentioned in ED202A/DO326A [185] as follows:

- Preventive: The aim is to discourage a malicious user from causing a malfunction
- Deterrent: The aim is to prevent an occurrence of a malfunction
- Detective: The aim is to detect and report a malfunction or malicious action of an attacker.
- Corrective: the aim is to react to a malfunction when it occurs
- Restorative: the aim is to put the system back to the normal status after a malfunction

3.3 Case study

In this section, we present the application of our methodology for a case study: "Drone-based highway observation" - a real application of the SOGILIS company. In this case study, a UAS is used to observe a highway in auto flight mode. The video captured by the UAV and the flight information are sent to the ground and displayed to operators on the screens of Ground Control Station (GCS) computers. During the operation, the UAV will fly and follow a pre-defined trajectory alongside the highway. From the start to the end of the flight, the UAV flies all the time in automatic mode under Beyond Visual Line Of Sight (BVLOS) observation of operators. The operators could use three simple commands: start the flight, end the flight (back to stand-by mode) and go home. The architecture of this UAS is shown in Figure 3.4. To simplify the case study, we suppose that this UAS is developed without any cybersecurity attention. It means that there is no measure in place to protect the UAS before applying our methodology.

From the description of the system operation, we defined three system functions which need to be protected:

- **Function 1: Fly the vehicle following automatically a pre-determined trajectory**: The drone must follow a flight plan predetermined by the manufacturer and embedded in the autopilot. A flight plan contains several way-points. Each way-point contains information on coordinates, altitude about sea level, or ground level.

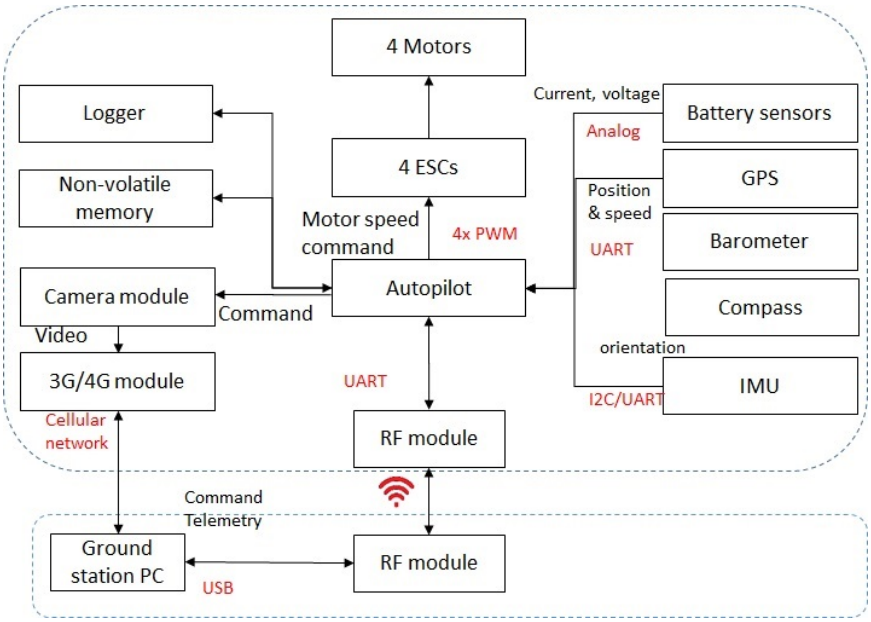


Figure 3.4: Architecture of a UAS.

- **Function 2: Provide flight information to operators**: all status information such as attitude, position, predetermined trajectory, battery information will be sent to the ground and displayed on the screen of the GCS computer. Only operators in charge have the right to access this information.
- **Function 3: Provide observation video to Operators**: the video captured by the camera is sent to the ground and displayed on the GCS computer. Only operators in charge have the right to access this information.

Based on the system functions above, we define malfunctions which the attacker wants to trigger. Each malfunction is related to the loss of one cyber-security attribute (integrity, availability, confidentiality) of a system function. The list of malfunctions is presented as follows:

- **Malfunction 1-Availability** - Crash of the UAV: Due to a malicious action, the UAV losses its attitude and crashes. Because of flying over a highway, the crash of the UAV could cause a lethal accident. Therefore, we assign this malfunction with a **very high level** of severity.
- **Malfunction 1-Integrity** - Deviation from the predefined trajectory: Under an attack, the UAV deviates from its trajectory and flies following the trajectory defined by the attacker. By manipulating the trajectory of the drone, the attacker could hijack the vehicle. In the worst case, the attacker could cause an intentioned lethal accident. Therefore, we assign this malfunction to a **very high level** of severity for this malfunction.
- **Malfunction 1-Confidentiality** - No relevant.

- **Malfunction 2-Availability** - Unavailability of flight information: Under an attack, the flight information is no more available, and the operators could not recognize the situation. This malfunction could help attackers launch other attacks or make the operation be canceled. We assign a **medium level** of severity for this malfunction.
- **Malfunction 2-Integrity** - Fake flight information: Fake flight information: Under an attack, the fake flight information is provided to operators, which makes them make incorrect decisions such as triggering the fail-safe function. We assign a **medium level** of severity for this malfunction
- **Malfunction 2-Confidentiality** - Disclosure of the flight information: Under an attack, the attacker could gain unauthorized access to the flight information, which could help the attacker launch other attacks. we assign a **medium level** of severity for this malfunction
- **Malfunction 3-Availability** - Unavailability of video: Under an attack, the operators could not access to the observation video. We assign a **low level** of severity for this malfunction.
- **Malfunction 3-Integrity** - Fake video: Under an attack, the operators receive the fake observation video made by the attacker. This malfunction does not directly impact the safety of the operation. We assign a **low level** of severity for this malfunction
- **Malfunction 3-Confidentiality** - Disclosure of video: Under an attack, the attacker could gain unauthorized access to observation video, which impacts the observed people's privacy. We assign a **high level** of severity

For each system malfunction, we build an attack tree. For this task, we use the ADTool [186] - an open-source software to draw the attack trees with the related requirements. For example, Figure 3.5 shows the attack tree related to the malfunction 2-integrity. For the next part of this chapter, we focus on analyzing only the malfunction 2-integrity "Fake flight information". Other malfunctions analysis (including attack trees, risk evaluation, requirements) are presented in Annexe C. Through the attack tree shown in Figure 3.5, we could determine five possible attack scenarios as follows:

- Scenario 2-integrity-1: In this scenario, the adversaries attack the UAS by the RF communication channel. If the RF communication channel is not protected well enough, the adversaries could create and send fake messages to the RF module on the ground and deceive the GCS and the pilot with the fault information. Therefore, the RF module shall verify each received package's integrity in terms of time, payload, and origin (requirement 14 - see Annexe C.2) to defend against this attack.
- Scenario 2-integrity-2: This scenario is similar to the first one, in which the RF module receives fake messages. The difference is that the adversaries do not create fake messages but only copy the transmitted messages and resent them afterward. The result of this attack is that the pilot is deceived with the fault information in terms of time. In

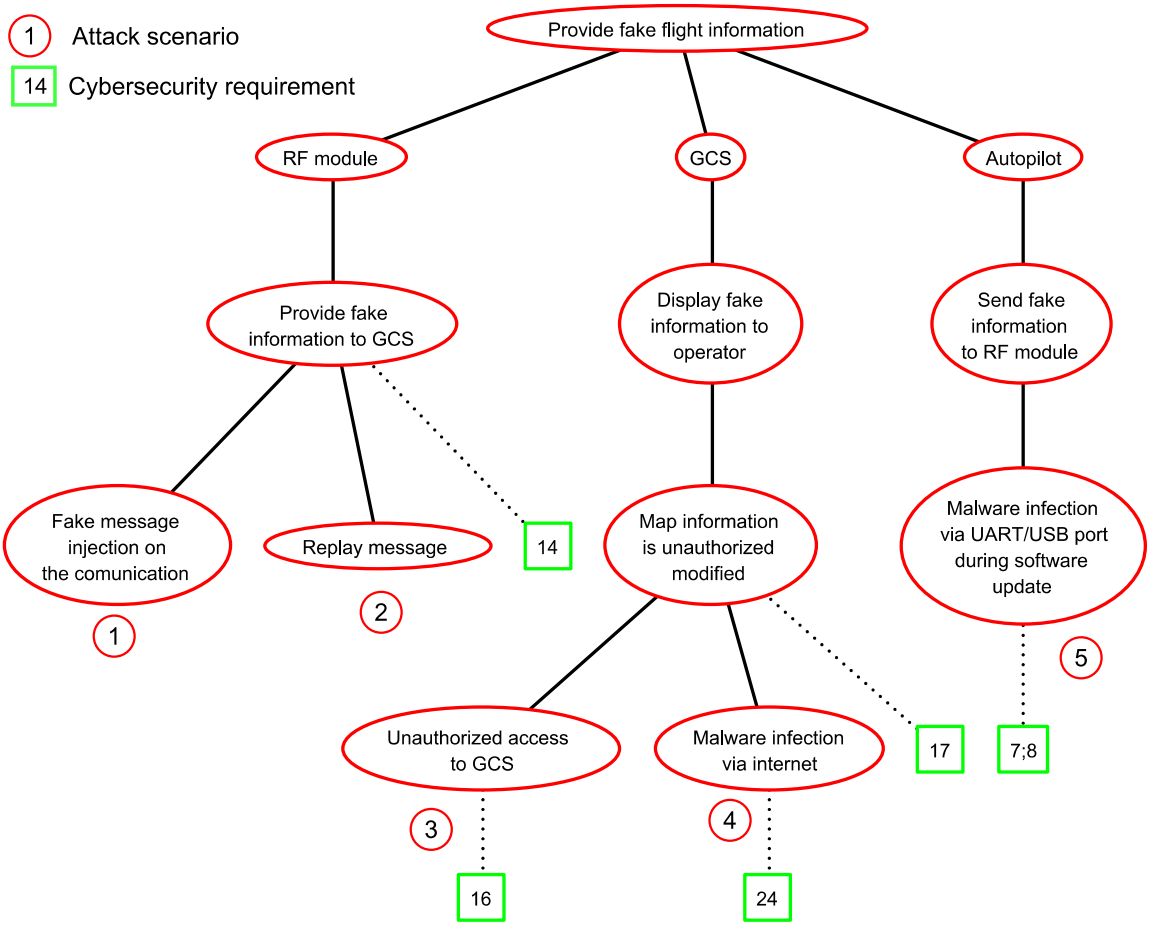


Figure 3.5: The complete attack tree related to the malfunction 2-Integrity

this scenario, the adversaries do not have to know the message's structure or the used encryption scheme if available. To defense against this attack, the RF module shall verify the integrity of each received package in terms of transition time/order (requirement 14 - see Annexe C.2).

- Scenario 2-integrity-3: In this scenario, the adversaries attack the UAS via the GCS. If the adversaries could reach the Ground Control Station (GCS), they could modify the Ground Control station's stored map. With the fault map, the pilot will be deceived with fault information on the vehicle's position. For a successful attack, the attacker does not have to have a high technical knowledge level, but she/he has to have the opportunity to access the GCS (e.g., disgruntled staff). The suitable countermeasure for this attack could be access-control mechanics, which allows the authorized person to access GCS (requirement 16 - see Annexe C.2).

- Scenario 2-integrity-4: In this scenario, the GCS computer is infected with a malware via the Internet, which could modify the stored map information without being detected. To

Scenario	DOA				Severity	Risk Level
	Preparation Means	Windows of Opportunity	Execution Means	Total		
2-integrity-1	2	1	6	9 (Basic)	Medium	Medium
2-integrity-2	2	1	6	9 (Basic)	Medium	Medium
2-integrity-3	6	6	10	22 (High)	Medium	Low
2-integrity-4	6	6	10	22 (High)	Medium	Low
2-integrity-5	6	6	10	22 (High)	Medium	Low

Table 3.7: Risk evaluation for the attack scenario related to the malfunction 2-Integrity

succeed in this attack, the attacker must have good technical knowledge of the malware and the targeted GCS. To defend against this scenario, the data flow between the Internet and GCS needs to be controlled. Only manufacturer-defined kind of data could reach GCS from the Internet or be sent to the Internet by GCS (requirement 24 - see Annexe C.2).

- Scenario 2-integrity-5: In this scenario, the autopilot is supposed to be infected with a malware during the software update. Due to installed malware, the autopilot sends the fake information during the flight to the GCS (via RF module). This scenario requires the attacker to have good knowledge on malware and the targeted autopilot. For this kind of attack, the autopilot should be capable of verifying the firmware's integrity to ensure that it is created by the manufacturer (requirement 7 - see Annexe C.2). Moreover, access control mechanics could be put in place to allow only the manufacturer to modify/update the firmware (requirement 8 - see Annexe C.2).

The risk levels of the above attack scenarios are evaluated as shown in Table 3.7.

3.3.1 Result analysis

Based on the attack tree, we identify 49 possible attack scenarios consisting of 9 high-risk scenarios, 28 medium risk scenarios, and 12 low-risk scenarios. These scenarios concern different components of the UAS. The distribution of attack scenarios to various target components is presented by the diagram shown in Figure 3.6. According to this diagram, the components the most targeted by the attack scenarios are the autopilot (11 scenarios), the ground control station or GCS (10 scenarios), the RF links (7 scenarios), and the 3G/4G links (7 scenarios). This argument is logical because the autopilot, the GCS, and the communication links involve all functionalities of the UAS. At this point, we could wonder if the scenario related to these

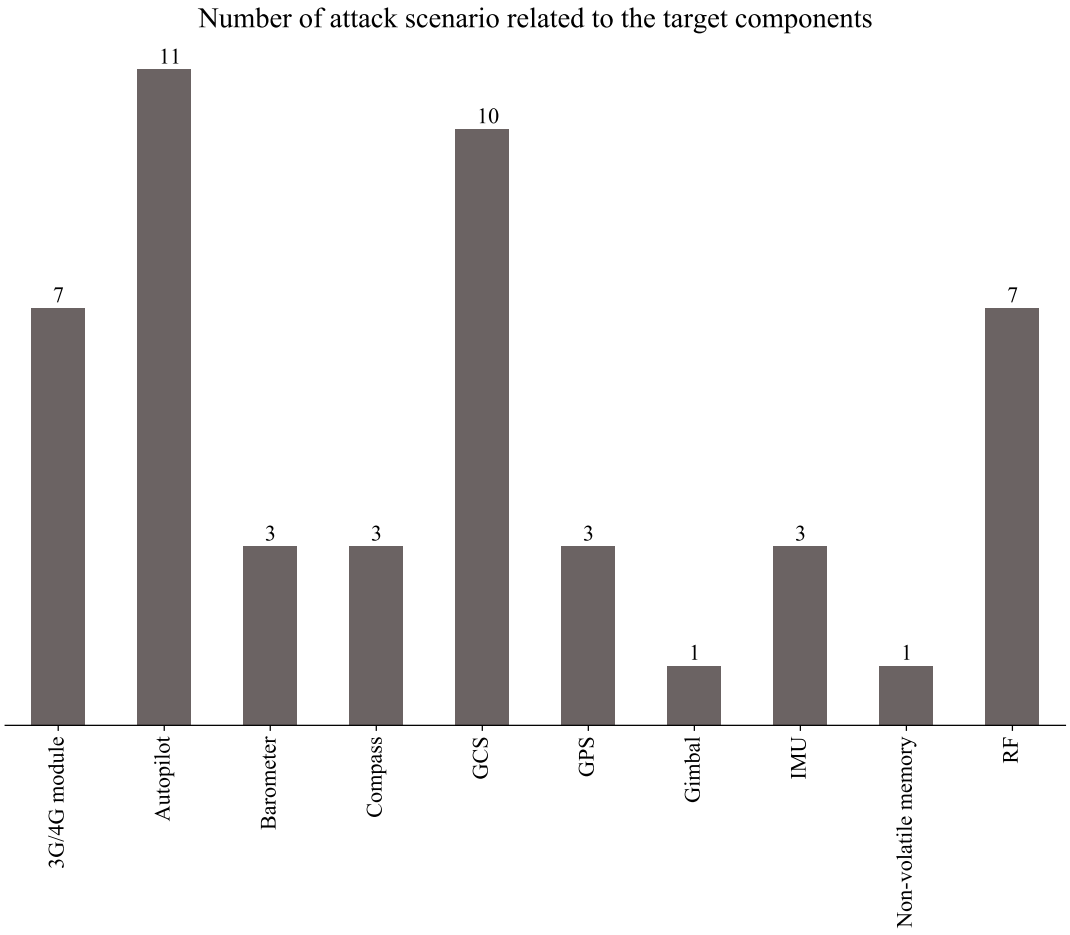
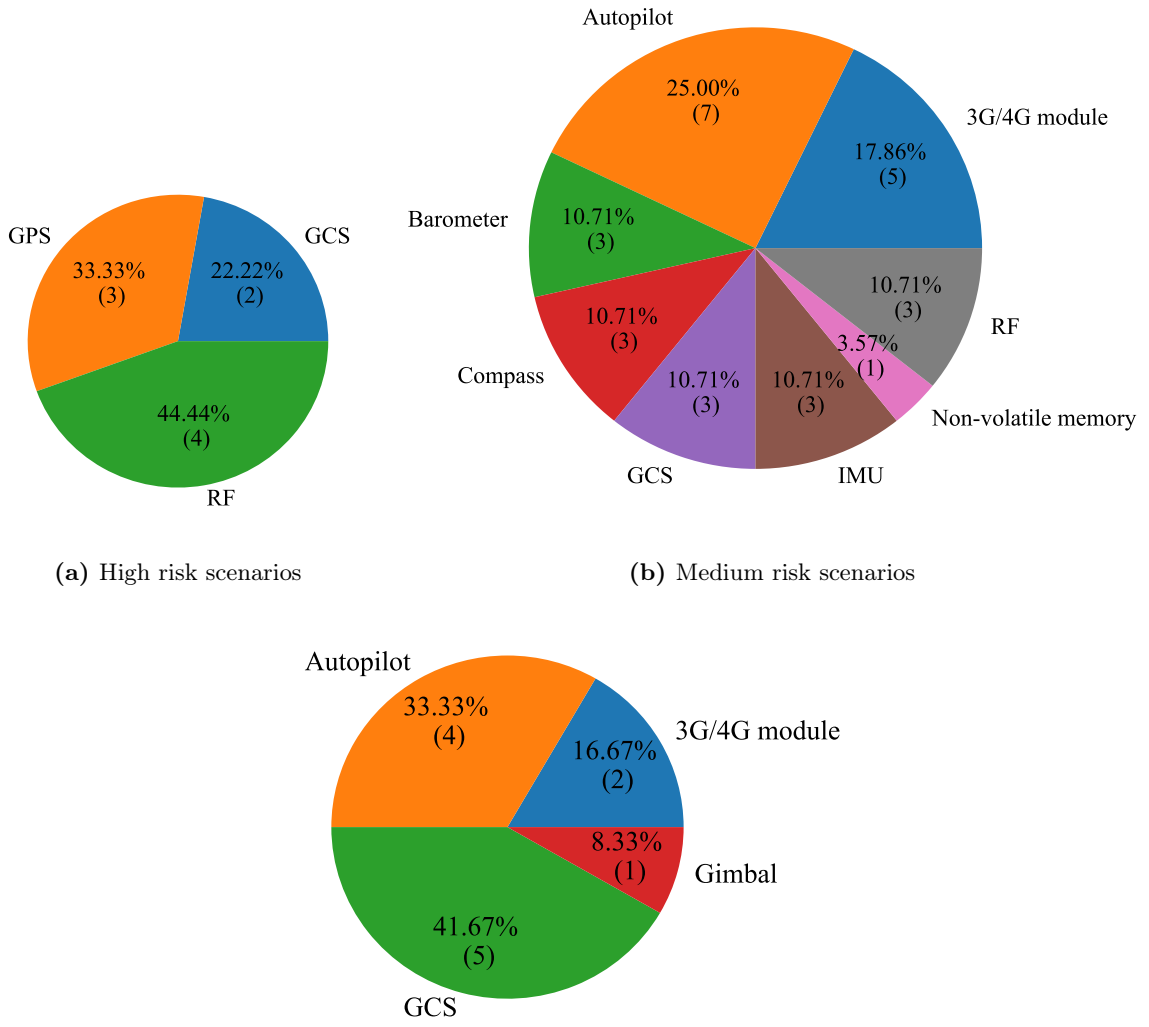


Figure 3.6: The distribution of attack scenarios to different target components

components should be the most considered in the risk treatment step. The answer is "Not sure". According to our methodology in particular and the general spirit of the risk management at large, in the treatment step, the scenario's priority in the treatment step depends on its risk level. The distribution of high-risk scenarios to different components is presented by the diagram shown in Figure 3.7.

As shown in Figure 3.7, the high-risk scenarios relate to only three components: GCS, GPS modules, and RF modules. Both RF modules and the GPS module are based on some kinds of wireless communication. By targeting to the RF module and GPS module, the attacker could launch an attack remotely. Meanwhile, the GCS provides a completed human-machine to control the vehicle easily. It means that the adversary could interfere with the vehicle's flight without much technical knowledge when reaching the GCS. Moreover, all of these components involve the essential function of the UAS: maintain the vehicle flying the predetermined trajectory in safety. For the other critical component - the autopilot, we assign the related risk scenarios to the medium risk level or the low-risk level only. The attacker has not much opportunity to reach the autopilot physically. Furthermore, it requires complex tools and knowledge on the autopilot software/hardware to mount a successful attack. Besides



(a) High risk scenarios

(b) Medium risk scenarios

(c) Low risk scenarios

Figure 3.7: The distribution of risk scenarios to different target components and risk levels

the autopilot, we also assign the risk scenarios involving the sensors (Barometer, compass, IMU) and the payload components (Gimbal, 3G/4G module) to the low or medium levels. We consider the sensor-based attack scenario almost impossible due to the limitation of the effective range of these attacks, as mentioned in Section 1.5. Meanwhile, the Gimbal and the 3G/4G module involve the non-critical functions only (taking and transferring video data). Based on the analysis above, we should first treat the risk related to GCS, GPS, and RF module (such as GPS spoofing, data disclosure, de-authentication). However, this conclusion is suitable only for this intended operation and the architecture, which is developed with the "without Cybersecurity attention" supposition.

3.4 Conclusion

This chapter presents our risk management methodology that addresses the cybersecurity issues of an existing (or designed) UAS. Our methodology consists of four steps: (1) Context establishment, (2) Risk identification, (3) Risk analysis and evaluation, (4) Risk treatment. In the first step - Context establishment, we collect information on the system architecture and the operation, which should be as detailed as possible. In the second step - Risk identification, we identify the possible cybersecurity attack scenarios. The attack scenarios are deduced from the information on the system (functionality, components, environment) collected in the first step. In this step, we use the attack tree diagram to support the reasoning process and visualize the scenarios. In the third step - Risk analysis and evaluation, we evaluate each identified attack scenario's risk level based on the severity of their impacts and their difficulty levels. To estimate the difficulty level, we adopt the scale defined in the DO326 standard. In the last step - Risk treatment, we determine the security requirements to defend against the attack scenarios. These requirements are developed/implemented according to the order of the associated attack's risk level. To illustrate this methodology, we presented a simple case study in which a UAS is used to observe a highway. In the risk identification step, we identified a total of 49 different risk scenarios. These scenarios cover all possible attack methods mentioned in the literature (real attack, test, or simulation). In the risk analysis and evaluation, we assigned 7 scenarios to the high-risk level, 28 scenarios to the medium risk level, and 12 scenarios to the low-risk level. This step depends heavily on the intuitive judgments, although this step is performed based on the classification scales defined in the aeronautic standard DO326A. The robustness of this step could be improved by combining the judgment of different experts. In the last step, we identified 24 cybersecurity requirements to take into account. They are all technical requirements. Some of them require considerable changes of the system architecture. The architecture changes could impact the cost-effectiveness of the development process in terms of time, finance, and workload. Therefore, we argued that it should take into consideration cybersecurity before the architecture was designed. This argument is the fundamental of our work presented in Chapter 4

Chapter 4

Operation risk assessment: From Safety to Cybersecurity

Contents

4.1 Introduction

In the previous section, we introduced a methodology to reinforce the cybersecurity of an existing UAS. This approach could be not cost-effective to the cybersecurity issue due to the cost of system modifications. Therefore, we aim to develop a methodology to consider cybersecurity aspects as soon as possible, at the beginning of the system design. For this purpose, we extend an existing safety methodology - Specific Operations Risk Assessment (SORA) toward cybersecurity. SORA is a well-known assessment methodology in the UAS sector. The methodology focuses on assessing the risks related to the safety of an operation, but cybersecurity is not taken into account. The remaining of this chapter is organized as follows. The concept of the SORA methodology is explained in Section 4.2. An approach to extend the methodology is given in Section 4.3. Two extensions of the SORA methodology are given in Section 4.4 and Section 4.5. A web-based risk assessment tool we developed, remotely accessible, is presented in Section 4.6. We conclude our works in Section 4.7.

4.2 Explanation of the SORA methodology

The Specific Operations Risk Assessment (SORA) is a holistic and operation-centric methodology [187] proposed by a group of experts from the National Aviation Authorities - Joint Authorities for Rulemaking on Unmanned Systems (JARUS) [188], [189]. The methodology is to analyze the UAS operation's safety and to determine the safety objectives which need to be achieved. These objectives refer to many aspects of an operation such as training, system performance, operator organization, system development. This methodology could be useful for different kinds of stakeholders. Operators (who operate the UAS) and the aviation authorities could use this methodology as a means to conform to the EU regulation. Manufacturers (who design and develop UAS) could use the SORA methodology to determine safety features that their designs need to reach for targeted operations under Specific category. This section explains the general concept of the methodology, including two parts: risk model, assessment process.

4.2.1 Risk model

The SORA methodology uses the bow-tie model to illustrate the risk scenarios under consideration. This model was introduced in detail in the first version of the methodology SORA [103] but was not mentioned clearly in the second version [104]. However, the methodology still bases on this model. Therefore, it is necessary to understand the model to understand the fundamental of the methodology. The principal elements of this model include (1) a Hazard, (2) Threats, (3) Harms, and (4) Barriers.

1. The Hazard is the central point of the bow-tie graph. It refers to the situation that an operation is conducted outside of the operator's intention (e.g the aircraft flies outside

of visual observation of the pilot in a Visual Line Of Sight operation).

2. Threats locate on the left of the Hazard and are grouped into different categories. They are the possible causes of the Hazard. Because the SORA methodology considers only the safety aspect, the bow-tie graph illustrates only some unintentional threat categories as shown in Figure 4.1.

3. Harms locate in the right side of the Hazard and represent the possible consequences of Hazard or the final outcome of the scenarios. At this moment, the SORA methodology considers only two kinds of Harms related to person's life: "fatal injuries to third parties on ground", "fatal injuries to third parties in air" (see Figure 4.1). To mitigate the risk scenario, several Barriers (or means of mitigation) could be applied.

4. There are two kinds of Barriers: threat Barriers and harm Barriers. Harm Barriers prevent the occurrence of Harms after a Hazard occurrence. Threat Barriers prevent the Hazard occurrences. For each category of Threats, different threat Barriers will be determined at the end of risk assessment under the form of Operation Safety Objectives (OSO). Each OSO is detailed in three levels of robustness (Low, Medium, High). An example is OSO#4 - "the UAS is developed to authority recognized design standards". At the low robustness level of this OSO, the applicant should only declare the required standards are achieved. Meanwhile, at the high robustness level, the applicant has to provide supporting evidences (such as analysis, simulation), which will be validated by competent third parties. The list of OSOs provided by this methodology is presented in Annex E of this document.

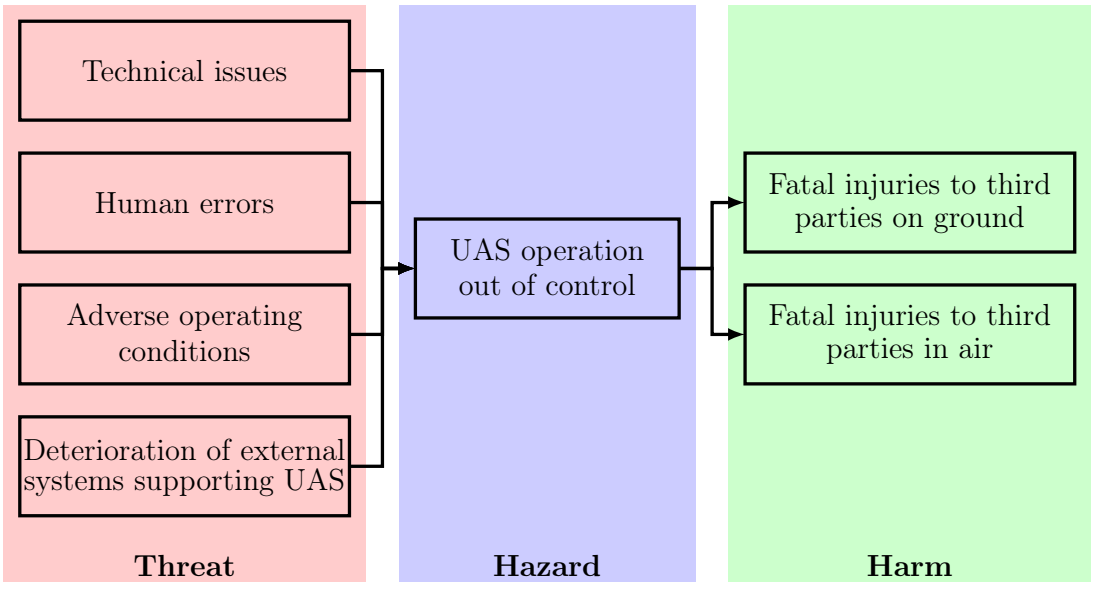


Figure 4.1: Risk model of the SORA methodology represented as a bow-tie graph

In the next part, we explain the assessment process of the SORA methodology based on the above risk model in both quantitative and qualitative approaches.

4.2.2 Assessment process

4.2.2.1 Quantitative approach

Traditionally, risk is defined as a combination of likelihood and severity. However, the risks in the SORA methodology is tied to only likelihood parameters [103] because the methodology basically focuses on only risks of Harms to the person's life. The severity of these Harms could be considered as extremely high. In other words, the safety objectives will be determined to maintain the likelihood of each Harm under the acceptable value (10^{-6} fatal injuries per flight hour, equivalent to a manned aircraft operation[103]). The likelihood of these Harms is decomposed into individual components as shown in Figure 4.2.

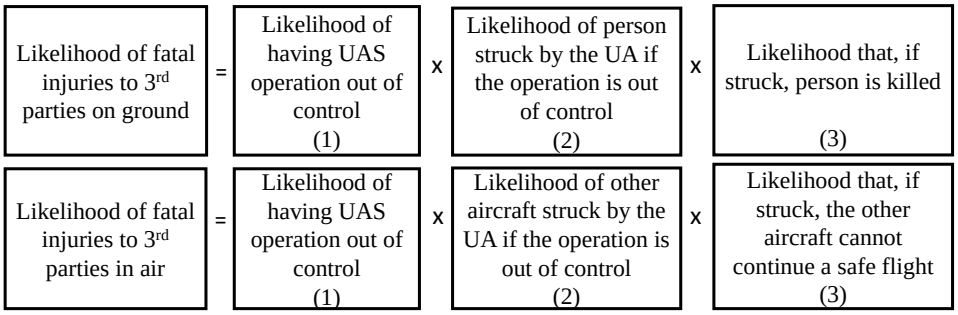


Figure 4.2: Likelihood of fatal injuries on ground and in air according to SORA[103]

The component (1) of each equation, "likelihood of having UAS operation out of control" is mainly affected by Threats and threat Barriers [103]. The combination of component (2) and component (3) in each equation represents the likelihood of the Harms in the case of having UAS operation out of control, which could be evaluated by analyzing the nature of operation under consideration (e.g location, altitude, kind of operation, harm Barriers in place). Under the above assumption, the general concept of this methodology in the quantitative approach could be explained as follows:

- **Objective:** Given a UAS operation, we need to maintain the likelihood of each Harm under an acceptable value: 10^{-6} fatal injuries per flight hour.
- **Firstly**, we collect the information on the intended operation of the UAS such as operation area, operation mode, pilot, weight of UA. This activity is called Concept Of Operations (CONOPS) description. The form of a CONCOPS description is provided in the annex A of the SORA methodology.
- **Secondly**, we estimate the likelihood that the Harms occur in the case of "UAS operation out of control" based on collected information (e.g. 10^{-4} fatal injuries on ground per hazard and 10^{-3} fatal injuries in air per hazard).
- **Thirdly**, from the estimated values above, we calculate an **acceptable** value for the likelihood of having UAS operation out of control (10^{-2} hazard per flight hour from the first equation and 10^{-3} hazard per flight hour from the second one). The more critical

value will be chosen as an objective needs to be reached (e.g 10^{-3} hazard per flight hour).

- **Lastly**, based on the objective value of "likelihood of having UAS operation out of control", the safety objectives with corresponding robustness will be defined.

4.2.2.2 Qualitative approach

The qualitative approach presented above is generally not realistic because of the lack of real data. Therefore, the SORA methodology proposes a qualitative approach based on the main ideas of the quantitative approach as shown in Figure 4.3. The qualitative approach could be explained as follows:

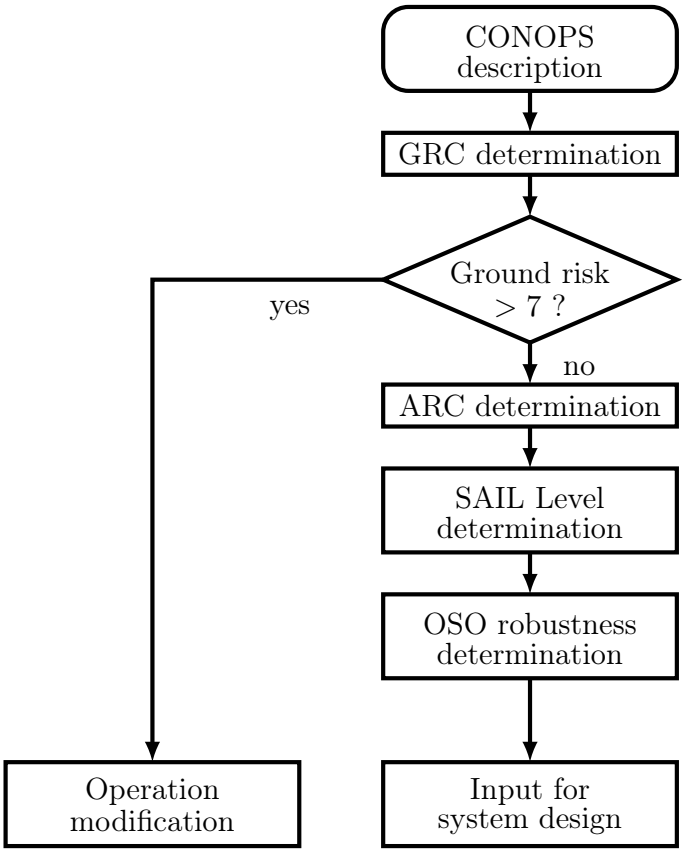


Figure 4.3: Simplified risk assessment process

- **Objective:** Given a UAS operation, we need to maintain the likelihood of each Harm at an acceptable level.

- **Firstly**, we collect the information on the intended operation (CONOPS description)

- **Secondly**, we determine two qualitative factors: Ground Risk Class (GRC) and Air Risk Class (ARC). These factors represent qualitatively the likelihoods that the Harms occur in the case of UAS operation out of control. The GRC and ARC are determined based on the intrinsic characteristics of the operation such as operational area, attitude, weight of the aircraft and the availability of harm Barriers.

- **Thirdly**, we determine two Specific Assurance and Integrity Levels (SAIL) values, which represent the level of confidence that the UAS operation will stay under control. One SAIL value corresponds to GRC and the other corresponds to ARC [103]. The SAIL values range from I to VI. Then, the higher SAIL value will be chosen as the level of confidence or SAIL corresponding to the UAS operation. This value is considered as an objective to drive the required safety objectives. In the most recent version of the SORA methodology, these activities are simplified by using Table 4.1.

SAIL Determination				
	ARC			
GRC	a (**)	b	c	d
≤ 2 (*)	I	II	IV	V
3	II	II	IV	V
4	III	III	IV	V
5	IV	IV	IV	V
6	V	V	V	V
7	VI	VI	VI	VI

Table 4.1: SAIL determination the SORA methodology [104]

Explanation of Table 4.1: The first value-line (*) contains the SAIL values corresponding to the ARC values. They could also be understood as the SAIL values of the operation in which GRC is negligible. The first value-column (**) shows the SAIL values corresponding to GRC. They could also be understood as the SAIL value of the operation in which ARC is negligible. The other SAIL values is the maximum of the SAIL values corresponding to GRC and the ones corresponding to ARC.

- **Lastly**, we chose Operation Safety Objective (OSO) and their robustness level corresponding to the SAIL level of the operation. A list of all possible OSOs is provided in the annex E of SORA [98].

In this section, we explained the original concept of the SORA methodology. It could be resumed as (1) firstly, evaluate the critical level of a UAS operation based on the likelihood of Harms in the case of "UAS operation out of control", (2) then determine threat Barriers corresponding to the critical level of the operation. In the next section, we propose a solution to extend this methodology to cover cybersecurity aspect based on this concept.

4.3 A Solution to extend the SORA methodology toward cybersecurity

Our proposed solution consists of two parts which are called Harm Extension and Threat Extension. Harm Extension extends the risk scenarios under consideration with new Harms; and completes the evaluation of critical level of a given UAS operation. Threat Extension extends the scenarios under consideration with new cyber security Threats; and determines the corresponding threat Barriers for a given UAS operation.

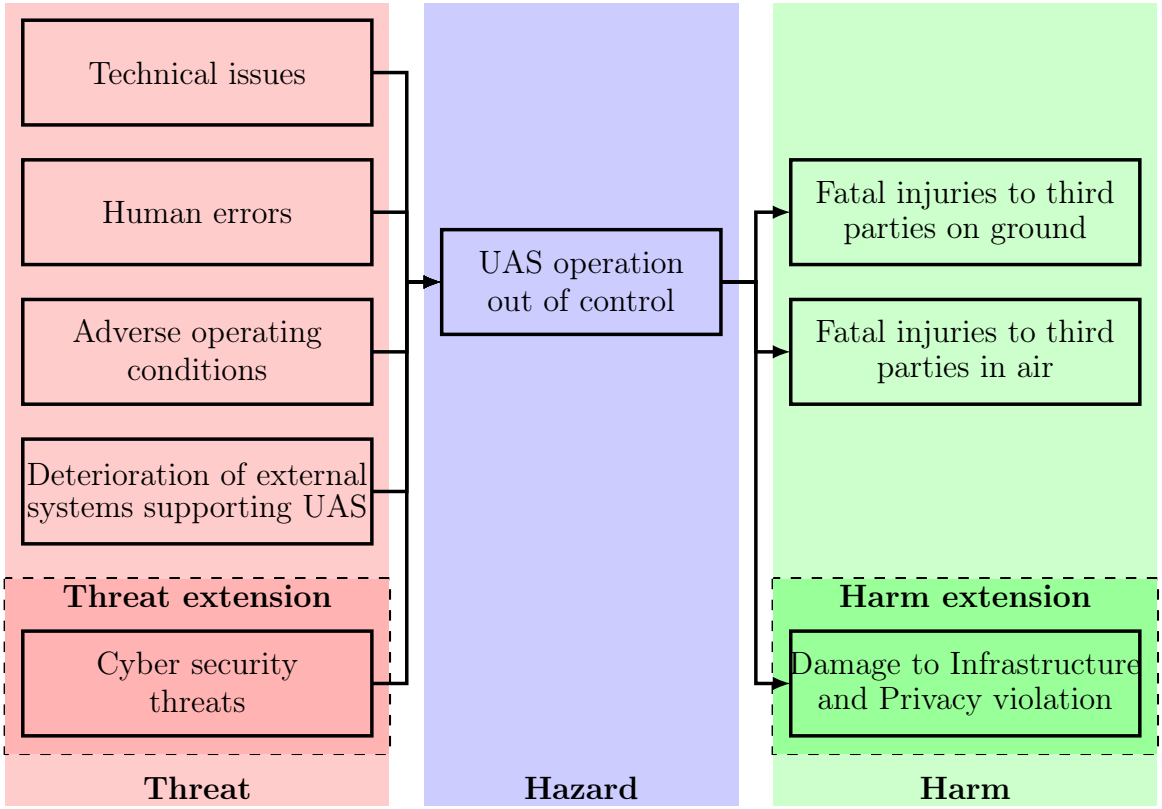


Figure 4.4: Extended risk model

In Harm Extension, we concern the harm-side of the risk model (see Figure 4.4). The original SORA methodology concerns only the Harms to the person's life. However, besides the Harms to the person's life the public concerns also the other Harms [103], [189]–[191] such as:

- **Privacy violation**: A UAS could have a small size, a long operational range and high-performance onboard sensors; so it could intrude itself into private locations and collect information [192]. That violates the privacy of the owner. The privacy violation could be caused by a cyber attack or an error of the system. For example, police-operated UASs may frequently cross private properties on their way to an operational area. Under

a cyber attack, the recorded video on the properties could be disclosed and then the privacy of owners overflown could be violated.

- **Physical damages to infrastructure**: It is supposed that a UA could fall down on critical infrastructures such as highway, electricity power line, nuclear plant due to a cyberattack or an accident. This Harm relates to only some specific operations in which UAs fly near or over critical infrastructures.
- **Digital damages to infrastructure**: It is supposed that a UAS could become a security breach to a critical infrastructure. For example, an attacker takes over control of the UAS and uses it to attack an infrastructure via the connection between the UAS and the infrastructure.

Therefore, these new Harms come to mind as important issues that should be taken into account in the extended methodology. In Harm Extension, our strategy to address the new Harms includes four steps as follows:

1. Chose a new Harm that needs to be addressed
2. Determine factors/characteristics of the UAS operation, which have an impact on the likelihood of the chosen Harm.
3. Establish formulas or tables to evaluate qualitatively the likelihood based on the determined factors
4. Extend "SAIL determination" step to cover the likelihood of the new Harm.

In Threat Extension, we will concern the threat-side of the risk model. The potential cybersecurity Threats need to be identified and grouped in new threat categories. In other words, this calls for a taxonomy of cybersecurity Threats related to a UAS operation. To illustrate the new scenarios, the new threat categories will be added into the threat-side of the risk model as shown in Figure 4.4. Corresponding to each new threat category, a list of possible threat Barriers will be also established. the detailed threat Barriers for a given UAS operation will be chosen from the proposed list in correspondence with the value of the SAIL factor. Our strategy to develop this extension could be described as follows:

1. Based on the literature review, create a taxonomy of cybersecurity Threats. The cybersecurity Threats will be added into the threat side of the SORA risk model.
2. Establish a list of generic threat Barriers for each threat category in the defined taxonomy. Each Barrier will be defined with three levels of robustness (Low, Medium and High) according to the SORA method. This work is also based on the state of the art of cybersecurity countermeasures in "close" domains such as smart vehicles, robotics...
3. Determine the mechanism to choose the robustness of cybersecurity threat Barriers for a given UAS operation.

Harm Extension and Threat Extension could be separately developed and then could be integrated into one complete methodology. The detail of Harm Extension related to privacy is given in Section 4.4, the Threat extension is presented in Section 4.5.

4.4 Harm extension: SORA with the privacy Harm

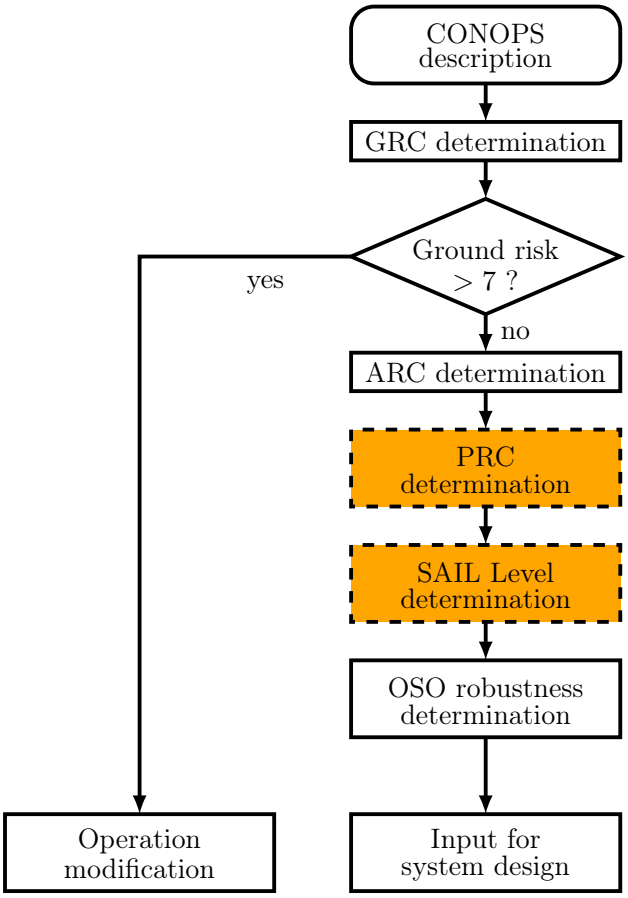


Figure 4.5: New steps for Harm Extension

Nowadays, the privacy violation is one of the most concerned issues for public acceptance of UAS applications [103], [191], [193]. Therefore, we consider it as an important issue and address it firstly in our works. However, the general privacy is a very large term. It is difficult to define precisely [194] and address this term at large, so we focus on only three aspects of this Harm: (1) disclosure of personal information; (2) illegal personal surveillance; and (3) intrusion into a private location. The first aspect is illustrated in the works of Li et al. [195]. The authors experimented a password-stealing attack based on videos captured by a drone. The second aspect is mentioned in [196]–[198]. In these papers, the authors examined how the surveillance UAS application could impact on the privacy of people on the ground. Moreover, Park et al. [197] and Babiceanu et al. [199] proposed criteria for judging privacy violations of a UAS operation based on the quality of captured images/videos. The last aspect was addressed

by Blank et al. [200]. The authors proposed a mechanism to recognize private spaces during creating flight-paths and to make sure that UAs would not fly over these private properties.

For the next, we first analyse the likelihood of the privacy violation to determine the possible factors related to this Harm, which could be used for the assessment (in 4.4.1). Then we propose extensions for the assessment process: (4.4.2) a new step named "Privacy risk class (PRC) determination" to evaluate the likelihood of this Harm in the case of "UAS operation out of control" and (4.4.3) an extension of the "SAIL determination" step (see Figure 4.5).

4.4.1 Likelihood of privacy violation

With the privacy Harm taken into account, the objective of risk assessment is extended to maintain that the likelihood of Harm to privacy is also under a certain acceptable level. Similar to the likelihood of Harms to the person's life, the one of the privacy Harm could be decomposed as shown in Figure 4.6. The combination of the two components (2) and (3) of this equation represents the likelihood that the privacy of third parties is violated after "UAS operation out of control".

For a given operation, the likelihood of a person exposed to the UA (inside the sensing range or under the UA) depends on the nature of the operational zone (urban zone vs. rural zone) and the type of operation (Beyond Light of Sight vs. Visual Light of Sight). In urban zones, the population density and the number of private locations are higher than in rural zones. Therefore, the likelihood of having a person or a private location exposed to a UA in an urban zone could be higher than in a rural zone. In a Beyond Visual Light Of Sight (BVLOS) operation, the operation range of the unmanned aircraft is greater than in a Visual Light Of Sight (VLOS) operation. Therefore, the number of persons under or near a UA in a BVLOS operation could be higher than in a VLOS operation. That's why the likelihood of having a person or a private location exposed to a UA could be higher in a BVLOS operation than in a VLOS operation.

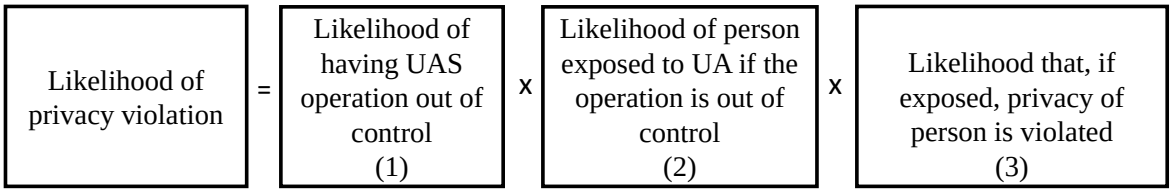


Figure 4.6: Likelihood of privacy violation

For a person exposed to the UA, the likelihood of privacy violation depends on the detail level of images captured by the onboard camera. For example, if the photo taken by the UAS is at a too low resolution, the image of the person is not detailed enough to recognize her/his face so the likelihood of privacy violation could be small. The detail level of the image could be evaluated by the pixel density - the number of pixels in a captured image representing a meter on the ground. To simplify the calculation we assume that the ground is flat. Therefore, for a UAS operation, the highest value of pixel density is reached when the camera direction

is perpendicular to the ground as shown in Figure 4.7. In this case, the pixel density is a function of the height above ground of UA (h), the resolution of the camera and the smallest angle of view of the camera (α) as follows:

$$PD = \frac{\text{number of horizontal pixels}}{2 * h * \tan\frac{\alpha}{2}}(pixels/m)$$

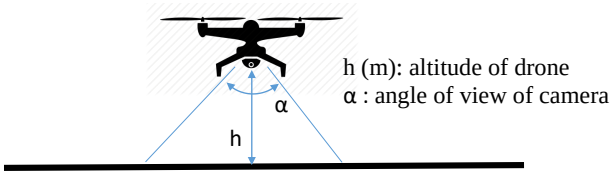


Figure 4.7: Maximum pixel density position

Because of common points related to privacy issue between UAS application and Closed-circuit television (CCTV) application [191], [197], [198], we adopt a classification of image detail levels introduced by the British Security Industry Association (BSIA) for CCTV application as shown in Table 4.2.

Level of quality	**Description**
Monitor (12.5 pixels/m)	Enable to view direction and speed of movement of people, if knowing their presence.
Detect (25 pixels/m)	Enable to determine if a person is present
Observe (62.5 pixels/m)	Enable to characterize some details of an individual
Recognize (125 pixels/m)	Enable to determine whether or not an individual shown is the same as someone they have seen before
Identity (250 pixels/m)	Enable identification of an individual beyond a reasonable doubt.
Inspect (1000 pixels/m)	Enable the identity of an individual

Table 4.2: Image detail classification [201]

Based on this analysis, we define three intrinsic features of a UAS operation to evaluate the likelihood of privacy violation in the case of "UAS operation out of control":

- Density of operational area: urban zone vs. rural zone
- Type of operation: BVLOS vs. VLOS
- Level of detail of the captured image.

Similar to the Harms introduced in the original methodology, the likelihood of privacy Harm could be reduced by applying some harm Barriers. In this extension, we address three types of harm Barriers to mitigate the privacy Harm:

- Privacy protection filters: these algorithms reduce unnecessary information that could violate the privacy of person from the video/image such as Blurring, Pixelization, Masking, Warping [198]
- Restriction on private space: the operator avoids making a flight path across a private space [200]
- Operation-aware announcement to public: the public under observation of a UAS operation should be informed about it.

In the next parts of the paper, we provide the details of the PRC determination step and the SAIL determination step.

4.4.2 Privacy Risk Class determination step

In this step, the likelihood of privacy violation in the case of "UAS operation out of control" is represented qualitatively by the Privacy Risk Class (PRC) value. We determine the operation's PRC based on the intrinsic features of operation and the applied harm Barriers. The intrinsic features under consideration include operation area (rural vs. urban), type of operation (VLOS vs. BVLOS), and image detail level, as mentioned in 4.4.1. The combination of these features expresses the operation's intrinsic PRC, as shown in Table 4.3.

Type of operation	Rural zone, VLOS	Rural zone, BVLOS	Urban zone, VLOS	Urban zone, BVLOS
Image detail level				
Monitor	A	B	C	C
Detect	B	B	C	C
Observe	B	C	D	D
Recognize	C	C	D	D
Identify	C	D	E	E
Inspect	C	D	E	F

Table 4.3: Intrinsic PRC determination

Then the determined intrinsic PRC could be reduced by the harm Barriers: "Privacy protection filters", "Restriction on private space" and "Operation-aware announcement to public". Each harm Barrier corrects the intrinsic PRC with a reduction factor shown in Table 4.4.

Harm Barrier	PRC correction factor	
	No applied	Applied
Privacy protection filters	0	-1
Restriction on private space	0	-1
Operation-aware announcement to public	0	-1

Table 4.4: PRC correction factor of harm Barriers

For example, an unmanned aircraft is equipped with a camera of 1920 x 1080 resolution and 10 degree view angle (α); flies in BVLOS mode and at 150 m above ground. In this operation, the maximum pixel density is 36 pixels/m and it corresponds to the Detect level (see Table 4.2). According to Table 4.3, the intrinsic PRC is at the C level. Upon analysis of the privacy issue, the operator decides to upgrade the onboard camera with a digital filter that makes image of a person blur and unable to be recognized. In this case, the PRC is reduced 1 level from the C level to the B level (see Table 4.4).

4.4.3 New SAIL Determination

In this extension, the SAIL of the UAS operation is the combination of three factors: GRC, ARC, and PRC. To distinguish the new SAIL value with the one determined according to the original methodology, we call the new value 3D-SAIL and the old SAIL value 2D-SAIL. We determine the 3D-SAIL in a similar way that the 2D-SAIL is determined. First, we choose three SAIL values corresponding to the GRC, ARC, and PRC values for a given operation. Currently, we propose the Table 4.5 to determine the SAIL corresponding to a GRC value. The corresponding SAIL value is simply proportional to the PRC value. Then, the 3D-SAIL value of the given operation is the highest value of three determined SAIL values. The 3D-SAIL determination step is described as follows:

PRC	A	B	C	D	E	F
Corresponding SAIL	I	II	III	IV	V	VI

Table 4.5: SAIL values corresponding to PRC values

1. For a given operation, determine the highest value of SAIL values corresponding to the ARC and GRC. This value is 2D-SAIL. We could use the table provided by the original SORA methodology (see 4.1).

2. Determine a SAIL value corresponding to PRC value (see Table 4.5).

3. Choose the higher SAIL value (more critical) between 2D-SAIL value and the one corresponding to PRC as the 3D-SAIL or final SAIL corresponding to the operation (see Table 4.6).

	2D-SAIL					
PRC	I	II	III	IV	V	VI
A	I	II	III	IV	V	VI
B	II	II	III	IV	V	VI
C	III	III	III	IV	V	VI
D	IV	IV	IV	IV	V	VI
E	V	V	V	V	V	VI
F	VI	VI	VI	VI	VI	VI

Table 4.6: 3D-SAIL determination

The 2D-SAIL and 3D-SAIL mentioned above are two different values. The 2D-SAIL is a combination of GRC and ARC without taking into account PRC (privacy Harm). Meanwhile 3D-SAIL takes into account the privacy Harm. But both of them represent the level of confidence that "the UAS operation will stay under control" that needs to be achieved. Therefore, with the same value of 3D-SAIL and 2D-SAIL, the OSO robustness levels determined based on 2D-SAIL and 3D-SAIL are similar.

For example, a UAS operation is assigned level 6 of GRC, level b of ARC and level B of PRC. Based on the ARC factor and the GRC factor, we obtain a value of V for the 2D-SAIL factor (see Table 4.1 - from the original methodology). Then based on the PRC factor and the 2D-SAIL factor, we obtain the same value for 3D-SAIL: level V (see Table 4.6 - from the extended methodology). In this case, the robustness levels of OSO determined by the extended methodology (3D-SAIL) are similar to the ones determined by the original methodology (2D-SAIL). It is why, in Harm Extension, we maintain the step "OSO robustness determination" unchanged. However, we consider that the original list of OSOs are not enough to protect the UAS operation in terms of cybersecurity. Because the original OSOs address only the unintentional Threat (such as development errors, incorrect behaviors of the pilot). Meanwhile, the intentional Threat is ignored (such as cyber-attacks), which could harm privacy and the person's life. This gap is fulfilled by the Threat Extension presented in Section 4.5

4.5 Threat extension: SORA with new cybersecurity Threats

In the previous lecture, we extend the left side of the "bow-tie" risk model of the SORA methodology with the new type of Harm. Next, we extend this model's right side with a new kind of Threat - cybersecurity Threat.

4.5.1 Cybersecurity taxonomy and Risk model extension

Based on the literature review presented in Section 1.5, we propose a taxonomy of cybersecurity Threats consisting of three categories (see Table 4.7). The first one is the "Attack

on Software/Hardware Architecture" category representing all possible attacks that focus on exploiting software and hardware of autopilots and ground control stations (GCS). The second one is "Attack on communication" category that covers all possible Threats targeting on the cybersecurity breach of the communication segment. The third one is "Attack on sensors" category. This category is typical for all cyber-physical systems as the UAS, where the sensors provide the systems with the capacity to sense the physical environment. Nevertheless, the sensors also allow the attacker to deceive the systems with fake data. Because our taxonomy is built on a literature review, the proposed categories could cover only the Cybersecurity Threats that have been proved in real life or simulation. This taxonomy could be extended in the future for uncovered Threats.

Description	**Categories**
Unauthorized modification waypoints loaded into the Autopilot [61]	Attack on software
Virus on GCS [2]	
Unauthorized modification of source code [152]	
Unauthorized access to the software [152]	
Video replay attack [3]	Attack on communication
De-authentication attack on communication [4]	
Take the UAV over control by interfering the communication [57]	
Video data disclosure [202]	
GPS jamming-spoofing [49], [50]	Attack on sensors
Camera-spoofing [203]	
IMU spoofing [51]–[53]	

Table 4.7: Categories of Cybersecurity Threats

With the proposed taxonomy, we extend the SORA risk model's threat side with the cybersecurity threat categories, as shown in Figure 3.8. Similar to the classic SORA methodology's idea, the "Operation Out of Control" hazard caused by cybersecurity Threats could be prevented or mitigated by threat Barriers. We call these Barriers as Operation CyberSecurity Objectives (OCSO), equivalent to Operation Safety Objectives (OSO) of the original methodology. Based on the guideline of the MEHARI methodology and a list of fundamental security services of the IEC62443, we proposed a list of OCSOs for three new cybersecurity categories (see Appendix A). This list consists of 13 OCSOs. The OCSOs from number 1 to number 7 provide the objectives of protecting the software (including stored data, source code, access authorization). The OCSOs from number 8 to number 12 provide the objectives of protecting data's availability, integrity and confidentiality within the communication channels. The last OCSO - number 13 refers to the protection related to the data provided by sensors. Similar to OSOs of the original methodology, each OCSO is defined in detail with three robustness levels (Low, Medium and High). For each operation, the OCSO's robustness level is determined based on (1) the required level of confidence that the UAS operation will stay under control (or SAIL) and (2) the operation's susceptibility to the cybersecurity attack. For example, the high robustness OCSOs are required for an operation having to always stay

under control (high SAIL) and being very susceptible to cybersecurity attacks. We characterize the operation susceptibility by a new factor: Operation Cybersecurity Susceptibility Level (OCSL).

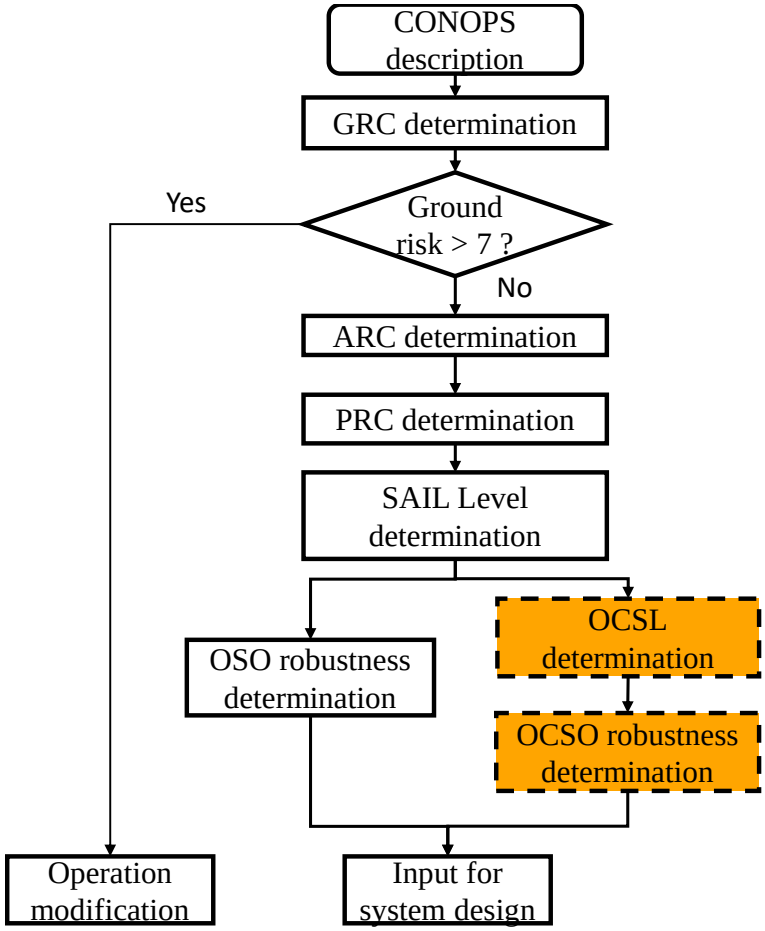


Figure 4.8: New steps for Harm Extension

To adapt to the extended risk model, we propose two new steps in the risk assessment process: **OCSL determination** and **OCSO robustness determination** (see Figure 4.8). For the next, we discuss these steps in detail.

4.5.2 OCSL determination

The susceptibility of a given operation to cybersecurity attacks depends on the intrinsic characteristics of the operation. The first characteristic is the nature of the communication solution used for the UAS operation. The more communication channels are isolated, the less the attacker can reach the UAS (for discovering, exploiting vulnerabilities). Hence, the operation is less susceptible to cyberattacks. For example, an operation using a private/dedicated/military communication solution is less reachable than using a communication solution using the Internet. However, at this point, it should be clear that we do not refer to "isolation" as a

protection solution against cybersecurity attack, but only a characteristic of a UAS operation. The second operation's characteristic under consideration is the type of operation (VLOS vs. BVLOS). In the BVLOS operation, the vehicle operates from a considerable distance and beyond the pilot's visual observation. Hence the attacker could have more chance to mount an attack without being detected, and the anomaly behavior of the vehicle could be hidden (e.g., in case of GPS spoofing). Meanwhile, in the VLOS operation, the vehicle's anomaly behavior due to a cybersecurity attack could be detected visually. Therefore, we consider BVLOS operations more susceptible to cyber attack than VLOS operations. The third characteristic that we take into account is the pilot's monitoring during the operation. The attacker could have less chance to mount a successful attack against a UAV flying under the continuous monitoring of the pilot than the one flying without the continuous monitoring. The last operation's characteristic is related to third-party services/devices. To realize operations, the operator of the UAS could use the services (e.g., maintenance, pilot, navigation,...) or the supplemental device (camera, computers, communication module) provided by third parties. The third-party services/devices not certified by the UAS constructor (or the manufacturer) could have unknown vulnerabilities or back-doors. The attack could exploit/use these vulnerabilities/back-doors to mount a cyberattack against the operation. For example, the maintenance staff of a third-party company could legally reach the UAS and illegally modify the parameter of the UAS. This characteristic will be more important when the full U-space concept will be available (see 1.4). At that moment, many tasks and equipment related to an operation will be provided by third-party providers.

In the OCSL determination step, we evaluate the operation susceptibility by analyzing the four mentioned characteristics: Communication, Type of operation, Monitoring level, and Third-party (reliability). We assign the points for each characteristic by using Table 4.8. The OCSL for the operation is the sum of the points.

For example, a company using a UAS to observe a highway. In this operation, the vehicle will fly automatically under the pilot's continuous monitoring from a ground station located far from the highway. To maintain the long-distance communication between the vehicle and the ground control station, the UAS uses the Internet (via 3G/4G mobile network) as the primary communication solution. The company uses a completed UAS provided by a professional drone constructor (including all materials and maintenance service). According to Table 4.8, this operation is evaluated as follows:

- Communication: because the operation use the internet for maintaining the communication, we assign 2 to this characteristic.
- Type of operation: Because of BVLOS, we assign 1 for this characteristic.
- Monitoring level: Since the pilot continuously monitors the operation, we assign 0 for this characteristic.
- Third-party reliability: the operation does not use any third-party service/device, therefore 0 is assigned for this characteristic.
- Finally, the Operation Cybersecurity Susceptibility Level or **OCSL** is 3.

Communication	Type of operation	Monitoring level	Third-party (*)
- 2 points Using a public network E.g. Internet.	- 1 point BVLOS	- 1 point If not continuous monitoring	- 2 points If non-trusted third party service/device is used for the UAS operation
- 1 point Using a shared network E.g. the internal network of a company which is used for other activities	- 0 point VLOS	- 0 point If continuous monitoring	- 1 point If only trusted third party services/devices are used for the UAS operation
- 0 point Using a dedicated network			- 0 point If no third party service/device is used
(*): A trusted third party is the one verified/trained or certificated by the UAS manufacturers			

Table 4.8: Operation's characteristics related to CS

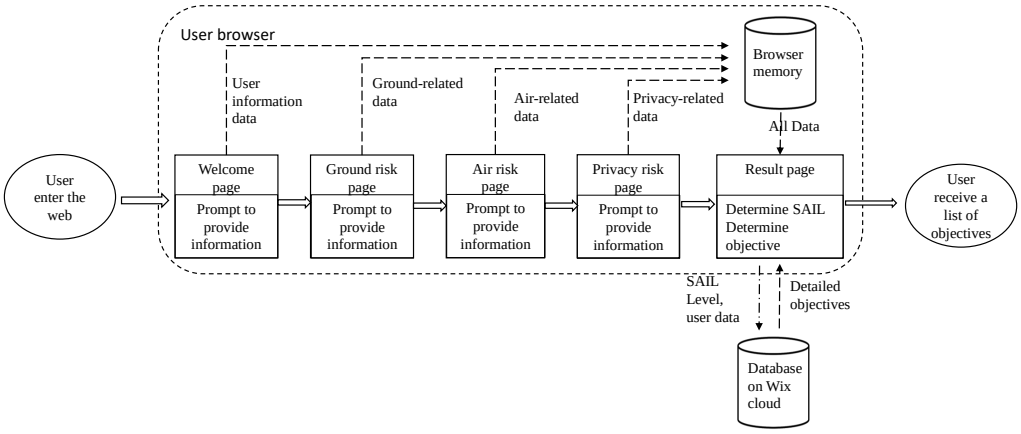


Figure 4.9: Overview of the application

4.5.3 OCSO robustness determination

The necessary robustness level of the Operation Cybersecurity Objective (OCSO) is determined from the operation's SAIL and OCSL by using Table 4.9. With the obtained OCSL, we could determine the detailed cybersecurity objectives by consulting the list of OCSOs in Appendix A.

OCSL	6	Medium	Medium	High	High	High	High
	5	Medium	Medium	Medium	High	High	High
	4	Medium	Medium	Medium	Medium	High	High
	3	Low	Medium	Medium	Medium	Medium	High
	2	Low	Low	Medium	Medium	Medium	Medium
	1	Low	Low	Low	Medium	Medium	Medium
		I	II	III	IV	V	VI
		SAIL					

Table 4.9: OCSO determination

4.6 An Extended-SORA Web-based tool for Risk assessment

4.6.1 Description and purpose

This tool helps users conduct automatically risk assessments based on the SORA methodology and its extension. The users are first prompted to provide input information on the extended operations. Based on this information, our tool then automatically determines the SAIL level corresponding to such operations and the associate safety objectives. This tool is developed for different kinds of users with different purposes: (1) Operator could determine rapidly the objectives related to the intended operation; (2) Operator could configure the intended

operation and balance the operational performance with the cost for satisfying the objectives; (3) UAS manufacturers/constructors could anticipate rapidly the objectives related to specific operations of their clients; (4) Authority could also use this tool to verify rapidly operations for which an authorization is asked. Moreover, this tool is developed so that it is easy to extend the tool for the new extensions of the SORA methodology in the future, such as taking into consideration new Harms and new Threats.

4.6.2 Design and implementation

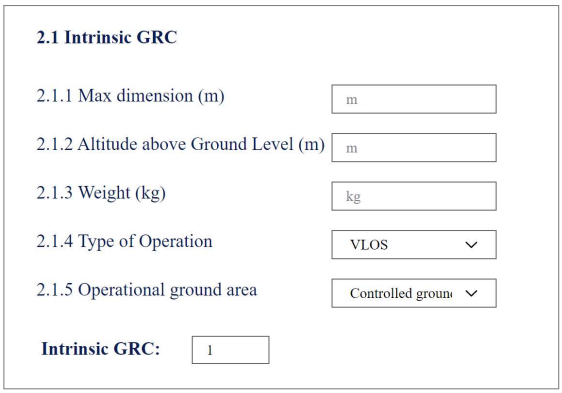


Figure 4.10: Some required information

The tool is a web application developed based on the Wix platform. This platform provides the necessary tools/services to create a website quickly, and it supports the Java-script language to create customized functions. The structure of the application is shown in Figure 4.9. Our website consists of five pages that the user will go through one to another during the risk assessment. In the first page, the user is prompted to provide the general user information (name, contact, role, purpose). On the second page, the user must provide information related to ground risks such as the size of the aircraft, operation area, and mitigation measures (a part of the page is shown in Figure 4.10). For some "yes/no" options, the user could explain how such options are satisfied. Such explanations will be used to create a final report at the end of the risk assessment. Similarly, the third and fourth pages prompt the user to provide information related to air risk and privacy risk. All provided information on each page is stored on the memory of the user browser. Based on such information, the last page runs the risk assessment. Firstly, the page determines the SAIL level. This page lets the user choose which kinds of risk are taken into consideration to determine the SAIL level (see Figure 4.11), for example, ground risk and air risk (original SORA) or all kinds of risk (extended SORA). Then the page sends a request to the database on the Wix cloud to get the detailed objectives associated with the determined SAIL level. Moreover, all the user-provided information is also sent to and stored on our database on the wix cloud. Finally, all required objectives corresponding to the intended operation are displayed to the user. The manual of this application is available in Appendix B.

With the current design, our tool could be easily extended to adopt other SORA method-

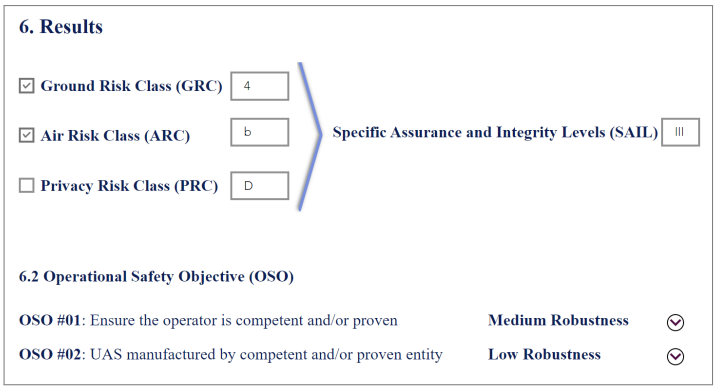


Figure 4.11: Result page with 2D-SAIL

ology extensions. For a new Harm extension, we need only to add a new page to prompt the user to provide information related to this kind of Harm and modify a little bit the result page. Meanwhile, we need only to add a new page to prompt the user to provide information related to this kind of Threats and add new objectives into the database for a new threat extension.

4.7 Conclusion

In this work, we aim to extend the original SORA methodology toward cybersecurity aspects. The SORA methodology's current document explains only how to use it but does not explain how it works. Therefore, we describe the methodology's concept based on available documents and our knowledge about the risk assessment. Then based on this concept, we propose an approach to extend the methodology. The approach consists of two parts. The first one (Harm extension) is to take into consideration new Harms that could result from cybersecurity/safety problems. Currently, we focus on the "privacy violation" Harm - an essential concern for the public acceptance of UAS operations. But we could also extend the SORA methodology for other kinds of Harms with the same strategy, such as finance Harm, material destruction, critical installations, etc. The second part (Threat extension) is to take into account the cybersecurity Threats (or attacks) (versus the unintended Threat covered by the original methodology) and also the relevant cybersecurity mitigation. After that, we proposed a risk assessment tool in the form of a web-based application. This tool is designed to simplify the risk assessment tasks and quickly adapt to the other proposed SORA extensions. In the next chapter of this dissertation, we illustrate our methodology with different case-studies.

Chapter 5

Illustrations of the extended SORA methodology

Contents

5.1 Introduction

In the previous chapter, we introduced an extended version of the SORA methodology that considers cybersecurity aspects. In this chapter, we use this methodology to assess different operations. Based on the risk assessment result, we discuss different aspects of our methodology and propose some improvements. Moreover, the SORA methodology was first designed as a communication tool between the operator and the authorities in administrative processes. It means that the primary purpose of using the SORA methodology is to verify if a defined UAS operation and system could be approved or not. But it could also be used for the development purpose. This chapter illustrates the position of the extended SORA methodology within the UAS development process. The remainder of this chapter is organized as follows. Firstly, we apply our methodology for a real operation assessed with the original methodology in the literature in Section 5.2. Then, we consider two other operations concerned by the market in Section 5.3. Next, we illustrate our approach to use the assessment result obtained from the extended SORA within the development process in Section 5.4. We conclude our works in Section 5.5

5.2 Comparison of our methodology with the one used in the project MULTIDRONE

In this section, we conduct a risk assessment for a UAS operation introduced within an EU-funded project - MULTIDRONE. In this operation, a UAS is deployed to film a boat-race event in rural areas with some public. A risk assessment for this operation was introduced in the work of Capitán et al. [204]. In that work, the authors conducted a risk assessment by using the original SORA methodology. In this case study, we conduct a risk assessment with our extended SORA methodology. We will compare the results at the end of the case study.

5.2.1 CONOPS description

A full description of the operation is very long (as mentioned in Annex A of the SORA methodology). Therefore, we only give a summarized description with some necessary information to conduct the risk assessment in this step. More detailed information could be found in [204], [205].

In this operation, the drone will fly following the boats to take photo-shots. Because the operation is conducted in a large area (with a race path of 15 km), the drone will fly Beyond Visual Light of Sight (BVLOS) of pilots and at the autonomous mode. The operation is taken place in the rural area with a low popular density. It is supposed that there could be many audiences on both sides of the river, and the drones will not fly over them. Table 5.1 summaries the essential information on the intended operation.

Main UAS and operation specification	
Frame	DJI S1000+
Autopilot	Pixhawk 2.1
Communication	Thales LTE/Wi-Fi Communication Module
Parachute	Galaxy GRS 10/350
Camera	BMMC + Panasonic Lumix G X Vario Lens
Size	1,45 m
Weight	11 kg
Altitude	10 m
Flight mode	Autonomous
Operation Type	BVLOS

Table 5.1: UAS and operation specifications (from the MULTIDRONE project)

5.2.2 GRC determination

We first determine the intrinsic GRC of the operation, which refers to the intrinsic risk to the people on the ground without considering safety measures. Because the drone flies in a rural area and does not fly over audiences, we classify the ground operation area as a Sparsely populated environment. With the information on the operation area and the size of the vehicle (less than 3 m), we assigned 4 for the intrinsic GRC as shown in Table 5.2.

Intrinsic Ground Risk Class				
Max vehicle dimension	1 m	3 m	8 m	>8 m
Operation scenario				
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS in sparsely populated environment	2	3	4	5
BVLOS in sparsely populated environment	3	4	5	6
VLOS in populated environment	4	5	6	8
BVLOS in populated environment	5	6	8	10
VLOS over gathering of people	7	No available		
BVLOS over gathering of people	9			

Table 5.2: Intrinsic GRC table from the SORA methodology

Then, we study the harm Barriers of the operation, including Emergency Response Plan, Strategic Mitigations, and Reducing the ground impact. The intended operation does not implement any Emergency Response Plan and does not mention any Strategic Mitigations for ground risk. That lead to an increase in the GRC (see Table 5.3). The operator only applied a parachute as a harm Barrier to reduce the ground impact. We suppose that the manufacturer tested this parachute, and the parachute does not affect the operation's safety in case of adverse activation. Therefore, this harm Barrier is at the Medium robustness level and helps decrease the GRC (see Table 5.3). The final GRC of the operation remains at 4.

	Robustness		
Harm Barriers	Low/None	Medium	High
Strategic mitigation for ground risk	0	-2	-4
Reducing the effect of ground impact	0	-1	-2
Emergency Response Plan	1	0	-1
Total corection	**0**		

Table 5.3: Mitigations for Final GRC determination

5.2.3 ARC determination

Because the aircraft flies at the altitude of 10 m above the ground level, in the rural area and uncontrolled airspace, the risk of collision with other aircraft is low. Therefore, the intended operation has an initial ARC of b with a generalized flight density of 1 (on a scale of 5 levels [104]). To reduce the operation's air risk, the operator implements *mitigation by boundary* as a harm Barrier to restrict operational volume. However, in this case, according to the SORA methodology, the harm Barrier is not useful because the initial probability of collision is too low to reduce. For this reason, the final ARC remains at b level.

5.2.4 PRC determination

As mentioned in our proposal, we analyze some features of the UAS and the operation to determine the Privacy Risk Class (PRC). Most of the input data for this step have been provided in Table 5.1, except the data/information on the camera's smallest Angle of View (AOV). The operation description does not provide information on AOV, but we could calculate it manually based on the camera specification. The camera specification is shown in Table 5.4.

BMMC camera with Panasonic Lumix G X Vario Lens	
Resolution	2432 x 1366
Sensor size	16.64 mm x 14.04 mm
Focal length	from 14 to 42 mm

Table 5.4: Camera specification (from the MULTIDRONE project)

The minimum AOV of the camera is calculated as follow:

$$minAOV = 2 * \arctan \frac{\text{sensor width}}{2 * \text{max focal length}} = 11.2^{\circ}$$

Then, we have the maximum pixel density of image captured by the UAV as follows:

$$PD = \frac{\text{number of horizontal pixels}}{2 * h * \tan \frac{\alpha}{2}} = 1240(pixels/m)$$

So the image detail is at the "Inspect" level (see Table 4.2). Additionally, the UA flies in BVLOS mode and over a rural zone. Therefore, we assign the intrinsic PRC of D for this operation (see Table 5.5)

Type of operation	Rural zone, VLOS	Rural zone, BVLOS	Urban zone, VLOS	Urban zone, BVLOS
Image detail level				
Monitor	A	B	C	C
Detect	B	B	C	C
Observe	B	C	D	D
Recognize	C	C	D	D
Identify	C	D	E	E
Inspect	C	D	E	F

Table 5.5: Intrinsic PRC determination

The final PRC of the operation is the initial PRC subtracting the risk reduction provided by harm Barriers. However, the operation description does not mention any harm Barrier for the loss of privacy of people on the ground. Therefore, we suppose that the operator does not apply any harm Barriers, and the final PRC is still D.

5.2.5 SAIL determination

The operation is assigned to an ARC of b and a GRC of 4. Therefore the value of the 2D-SAIL (taking into account ARC and GRC) is III (see Table 5.6). With the 2D-SAIL of III and the PRC of D, the value of 3D-SAIL (taking account of ARC, GRC, PRC) is IV (see Table 5.7).

SAIL Determination				
	ARC			
GRC	a	b	c	d
≤ 2	I	II	IV	V
3	II	II	IV	V
4	III	III	IV	V
5	IV	IV	IV	V
6	V	V	V	V
7	VI	VI	VI	VI

Table 5.6: SAIL determination [104]

	2D-SAIL					
PRC	I	II	III	IV	V	VI
A	I	II	III	IV	V	VI
B	II	II	III	IV	V	VI
C	III	III	III	IV	V	VI
D	IV	IV	IV	IV	V	VI
E	V	V	V	V	V	VI
F	VI	VI	VI	VI	VI	VI

Table 5.7: 3D-SAIL determination

5.2.6 OSO robustness determination

With the final SAIL value (3D-SAIL) of IV, we could determine each OSO's robustness level and then the detailed objectives that need to be achieved. The detail objectives are shown in Annex E. Because the SORA methodology is designed to support an application for authorization to operate a UAS, some objectives relate to the operators rather than the manufacturer (such as evaluating weather conditions and operator competence). Therefore, in this case study, from the point of view of the manufacturer, we address some critical OSOs that could be considered inputs of a development process of a UAS for the intended operation:

- OSO#04 at a **Low level** of robustness. It requires that the UAS has to be developed to standards considered adequate by the competent authority. The standards should be applied with Low level of integrity (defined with these standards). The manufacturer does not have to provide supporting evidence and needs only to declare standard compliance. Nevertheless, nowadays, there are not any standards dedicated to UAS development. Alternatively, the manufacturer could apply some safety standards widely accepted in the aeronautic domain, such as DO178C, DO256. The manufacturer has to also take into account standards related to privacy and data protection.

- OSO#06 at **Medium level** of robustness. It requires that the characteristics of the communication link are appropriate for the operation. Because the unmanned aircraft flies in uncontrolled airspace and the pilot does not have to maintain the communication with the Air Control Traffic (ATC), the communication link is only to control the vehicle. The UAS could use an unlicensed band for communication such as 2.4 GhZ. However, the UAS needs to provide the pilot with means to monitor the communication link (such as signal strength, drop packet rate). Related to privacy issues, the communication link has to be capable of protecting the confidentiality of exchanged data. These protection features of UA have to be validated by competent third parties.

- OSO#18 at **Medium level** of robustness. It requires that the UAS is able to detect and prevent the incorrect pilot input that makes the UA excess its flight performance (e.g., the pilot let the UA go down too quickly). The automatic protection of the flight envelope has been developed to standards considered adequate by the competent authority.

5.2.7 OCSL determination

In this step, we analyze four characteristics: Communication, Type of operation, Monitoring level, and Third-party. For the communication, the UAS is equipped with a Thales LTE/wifi communication module. We do not have any technical information on this communication module. We suppose that it is a dedicated and high-quality for the UAS. In this operation, the vehicle flies at BVLOS mode and under the pilot's continuously monitoring. The considered UAS is built based on some open-source components (such as autopilot), which we consider a non-trusted third party device. Base on this analysis, we assign OCSL of 3 for this operation (see Table 5.8).

Characteristic	Description	Points
Communication	Dedicated solution	0
Type of Operation	BVLOS	1
Monitoring level	Continuously monitored by pilots	0
Third party	Non trusted devices	2
OCSL		**3**

Table 5.8: Result of OCSL determination

5.2.8 OCSO robustness determination

With the final SAIL of IV and the OCSL of 3, for this operation, all OCSOs should be satisfied with the Medium robustness level (see Table 4.9). For example:

- **OCSO#1 - Prevent malicious actions carried out by a non-authorized person**. At the Medium robustness level, this OCSO requires mechanisms to verify the identification of the person trying to access to the Ground Control Station (GCS) or the autopilot. However, currently, these features are not available for the autopilot used in this operation.
- **OCSO#13 - Detect anomalies of sensor data**. At the Medium robustness level, this OCSO requires to verify the sensors data by two approaches. The first one is to check if the data from a sensor exceeds reasonable thresholding. This approach is currently adopted by autopilot software used in this operation. The second approach is to check the cross-consistence between different sensors. For the autopilot used in this operation, we do not have any information on this mechanism.

5.2.9 Result discussion

For this case study, we have conducted a risk assessment with our extended SORA methodology for a UAS operation mentioned in the EU-funded MULTIDRONE project. As aforemen-

tioned, Capitán et al. [204] conducted a risk assessment for the same operation based on the original SORA methodology. A summary of these results are presented in Table 5.9.

	Capitán et al assessment [204]	Our assessment
Methodology	SORA	Extended SORA
GRC	2	4
ARC	a	b
PRC	Not applied	D
Final SAIL	I	IV
OCSL	Not applied	3

Table 5.9: Result comparison

According to the table above, our risk assessment gives a more critical value of SAIL than the one given by Capitán et al. (SAIL of IV vs. I). As a result, the safety objectives (OSO) are required with a higher robustness level in our assessment. For example, in our assessment, the drone must be designed to determine possible malfunctions and minimize their occurrences. Meanwhile, in the assessment of Capitán et al., this objective is not required. There are two reasons for this difference. The first one is that Capitán et al. used an old version of the original SORA methodology, which was still under-development version at the moment of the assessment and lacked clear instructions. This leads to the overestimation of the harm Barriers' robustness level (e.g., parachute). The second reason is that our assessment considers the privacy Harm to the people on the ground. In this operation, the privacy Harm is an essential aspect, because the UAS is equipped with a high-performance camera, and the operation takes place in a crowded event. Moreover, in comparison with the work of Capitán et al., our work go further by considering new cybersecurity Threats and determine the objectives related to cybersecurity. Some of the determined cybersecurity objectives are not fulfilled in the considered operation. To fulfill these objectives, it requires to change the operation and the UAS dramatically. This change could make the operation more secure/safe but could also impact the cost-effectiveness of the operation.

5.3 Application to other case studies

In the previous section, we applied our proposed methodology for a real UAS operation that is well documented in a European research project. In this section, we introduce two other case studies: "Drone for delivery in an urban zone" and "Industrial site monitoring" to analyze further our proposed methodology. These operations represent two kinds of UAS operations very concerned by the UAS application market.

5.3.1 "Drone for delivery in a urban zone" operation

5.3.1.1 Operation description

In this operation, an e-commerce company will use UASs to transport goods from its warehouse to customers in a city. To optimize the operation's cost-effect, the operator (e-commerce company) will establish the warehouse in the city center and provide services to the clients within 6 km around the warehouse. Therefore, the aircraft flies totally in the city center (urban zone).

The flight is planned to take place at an altitude of 40 m and beyond the pilot's visual range (BVLOS modes). For each delivery, the aircraft will follow a different trajectory depending on the client's position. Therefore, the pilot should prepare the flight plan and upload it to the UAS before operations. During the operation, the aircraft flies automatically following the predefined flight plan and under the pilot's monitoring. Therefore, the major tasks that the pilot needs to perform are: preparing flight plans, starting and ending the flight, monitoring the flight, resolving anomaly situations. The aircraft will be equipped with a small RGB camera to help the pilots monitor the delivery. The camera's resolution is 1920x1080 pixels, and its angle of view is 40°. We suppose that the camera is capable of detecting people on the ground and automatically blurring their images to protect their privacy (Privacy protection filters).

The operator plans to use an unmanned aircraft with a maximum dimension of 1.5 m and a maximum weight of 10 kg. Because the flights take place over people, The aircraft is equipped with parachutes. We suppose that the operator will establish an Emergency Response Plan (ERP) to react to emergency situations. This document of the operation clarifies the tasks, roles of each crew member in emergencies. It is supposed that both the parachute and ERP conform with the standards adopted by the authorities.

5.3.1.2 Extended SORA analysis

We perform a risk assessment based on the extended methodology to determine the safety objectives (OSOs) and the cybersecurity objectives (OCSOs).

1. Firstly, we determine the Ground Risk Class (GRC) of the intended operation. Because the flights occur at the BVLOS mode in an urban zone and the aircraft's dimension is less than 3 m, the intrinsic GRC is assigned to 7. The GRC could be reduced by two harm Barriers: the Emergency Response Plan (ERP) and a parachute. According to the operation description, these Barriers will be at a Medium level of robustness and help reduce the GRC by 1 point. Therefore, the final GRC of this operation is 6.

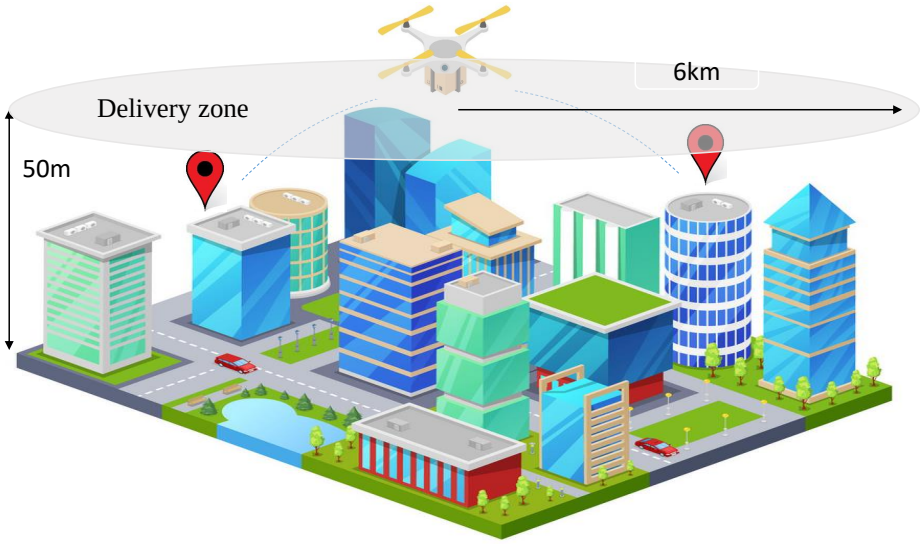


Figure 5.1: Delivery Operation

2. We determine the Air Risk Class (ARC) of the intended operation. The aircraft will fly above the city center, under an altitude of 150 m, and far from the airports. Therefore, according to the SORA methodology, ARC of this operation is c.

3. Combining the ARC of c and the GRC of 6, we have a 2D-SAIL of V (see Table 4.1).

4. we determine the Privacy Risk Class (PRC) of the intended operation. Based on the camera's specification (1920x1080 resolution, 40° angle of view) and the altitude of flights, we calculate the captured image's pixel density. It is 65.9 pixels per meter, equivalent to the detail level of "Observer"(see Table 4.2). Because the flights occur in the urban zone and at BLVOS mode, we assign the intrinsic PRC of D. Additionally, the camera could automatically detect and blur the image of people. This functionality helps to protect people's privacy on the ground and reduce the PRC by 1 point. Therefore, the operation's final PRC is C.

5. Combining the 2D-SAIL of V and PRC of C, we obtain the SAIL 3D of V. With this SAIL value, the operation shall satisfy the OSOs mostly at the High robustness level. The detailed objectives are presented in Annex E of the SORA methodology [98].

6. We evaluate the cybersecurity susceptibility (OCSL) of the intended operation. We suppose that the UAS will use the mobile network (4G) to maintain the communication between the aircraft and the ground station. The data will be transmitted via a cloud provided by a trusted third-party service. Therefore we assign the operation the OCSL of 4, as shown in Table 5.10.

7. With the 3D-SAIL of V and the OCSL of 4, the operation shall satisfy the OCSOs at the High robustness level. The OCSOs are detailed in Annex A.

Characteristic	Description	Points
Communication	public network	2
Type of Operation	BVLOS	1
Monitoring level	Continuously monitored by pilots	0
Third party	Only trusted devices	1
OCSL		**4**

Table 5.10: Result of OCSL determination

Analysis			
GRC	6	2D-SAIL	V
ARC	c	3D-SAIL	V
PRC	C	OCSL	4

(a) With privacy protection filters

Analysis			
GRC	6	3D-SAIL	V
ARC	c	3D-SAIL	V
PRC	D	OCSL	4

(b) Without privacy protection filters

Table 5.11: Analysis result for the delivery operation

5.3.1.3 Result discussion

The analysis result is resumed in Table 5.11a. According to the analysis, with the operation description above, the operator will have to satisfy most of Operation Safety Objectives at a high robustness level (20/24 objectives) and all Operation Cyber Security Objectives at a high robustness level. To the best of our knowledge, currently, there is no system on the market, which could satisfy these objectives (SAIL of V or VI) [1]. On the one hand, we find that this operation will be very costly. Because it requires many resources to implement sophisticated cybersecurity solutions and conform to different standards (development, design, maintenance, etc.). On the other hand, we could still reduce a little the cost of the operation for this operation. In the operation description, it was supposed that the camera could identify images of people on the ground and removed them from the video. This kind of camera could be more expensive than a standard camera without this function. What happens if we remove this function (Privacy protection filters). In this case, the PRC of the operation will be D instead of C. The new analysis is shown in Table 5.11b. We have the same value of 3D-SAIL then the same OCSOs and OSOs. Because in this operation, the aircraft flies too high, and the camera's resolution is too low to impact people's privacy on the ground. Therefore, in this operation, we could use a standard camera to reduce the cost of operation without increasing the complexity of OCSOs and OSOs.

Let consider the same case study but with a lower altitude (20 m) and a higher performance camera (resolution of 4000x3000 pixels, the minimum angle of view of 11°). The analysis results are shown in Table 5.12a and 5.12b. In operation description, if the privacy protection filter is not mentioned, the 3D-SAIL increases from V to VI, and we have to satisfy all OSOs

[1] A branch of Sogilis company is participating in the CEDSO project (CErfiried Drone System for Safe Operations) to develop a certified UAS for an operation in an urban zone corresponding to SAIL VI

at a high robustness level (instead of only 20/24 objectives). That makes the cost of operation increases.

Analysis			
GRC	6	2D-SAIL	V
ARC	c	3D-SAIL	V
PRC	E	OCSL	4

(a) With privacy protection filters

Analysis			
GRC	6	2D-SAIL	V
ARC	c	3D-SAIL	VI
PRC	F	OCSL	4

(b) Without privacy protection filters

Table 5.12: Analysis result for the modified delivery operation

Through these discussions, we argue that the SORA methodology (extended or original version) should be used in a way optimizing the cost of the operation. In detail, we could adjust some parameters of the operation description to obtain the OCSOs and OSOs with lower robustness levels if possible. This argument is especially helpful for the operator and the manufacturer. Therefore, we take this argument into consideration when we use the extended SORA methodology with in a development process (see 5.4).

5.3.2 Industrial site monitoring

5.3.2.1 Operation description

In this operation, an industrial company will use a UAS to monitor its industrial site. Suppose that this site is far from residential zones and airports. Therefore we could consider that aircraft flies above a rural zone. The aircraft is about 20 kg, and its maximum dimension is 2 m in width.

The aircraft will fly following a pre-determined trajectory around the factory at an altitude of 30 m. The aircraft is not allowed to fly across the factory zone. Because the industrial site is very large, the aircraft will fly beyond the pilot's visual range and automatically operate. During the flight, the pilot keeps the aircraft under observation based on the aircraft's flight information. The flight information is transmitted to the ground control station via a dedicated wireless connection.

In malfunction, the company wishes to determine the flight as soon as possible within the operation area (no person inside). Moreover, the parachute will not be used to prevent the aircraft from falling on factories.

The aircraft will be equipped with an RGB camera to monitor the industrial site. The camera has a resolution of 1920 x 1080 pixel and a min angle of view of 20°

5.3.2.2 Extended SORA analysis

we perform a risk assessment based on the extended methodology to determine the safety objectives (OSOs) and the cybersecurity objectives (OCSOs).

1. Firstly, we determine the Ground Risk Class (GRC) of the intended operation. Because the flights take place at the BVLOS mode in a rural zone (sparsely populated environment) and the aircraft's dimension is less than 3 m, the intrinsic GRC is assigned to 4.

2. We determine the Air Risk Class (ARC) of the intended operation. The aircraft will fly above a rural zone, under the altitude of 150 m, and far from airports. Therefore, according to the SORA methodology, the ARC of this operation is b.

3. Combining the ARC of b and GRC of 4, we have a 2D-SAIL of III (see Table 4.1).

4. We determine the Privacy Risk Class (PRC) of the intended operation. Based on the camera's specification (1920x1080 resolution, 20° angle of view) and the altitude of flights, we calculate the captured image's pixel density. It is 181 pixels per meter, equivalent to the detail level of "Recognize"(see Table 4.2). Because the flights occur in a rural zone and at BLVOS mode, we assign the intrinsic PRC of C. Because the UAS is used to monitor a site, no privacy protections are applied. Therefore, the operation's final PRC remains at the C level.

5. Combining the 2D-SAIL of III and PRC of C, we obtain the SAIL 3D of III. With this SAIL value, the operation shall satisfy the OSOs with a low or medium robustness level. The detailed objectives are presented in Annex E of the SORA methodology [98].

6. We evaluate the cybersecurity susceptibility (OCSL) of the intended operation as shown in Table 5.13. The operation's OCSL is 2.

Characteristic	**Description**	**Points**
Communication	Dedicated solution	0
Type of Operation	BVLOS	1
Monitoring level	Continuously monitored by pilots	0
Third party	Only trusted devices	1
OCSL		**2**

Table 5.13: Result of OCSL determination

7. With the 3D-SAIL of III and the OCSL of 2, the operation shall satisfy the OCSOs at the Medium robustness level. The OCSOs are detailed in Annex A.

Analysis			
GRC	4	2D-SAIL	III
ARC	b	3D-SAIL	III
PRC	C	OCSL	2

Table 5.14: With privacy protection filters

5.3.2.3 Result discussion

The analysis result is resumed in Table 5.14. According to this result, the operator has to satisfy the objectives with only a low or medium robustness level (versus high robustness level in the delivery operation). This result is typical for the "industrial site monitoring" operations. Industrial sites are usually spread over a large area, far from residential zones, far from airports. Therefore, "industrial site monitoring" operations have some common features such as rural operation area, BLVOS, low activity density airspace. According to the SORA methodology, the operation with these features is usually not critical. It is not reasonable. For example, considering three operations: "nuclear power plant monitoring", "solar power plan monitoring" and "a field monitoring", we have the same result. The reason is that the current version of (original or extended) takes into consideration only the direct Harm to the human-being (loss of life or privacy). The Harm to infrastructures or industrial sites has not yet been developed. In fact, this subject is very complex because harm evaluation in different industrial domains could be various.

At this moment, we propose a temporary solution to resolve the problem above. For the "industrial site monitoring" operations, we will add "supplemental points" to the 3D-SAIL. These points partially present the critical nature of industrial sites. The points will be evaluated based on two questions: (1) "Does the industrial site produce or store dangerous products (such as toxic, gasoline, radiation material)?", (2) "Does this site store sensitive information?" (see Table 5.15).

Supplemental points		
Type of industrial site	No sensitive infor	Sensitive infor
No dangerous product	0	2
Dangerous product	1	3

Table 5.15: "Supplemental point" evaluation

Using this solution for the three operations mentioned above, we have the new results, as shown in Table 5.16. The nuclear power plant is one the most critical infrastructures. Therefore the 3D-SAIL of VI and the OSOs at the Highest robustness level is suitable. If we do not consider the possible "finance" Harm, the operation over a solar plan power has the same critical level as the operation over a field.

	Monitoring operation		
	Nuclear power plant	Solar power plant	a field
Supplemental points	3	0	Not applied
Final 3D-SAIL	VI	III	III

Table 5.16: Comparison between three monitoring operations after applying the supplemental points

5.4 Utilisation of the extended SORA methodology for system development

The extended SORA methodology requires some simple information on the intended operation (such as operation area, operation types) to perform a risk assessment. The result of this assessment is a list of safety and cybersecurity objectives. These objectives could be satisfied when we define the operation's detailed features (such as organization, operation procedures, training) and the system specifications. It means that we could use the extended SORA analysis to refine the operation description and the system description. Therefore, we propose integrating the extended SORA analysis into the early phase of the development process when the client's requirements are translated into a system description. Figure 5.2 shows our proposal. This proposal is explained in detail as follows:

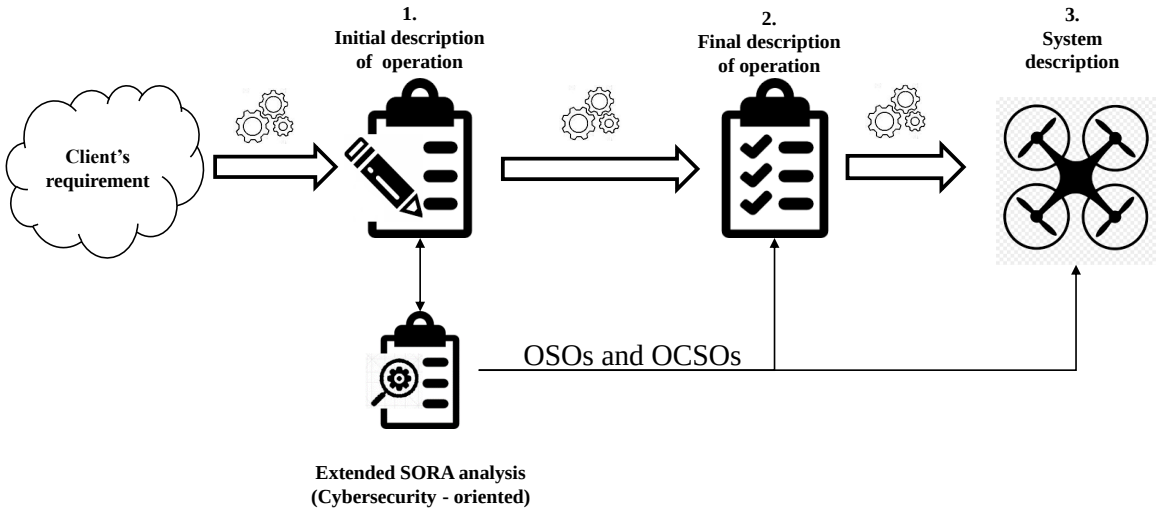


Figure 5.2: a proposed approach to integrate the extended SORA analysis into the development process

1. **Initial operation description**: At the beginning of the development process, we suppose that the client could provide only simple information on the desired operation. The information could be the client's needs or ideas about the operation. For example, the client needs a UAS to monitor thousands of hectares or deliver small packages. This information is not detailed enough to perform the extended SORA analysis. Therefore,

we first establish the initial operation description. This document includes the input information to perform the extended SORA analysis (For example, operation purpose, VLOS operation or BLVOS operation, operation area, size of aircraft, harm barriers, etc.). These are the operating parameters assessed in the extended SORA methodology. We could collect, reason, or chose these parameters based on the discussion with the client about their requirements.

2. **Extended SORA analysis:** Based on the initial operation description, we perform the extended SORA methodology. As a result, we obtain the "operation" safety objectives (OSOs) and the "operation" cyber-security objectives (OCSOs). At this step, we could apply flexibly the methodology to optimize the operation cost as our previous conclusion (see 5.3.1.3). For example, we could add new harm barriers and satisfy the objectives at a lower robustness level; or remove some harm barrier but satisfy the objectives at the same level.

3. **Final operation description:** In this step, we establish the final operation description based on the form provided by JARUS in [184]. The final operation description should conform with the safety/cybersecurity objectives and the initial description defined in the previous step. Moreover, this description should clarify as much as possible how the UAS will be used.

4. **System description** Finally, we describe the system architecture that satisfies the final operation description, the safety and cybersecurity objectives.

For the next, we illustrate the approach above for the case study "Industrial site monitoring".

5.4.1 Initial Operation Description

To monitor a high sensitive industrial plant (e.g. a nuclear plan power, a chemical factory), the owner company will deploy a UAS equipped with a thermal camera. The UAS will be deployed to make flights around the plant which locates in a rural zone. The flight plan is defined by the owner company and repeated for all flights. According to the flight plan, the drone does not fly across the plant and keeps a distance of 200 m from the plant. There is not any airport near the inspected area. The drone is 20 kg and its maximum dimension is 2 m width; it is designed to fly automatically at Beyond Visual Line Of Sight (BVLOS), and the altitude is 30 m above the ground during the whole operation.

During the flight, the pilot observes the drone's status drone and the highway in real-time via the GCS computer. The pilot needs to carry out only three simple actions: start the flight, end the flight (back to stand-by mode), go home. The data exchanged between the GCS and the aircraft is transmitted via wireless communication channels.

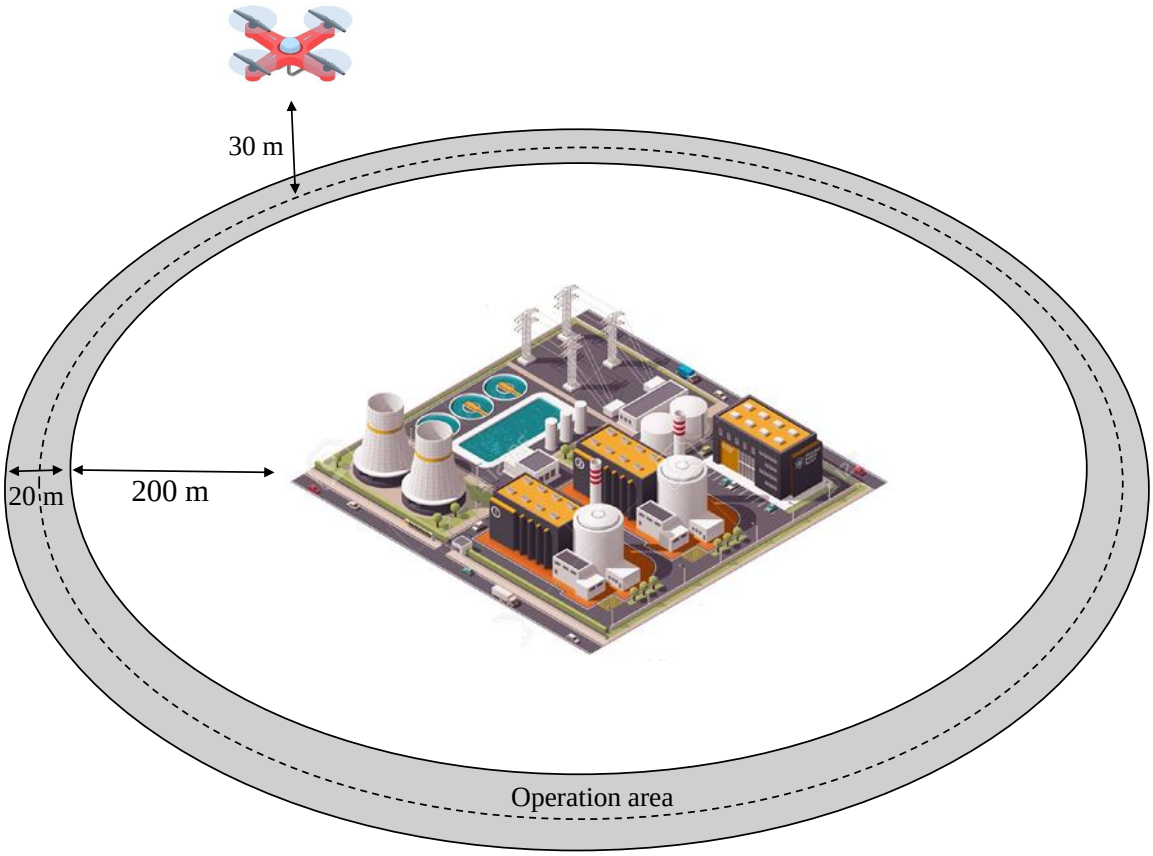


Figure 5.3: UAS Operation

The aircraft is equipped with a video camera with the characteristics as follows:

- Resolution: 1920 x 1080
- Min angle of view: 10 degrees.

5.4.2 Extended SORA analysis

Performing the extended SORA analysis, we obtain the 3D-SAIL of VI and the OCSL (Operation Cybersecurity Susceptible Level) of 2 for the given operation. The detail of this analysis was presented in 5.3.2. According to the methodology, we should satisfy the OSO at the Highest robustness level and the OCSO at a Medium level. These OSOs are presented in Annex E of the original SORA methodology (readers could find them in E of this thesis), and the OCSOs are detailed in Table 5.17.

Name	Description
OCSO#01	- Define processes/mechanisms to identify and authenticate the person trying to access the GCS and the autopilot. - Define process/mechanisms to create/modify/delete a person's identification
OCSO#02	-Define the rights of each person in its organization, who could interact with the autopilot and GCS. - Define the process/mechanisms to allocate/modify/revoke the rights of each person
OCSO#03	- Define process/mechanism to restrict the actions that a person could carry out as his allocated rights
OCSO#04	- Define security mechanisms to protect the integrity of the flight plan, the flight parameters (PID parameters, filter Kalman parameters, sensors calibrations, etc.) and recorded data (video data, log data) stored in the GCS and the autopilot.
OCSO#05	- Define security mechanisms to protect the confidentiality of the data/information stored in the GCS and the autopilot
OCSO#06	- Analyze the anomaly behavior on software/hardware after the flight to detect anomaly behavior in the post-flight inspection.
OCSO#07	- Partition of the software/hardware architecture into different "zones" with different levels of criticality. Some hardware/software could be vulnerable to cyberattack than the others, but they provide functionality less critical than the others
OCSO#08	- Define mechanisms to ensure the confidentiality of each data transmitted via communication equipment.
OCSO#09	- Define mechanisms to ensure the integrity of each data packet/message transmitted via communication equipement
OCSO#10	- Define parameters used to measure the performance of communication channels. - The GCS displays the defined parameters to pilots - Establish a security instruction that the pilot could use to detect a drop-in communication channels' performance
OCSO#11	- Define the mechanisms to re-establish the communication or maintain several essential services in case of a drop in communication performance.
OCSO#12	- Define parameters used to diagnose the performance of the communication channel after each flight. These parameters will be recorded on both the autopilot and the GCS. - Establish a security instruction that the pilot or maintenance staff could use to detect anomalies by inspecting the log
OCSO#13	- Partition of the communication system into different channels according to the criticality levels and vulnerability levels of transmitted data.
OCSO#14	- Define mechanisms to detect anomaly sensors data by analyzing the consistency and the coherence between data from different sensors.
OCSO#15	- Define the solution to protect sensors against interference from the environment (The attacker could manipulate the output of the accelerator sensor by using the interference at its resonant frequency)

Table 5.17: Definition of OCSO with a Medium robustness level

5.4.3 Final Operation description

We could establish a final operation description based on the defined OCSOs and OSOs and the initial operation description. According to the form provided by JARUS [184], this description includes many kinds of information such as organization structure, operation procedures, training, manufacturers, development standards, etc. Focusing on this dissertation's subject - cybersecurity, we mention here only the information related to the cybersecurity aspect.

5.4.3.1 Operators

We intend that the UAS will be operated by three people: an operational manager, a primary pilot, and a secondary pilot. The operation manager is responsible for the whole operation and manages the pilots. The primary pilot is in charge of observing and controlling the aircraft. The secondary pilot is in charge of operating the camera, observing the factories. Based on the role of each member, their rights are defined as follows:

- An operation manager could create/modify/delete pilot accounts
- To control and observe the flight, the primary pilot could:
  - Send commands to the vehicle from the GCS (takeoff, land, fly following a plan, flight termination).
  - Access to flight information (altitude, position, attitude, battery info, communication status).
  - Control and command the vehicle.
  - Access to video captured by the camera.
  - Access to logged files to perform post-flight analysis.
- To control the camera and observe the industrial site, the secondary pilot could:
  - Access to video captured by the camera.
  - Control and command the camera.

By defining the specific rights of each member, we satisfy the OCSO#2.

5.4.3.2 Operational procedure description

The operational procedure contains step-by-step tasks performed by the pilots to react effectively to different situations. The operation procedures covers the normal situation, contingency situation and emergency. These situations are differentiated based on the airspace

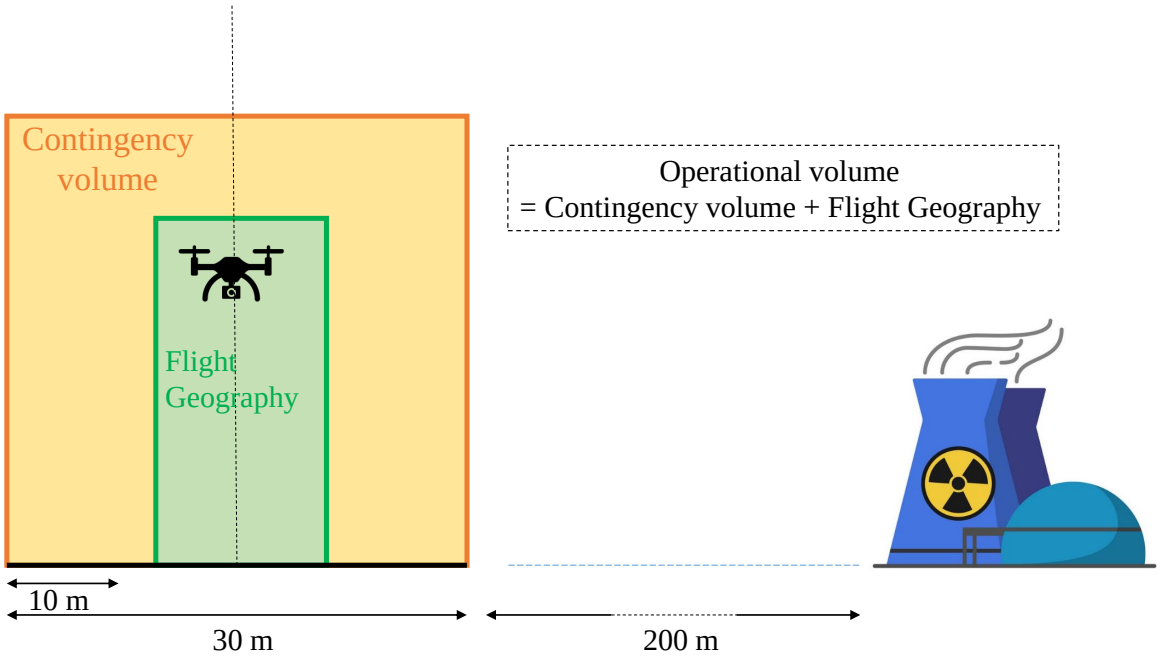


Figure 5.4: Operational volume

volume that the aircraft located. We divide spatially and temporally the operation volume into two airspace volumes: flight geography and contingency volume as shown in Figure 5.4. Flight geography is the airspace volume where the aircraft operates normally and the Normal procedures are applied. In this operation, the flight geography is a 10 m-width corridor going along with and covering the pre-determined trajectory. It means that in this operation, we accept a tolerance of 5 m for the position of the aircraft. The contingency volume is the volume of airspace outside the flight geography, where we consider that the operation is in anomaly situations but still under control. When the operation is in abnormal situation, the pilots should follow the Contingency procedures to recover the operation under control. If the aircraft goes outside the contingency volume, it is considered as a loss of control or in emergency situations. When the operation is out of control, the pilots should follow the Emergency procedures to limit escalating effects. The detail of the operation procedures is presented as follows.

(a) **Normal flight procedures**

Normal procedures are put in place when the UAS operates normally as the operator's intention. The aircraft flies automatically, and the pilots need to only observe the flight in the ground station

(b) **Contingency procedures**

We activate the contingency procedures when the aircraft operates anomaly and goes outside the Flight Geography, and enters Contingency volume. We suppose that the

operation area is empty (no people, no building, no facility, etc...) and protected. Therefore, when the aircraft goes outside the Flight Geography, we intend to cancel the flight and land the vehicle within the operation area as soon as possible. Because the aircraft could go outside the operation volume and crash on the plant if it continues to fly. It should enter landing mode automatically and warms the pilot. This requirements could be fulfilled by a geo-fencing solution (limit the flight within the define boundary). Suppose the aircraft still tends to go outside the Contingency volume during landing. In that case, the primary pilot takes over to control the aircraft manually and lands it inside the operation volume. During this situation, the UAS shall inform and warm the pilots of the possible causes. The following causes should be taken into consideration:

- Degradation of navigation data (from GPSs, IMUs): In this case, the navigation data is not precise enough to keep the aircraft tracking the pre-determined trajectory but accurate enough to keep the aircraft flying.
- Degradation of mechanical component (motor, blade, airframe).
- Run out of batteries
- Lost of communication: For this situation, the pilot could not recognize the situation and could not take over control the aircraft. The aircraft shall enter the landing mode and lands automatically.
- Adverse weather conditions.

(c) **Emergency procedures**

When the aircraft goes outside the contingency volume, we consider that the operation is out of control. It requires a flight termination. The geo-fencing mechanisms shall turn off all motors and let the aircraft fall down automatically. If the automatic flight termination is failed, the primary pilot shall activates the flight termination manually. The secondary pilot shall warm the manager and the people on the ground the emergency situation.

(d) **Post-flight**

In this phase, the pilots look for any anomalies of aircraft behavior and the communication links (e.g., drop package rate, invalidate package, signal strength). These anomalies could indicate the failures or the cyber-attacks that happened during the flight. For example, the aircraft's small vibration could indicate a GPS degradation or a possible attack on the IMU. It could be difficult for the pilot to detect this issue immediately during the flight. However, by observing and analyzing the whole data, the pilot could recognize the vibration easily in the post-flight phase. Any anomalies must be noted, logged, and reported to the manufacturer. The post-flight procedure allows us to satisfy the objectives mentioned in OCSO#06, OCSO#10, and OCSO#14 related to anomaly detection in post-flight analysis.

5.4.4 System description

By analyzing the defined cybersecurity objectives and the operation description, we propose a UAS architecture, as shown in Figure 5.5. In the remainder of this section, we explain why we chose this system.

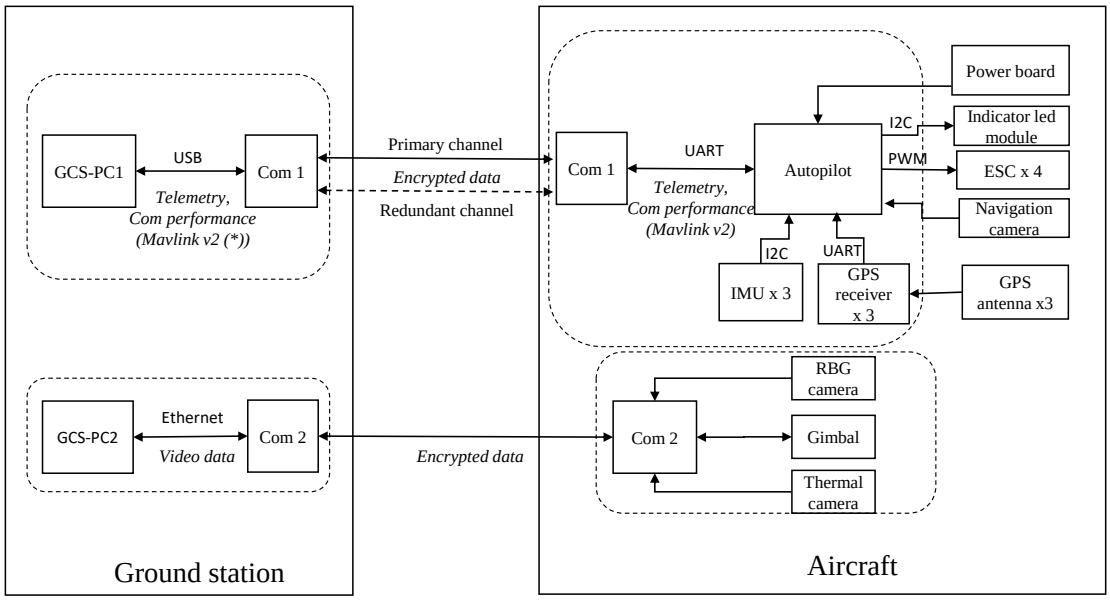


Figure 5.5: System Architecture

5.4.4.1 Ground station

The ground station provides pilots the human-machine interface to interact with the system. As mentioned in (5.4.3.1), two pilots (primary pilot and secondary pilot) are involved directly in operating the UAS with different attributed tasks. To ensure that the pilots could perform only the action defined for their role (OCSO#03), the ground station should provide them with different interfaces. There will be two separate interfaces. We call them primary-pilot interface and secondary-pilot interface. The primary-pilot interface allows the primary pilot to recognize the flight status (position, altitude, attitude, battery status). This interface also allows the primary pilot to manipulate the flight with different on-screen buttons: Arm (start), Disarm (stop motors), takeoff, landing, go-home, fail-safe. When the pilot clicks on these buttons, the associated commands are sent to the aircraft. The secondary interface displays the cameras' videos, the vehicle's position, the geography map, and the camera's direction. The secondary pilot could control the camera's movement via a joystick.

The primary-pilot interface and the secondary-pilot interface provides the pilots with functionalities at different critical levels. The primary-pilot interface provides the functionalities to control and command the aircraft, which are vital for the operation's safety. Meanwhile, the

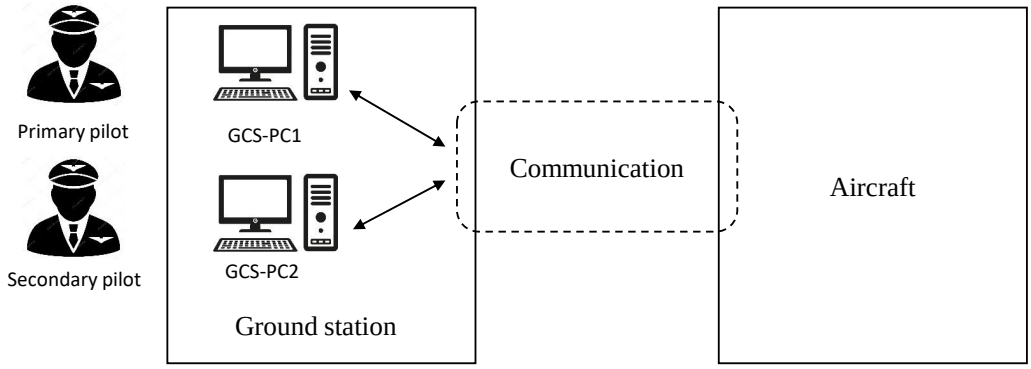


Figure 5.6: Ground station

secondary-pilot interface almost relates to the functionalities to control, command the camera. These functionalities are considered essential to fulfill the operation's objective (monitoring the industrial site) but not critical for the flight. For example, suppose the adversary manipulates the secondary-pilot interface. In that case, the flight could still be under control without any significant impacts on the vehicle and the factory. Therefore, according to the OCSO#07 (software/hardware partition), we decompose the Ground Control segment into two separate parts, as shown in 5.6. The first part includes a ground control station computer (GCS-PC1) with associated software to control and command the aircraft (primary-pilot interface). The second part consists of another computer with associated software to control and command the camera (secondary-pilot interface). The GCS-PCs usage should be strictly limited to the assigned pilots to avoid misusage or sabotage. For this purpose, the GCS-PCs shall identify and authenticate users trying to access, as mentioned in OCSO#01 (user identification and authentication). The pilots will be prompted to provide their pilot account information, including an account id and a password when accessing the GCS-PCs. As mentioned in 5.4.3.1, the operation manager will manage the pilot accounts. Therefore, we propose that both GCS-PCs provide the operation manager a specific interface to create, modify, or delete the pilot accounts. This interface could only be accessed with an admin account.

To support the post-flight analysis (see 5.4.3.2), the GCS-PC1 shall record and store the aircraft's flight information, and the GCS-PC2 shall record the video captured by the camera during the flight. As mentioned in the OCSO#04 and OCSO#05, we should protect the stored data's integrity and confidentiality. For this purpose, we could use cryptographic hash algorithms such as SHA-224, SHA-256, SHA-384, etc., to protect the data integrity and the encryption algorithm such as AES-128, AES-256 to protect the data's confidentiality.

5.4.4.2 Aircraft segment

(a) **Autopilot**

During a normal situation, the aircraft will fly automatically without the pilot's interaction. The autopilot shall navigate the aircraft following the pre-determined trajectory. The trajectory is repeated, and the airframe is not changed for all flights. Therefore, we could embed the flight plan, operation volume boundaries (mentioned in 5.4.3.2), and flight control parameters into the autopilot firmware (for some commercial autopilot, these parameters are adjustable and stored in the flash memory). That helps prevent the adversary from accessing and modifying these parameters illegally. This configuration conforms with OCSO#04 and OCSO#05 (data integrity and confidentiality protection). To give a higher protection level, we could consider also the mechanisms to protect firmware's integrity, for example, ones mentioned in [206]–[208].

As mentioned in the post-flight procedure (see 5.4.3.2), the pilot perform a post-flight analysis after each flight. For this activity, the autopilot shall record and store the flight information as encrypted data accompanied by a cryptographic hash. That help protect data confidentiality and data integrity (as required by the OCSO#04 and the OCSO#05)

(b) **IMU and GPS**

The IMU (accelerometers, gyroscope, and compass) and the GPS receiver are the essential sensors that provide the autopilot with navigation data. The sensor redundancy shall be put in place, as mentioned in OCSO#15. There shall be two forms of redundancies: component redundancy and data redundancy. The component redundancy offers a tripled IMU and a tripled GPS receiver. If one of the GPSs (or IMUs) is failed, the autopilot shall detect the failure based on the remaining GPSs (or IMUs) and send an alert to the ground station. For the data redundancy, the aircraft will be equipped with an embedded camera module that provides the third navigation data source besides GPSs and IMUs. The autopilot shall detect if one of the three data sources is not reliable. These redundancies make attacks via sensors (especially GPS spoofing) more difficult.

(c) **Payload**

The aircraft is equipped with a camera module, including an RGB camera, a thermal camera to film the monitored site, and a gimbal to stabilize and control camera direction. As aforementioned in 5.4.4.1, we considered that the functionalities related to video record are less critical than those related to the flight. According to the OCSO#07 (software/hardware partition), the camera module shall be independent of the autopilot.

5.4.4.3 Communication segment

The communication system shall ensure the flow of data between the ground control segment and the aircraft segment. There are two kinds of transmitted data: telemetry data (flight status and pilot command) between GCS and autopilot; camera data between GCS and the

camera module. According to OCSO#08 and OCSO#09, the encryption scheme should be put in place to protect the transmitted data's integrity and confidentiality. However, each kind of data's encryption mechanisms could be different because of their various performance requirements. For the telemetry data, low latency transmission is necessary, but low bandwidth is acceptable. While for camera data, low transmission latency is not strictly required, but high bandwidth is needed. Moreover, we consider that the telemetry data is more critical for the operation's safety than camera data. Therefore, according to OCSO#13 (communication partition), these kinds of data shall be transmitted within two independent communication links: Com 1 (telemetry data) and Com 2 (camera data).

As the telemetry data is critical to control and command the flight, the Com 1 link should offer a redundant mechanism to ensure the data's availability and reliability (as mentioned in OCSO#11). For example, the data could be transmitted on two different frequency bands. One frequency is active all the time, and the other is activated if the communication performance on the first one is degraded.

To support the post-flight procedure (see 5.4.3.2) and satisfy OCSO#12, the communication link performance shall be estimated and stored on the GCS-PCs and the autopilot. We propose three parameters to evaluate the link performances: percentage of package lost, signal strength, delay time.

5.5 Conclusion

To illustrate and discuss our proposed extended SORA methodology, we conduct risk assessments for different UAS operations. The first one is "Aerial photography in rural zone" operation - a real operation well documented in the European funded project. The other ones are "drone delivery in urban zone" and "industrial site monitoring" operations that we establish based on the market's need. Analyzing the result, we have some arguments as follows:

- The extended methodology requires the safety objectives more robust than the original methodology. On the one hand, it means that the UAS operation could reach a higher safety and security level using the extended methodology. On the other hand, to satisfy the higher safety level, it could require more resources and impact a UAS operation's cost-effectiveness.
- The SORA methodology (extended or original version) could be used flexibly to optimize the operation cost. This argument is especially helpful for the operator and the manufacturer.
- The SORA methodology (extended or original version) does not currently adapt to the operations related to the industrial zone. We introduce a simple solution to evaluate the

industrial zone and improve the SORA methodology for such operations to resolve this problem.

Besides illustrating the risk assessments with our proposed methodology, this chapter also positions the usage of the assessment's result within the development process. We suggest using this risk assessment to consider cybersecurity (also safety) aspects when transforming the client's requirements to the system description. Based on the client's requirements, we first establish the operation description then the system description conforming to the defined cybersecurity objectives. We demonstrate this proposal with the case study "industrial site monitoring". Keeping in mind that this proposal does not aim at introducing a complete development process. It is just an idea to integrate cybersecurity into a development process.

Global conclusion and perspectives

Conclusion

This dissertation presents our work on cybersecurity of Unmanned Aircraft Systems. Cybersecurity concern is one of the problems that prevent the public acceptance of UAS applications. In this work, we focus on developing cybersecurity risk assessment methodologies for UASs. A risk assessment (including risk analysis and further risk management) is a critical part of the decision-making process to ensure a system's cybersecurity. Moreover, the risk assessment should be considered as a part of the system development process. Our works have two main contributions:

- A methodology to manage cybersecurity risks of a UAS (Chapter 3). Risk management is a term larger than risk assessment. Besides risk assessment, risk management contains other activities: context establishment, treatment, and possibly communication activity between the stakeholders. But the focus point of our methodology is the risk assessment. In this methodology, the risk assessment includes risk identification and risk analysis/evaluation. The risk identification does not focus on identifying new kinds of attacks for UAS in general. But it focuses on listing the possible attacks against the considered UAS and presenting them on attack tree graphs. The risk analysis/evaluation aims to evaluate the attacks' severity based on their difficulty and their impact. The evaluation helps determine attacks that should be considered or treated first, and attacks that should be considered later or neglected. This work provides the readers with a tool to systematically evaluate the cybersecurity risk and establish cybersecurity requirements for a UAS. The result of the methodology's application depends on the user initiative judgments and their knowledge. Therefore, the result's coverage could be improved by the participation of different experts. We could use this methodology after the UAS architecture is defined and before the implementation in the development process. The weak-point of this methodology is cost-effectiveness. Implementing the resulted cybersecurity requirements could require modifying the system architecture dramatically; it could be costly.
- An integrated cybersecurity-safety risk assessment methodology based on the SORA methodology (Chapter 4 & Chapter 5). The SORA methodology originally is a risk assessment methodology dedicated to the **operation** safety. The original methodology considers a set of safety risks, which is modeled by a bow-tie model. This model includes Threats, a Hazard, Harms and Barriers. The original methodology focuses only on safety; therefore, it considers only accidental or "non-intentional" Threats and Harms to human life. With the provided evaluation tables, the users could evaluate the risks and determine the safety objectives. To extend the SORA methodology toward cybersecurity, we first extend the risk model with the three new "intentional" Threats and the privacy Harm. Then, we introduce our evaluation mechanism, which conforms

with the philosophy of the original methodology. Based on this mechanism, the user could evaluate the risks and determine both safety and cybersecurity objectives. Our proposed strategy could be used to extend the methodology to cover other unknown Threats and other Harms. The original methodology is designed primarily for a UAS operation verification in the administrative process, not for the development process. Therefore, we introduce our approach to integrate the extended SORA assessment into the development process. This approach starts with the client's need and ends with a system architecture. The strong points of our proposed solution are: (1) it is quite easy to perform a risk assessment (especially with our web-based tool), (2) it considers cybersecurity issues early (before the system architecture design). However, it also has a weak-point. This methodology considered only a set of limited risks presented in the risk model and the objectives listed on the provided list. Therefore it is difficult to take into account new attack techniques which evolve day by day.

Perspective

As the perspective of our work, we consider the following works:

1. **Further extensions for the SORA methodology:** Currently, our extended SORA methodology considers only Harms to human life and privacy. Therefore, it does not fit the UAS operations related to infrastructures or industrial sites where consequences of attacks or accidents could be facility damages or sensitive information disclosure. In our work, we propose a simple solution for this default. However, it should be considered as a temporary solution. In the future, it needs to analyze more profoundly this kind of operation and create a new kind of Harms (for example "industrial infrastructure damages").

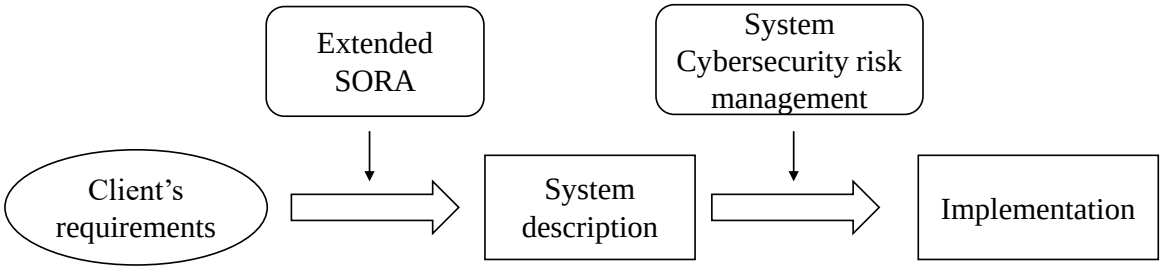


Figure 5.7: Two proposed methodologies within the development process

2. **Combining the proposed methodologies within the development process:** we have proposed two different methodologies. One could be used early in the development process, but it is not evolutive enough to consider new attack technologies. The other could be used later in the development process and flexible enough to consider new attacks (depending on the user's expertise). Therefore, we could use the two methodologies in the same development process, as shown in Figure 5.7. That allows us to take

into consideration cybersecurity aspects along with the development process. At this moment, we do not verify this idea.

3. **Web-based tool:** Currently, we have only a web-based tool for the extended SORA methodology. In the future, it needs to develop another tool for another methodology.

4. **Feedback:** We tested and evaluated our proposed methodologies with some case studies. However, to get the objective evaluations and improve our works, these methodologies should be diffused, tested, and commented on by the industrial experts.

Appendix A

Operational CyberSecurity Objectives

A. OCSOs related to attacks on Software/Hardware Architecture

Description	Level of integrity		
	Low	**Medium**	**High**
OCSO #1 _Software/Hardware Identify and authenticate the entity(*) trying to access to the GCS and autopilot Keyword: **identification and authentication** *Note: An entity could be a human, or a component (hardware/software)*	Optional	- Define processes/mechanisms to identify and authenticate the **person** trying to access to the GCS and the autopilot. - Define process/mechanisms to create/modify/delete a person's identification These activities should align to **OSO# 02,** which require to define the duties and responsibilities of the operator's personnel	- Same as Medium
		Example - Password is used to verify user's identity when someone tries to access to GCS/autopilot	
OCSO #2_Software/Hardware Manage the entity's authorization. Keyword: **authorization management** *Note 1: This objective focuses on the operational procedures to define/ allocate/ modify/ revoke the entity's authorization.* *Note 2: An entity could be a human, or a component (hardware/software)*	Optional	- Define the rights of each person in its organization, who could interact with the autopilot and GCS. - Define the process/mechanisms to allocate/modify/revoke the rights of each person.	- Same as Medium
		Example The authorization of each person is defined as follows: - Manager - Pilot could access to GCS to monitor and control the vehicle. - Maintenance staff could access to autopilot and download data after and before the flight. In order to have the rights of a maintenance staff, a person has to ask the manager for these rights.	
OCSO #3_Software/Hardware For each entity (*) accessing to GCS or autopilot, ensure that it could only carry out the authorized actions. Keyword: **access control** *Note: An entity could be a human, or a component (hardware/software)*	Optional	- Define process/mechanism to restrict the actions that a **person** could carry out as his allocated rights. - These activities should align to **OSO# 02,** which require to define the duties and responsibilities of the operator's personnel	- Same as Medium Additionally - Define process/mechanism to restrict the actions that **other components** could carry out to their rights
		Example - Depending on the role of a user, the GCS could provide a specific Human-machine interface that let the user perform the authorized action	Example - The connection *port* of the autopilot allows the GPS module to send position data to the autopilot only, but not other kinds of data

OCSO #4_Software/Hardware Detect the unauthorized entity (*) from modifying the data/ information stored in the GCS and the autopilot. Keyword: **Integrity** *Note1: This objective refers to the case that the protection mechanisms defined in OCSO #3 are bypassed* *Note 2: An entity could be a human, or a component (hardware/software)*	Optional	- Define security mechanisms to protect the integrity of the flight plan, the flight parameters (PID parameters, filter Kalman parameters, sensors calibrations, etc.) and recorded data (video data, log data) stored in the GCS and the autopilot.	- Same as Medium Additionally - Define security mechanisms to protect the integrity of source code of the autopilot and the GCS
		Example - The autopilot and the GCS generate an encrypted hash to protect the integrity of the flight plan.	**Example** - The autopilot could check the software's integrity at the booting time
OCSO #5_Software/Hardware Prevent the unauthorized entity (*) from accessing to the data/information stored in the GCS and the autopilot. Keyword: **Confidentiality** *Note 1: This objective refers to the case that the protection mechanisms defined in OCSO #3 are bypassed* *Note 2: An entity could be a human, or a component (hardware/software)*	Optional	- Define security mechanisms to protect the confidentiality of the data/information stored in the GCS and the autopilot	- Same as Medium
		Example - AES algorithm is used to protect the confidentiality of flight plan	
OCSO #6_Software/Hardware Analyze the anomaly behavior on software/hardware after the flight (post-flight inspection) Keyword: **anomaly detection**	Analyze the anomaly behavior on software/hardware after the flight to detect anomaly behavior in the post-flight inspection. *Note: this activity should align to the OSO #6 of the SORA methodology, which requires to define a post-flight inspection procedure.*	- Same as Low	- Same as Low
	Example - After the flight, the pilot shall analyze the flight data and flight command recorded during the flight. - Supporting the above activity, the autopilot and GCS shall record the data and event during the flight.		

OCSO #7_Software/Hardware Partition of the software/hardware architecture into different "zones" with different levels of criticality. Keyword: **hardware/software partition**	Optional	- Partition of the software/hardware architecture into different "zones" with different levels of criticality. Some hardware/software could be vulnerable to cyberattack than the others, but they provide functionality less critical than the others.	- Same as Medium
	.	**Example** - The GCS includes 2 PCs with two different software. One PC is used to control and observe the aircraft. This PC is critical for the UAS. The other one is used to control the payload. This functionality is less critical.	

B. OCSO related to attacks on Communication:

Description	**Level of integrity**		
	Low	**Medium**	**High**
OCSO #8_ Communication Prevent a non-authorized entity (*) from accessing to the data/information within the communication between the GCS and the aircraft Keyword: **Confidentiality** *Note: An entity could be a human, or a component (hardware/software)*	- Define mechanisms to ensure the confidentiality of each data transmitted via **communication equipment.**	- Same as Low	- Same as Low Additionally - Define mechanisms to ensure the confidentiality of each message transmitted between the GCS software and the autopilot software. (**applications level**)
	Example - In a simple case, the GCS and autopilot communicate together via a pair of radio modules. The confidentiality of data is protected based on the encryption algorithm and frequency hopping mechanisms provided by this module.		**Example** - The GCS software and the autopilot software have their mechanisms to protect the confidentiality of the message transmitted between them.
OCSO #9_ Communication	- Define mechanisms to ensure the integrity of each data packet/message	Same as Low	- Same as Low

Description	Level of integrity		
	Low	**Medium**	**High**
Prevent a non-authorized entity from modifying the data/information within the communication between the GCS and the aircraft Keyword: **Integrity** *Note: It's to ensure that the data have not been modified in terms of content, time (prevent replay attack), and source.*	transmitted via **communication equipment**.		Additionally - Define mechanisms to ensure the integrity of each message transmitted between the GCS software and the autopilot software. (**communication between applications**)
	Example - In a simple case, the GCS and autopilot communicate together via a pair of radio modules. The integrity of data is protected based on the encryption algorithm provided by this module.		**Example** - The GCS software and the autopilot software have their mechanisms to protect the confidentiality of messages transmitted between them.
OCSO #10_ Communication **Detect anomalies** in the communication channels between the GCS and the aircraft during the operation Keyword: **anomalies detection**	- Define parameters used to measure the performance of communication channels. - The GCS displays the defined parameters - Establish a security instruction that the pilot could use to detect a drop in communication channels' performance by observing communication channels 'status. At a low level, the anomalies refer to only the drop in **communication performance.** These activities should align to the OSO #6, which require the operator to identify the communication characteristics	- Same as Low	- Same as Low Additionally - Define mechanisms to detect the anomalies automatically in the communication channels At this level, the anomalies refer to the drop in communication performance and the content of the messages/packet transmitted via the communication channels.
	Example The parameters used to evaluate the communication quality are signal strength, drop-packet ratio, and bitrate. These parameters will be displayed to the pilot.		**Example** - Using a firewall in case that the communication of UAS is based on a complex network that is used for the other applications, operations, or systems
OCSO #11_ Communication Maintain a minimum communication performance Keyword: **Availability**	- A plan or a procedure that permits the user, pilot, to re-establish the communication or maintain several essential services in case of recognizing a drop in communication performance.	- Define the mechanisms to re-establish the communication or maintain several essential services in case of a drop in communication performance.	- Same as Medium
	Example - In case of a drop in communication performance, the pilot should change the communication frequencies.	**Example** - In case of a drop in communication performance, the communication module shall transmit the important information /message /packet (such as position, attitude information, and pilot command information) in priority.	

Description	Level of integrity		
	Low	**Medium**	**High**
OCSO #12_ Communication Analyze anomalies in communication channels after the flights (post flight inspection) Keyword: **anomalies detection**	- Define parameters used to diagnose the performance of communication channel after each flight. These parameters will be recorded on both the autopilot and the GCS. - Establish a security instruction that the pilot or maintenance staff could use to detect anomalies by inspecting the log.	- Same as Low	- Same as Low
	Example - The autopilot and GCS record the parameters: Package lost percentage, signal strength, delay time. - The GCS provides an interface that allows the pilot/staff to analyze the recorded data.		
OCSO #13_ Communication Partition of the communication system into different channels. Keyword: **Communication partition**	Optional	Partition of the communication system into different channels according to the criticality levels and vulnerability levels of transmitted data.	Same as Medium
		Example - The communication system is partitioned into two channels. One is used to transmit flight data, which is critical. Another one is used to transmit the video data, which is less critical.	

C. OCSO related to attacks on Sensors

Description	Level of integrity		
	Low	**Medium**	**High**
OCSO #14_Sensor Detect anomaly behaviors of sensors due to attacks Keyword: **anomaly detection**	- Define the characteristics of sensors (about output value, sampling frequency, noise) and their acceptable thresholds. The excess of these thresholds is considered as an anomaly behavior.	- Same as Medium Additionally - Define mechanisms to detect anomaly sensors data by analyzing the consistency and the coherence between data from different sensors.	Same as Medium
	Example - An acceptable threshold for data from the accelerometer such as +- 3m/s^2. The data out of this scope could be considered as a possible attack.	**Example** - Compare position data from GPS with data from IMU and a stereo-camera to detect GPS spoofing	

OCSO #15_Sensors Ensure the availability of the sensor data under attack. Keyword: **Availability**	- Define the solution to protect sensors against the interference from the environment (The attacker could manipulate the output of the accelerometer sensor by using the interference at its resonant frequency)	- Same as Low Additionally - Define mechanisms or architectures that provide redundancies of sensor data	Same as Medium
	Example - The accelerometer (IMU at large) is shelled within a metal box to defense against the interference at resonant frequencies	**Example** - In the case that the GPS is unreliable, the data from the camera could provide position data alternatively	

.

Appendix B

Web tool Manual

B.1 General Information Page

This is the first step of our application. In this step, users are prompted to provide some type of general information on the intended UAS operations. The provided information is not used for the risk assessment but helps us improve our application. The general information includes:

Figure B.1: General information page

- Name of applicant (or user)
- Email
- Type of organization. There are three options, as follows:
  - Manufacturer, if the user is a member of a manufacturer.
  - Operator, if the user is a member of an operator.
  - Administrator, if the user is an administrator.

- Purpose of UAS operation: for which purpose will the UAS be deployed? For example: observe of a highway, transport good.
- Purpose of this risk assessment. There are two options, as follows:
  - Verify an existing UAS operation. In this case, we assume that the intended operation is developed and well documented. The operation is then considered valid if it covers all the safety and security objectives resulting from the risk assessment.
  - Develop a new UAS operation. In this case, at the beginning of the risk assessment, we have only some basic information on the intended operation (e.g., purpose, altitude, location). Then, the result of the risk assessment (objectives) will be used to refine and complete the operation description.

To start the risk assessment process, click on the "Create a new assessment" button.

B.2 Ground Risk Class (GRC) determination

This step of our application corresponds to two steps of the SORA methodology: Intrinsic GRC determination and Final GRC determination.

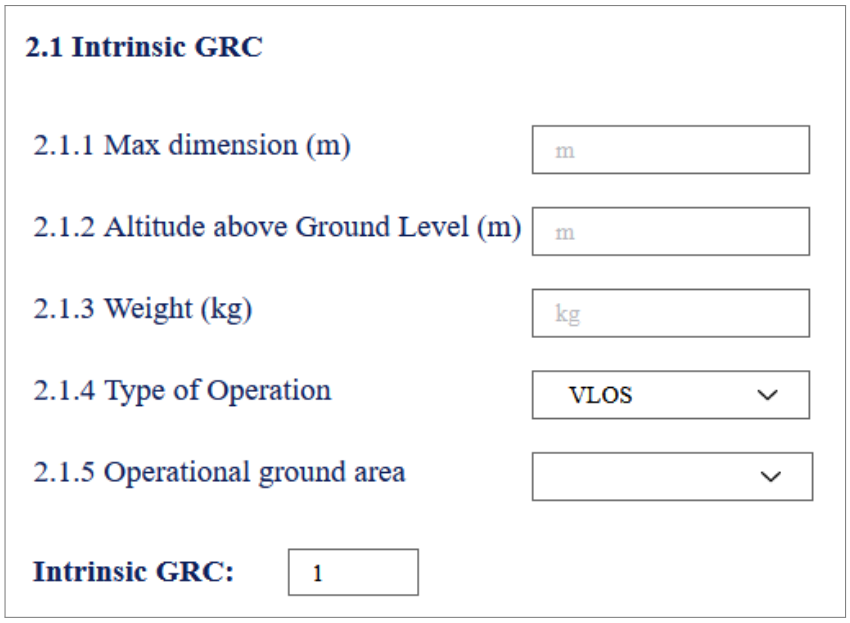


Figure B.2: Information to calculate Intrinsic GRC

To determine the intrinsic GRC of the intended operation, the user is prompted to provide the following information:

- Max dimension of the aircraft (unit: meter).
- Altitude above Ground Level of the aircraft during the operation (unit meter).
- Weight of the aircraft (unit: kg).
- Type of Operation. There are two options for this information:
  - VLOS or Visual Line Of Sight, if the aircraft operates within the visual range of pilot.
  - BVLOS or Beyond Visual Line Of Sight, if the aircraft operates outsides the visual range of pilot.
- Operational ground area. There are four options for this information:
  - Controlled ground area, if only active participants involving directly with the operation in the operational are.
  - Sparsely populated environment
  - Populated environment
  - Gathering of people, if the aircraft flies over a crowd.

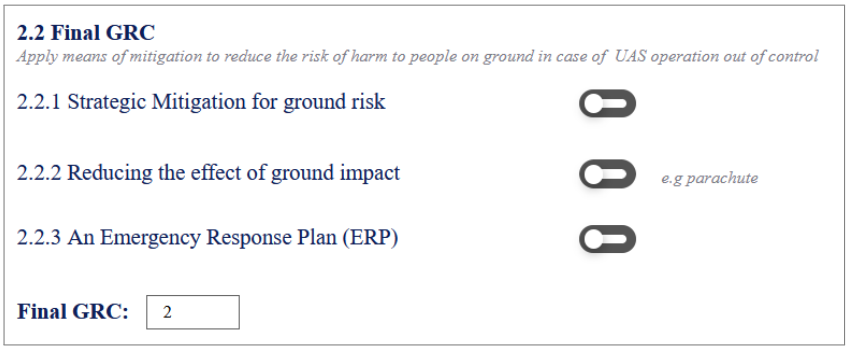


Figure B.3: Information to calculate Final GRC

To determine the final GRC of intended operation, the user is prompted to provide the information on measures applied to mitigate the likelihood of fatal injuries on the ground in case of "UAS operation out of control". There are three potential mitigations:

- Strategic Mitigation for ground risk. That helps reduce the likelihood of having a person within a dangerous area if UAS operation out of control.
- Reducing the effect of ground impact. That helps reduce the likelihood of having fatal injuries if unfortunately, a person on the ground is struck by the aircraft (e.g., parachute).
- An Emergency Response Plan. Plan of actions to be conducted in a specific order or manner in response to an emergency event.

If mitigation is mentioned or considered within the intended operation, the user could activate the presented mitigation by click/switch the corresponding button. Once mitigation is activated, the relevant characteristics of this mitigation will appear. Then the user could choose to activate the characteristic mentioned or considered within the intended operation. Based on the activated characteristics, the application could estimate the robustness of the mitigation.

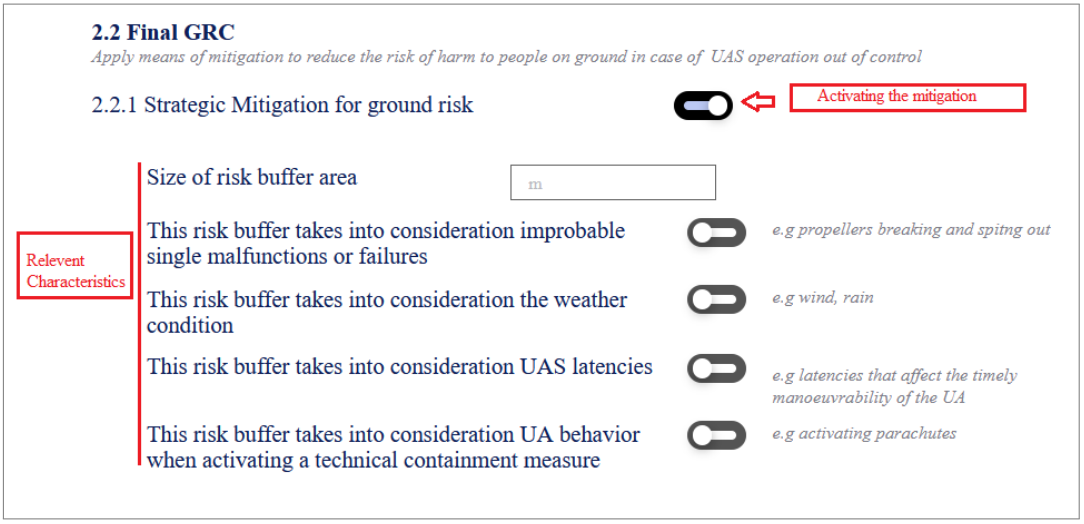


Figure B.4: The relevant characteristics of Strategic Mitigation

For each activated characteristic, the user could provide more information on how the relevant characteristic is mentioned or considered in the intended operation. This information will be used to generate the final report but not used for the risk assessment.

Based on the intrinsic GRC and the information on applied mitigations, the final GRC is calculated at the bottom of the page.

B.3 Air Risk Class (ARC) determination

This step of our application corresponds to two steps of the SORA methodology: Initial ARC determination and Final ARC determination. The initial ARC presents a generalized qualitative classification of the rate at which a UAS would encounter a manned aircraft in the specific airspace environment. Suppose an applicant considers that the generalized Initial ARC assigned is too high for the local Operational Volume condition. In that case, the mitigation could be considered to reduce the initial ARC value. If the initial ARC is not correct, the final ARC is equal to the initial ARC.

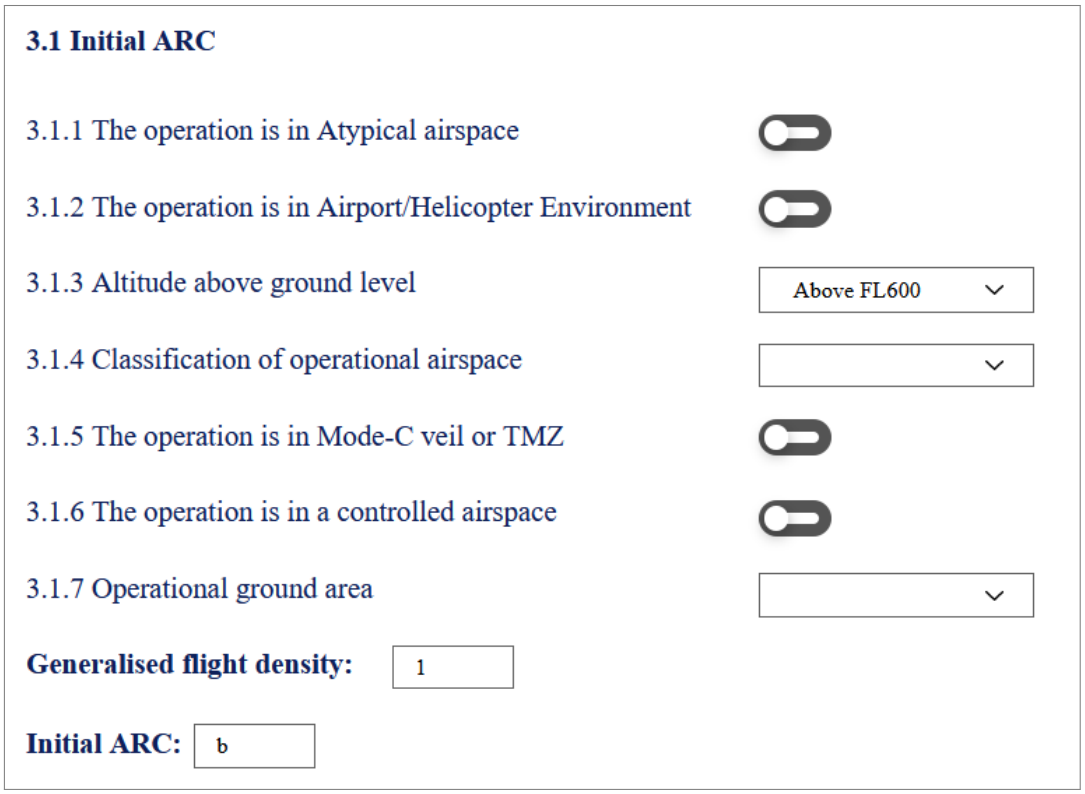


Figure B.5: Information to calculate Initial ARC

To determine the initial ARC of intended operation, based on the description of the intended operation, the user will answer the following question:

- Does the aircraft fly within Atypical airspace? Atypical airspace is defined as:
  - Restricted Airspace or Danger Areas;
  - Airspace where normal manned aircraft cannot go (e.g., airspace within 100 ft. of buildings or structures);
  - Airspace characterization where the encounter rate of manned aircraft can be shown to be less than 1E-6 per flight hour during the operation;
- Does the aircraft fly in Airport/Helicopter Environment?
- At which altitude above ground level does the aircraft operate? There are three available options:
  - Above FL600 level (environ 18000m above ground level)
  - Above 500 ft (environ 150m) et FL600
  - Under 500 ft
- In which airspace class does the aircraft operate? There are three options:

- Class A or E
- Class B, C, or D
- Class F or G

These classes are defined by the national aviation authority in terms of flight rules and interactions between aircraft and air traffic control (ATC). They could vary from a national authority to another.

- Does the aircraft operate in mode C veil or TMZ?
- Does the aircraft operate in controlled airspace?

The application could calculate the initial ARC of related airspace and the corresponding "generalized flight density" level based on the provided information.

Figure B.6: Mitigation options to reduce ARC

To reduce the initial ARC, the two types of mitigation could be taken into consideration. They are:

- Mitigation by Operation Restrictions
- Mitigation by Common Structures and Rules

Based on the initial ARC and the information on applied mitigations, the final ARC is calculated at the bottom of the page.

B.4 Privacy Risk Class (PRC) determination

This step of our application relates to our extended version of the SORA methodology, in which the privacy violation risk is taken into account.

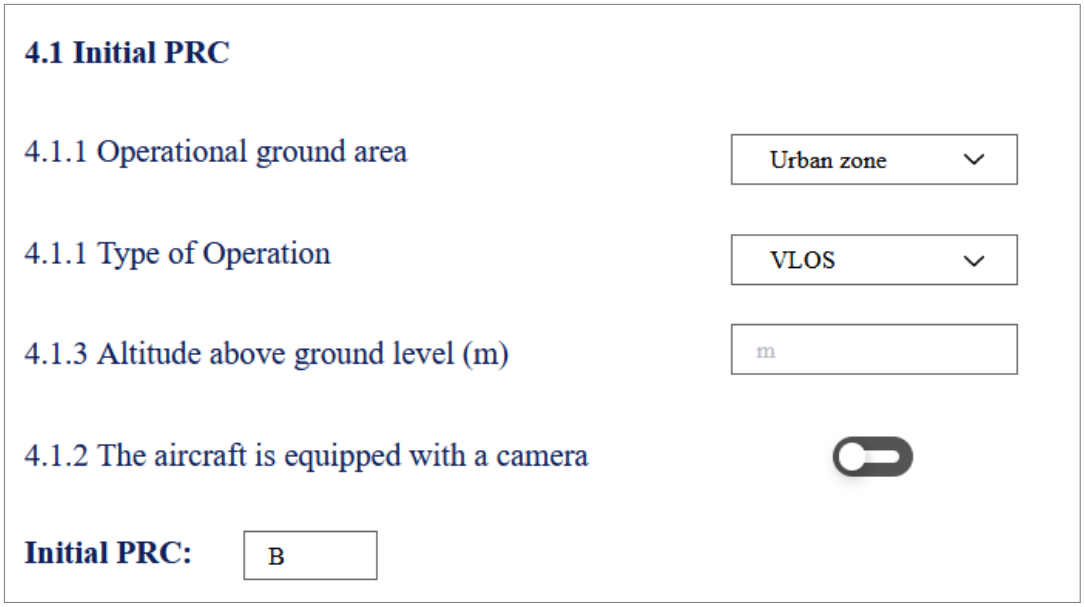


Figure B.7: Information to calculate the initial PRC

First, the user is demanded to provide the following information to calculate the initial PRC value of the operation:

- Operational ground area: Urban zone vs. rural zone.
- Type of operation : VLOS vs. BVLOS
- Does the aircraft is equipped with a camera? If yes, switch the button for this option and provide more information on the resolution and the min angle of view.

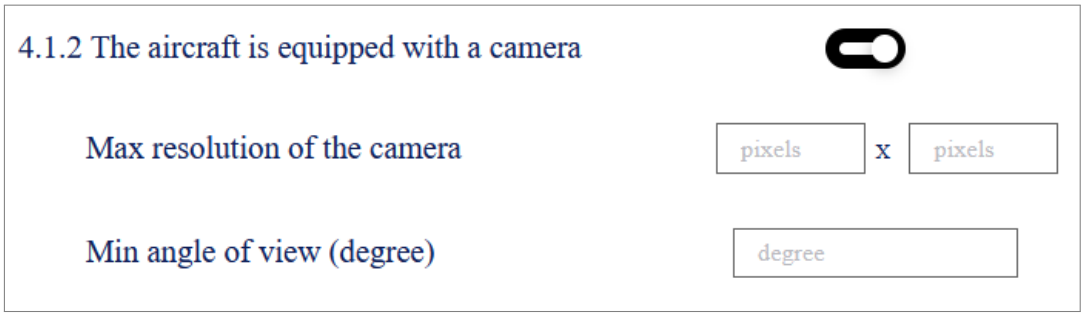


Figure B.8: Camera characteristics

The user is then prompted to provide the information on measures applied to mitigate the likelihood of privacy violation in case of "UAS operation out of control". Here, we propose three types of mitigation:

- Privacy protection filters.
- Private space restriction
- Operation aware announcement to the public

For each chosen mitigation, the user could provide more information on how the mitigation is mentioned or considered in the intended operation. This information will be used only to generate the final report but not used for the risk assessment.

Based on the intrinsic PRC and the information on applied mitigations, the final PRC is calculated at the bottom of the page.

B.5 Operation Cybersecurity Susceptible Level (OCSL) determination

This step of our application relates to our extended SORA methodology, in which the cybersecurity threats are taken into account.

In this step, the user is prompted to provide information on some characteristics of the intended operation, which help to evaluate the intended operation's vulnerability. They are:

- Nature of communication link. There are three options:
  - Dedicated communication link: The ground control station communicates with the aircraft via a communication link that is used for only the UAS operation (e.g., RF module)
  - Shared network: The ground control station communicates with the aircraft via the operator organization's internal network. Besides the UAS operation, this network could serve other activities of the organization.
  - Public network: The ground control station communicates with the aircraft via a network shared with external organizations or person. (e.g. internet connection, cloud service).
- Monitoring level. There are three options:

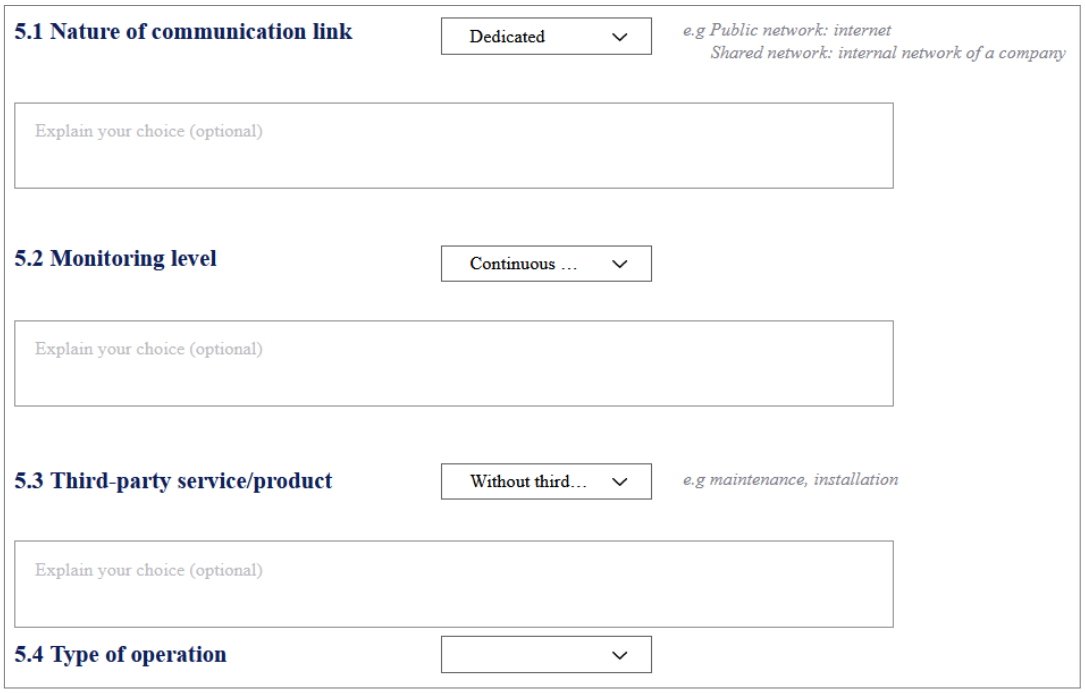


Figure B.9: Information to calculate OCSL

  - Continuous monitoring: The ground control station and the aircraft frequently communicate during the operation. The data is transferred in real-time or almost real-time.
  - Without Continuous monitoring. The ground control station and the aircraft communicate periodically during the operation. The data is not transferred in real-time or almost real-time.

- Does the system use the services provided by third parties? (e.g., maintenance service, installation service):
  - Without third party: If no third-party service/device is used.
  - Trusted third party: If only trusted third-party services/devices are used for the UAS operation.
  - Non-trusted third party: If a non-trusted third-party service/device is used for the UAS operation.

- Type of operation: VLOS vs. BVLOS.

Based on the provided information, the OCSL is calculated at the bottom of the page.

B.6 Result

On this page, the result of the risk assessment for the intended operation will be shown.

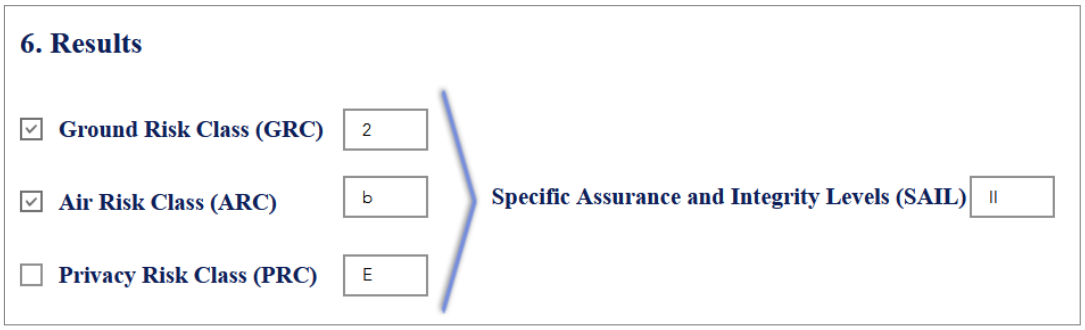


Figure B.10: SAIL calculated based on GRC and ARC values

First, the SAIL value corresponding to the provided information is calculated. In the classical SORA methodology, the SAIL value is a combination of GRC value and ARC value. Meanwhile, in our extended SORA methodology, the SAIL value is calculated based on GRC, ARC, and PRC values. To choose the parameters used to calculate the SAIL value, the user can click on the checkbox on the left of the parameter.

The different OSOs and OCSOs with their robustness level determined based on SAIL level are shown. To see in detailed the objectives, click on the fletch button.

Appendix C

Risk management result

C.1 Malfunctions

In this document, I present my 24 security requirements which could be used to secure the UAS operation. The requirements are used to treat or mitigate the impacts of the following system malfunction.

1. **Crash of UAV**: Due to malicious action, the UAV losses its attitude and crashes. Because of flying over a highway, the cash of the UAV could cause a lethal accident. (Loss of **Availability**)

2. **Deviation from trajectory**: Under an attack, the UAV deviates from its trajectory and flies following the trajectory defined by attacker. (Loss of **Integrity**)

3. **Unavailability of flight information**: Under an attack, the operator could not access to the flight information. (Loss of **Availability**).

4. **Fake flight information**: Under an attack, the fake flight information is provided to operators which makes them make incorrect decisions. (Loss of **Integrity**)

5. **Disclosure of flight information**: Under an attack, the attacker could gain unauthorized access to the flight information, which could help the attacker launch other attacks. (Loss of **Confidentiality**)

6. **Fake video**: Under an attack, the operators receive the fake observation video made by attacker. This malfunction do not impact directly the safety of the operation, but it makes the objective of operation totally failed. (Loss of **Integrity**)

7. **Unavailability of video**: Under an attack, the operators could not access to the observation video. (Loss of **Availability**)

8. **Disclosure of video**: Under an attack, the attacker could gain unauthorized access to observation video which impact on the private of the people under observation. (Loss of **Confidentiality**)

C.2 Cybersecurity requirements

C.2.1 Security requirement 1

(Fail-safe)

Object: In case the GPS module is unavailable, the autopilot needs to detect this problem and land the vehicle based on the data from the available sensors.

Related malfunctions: 1

C.2.2 Security requirement 2

Object: The autopilot needs to verify the integrity of the position data provided by the GPS module. If the incorrect data is detected, the autopilot needs to report to operators and land the vehicle.

Related malfunctions: 1, 2

C.2.3 Security requirement 3

(Fault mode)

Object: In case of the IMU module is unavailable, the autopilot needs to detect the failure and terminate the flight

Related malfunctions: 1

C.2.4 Security requirement 4

Object: Whenever receiving the raw acceleration and angular speed data from IMU module, the autopilot needs to verify the integrity of this data. When the incorrect data is detected, the autopilot needs to terminate the flight

Related malfunctions: 1, 2

C.2.5 Security requirement 5

Object: The autopilot needs to verify the navigation data's integrity. The faked data needs to be detected.

Related malfunctions: 1, 2

C.2.6 Security requirement 6

Object: At the begin of an operation, the autopilot needs to verify that flight plan, flight control parameters, navigation parameters have not been modified by unauthorized people.

Related malfunctions: 1, 2

C.2.7 Security requirement 7

Object: The autopilot needs to verify that the firmware have not been modified in term of the content and the origin.

Related malfunctions: 1, 2, 3, 4, 5, 7

C.2.8 Security requirement 8

Object: The autopilot needs access-control mechanics which allow only authorized party to access to autopilot and effect the actions as their attributed right (for example, only manufacture could modify the firmware, the operator could start/stop a mission, etc). The role of each involved party needs to be defined in detail.

Related malfunctions: 1, 2, 3, 4, 5, 7

C.2.9 Security requirement 9

(Fail-safe)

Object: if the barometer module is unavailable, the altitude of the vehicle shall be estimated based on the data from the other available sensors to land the vehicle.

Related malfunctions: 1

C.2.10 Security requirement 10

Object: Whenever receiving the air pressure data from barometer module, the autopilot shall verify the integrity of this data. When the incorrect data is detected, the autopilot should land the vehicle.

Related malfunctions: 1,2

C.2.11 Security requirement 11

(Fail-safe)

Object: if the compass module is unavailable, the autopilot needs to detect this problem and land the vehicle based on the data from the available sensors.

Related malfunctions: 1

C.2.12 Security requirement 12

Object: Whenever receiving the magnetic field data from compass module, the autopilot needs to verify the integrity of this data. When the incorrect data is detected, the autopilot should land the vehicle.

Related malfunctions: 1,2

C.2.13 Security requirement 13

Object: Whenever reading the data about the compass calibration from non-volatile memory, the autopilot needs to verify the integrity of the data.

Related malfunctions: 1

C.2.14 Security requirement 14

(Secured C2 link)

Object: In order to protect the communication between the autopilot and GCS, a secured protocol needs to be implemented. This protocol ensures that:

1. The integrity of exchanged data. Whenever receiving data from RF module, both autopilot and GCS could verify that the packet have not been modified in term of content, time (order), original source (authentication).
2. The confidentiality of exchanged data. Only authorized equipments (autopilot, GCS) could interpret the information from the exchanged data.

3. The availability of exchanged data. Both autopilot and GCS have mechanics to control the quality of communication by them-self. They need verify that every message reaches the destination. If the communication link is unavailable, the fail-safe process is triggered and the autopilot land the vehicle.

Related malfunctions: 1,2,3,4,5,7

C.2.15 Security requirement 15

Object: Whenever receiving a command from GCS, the autopilot needs to verify that this command doesn't have any impact on the safety of the operation (for example, change flight parameters, flight plan during the flight, etc). If this is a danger command, the autopilot needs to re-verify the identification of the operator and prompt him for the verification of this command before implementing.

Related malfunctions: 1,2

C.2.16 Security requirement 16

Object: The GCS shall allow only the authorized parties to access. The GCS needs to verify their identification (authentication) and to have access control mechanics (access control). The role of each involved party needs to be defined in detail.

Related malfunctions: 1,2,5,8

C.2.17 Security requirement 17

Object: The GCS needs to to verify that the the map and the flight plan stored in the GCS computer have not been maliciously modified. The integrity violation of these data needs to be reported to the operators.

Related malfunctions: 4

C.2.18 Security requirement 18

Object: The data flows between autopilot and their external environment via the connection ports needs to be controlled. Different kinds of data need to be sent or received via separated ports.This requirement could be implemented by both software and hardware design. Related malfunctions: 1, 2, 3, 5, 7

C.2.19 Security requirement 19

Object: When the Camera is not available, 3G/4G module needs to send alert message to GCS.

Related malfunctions: 7

C.2.20 Security requirement 20

Object: When the video data is not available, the GCS needs to display an alert message to operator.

Related malfunctions: 7

C.2.21 Security requirement 21

Object: The gimbal allows only authorized person to access and modify its firmware. An access control mechanics should be implemented.

Related malfunctions: 6, 7

C.2.22 Security requirement 22

Object: The parameters of gimbal need to be protected in term of integrity. At the begin of operation, the gimbal needs to verify that these parameters was created by the authorized person and have not been modified.

Related malfunctions: 7

C.2.23 Security requirement 23

(Secured protocol for video transmission)

Object The secured communication protocol needs to be implemented for transmitting video data to GCS. This protocol needs to ensure:

1. The integrity of exchanged data. Whenever receiving the video data from Internet GCS could verify that the data have been modified in term of content, time (order), original source (authentication).

2. The confidentiality of exchanged data. Only authorized GCS could interpret the information from the data.
3. The availability of exchange data. The GCS need to measure the link quality and report to operator.

Related malfunctions: 6, 7, 8

C.2.24 Security requirement 24

Object The data flow between the Internet and GCS needs to be controlled. Only manufacturer-defined kind of data could reach GCS from Internet or be sent to Internet by GCS.

Related malfunctions: 6, 7, 8

C.3 Risk level

(See the next page)

Scenario	Prepare	Opportunity	Execution	Total	DOA	Severity	Level	Target component	Requirement
1_Availability_1	2	1	4	7	Basic	High	High	GPS	1
1_Availability_2	2	1	8	11	Basic	High	High	GPS	2
1_Availability_3	6	1	12	19	High	High	Medium	IMU	3
1_Availability_4	6	1	12	19	High	High	Medium	IMU	4
1_Availability_5	6	8	10	24	High	High	Medium	Autopilot	7,8
1_Availability_6	6	6	10	22	High	High	Medium	Autopilot	18
1_Availability_7	6	8	10	24	High	High	Medium	Autopilot	7,8,6,5
1_Availability_8	6	8	10	24	High	High	Medium	Autopilot	7,8,6
1_Availability_9	6	8	10	24	High	High	Medium	Autopilot	7,8,6
1_Availability_10	2	1	12	15	Moderate	High	Medium	Barometer	9
1_Availability_11	2	1	12	15	Moderate	High	Medium	Barometer	10
1_Availability_12	6	1	12	19	High	High	Medium	Compass	11
1_Availability_13	6	1	12	19	High	High	Medium	Compass	12
1_Availability_14	6	2	6	14	Moderate	High	Medium	Non-volatile memory	13
1_Availability_15	5	1	6	12	Basic	High	High	RF	14,15
1_Availability_16	5	1	6	12	Basic	High	High	RF	14,15
1_Availability_17	6	3	2	11	Basic	High	High	GCS	14,15,16,24
1_integrity_1	2	1	8	11	Basic	Very High	High	GPS	2
1_integrity_2	6	8	10	24	High	Very High	Medium	Autopilot	5,6,7,8
1_integrity_3	6	8	10	24	High	Very High	Medium	Autopilot	6,7,8
1_integrity_4	6	1	12	19	High	Very High	Medium	IMU	4
1_integrity_5	5	1	6	12	Basic	Very High	High	RF	15,14
1_integrity_6	5	1	6	12	Basic	Very High	High	RF	14,15
1_integrity_7	6	1	12	19	High	Very High	Medium	Compass	12
1_integrity_8	6	1	12	19	High	Very High	Medium	Barometer	10
2_Integrity_1	2	1	6	9	Basic	Medium	Medium	RF	14
2_Integrity_2	2	1	6	9	Basic	Medium	Medium	RF	14
2_Integrity_3	6	6	10	22	High	Medium	Low	GCS	17
2_Integrity_4	6	6	10	22	High	Medium	Low	GCS	24
2_Integrity_5	6	6	10	22	High	Medium	Low	Autopilot	7,8
2_Confidentiality_1	5	1	6	12	Basic	Medium	Medium	RF	14
2_Confidentiality_2	6	6	10	22	High	Medium	Low	Autopilot	7,8,18
2_Confidentiality_3	6	6	10	22	High	Medium	Low	Autopilot	7,8,18
2_Confidentiality_4	6	3	2	11	Basic	Medium	Medium	GCS	16,24
3_availability_1	6	6	10	22	High	Low	Low	GCS	24
3_availability_2	6	6	10	22	High	Low	Low	GCS	16,24
3_availability_3	6	3	2	11	Basic	Low	Low	GCS	16,24
3_availability_4	6	6	10	22	High	Low	Low	Autopilot	7,8
3_availability_5	4	1	6	11	Basic	Low	Low	3G/4G module	23
3_availability_6	6	8	12	26	Very High	Low	Low	3G/4G module	23
3_availability_7	6	6	10	22	High	Low	Low	Gimbal	21,22
3_Confidentiality_1	6	1	12	19	High	High	Medium	3G/4G module	23
3_Confidentiality_2	6	1	10	17	Moderate	High	Medium	3G/4G module	23
3_Confidentiality_3	6	1	10	17	Moderate	High	Medium	GCS	24
3_Confidentiality_4	6	3	2	11	Basic	High	High	GCS	16
3_integrity_1	6	6	10	22	High	High	Medium	GCS	24

3_integrity_2	6	1	12	19	High	High	Medium	3G/4G module	23
3_integrity_3	6	1	12	19	High	High	Medium	3G/4G module	23
3_integrity_4	6	1	12	19	High	High	Medium	3G/4G module	23

C.4 Attack trees

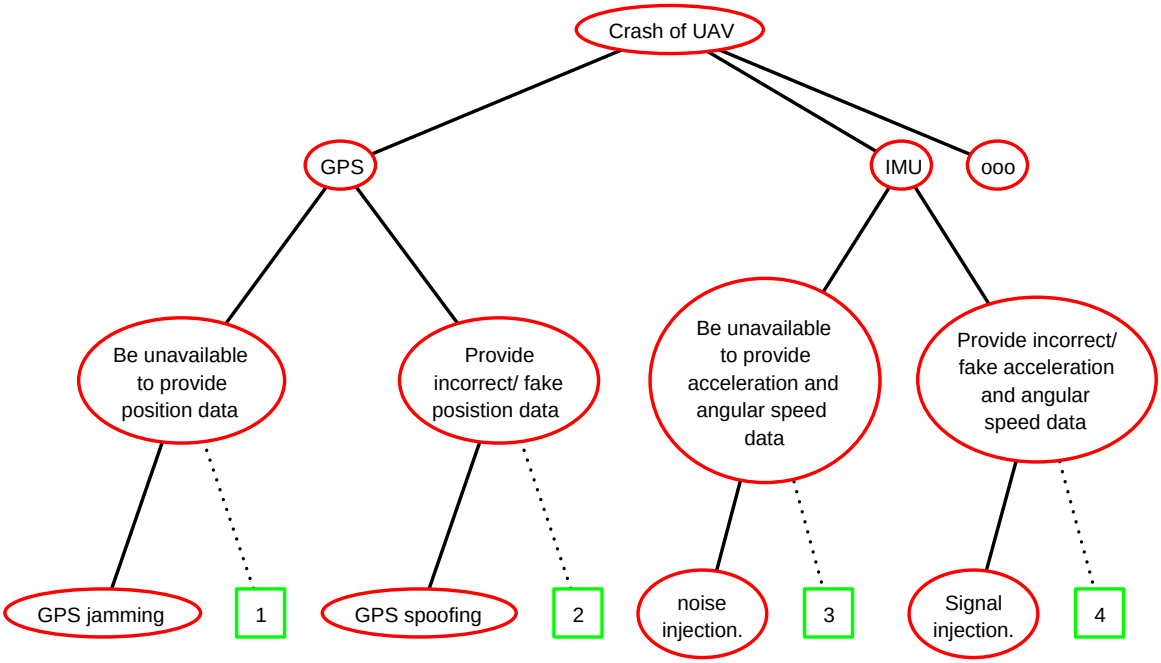


Figure C.1: The attack tree for the 1-availability malfunction - part 1

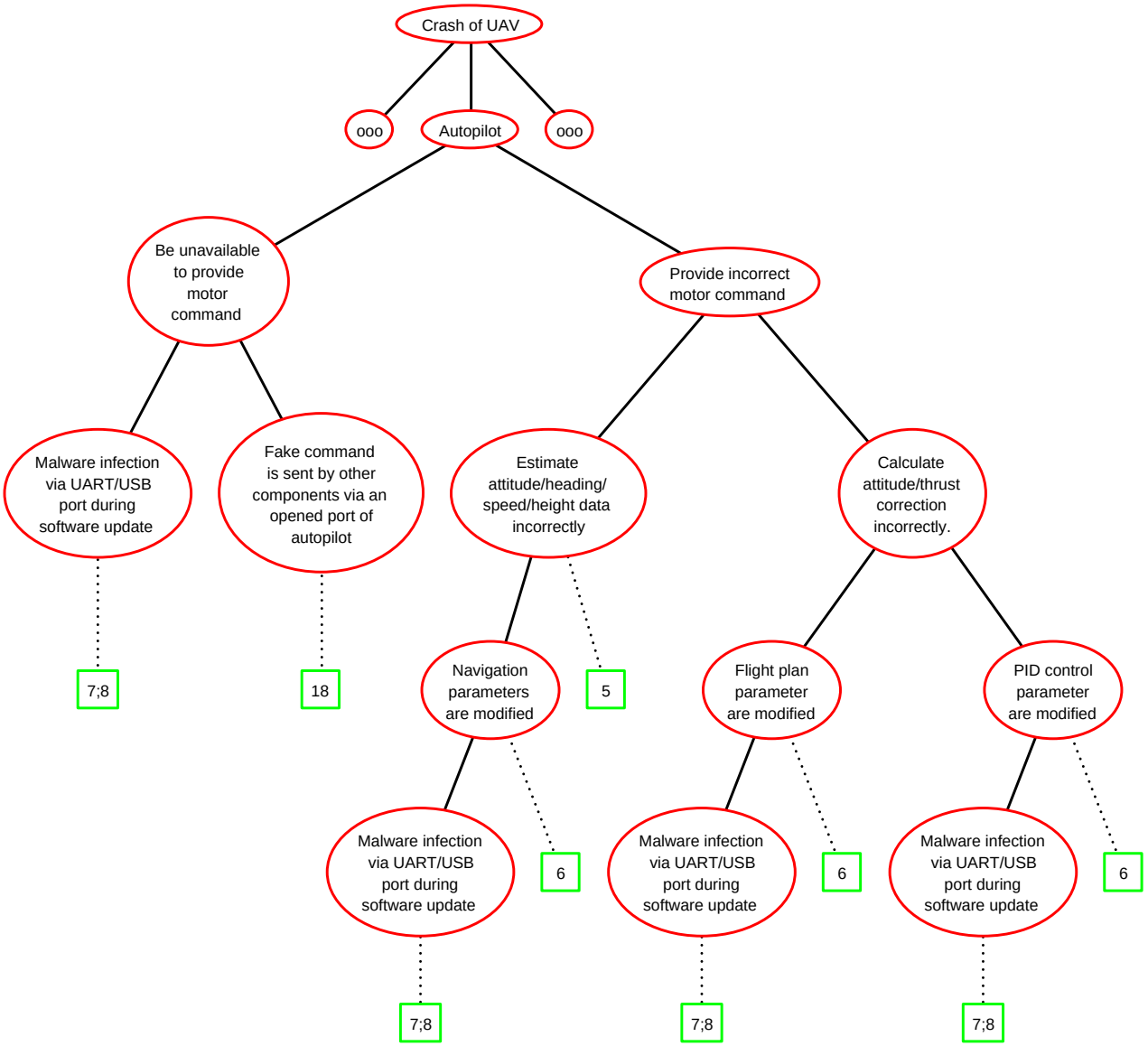


Figure C.2: The attack tree for the 1-availability malfunction - part 2

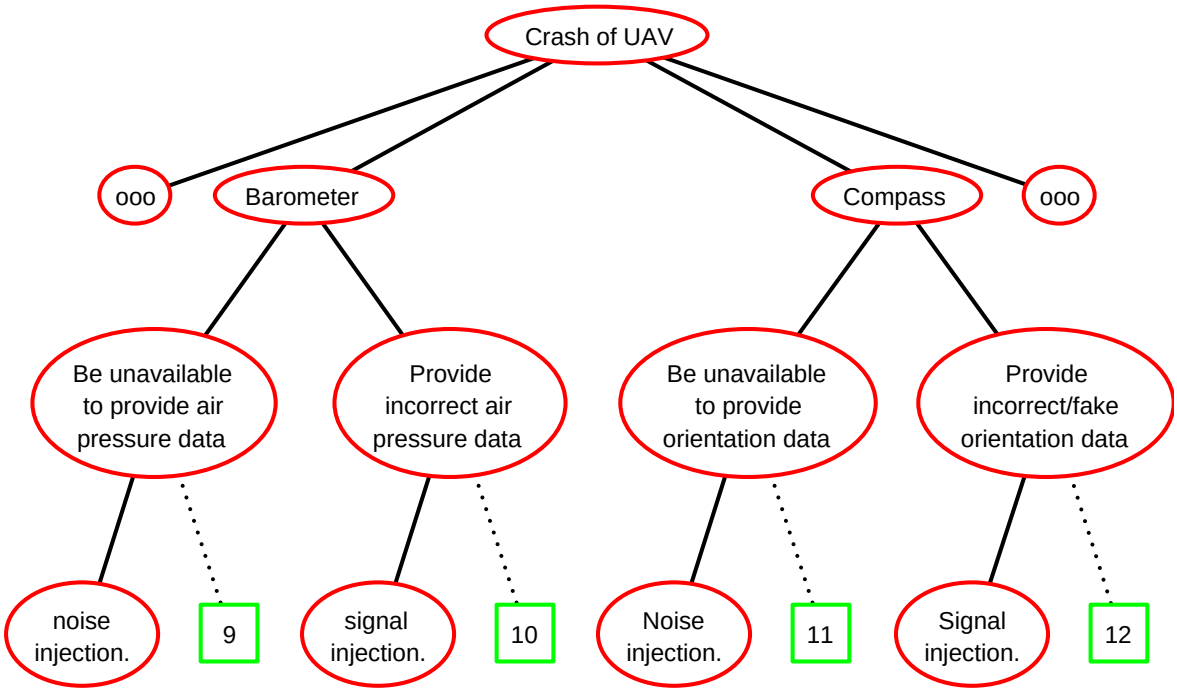


Figure C.3: The attack tree for the 1-availability malfunction - part 3

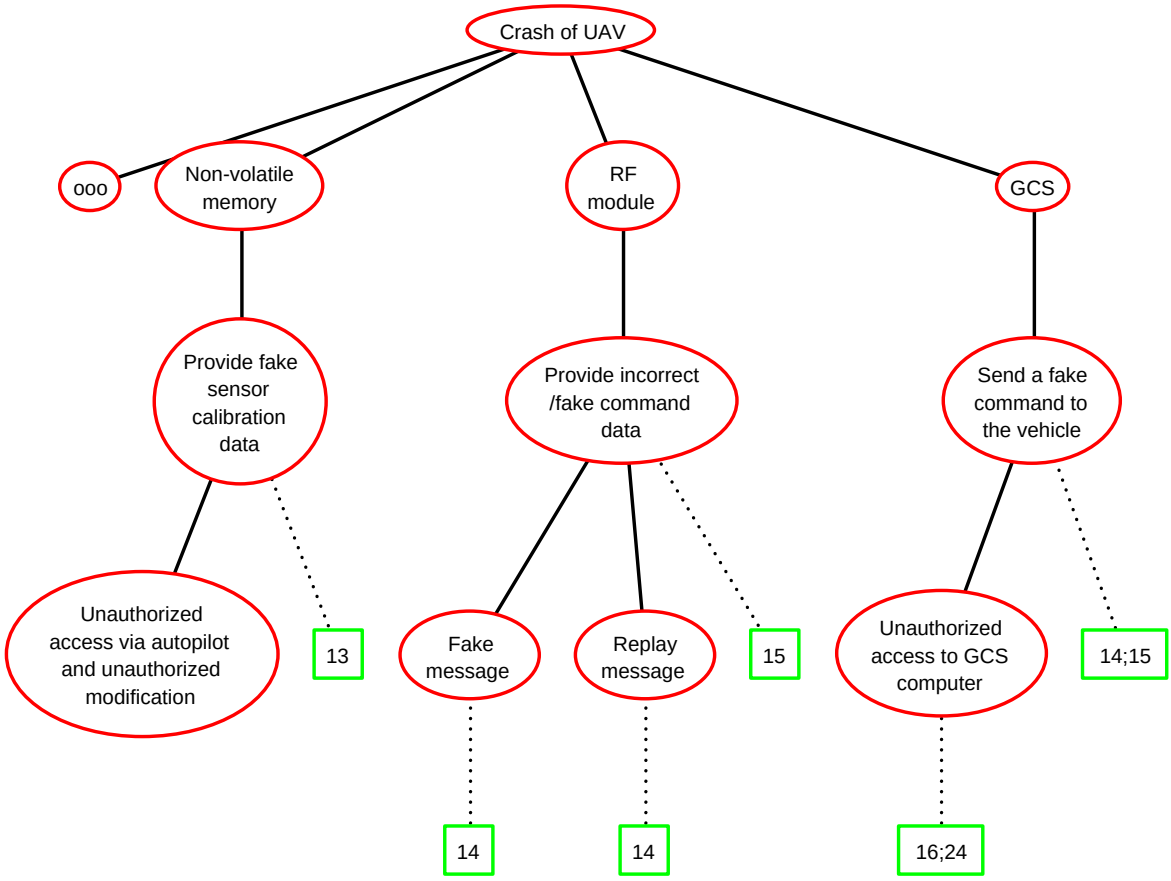


Figure C.4: The attack tree for the 1-availability malfunction - part 4

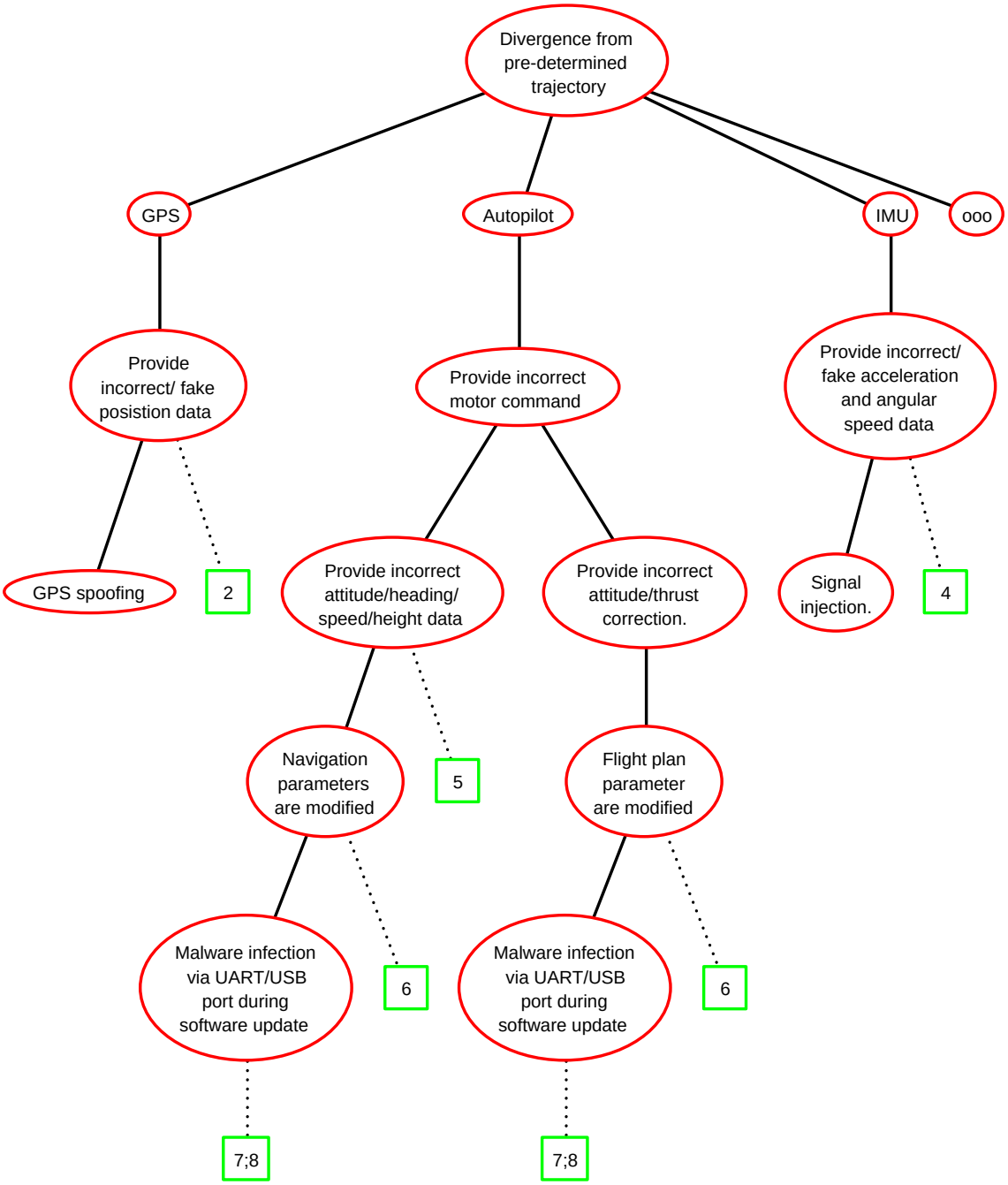


Figure C.5: The attack tree for the 1-integrity malfunction - part 1

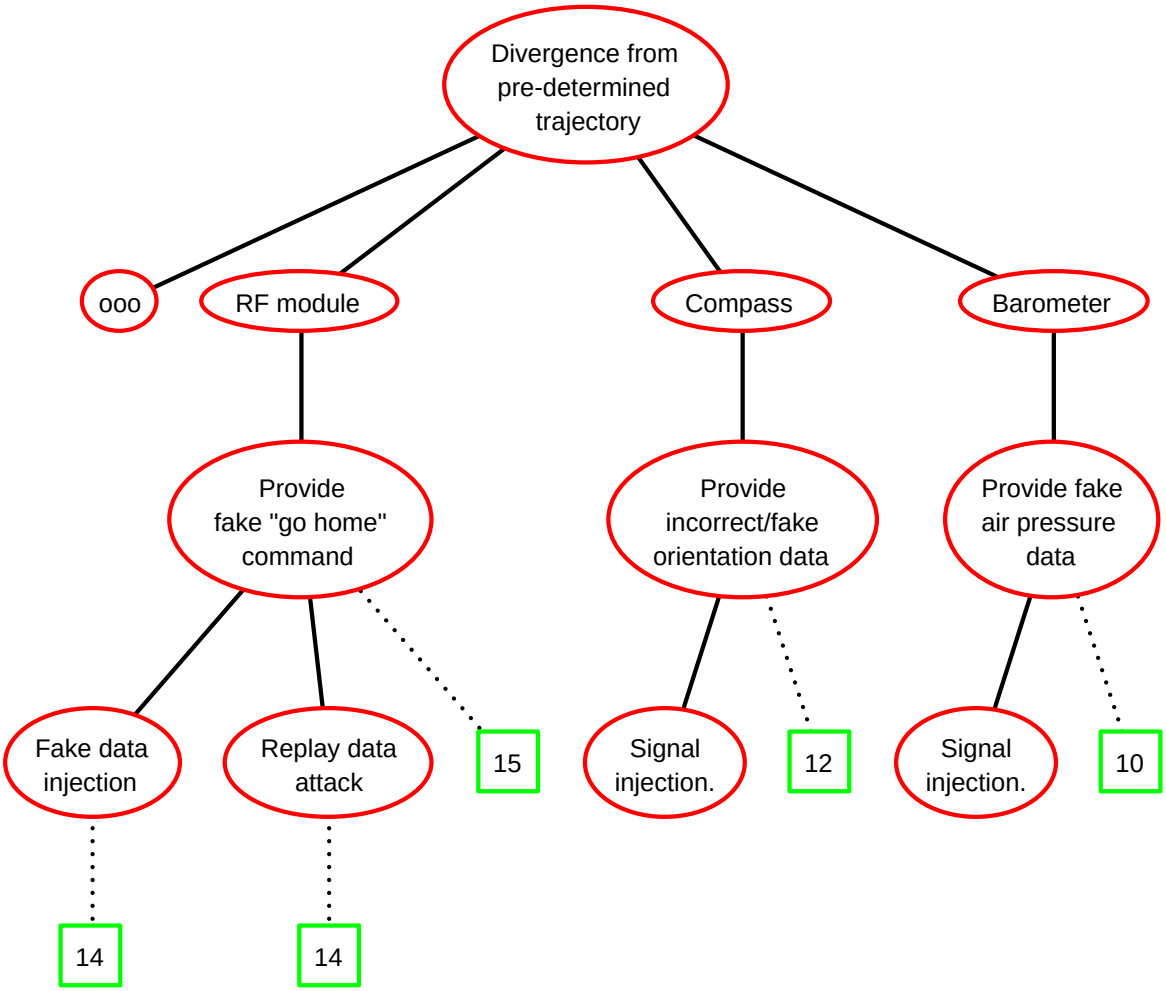


Figure C.6: The attack tree for the 1-integrity malfunction - part 2

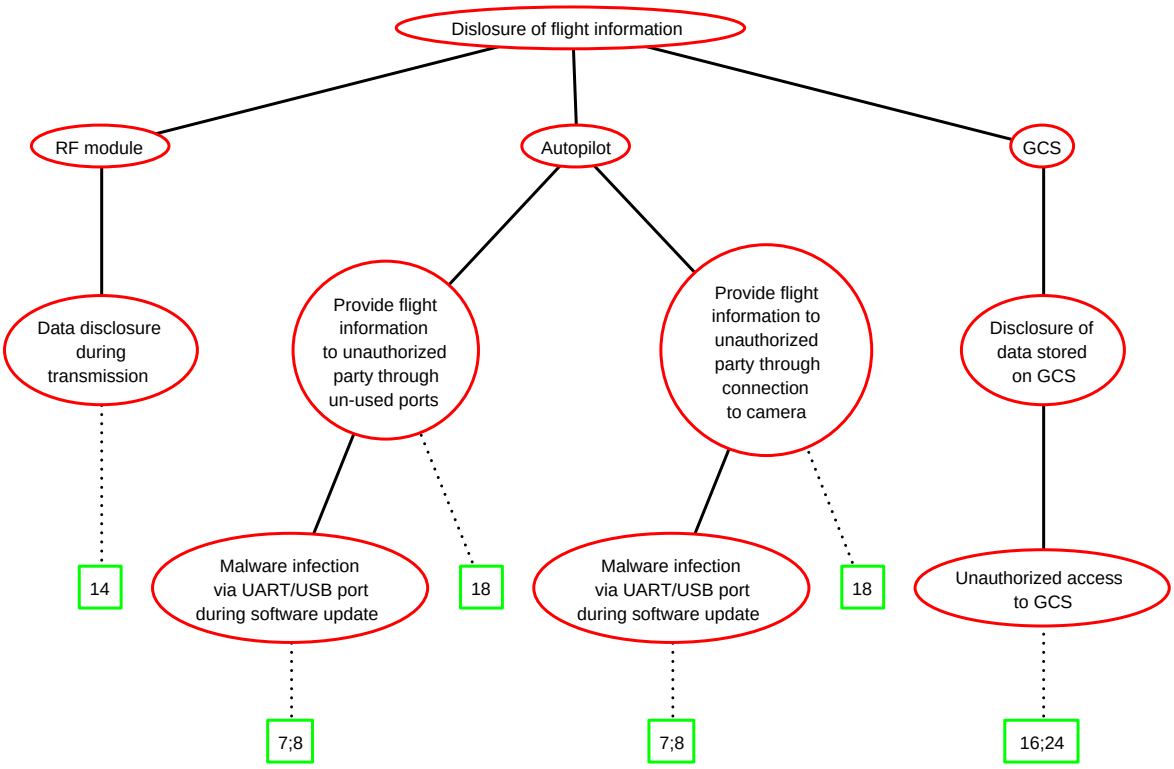


Figure C.7: The attack tree for the 2-confidentiality malfunction

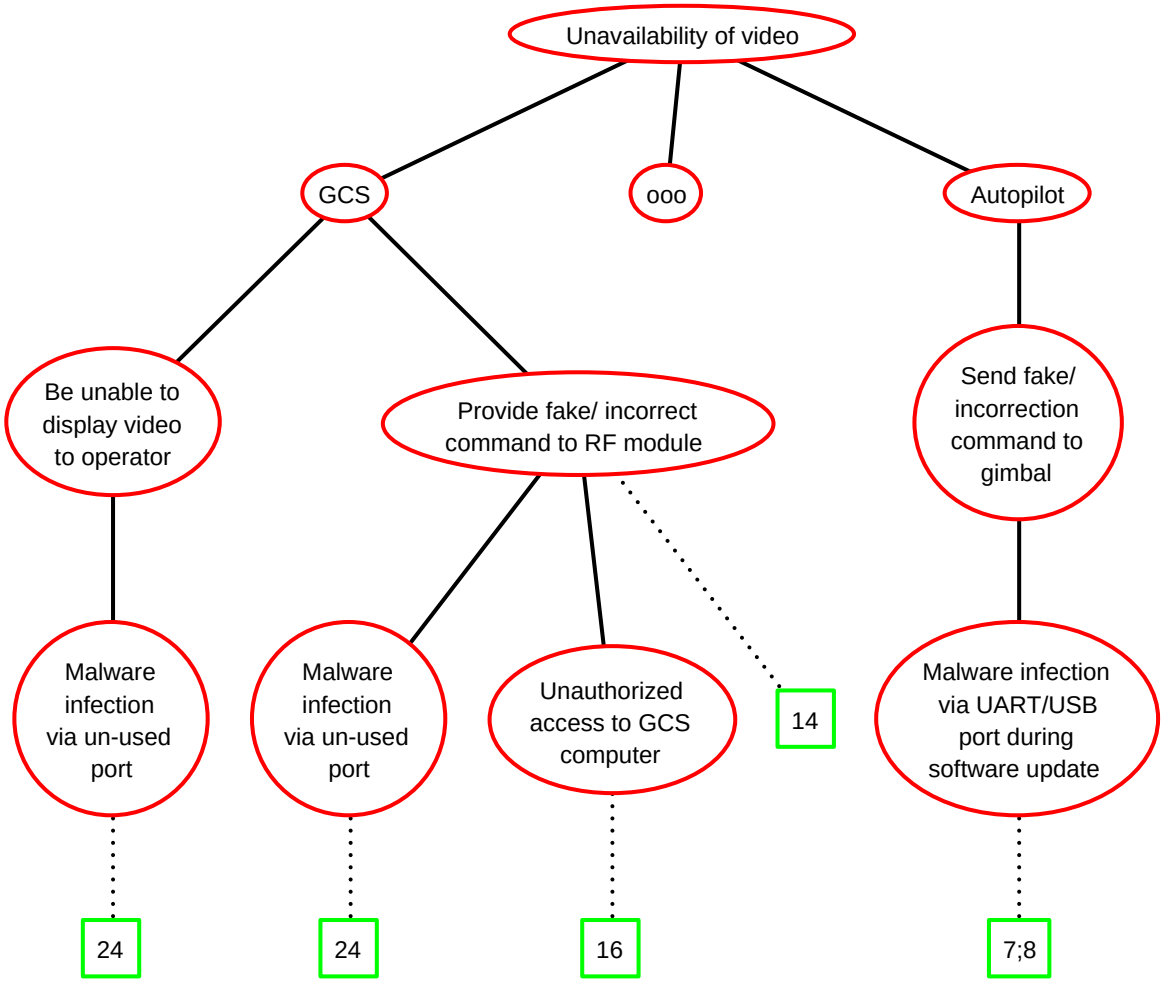


Figure C.8: The attack tree for the 2-confidentiality malfunction - part 1

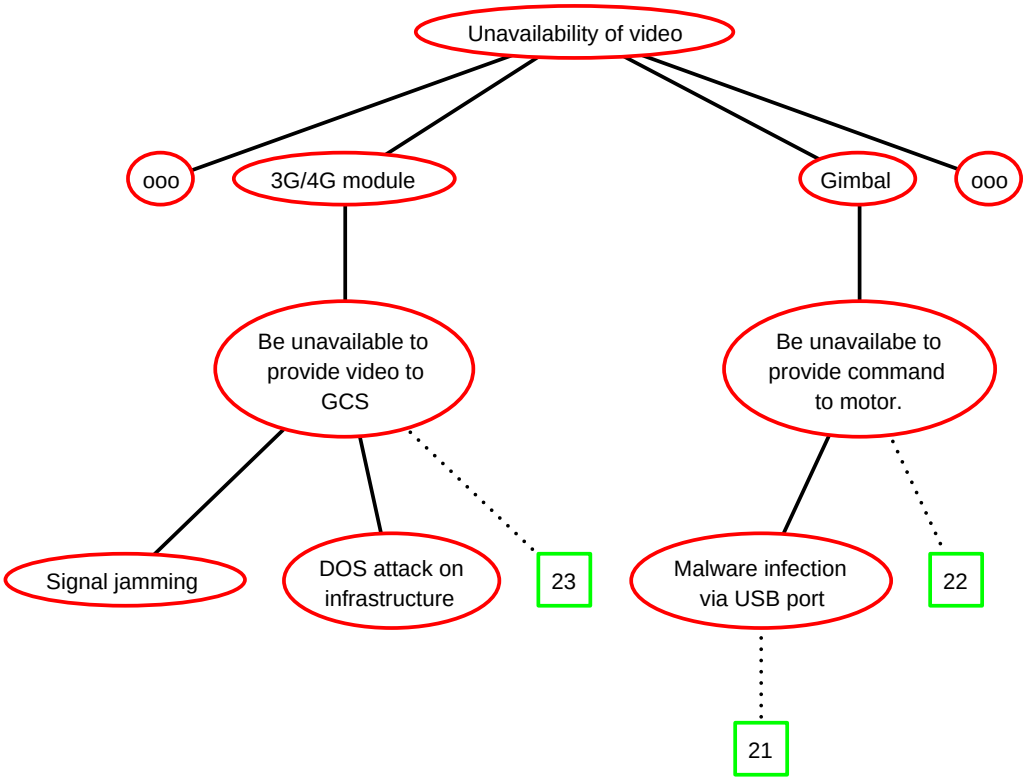


Figure C.9: The attack tree for the 2-confidentiality malfunction - part 2

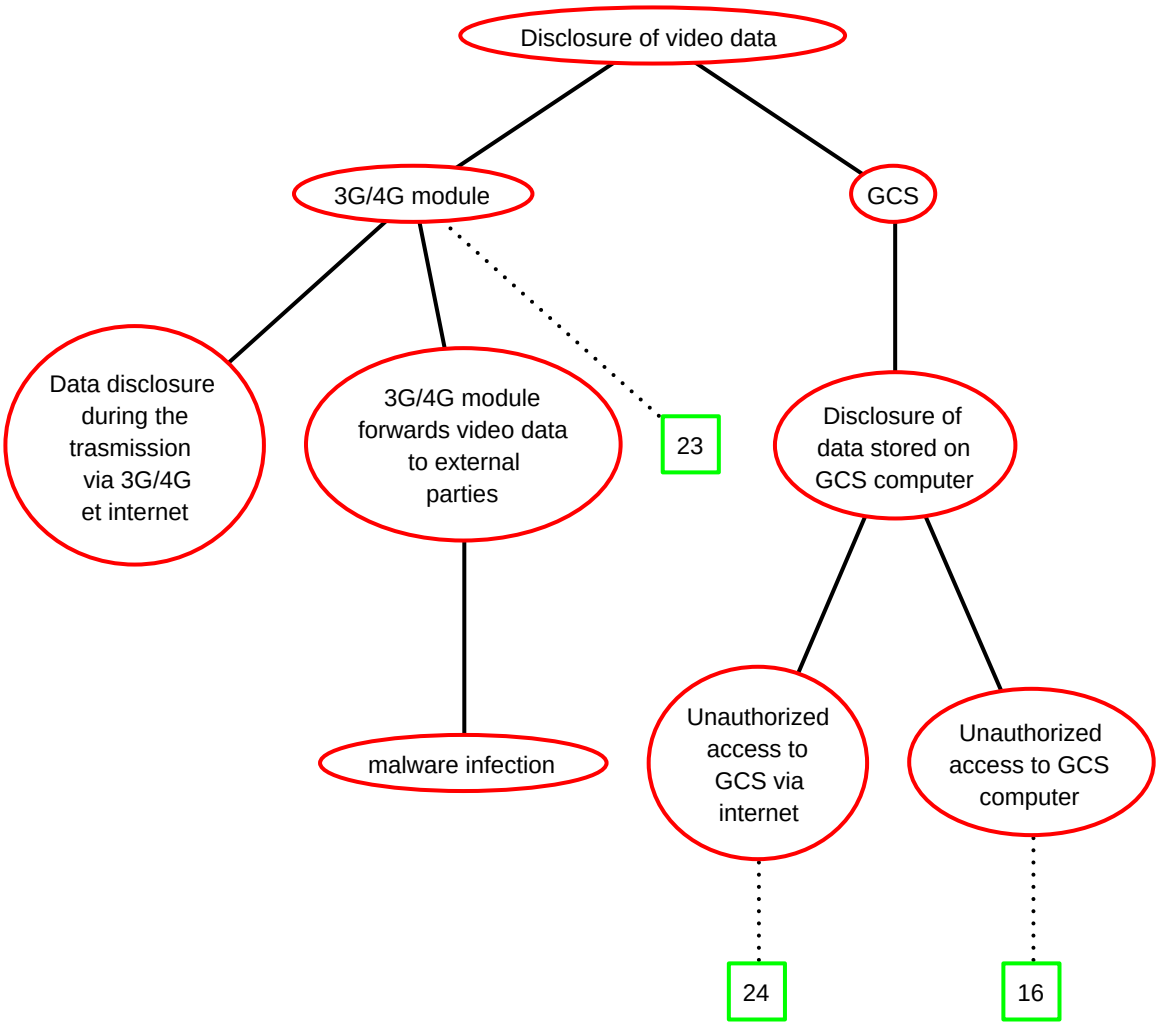


Figure C.10: The attack tree for the 3-confidentiality malfunction

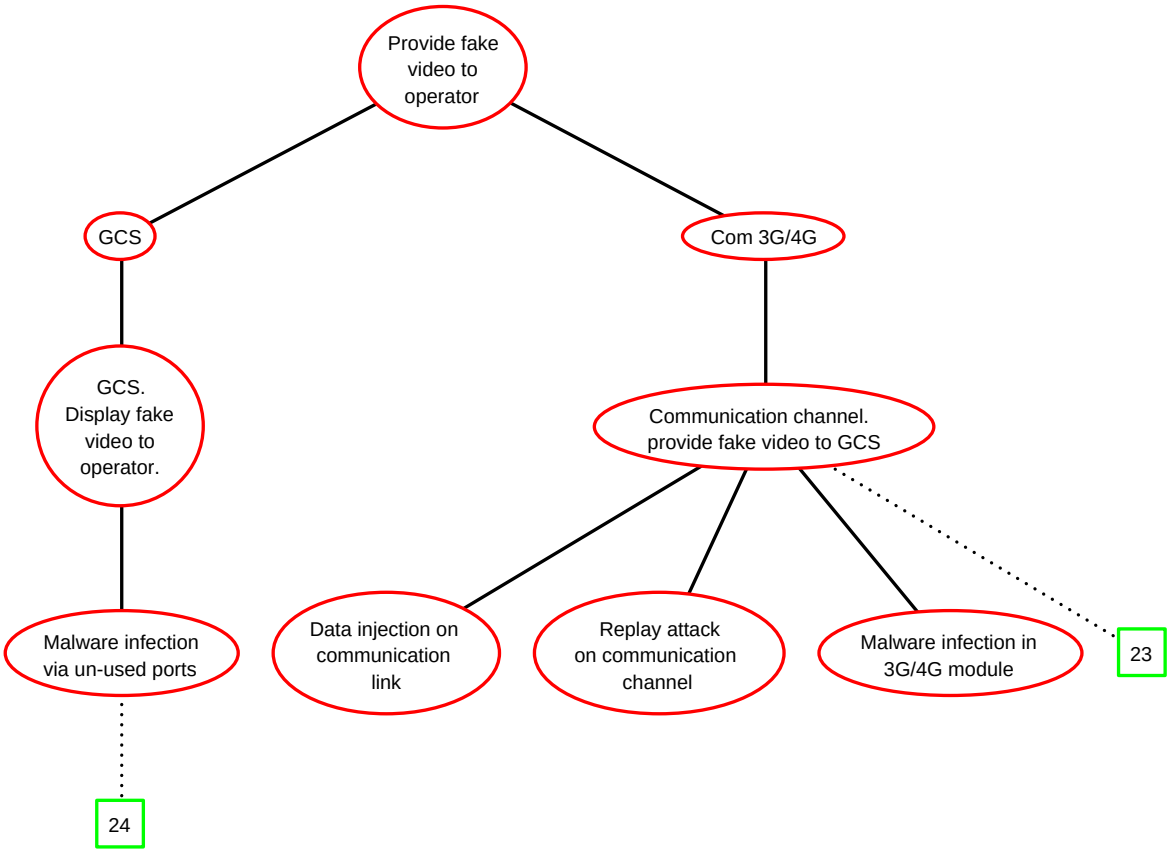


Figure C.11: The attack tree for the 3-integrity malfunction

Appendix D

GPS spoofing and countermeasure

D.1 GPS fundamental

The Global Position System (GPS) is a Global Navigation Satellite System (GNSS) that has been developed and maintained by the US army since 1973 [209]. The GPS satellites provide reference points for which the GPS receivers on the planet could estimate their position. The position estimation bases on the observation of signals transmitted by the satellites. Each GPS satellite broadcasts simultaneously signals on both two carrier frequencies L1 = 1575.42 MHz and L2=1227.6 MHz. The signals are modulated with two kinds of PRN (PseudoRandom Noise) codes: C/A (Coarse/Acquisition) and P (Precision). While the C/A code is opened for the civil application and unique for each satellite, while the P code is encrypted and used for the military application.

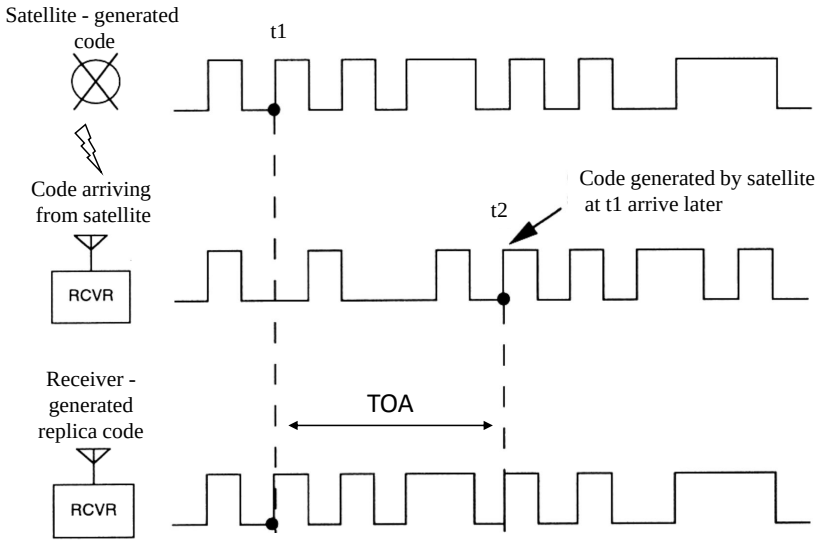


Figure D.1: Time of arrive measurement [210]

Because these satellites fly at precise orbits with stable speed, their positions could be mathematically estimated. Ideally, to determine the position of the receiver on the earth, we need to know the distances from this point to at least three satellites. The distance between the GPS receiver and a GPS satellite is obtained by observing the Time Of Arrival (TOA) of satellite signals. As mentioned, the GPS satellite continuously generates and transmits signals modulated with PRN codes. At the same time, on the earth, the GPS receiver also generates the signal modulated with PRN codes. When receiving the signal from a satellite, the receiver compares the received code with the code generated by itself to determine the TOA (see Figure D.1). Then the satellite-receiver distance is calculated by multiplying the TOA with the radio propagation speed. However, in reality, the calculation presented does not give the real range from the satellite to the receiver but only pseudo-range. The reason is that the receiver clock usually is not strictly synchronized with the ones of satellites. That leads to biases in the TOA estimation and then the range estimation. The relationship between the receiver position and the pseudo-range is presented, as shown in Equation D.1. In this equation, we have four unknown variables (three coordinations and one clock bias). Therefore,

to determine the receiver position, it is required to know pseudo ranges from four satellites instead of three satellites.

$$\rho = \sqrt[2]{(x_s - x_r)^2 + (y_s - y_r)^2 + ((z_s - z_r)^2)} + c * \delta_t \tag{D.1}$$

where:

ρ is pseudo-range from a satellite to the receiver

(x_s, y_s, z_s) is position of the satellite

(x_r, y_r, z_r) is position of the receiver

c is the radio propagation speed

δ_t is the receiver clock bias

D.1.1 Spoofing attack strategies

As the GPS signals for civil applications are not protected, the principle of GPS spoofing attack is to deceive the GPS receive with the fake GPS signal. The strategies for generating fake GPS signals could follow one of the following approaches: GPS signal generator, intermediate receiver based spoofer, and sophisticated receiver-based spoofer [211].

- **GPS signal generator** is the most straightforward approach in which the attacker uses a GPS simulator to generate a fake GPS signal. The signal generated by this technique is usually unsynchronized to the authentic GPS signal. Therefore the fake signals could be detected by different anti-spoofing techniques such as amplitude monitoring, consistency checks among different measurements [212]

- **Receiver based spoofer** is a more advanced approach, in which the spoofer consists of a GPS receiver and a signal transmitter. The spoofer first synchronizes with the authentic GPS signal and extracts the navigation message. Then the spoofer generates the fake signal with the extracted information to the target receiver. This kind of attack is difficult to detect and is more complicated than the first category. The main challenge of this approach is projecting the spoofing signals to the target receiver with the correct signal delay and strength [212].

- **Sophisticated receiver based spoofer** Sophisticated receiver-based spoofer is the most sophisticated and effective technique. It aims to generate the fake signal similar to the authentic one in terms of the carrier phase, signal power, noise at the receiver position. For that purpose, the spoofer has to be capable of precisely tracking the position and the movement of the receiver. Compared with the previous ones, this kind of attack is much more complex and challenging to realize but also difficult to detect [212].

D.2 State of the art of countermeasure

There are many works in the literature, which have proposed different countermeasures to deal with GPS spoofing attacks. This section provides a review of spoofing countermeasures that focus on GPS spoofing detection. There are three main approaches: (1) signal processing, (2) spatial processing, and (3) data processing.

1. **Signal processing**: The principal of GPS spoofing is to deceive GPS receiver by fake signals. Therefore, an approach to detect un attack is signal monitoring. The sudden unreasonable jumps in the signal characteristics (such as carrier amplitude, carrier phase, signal strength, signal power) could reveal an attack [213]. Wen et al. proposed to monitor the Signal to Noise Ratio (SNR) indicator[214]. The proposed technique compares the SNR level of received signals with a predefined threshold to discriminate fake signals. Shepard [215] proposed another technique based on signal power monitoring. Due to the distance between the spoofer and the target receiver, it is difficult to adjust the fake signal with a suitable power level that is high enough to deceive the receiver but lower than the usual strength level of authentic signals. Instead of monitoring a singular characteristic, Jovanovic et al. [216] proposed an algorithm to monitor the statistical properties of many signal characteristics and check for inconsistency.

2. **Spatial processing**: In normal conditions, the GPS receiver will receive the signals transmitted by different satellites. Hence the signal will come to the receiver from different directions. In the case of attacks, the attacker could generate the multi fake versions of different satellite signals and transmits them by using a single antenna. That leads to the spatial correlation of the fake signals. This argument is the principle of several GPS spoofing detection solutions based on spatial characteristics. McDowell [217] and Montgomery et al. [218] deployed a multi-antenna receiver to detect spoofing signals based on monitoring the phase difference between different antenna elements. Instead of a multi-antenna receiver, Nielsen et al. [219] use a moving receiver with a single antenna to form a synthetic antenna array structure, as shown in Figure D.2.

3. **Data processing**: The primary purpose of GPS spoofing is to make the GPS receiver provide incorrect position data. Therefore, it comes naturally to mind that we could look for the abnormality of the receiver's output data to detect the GPS spoofing attack. Most GPS receivers deploy the Receiver Autonomous Integrity Monitoring (RAIM) algorithm to detect and reject outlier measurements. The RAIM algorithm looks for the inconsistent set of five or more pseudo-ranges to detect abnormal measurements. Psiaki et al. [213] argued that this technique could provide a rudimentary defense against unsophisticated spoofers that transmit only one or two fake signals among the authentic signals received by the receiver. For more sophisticated attacks such as the one realized by Humphreys [49], this technique is not practical. To deal with the sophisticated attacks, some researchers look for the solution by looking for the inconsistency between GPS data and other sensors (other sensors). Qiao et al. [220] pproposed a GPS spoofing solution for UAV by using an IMU and a monocular camera. The data fusion applied for

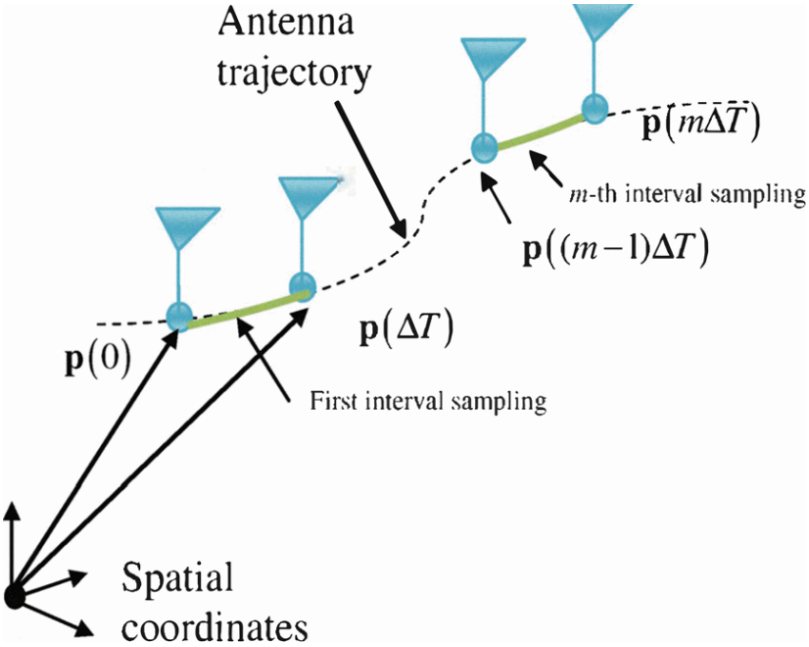


Figure D.2: a synthetic antenna array structure [219]

IMU data, and the camera data allows determining the UAV's velocity. Then, this value is compared with the one obtained from GPS data. This solution could work well when the UAV flies close to the ground. However, at the high altitude, the degradation of the image detail captured by the camera could make this solution less effective. Panice et al. [221] proposed a solution using Support Vector Machine (SVM - a kind of machine learning). This solution requires only the data from the GPS and IMU. The position information obtained from GPS data and the one obtained from IMU data are compared to look for the inconsistency. To estimate the position from IMU measurement, it required integrating acceleration over time. In this operation, the error, however small, is accumulated over time. That leads to the drift effect in position estimation from IMU data. This solution proposed by Panice et al. is not robustness for a long time attack (more than 30 seconds). Feng et al. [222] proposed another solution based on IMU/GPS data analysis. Instead of the UAV position, this solution focus on the acceleration values obtained from IMU data and GPS data. That allows for avoiding the error accumulation effect and makes the result more robust. However, this solution requires calibrating some parameters and thresholds manually, which depends on the nature of UAV.

Summary: In this section, we provided a short review of GPS spoofing detection solutions. We group the proposed solution into three approaches: (1) signal processing, (2) spatial processing, and (3) data processing. The two first approaches require to develop the specific GPS receivers (both hardware and software). Meanwhile, most solutions related to the third approach could be implemented with existing products on the market. Some of them required only to modify the autopilot software.

Appendix E

Operation Safety Objectives in the original SORA methodology

Joint Authorities for Rulemaking of Unmanned Systems

JARUS guidelines on SORA

Annex E

Integrity and assurance levels for the Operation Safety Objectives (OSO)

DOCUMENT IDENTIFIER : JAR-DEL-WG6-D.04

Edition Number	:	**1.0**
Edition Date	:	**25.01.2019**
Status	:	**Final / Public Release**
Intended for	:	**Publication**
Category	:	**Guidelines**
WG	:	**6**

CONTENTS

Annex E:

Integrity and assurance levels for the Operation Safety Objectives (OSO)

1. How to use SORA Annex E

The following table provides the basic principles to consider when using SORA Annex E.

	Principle description	Additional information
#1	Annex E provides assessment criteria for the integrity (i.e. safety gain) and assurance (i.e. method of proof) of Operation Safety Objectives (OSOs) proposed by an applicant.	The identification of Operation Safety Objectives for a given operation, is the responsibility of the applicant.
#2	Annex E does not cover the Level of Involvement (LoI) of the Competent Authority. LoI is based on the Competent Authority assessment of the applicant's ability to perform the given operation.	Some JARUS groups (e.g. WG-7) might provide criteria for level of involvement for use by the Competent Authorities.
#3	To achieve a given level of integrity/assurance, when more than one criterion exists for that level of integrity/assurance, all applicable criteria need to be met.	
#4	"Optional" cases defined in SORA Main Body Table 8 do not need to be defined in terms of integrity and assurance levels in Annex E.	All robustness levels are acceptable for Operation Safety Objectives for which an "optional" level of robustness is defined in Table 6 "Recommended operation safety objectives (OSO)" of the SORA Main Body.
#5	When criteria to assess the level of integrity or assurance of an Operation Safety Objective rely on "standards" not yet available, the OSO needs to be developed in a manner acceptable to the competent authority.	
#6	Annex E intentionally uses non-prescriptive terms (e.g. suitable, reasonably practicable) to provide flexibility to both the applicant and the Competent Authorities. This does not constrain the applicant in proposing mitigations, nor the Competent Authority in evaluating what is needed on a case by case basis.	
#7	This annex in its entirety also applies to single-person organizations.	

2. Technical issue with the UAS

OSO #01 - Ensure the operator is competent and/or proven

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #01 Ensure the operator is competent and/or proven	Criteria	The applicant is knowledgeable of the UAS being used and as a minimum has the following relevant operational procedures: checklists, maintenance, training, responsibilities, and associated duties.	Same as Low. In addition, the applicant has an organization appropriate[1] for the intended operation. Also the applicant has a method to identify, assess, and mitigate risks associated with flight operations. These should be consistent with the nature and extent of the operations specified.	Same as Medium.
	Comments	*N/A*	*[1] For the purpose of this assessment appropriate should be interpreted as commensurate/proportionate with the size of the organization and the complexity of the operation.*	*N/A*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #01 Ensure the operator is competent and/or proven	Criteria	The elements delineated in the level of integrity are addressed in the ConOps.	Prior to the first operation, a competent third party performs an audit of the organization	The applicant holds an Organizational Operating Certificate or has a recognized flight test organization. In addition, a competent third party recurrently verifies the operator competences.
	Comments	*N/A*	*N/A*	*N/A*

OSO #02 - UAS manufactured by competent and/or proven entity

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #02 UAS manufactured by competent and/or proven entity	Criteria	As a minimum, manufacturing procedures cover: • specification of materials • suitability and durability of materials used, • processes necessary to allow for repeatability in manufacturing and conformity within acceptable tolerances.	Same as Low. In addition, manufacturing procedures also cover: • configuration control, • verification of incoming products, parts, materials, and equipment, • identification and traceability, • in-process and final inspections & testing, • control and calibration of tools, • handling and storage, • non-conforming item control.	Same as Medium. In addition, the manufacturing procedures cover at least: • manufacturing processes, • personnel competence and qualification, • supplier control.
	Comments	*N/A*	*N/A*	*N/A*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #02 UAS manufactured by competent and/or proven entity	Criteria	The declared manufacturing procedures are developed to a standard considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.	Same as Low. In addition, evidence is available that the UAS has been manufactured in conformance to its design.	Same as Medium. In addition: • manufacturing procedures, • conformity of the UAS to its design and specification are recurrently verified through process or product audit by a competent third party(ies).
	Comments	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*	*N/A*

OSO #03 - UAS maintained by competent and/or proven entity

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #03 UAS maintained by competent and/or proven entity (e.g. industry standards)	Criteria	• The UAS maintenance instructions are defined and when applicable cover the UAS designer instructions and requirements. • The maintenance staff is competent and has received an authorisation to carry out UAS maintenance. • The maintenance staff use the UAS maintenance instructions while performing maintenance.	Same as Low. In addition: • Scheduled maintenance of each UAS is organised and in accordance with a Maintenance Programme. • Upon completion, the maintenance log system is used to record all maintenance conducted on the UAS including releases. A maintenance release can only be accomplished by a staff member who has received a maintenance release authorisation for that particular UAS model/family.	Same as Medium. In addition, the maintenance staff works in accordance with a maintenance procedure manual that provides information and procedures relevant to the maintenance facility, records, maintenance instructions, release, tools, material, components, defect deferral…
	Comments	*N/A*	*N/A*	*N/A*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #03 UAS maintained by competent and/or proven entity (e.g. industry standards)	Criterion #1 (Procedure)	• The maintenance instructions are documented. • The maintenance conducted on the UAS is recorded in a maintenance log system[1/2]. • A list of maintenance staff authorised to carry out maintenance is established and kept up to date.	Same as Low. In addition: • The Maintenance Programme is developed in accordance with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority[3]. • A list of maintenance staff with maintenance release authorisation is established and kept up to date.	Same as Medium. In addition, the maintenance programme and the maintenance procedures manual are validated by a competent third party.
	Comments	*[1] Objective is to record all the maintenance performed on the aircraft, and why it is performed (defects or malfunctions rectification, modification, scheduled maintenance etc.)* *[2] The maintenance log may be requested for inspection/audit by the approving authority or an authorized representative.*	*[3] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*
	Criterion #2 (Training)	A record of all relevant qualifications, experience and/or trainings completed by the maintenance staff is established and kept up to date.	Same as Low. In addition: • Initial training syllabus and training standard including theoretical/practical elements, duration, etc. is defined and commensurate with the authorisation held by the maintenance staff. • For staff holding a maintenance release authorisation, the initial training is specific to that particular UAS model/family. • All maintenance staff have undergone initial training.	Same as Medium. In addition: • A programme for recurrent training of staff holding a maintenance release authorisation is established; and • This programme is validated by a competent third party.
	Comments	*N/A*	*N/A*	*N/A*

OSO #04 - UAS developed to authority recognized design standards

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #04 UAS developed to authority recognized design standards	Criteria	The UAS is designed to standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. The standards and/or the means of compliance should be applicable to a Low Level of Integrity and the intended operation.	The UAS is designed to standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. The standards and/or the means of compliance should be applicable to a Medium Level of Integrity and the intended operation.	The UAS is designed to standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. The standards and/or the means of compliance should be applicable to a High Level of Integrity and the intended operation.
	Comments	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*		

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #04 UAS developed to authority recognized design standards	Criteria	Consider the criteria defined in section 9		
	Comments	*N/A*	*N/A*	*N/A*

OSO #05 - UAS is designed considering system safety and reliability

(a) This OSO complements:

- The safety requirements for containment defined in the main Body
- OSO #10 and OSO #12, which is only addressing the risk of a fatality while operating over populous areas or gatherings of people.

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #05 UAS is designed considering system safety and reliability	Criteria	The equipment, systems, and installations are designed to minimize hazards[1] in the event of a probable[2] malfunction or failure of the UAS.	Same as Low. In addition, the strategy for detection, alerting and management of any malfunction, failure or combination thereof, which would lead to a hazard is available.	Same as Medium. In addition: • Major Failure Conditions are not more frequent than Remote[3]; • Hazardous Failure Conditions are not more frequent than Extremely Remote[3]; • Catastrophic Failure Conditions are not more frequent than Extremely Improbable[3]; • Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) may cause or contribute to hazardous or catastrophic failure conditions are developed to an industry standard or a methodology considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority[4].
	Comments	*[1] For the purpose of this assessment, the term "hazard" should be interpreted as a failure condition that relates to major, hazardous, or catastrophic.* *[2] For the purpose of this assessment, the term "probable" should be interpreted in a qualitative way as, "Anticipated to occur one or more times during the entire system/operational life of an UAS".*	*N/A*	*[3] Safety objectives may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the UAS class or an equivalent risk-based methodology acceptable to the competent authority.* *[4] Development Assurance Levels (DALs) for SW/AEH may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the UAS class or an equivalent risk-based methodology acceptable to the competent authority.*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #05 UAS is designed considering system safety and reliability	Criteria	A Functional Hazard Assessment[1] and a design and installation appraisal that shows hazards are minimized are available.	Same as Low. In addition: • Safety analyses are conducted in line with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. • A strategy for detection of single failures of concern includes pre-flight checks.	Same as Medium. In addition, safety analyses and development assurance activities are validated by a competent third party.
	Comments	*[1]Severity of failures conditions (No Safety Effect, Minor, Major, Hazardous and Catastrophic) should be determined according to the definitions provided in JARUS AMC RPAS.1309 Issue 2.*	*N/A*	*N/A*

OSO #06 - C3 link characteristics (e.g. performance, spectrum use) are appropriate for the operation

(a) For the purpose of the SORA and this specific OSO, the term "C3 link" encompasses:

- the Command and Control (C2) link, and
- any communication link required for the safety of the flight.

(b) To correctly assess the integrity of this OSO, the applicant should identify:

1) The C3 links performance requirements necessary for the intended operation.
2) All C3 links, together with their actual performance and Radio Frequency (RF) spectrum usage.
   Note: The specification of performance and RF spectrum for a C2 Link is typically documented by the UAS designer in the UAS manual.
   Note: Main parameters associated with C2 link performance (RLP) and the performance parameters for other communication links (e.g. RCP for communication with ATC) include, but are not limited to the following:
   - Transaction expiration time
   - Availability
   - Continuity
   - Integrity

   Refer to ICAO references for definitions.
3) The RF spectrum usage requirements for the intended operation (including the need for authorization if required).
   Note: Usually, countries publish the allocation of RF spectrum bands applicable in their territory. This allocation stems mostly from the International Communication Union (ITU) Radio Regulations. However, the applicant should check the local requirements and request authorization when needed since there may be national differences and specific allocations (e.g. national sub-division of ITU allocations). Some aeronautical bands (e.g. AM(R)S, AMS(R)S 5030-5091MHz) were allocated for potential use in UAS operations under ICAO scope for UAS operations classified as cat. C ("certified"), but their use may be authorized for operations under the specific category. It is expected that the use of other licensed bands (e.g. those allocated to mobile networks) may also be authorized under the specific category. Some un-licensed bands (e.g. ISM (Industrial, Scientific, Medical) or SRD (Short Range Devices)) may also be acceptable under the specific category, for instance for operations with lower integrity requirements.
4) Environmental conditions that might affect the C3 links performance.

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #06 C3 link characteristics (e.g. performance, spectrum use) are appropriate for the operation	Criteria	• The applicant determines that performance, RF spectrum usage[1] and environmental conditions for C3 links are adequate to safely conduct the intended operation. • The UAS remote pilot has the means to continuously monitor the C3 performance and ensures the performance continues to meet the operational requirements[2].	Same as Low[3].	Same as Low. In addition, the use of licensed[4] frequency bands for C2 Link is required.
	Comments	*[1] For a low level of integrity, unlicensed frequency bands might be acceptable under certain conditions, e.g.:* • *the applicant demonstrates compliance with other RF spectrum usage requirements (e.g. for EU: Directive 2014/53/EU, for US: CFR Title 47 Part 15 Federal Communication Commission (FCC) rules), by showing the UAS equipment is compliant with these requirements (e.g. FCC marking), and* • *the use of mechanisms to protect against interference (e.g. FHSS, frequency deconfliction by procedure).* *[2] The remote pilot has continual and timely access to the relevant C3 information that could affect the safety of flight. For operations requesting only a low level of integrity for this OSO, this could be achieved by monitoring the C2 link signal strength and receiving an alert from the UAS HMI if the signal becomes too low.*	*[3] Depending on the operation, the use of licensed frequency bands might be necessary. In some cases, the use of non-aeronautical bands (e.g. licensed bands for cellular network) may be acceptable.*	*[4] This ensures a minimum level of performance and is not limited to aeronautical licensed frequency bands (e.g. licensed bands for cellular network). Nevertheless some operations may require the use of bands allocated to the aeronautical mobile service for the use of C2 Link (e.g. 5030 – 5091 MHz).* *In any case, the use of licensed frequency bands needs authorization.*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #06 C3 link characteristics (e.g. performance, spectrum use) are appropriate for the operation	Criteria	Consider the assurance criteria defined in section 9 (low level of assurance)	Demonstration of the C3 link performance is in accordance with standards considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority.	Same as Medium. In addition, evidence is validated by a competent third party.
	Comments	*N/A*	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*

OSO #07 - Inspection of the UAS (product inspection) to ensure consistency to the ConOps

(a) The intent of this OSO assure the UAS used for the operation conforms to the UAS data used to support the approval/authorization of the operation.

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #07 Inspection of the UAS (product inspection) to ensure consistency to the ConOps	Criteria	The remote crew ensures the UAS is in a condition for safe operation and conforms to the approved concept of operations.[1]		
	Comments	*[1] The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #07 Inspection of the UAS (product inspection) to ensure consistency to the ConOps	Criterion #1 (Procedures)	Product inspection is documented and accounts for the manufacturer's recommendations if available.	Same as Low. In addition, the product inspection is documented using checklists.	Same as Medium. In addition, the product inspection is validated by a competent third party.
	Comments	*N/A*	*N/A*	*N/A*
	Criterion #2 (Training)	The remote crew's is trained to perform the product inspection, and that training is self-declared (with evidence available).	• A training syllabus including a product inspection procedure is available. • The operator provides competency-based, theoretical and practical training.	A competent third party: • Validates the training syllabus. • Verifies the remote crew competencies.
	Comments	*N/A*	*N/A*	*N/A*

3. OSOs related to Operational procedures

OSO #08 - Operational procedures are defined, validated and adhered to (to address technical issues with the UAS)

OSO #11 - Procedures are in-place to handle the deterioration of external systems supporting UAS operation

OSO #14 - Operational procedures are defined, validated and adhered to (to address Human Errors)

OSO #21 - Operational procedures are defined, validated and adhered to (to address Adverse Operating Conditions)

<table>
<tr><th colspan="2" rowspan="2">OPERATIONAL PROCEDURES</th><th colspan="3">LEVEL of INTEGRITY</th></tr>
<tr><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><td rowspan="8">OSO #08, OSO #11, OSO #14 and OSO #21</td><td>Criterion #1 (Procedure definition)</td><td colspan="3">• Operational procedures[1] appropriate for the proposed operation are defined and as a minimum cover the following elements:
○ Flight planning,
○ Pre and post-flight inspections,
○ Procedures to evaluate environmental conditions before and during the mission (i.e. real-time evaluation),
○ Procedures to cope with unintended adverse operating conditions (e.g. when ice is encountered during an operation not approved for icing conditions)
○ Normal procedures,
○ Contingency procedures (to cope with abnormal situations),
○ Emergency procedures (to cope with emergency situations), and
○ Occurrence reporting procedures.
• Normal, Contingency and Emergency procedures are compiled in an Operation Manual.
• The limitations of the external systems supporting UAS operation[2] are defined in an Operation Manual.</td></tr>
<tr><td>Comments</td><td colspan="3">[1]Operational procedures cover the deterioration[3] of the UAS itself and any external system supporting UAS operation.

[2] In the scope of this assessment, external systems supporting UAS operation are defined as systems not already part of the UAS but used to:
• launch / take-off the UAS,
• make pre-flight checks,
• keep the UA within its operational volume (e.g. GNSS, Satellite Systems, Air Traffic Management, UTM).
External systems activated/used after the loss of control of the operation are <u>excluded</u> from this definition.

[3]To properly address deterioration of external systems required for the operation, it is recommended to:
• identify these “external systems”,
• identify the “external systems” deterioration modes (e.g. complete loss of GNSS, drift of the GNSS, latency issues, …) which would lead to a loss of control of the operation,
• describe the means to detect these deterioration modes of the external systems/facilities,
• describe procedure(s) used when deterioration is detected (e.g. activation of the Emergency Recovery Capability, switch to a manual control …).</td></tr>
<tr><td>Criterion #2 (Procedure complexity)</td><td>Operational procedures are complex and may potentially jeopardize the crew ability to respond by raising the remote crew’s workload and/or the interactions with other entities (e.g. ATM…).</td><td>Contingency/emergency procedures require manual control by the remote pilot[2] when the UAS is usually automatically controlled.</td><td>Operational procedures are simple.</td></tr>
<tr><td>Comments</td><td>N/A</td><td>[2] This is still under discussion since not all UAS have a mode where the pilot could directly control the surfaces; moreover, some people claim it requires significant skill not to make things worse.</td><td>N/A</td></tr>
<tr><td>Criterion #3 (Consideration of Potential Human Error)</td><td>At a minimum, operational procedures provide:
• a clear distribution and assignment of tasks
• an internal checklist to ensure staff are adequately performing assigned tasks.</td><td>Operational procedures take human error into consideration.</td><td>Same as Medium. In addition, the Remote Crew[3] receives Crew Resource Management (CRM)[4] training.</td></tr>
<tr><td>Comments</td><td>N/A</td><td>N/A</td><td>[3] In the context of SORA, the term “Remote crew” refers to any person involved in the mission.
[4] CRM training focuses on the effective use of all remote crew to assure a safe and efficient operation, reducing error, avoiding stress and increasing efficiency.</td></tr>
</table>

OPERATIONAL PROCEDURES		LEVEL of ASSURANCE		
		Low	**Medium**	**High**

OSO #08, OSO #11, OSO #14 and OSO #21	Criteria	• Operational procedures do not require validation against either a standard or a means of compliance considered adequate by the competent authority.
		• The adequacy of the operational procedures is declared, except for Emergency Procedures, which are tested.
			• Operational procedures are validated against standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority[1].
			• Adequacy of the Contingency and Emergency procedures is proven through:
			  ○ Dedicated flight tests, or
			  ○ Simulation provided the simulation is proven valid for the intended purpose with positive results.
				Same as Medium. In addition:
				• Flight tests performed to validate the procedures and checklists cover the complete flight envelope or are proven to be conservative.
				• The procedures, checklists, flight tests and simulations are validated by a competent third party.

	Comments	*N/A*	[1] *National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	

4. OSOs related to Remote crew training

OSO #09 - Remote crew trained and current and able to control the abnormal and emergency situations (i.e. Technical issue with the UAS)

OSO #15 - Remote crew trained and current and able to control the abnormal and emergency situations (i.e. Human Error)

OSO #22 - The remote crew is trained to identify critical environmental conditions and to avoid them

(a) The applicant needs to propose competency-based, theoretical and practical training:
- appropriate for the operation to be approved, and
- including proficiency requirements and training recurrences.

(b) The entire remote crew (i.e. any person involved in the operation) should undergo a competency-based, theoretical and practical training specific to their duties (e.g. pre-flight inspection, ground equipment handling, evaluation of the meteorological conditions …).

REMOTE CREW COMPETENCIES		**LEVEL of INTEGRITY**		
		Low	**Medium**	**High**
OSO #09, OSO #15 and OSO #22	Criteria	The competency-based, theoretical and practical training ensures knowledge of: a) UAS regulation b) UAS airspace operating principles c) Airmanship and aviation safety d) Human performance limitations e) Meteorology f) Navigation/Charts g) UA knowledge h) Operating procedures and is adequate for the operation.[1/2]		
	Comments	*[1]The details of the areas to be covered for the different subjects listed above will be provided by JARUS WG1 in 2019.* *[2] The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		

REMOTE CREW COMPETENCIES		**LEVEL of ASSURANCE**		
		Low	**Medium**	**High**
OSO #09, OSO #15 and OSO #22	Criteria	Training is self-declared (with evidence available).	• Training syllabus is available. • The operator provides competency-based, theoretical and practical training.	A competent third party: • Validates the training syllabus. • Verifies the remote crew competencies.
	Comments	*N/A*	*N/A*	*N/A*

5. OSOs related to Safe design

OSO #10 - Safe recovery from technical issue

OSO #12 - The UAS is designed to manage the deterioration of external systems supporting UAS operation

(a) The objective of OSO#10 and OSO#12 is to complement the technical containment safety requirements by addressing the risk of a fatality while operating over populous areas or gatherings of people.

(b) In the scope of this assessment, external systems supporting UAS operation are defined as systems not already part of the UAS but used to:

- launch / take-off the UAS,
- make pre-flight checks,
- keep the UA within its operational volume (e.g. GNSS, Satellite Systems, Air Traffic Management, UTM).

External systems activated/used after the loss of control of the operation are excluded from this definition.

		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #10 & OSO #12	Criteria	When operating over populous areas or gatherings of people, it can be reasonably expected that a fatality will not occur from any probable[1] failure[2] of the UAS or any external system supporting the operation.	When operating over populous areas or gatherings of people: • It can be reasonably expected that a fatality will not occur from any single failure[3] of the UAS or any external system supporting the operation. Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to a failure affecting the operation in such a way that it can be reasonably expected that a fatality will occur are developed to a standard considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority[4].	Same as Medium
	Comments	*[1] For the purpose of this assessment, the term "probable" should be interpreted in a qualitative way as, "Anticipated to occur one or more times during the entire system/operational life of an UAS".* *[2] Some structural or mechanical failures may be excluded from the criterion if it can be shown that these mechanical parts were designed to aviation industry best practices.*	*[3] Some structural or mechanical failures may be excluded from the no-single failure criterion if it can be shown that these mechanical parts were designed to a standard considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority* *[4] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	

		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #10 & OSO #12	Criteria	A design and installation appraisal is available. In particular, this appraisal shows that: • the design and installation features (independence, separation and redundancy) satisfy the low integrity criterion; • particular risks relevant to the ConOps (e.g. hail, ice, snow, electro-magnetic interference…) do not violate the independence claims, if any.	Same as Low. In addition, the level of integrity claimed is substantiated by analysis and/or test data with supporting evidence.	Same as Medium. In addition, a competent third party validates the level of integrity claimed.
	Comments	*N/A*	*N/A*	*N/A*

6. Deterioration of external systems supporting UAS operation

OSO #13 - External services supporting UAS operations are adequate to the operation

For the purpose of the SORA and this specific OSO, the term "External services supporting UAS operations" encompasses any service provider necessary for the safety of the flight , e.g.

- Communication Service Provider (CSP),
- UTM service provider, …

DETERIORATION OF EXTERNAL SYSTEMS SUPPORTING UAS OPERATION BEYOND THE CONTROL OF THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #13 External services supporting UAS operations are adequate to the operation	Criteria	The applicant ensures that the level of performance for any externally provided service necessary for the safety of the flight is adequate for the intended operation. If the externally provided service requires communication between the operator and service provider, the applicant ensures there is effective communication to support the service provisions. Roles and responsibilities between the applicant and the external service provider are defined.		
	Comments	*N/A*	*N/A*	*Requirements for contracting services with Service Provider may be derived from ICAO Standards and Recommended Practices - SARPS (currently under development).*

DETERIORATION OF EXTERNAL SYSTEMS SUPPORTING UAS OPERATION BEYOND THE CONTROL OF THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #13 External services supporting UAS operations are adequate to the operation	Criteria	The applicant declares that the requested level of performance for any externally provided service necessary for the safety of the flight is achieved (without evidence being necessarily available).	The applicant has supporting evidence that the required level of performance for any externally provided service required for safety of the flight can be achieved for the full duration of the mission. This may take the form of a Service-Level Agreement (SLA) or any official commitment that prevails between a service provider and the applicant on relevant aspects of the service (including quality, availability, responsibilities). The applicant has a means to monitor externally provided services which affect flight critical systems and take appropriate actions if real-time performance could lead to the loss of control of the operation.	Same as Medium. In addition: • The evidence of the externally provided service performance is achieved through demonstrations. • A competent third party validates the claimed level of integrity.
	Comments	*N/A*	*N/A*	*N/A*

7. Human Error

OSO #16 - Multi crew coordination

(a) This OSO applies only to those personnel directly involved in the flight operation.

HUMAN ERROR		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #16 Multi crew coordination	Criterion #1 (Procedures)	Procedure(s) to ensure coordination between the crew members and robust and effective communication channels is (are) available and at a minimum cover: • assignment of tasks to the crew, • establishment of step-by-step communications.[1]		
	Comments	*[1] The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		
	Criterion #2 (Training)	Remote Crew training covers multi crew coordination	Same as Low. In addition, the Remote Crew[2] receives Crew Resource Management (CRM)[3] training.	Same as Medium.
	Comments	*N/A*	*[2] In the context of SORA, the term "Remote crew" refers to any person involved in the mission.* *[3] CRM training focuses on the effective use of all remote crew to assure a safe and efficient operation, reducing error, avoiding stress and increasing efficiency.*	*N/A*
	Criterion #3 (Communication devices)	N/A	Communication devices comply with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority[4].	Communication devices are redundant[5] and comply with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority[6].
	Comments	*N/A*	*[4] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*[5] This implies the provision of an extra device to cope with the failure case of the first device.* *[6] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #16 Multi crew coordination	Criterion #1 (Procedures)	• Procedures do not require validation against either a standard or a means of compliance considered adequate by the competent authority. • The adequacy of the procedures and checklists is declared.	• Procedures are validated against standards considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority[1]. • Adequacy of the procedures is proven through: ○ Dedicated flight tests, or ○ Simulation, provided the simulation is proven valid for the intended purpose with positive results.	Same as Medium. In addition: • Flight tests performed to validate the procedures cover the complete flight envelope or are proven to be conservative. • The procedures, flight tests and simulations are validated by a competent third party.
	Comments	*N/A*	*[1] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*
	Criterion #2 (Training)	Training is self-declared (with evidence available)	• Training syllabus is available. • The operator provides competency-based, theoretical and practical training.	A competent third party: • Validates the training syllabus. • Verifies the remote crew competencies.
	Comments	*N/A*	*N/A*	*N/A*

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
	Criterion #3 (Communication devices)	Consider the criteria defined in section 9		
	Comments	*N/A*	*N/A*	*N/A*

OSO #17 - Remote crew is fit to operate

(a) For the purpose of this assessment, the expression "fit to operate" should be interpreted as physically and mentally fit to perform duties and discharge responsibilities safely.

(b) Fatigue and stress are contributory factors to human error. Therefore, to ensure vigilance is maintained at a satisfactory level of safety, consideration may be given to the following:

- Remote Crew duty times;
- Regular breaks;
- Rest periods;
- Handover/Take Over procedures.

HUMAN ERROR		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #17 Remote crew is fit to operate	Criteria	The applicant has a policy defining how the remote crew can declare themselves fit to operate before conducting any operation.	Same as Low. In addition: • Duty, flight duty and resting times for the remote crew are defined by the applicant and adequate for the operation. • The operator defines requirements appropriate for the remote crew to operate the UAS.	Same as Medium. In addition: • The remote crew is medically fit, • A Fatigue Risk Management. System (FRMS) is in place to manage any escalation in duty/flight duty times.
	Comments	*N/A*	*N/A*	*N/A*

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #17 Remote crew is fit to operate	Criteria	• The policy to define how the remote crew declares themselves fit to operate (before an operation) is documented. • The remote crew declaration of fit to operate (before an operation) is based on policy defined by the applicant.	Same as Low. In addition: • Remote crew duty, flight duty and the resting times policy is documented. • Remote crew duty cycles are logged and cover at minimum: ○ when the remote crew member's duty day commences, ○ when the remote crew members are free from duties, ○ resting times within the duty cycle. • There is evidence that the remote crew is fit to operate the UAS.	Same as Medium. In addition: • Medical standards considered adequate by the competent authority and/or means of compliance acceptable to that authority[1] are established and a competent third party verifies the remote crew is medically fit. • A competent third party validates the duty/flight duty times. • If a FRMS is used, it is validated and monitored by a competent third party.
	Comments	*N/A*	*N/A*	*[1] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*

OSO #18 - Automatic protection of the flight envelope from human errors

(a) Unmanned Aircraft (UA) are designed with a flight envelope that describes its safe performance limits with regard to minimum and maximum operating speeds, and operating structural strength.

(b) Automatic protection of the flight envelope is intended to prevent the remote pilot from operating the UA outside its flight envelope. If the applicant demonstrates that the remote-pilot is not in the loop, this OSO is not applicable.

(c) UAS implementing such automatic protection function will ensure the UA is operated within an acceptable flight envelope margin even in the case of incorrect remote-pilot control input (human error).

(d) UAS without automatic protection function are susceptible to incorrect remote-pilot control input (human error) which can result in loss of the UA if the designed performance limits of the aircraft are exceeded.

(e) Failures or development errors of the flight envelope protection are addressed in OSOs #5, #10 and #12.

HUMAN ERROR		**LEVEL of INTEGRITY**		
		Low	**Medium**	**High**
OSO #18 Automatic protection of the flight envelope from human errors	Criteria	The UAS flight control system incorporates automatic protection of the flight envelope to prevent the remote pilot from making any single input under normal operating conditions that would cause the UA to exceed its flight envelope or prevent it from recovering in a timely fashion.	The UAS flight control system incorporates automatic protection of the flight envelope to ensure the UA remains within the flight envelope or ensures a timely recovery to the designed operational flight envelope following remote pilot error(s).[1]	
	Comments	*N/A*	*[1]The distinction between a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*	

HUMAN ERROR		**LEVEL of ASSURANCE**		
		Low	**Medium**	**High**
OSO #18 Automatic protection of the flight envelope from human errors	Criteria	The automatic protection of the flight envelope has been developed in-house or out of the box (e.g. using Component Off The Shelf elements), without following specific standards.	The automatic protection of the flight envelope has been developed to standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.	Same as Medium. In addition, evidence is validated by a competent third party.
	Comments	*N/A*	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*

OSO #19 - Safe recovery from Human Error

(a) This OSO addresses the risk of human errors which may affect the safety of the operation if not prevented or detected and recovered in a timely fashion.
   i) Errors can be from anyone involved in the operation
   ii) An example could be a human error leading to incorrect loading of the payload, with the risk to fall off the UA during the operation.
   iii) Another example could be a human error not to extend the antenna mast, reducing the C2 link coverage.

   Note: the flight envelope protection is excluded from this OSO since it is specifically covered by OSO #18.

(b) This OSO covers:
   i) Procedures and lists,
   ii) Training, and
   iii) UAS design, i.e. systems detecting and/or recovering from human errors (e.g. safety pins, use of acknowledgment features, fuel or energy consumption monitoring functions …)

HUMAN ERROR		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #19 Safe recovery from Human Error	Criterion #1 (Procedures and checklists)	Procedures and checklists that mitigate the risk of potential human errors from any person involved with the mission are defined and used. Procedures provide at a minimum: • a clear distribution and assignment of tasks, • an internal checklist to ensure staff are adequately performing assigned tasks.		
	Comments	*N/A*	*N/A*	*N/A*
	Criterion #2 (Training)	• The Remote Crew[1] is trained to procedures and checklists. • The Remote Crew[1] receives Crew Resource Management (CRM)[2] training.[3]		
	Comments	*[1] In the context of SORA, the term "Remote crew" refers to any person involved in the mission.* *[2] CRM training focuses on the effective use of all remote crew to assure a safe and efficient operation, reducing error, avoiding stress and increasing efficiency.* *[3]The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		
	Criterion #3 (UAS design)	Systems detecting and/or recovering from human errors are developed to industry best practices.	Systems detecting and/or recovering from human errors are developed to standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.	Same as medium.
	Comments	*N/A*	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**

OSO #19 Safe recovery from Human Error	Criterion #1 (Procedures and checklists)	• Procedures and checklists do not require validation against either a standard or a means of compliance considered adequate by the competent authority.
		• The adequacy of the procedures and checklists is declared.
			• Procedures and checklists are validated against standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority[1].
			• Adequacy of the procedures and checklists is proven through:
			  ○ Dedicated flight tests, or
			  ○ Simulation provided the simulation is proven valid for the intended purpose with positive results.
				Same as Medium. In addition:
				• Flight tests performed to validate the procedures and checklists cover the complete flight envelope or are proven to be conservative.
				• The procedures, checklists, flight tests and simulations are validated by a competent third party.

	Comments	*N/A*	*[1] National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*	*N/A*
	Criterion #2 (Training)	Consider the criteria defined for level of assurance of the generic remote crew training OSO (i.e. OSO #09, OSO #15 and OSO #22) corresponding to the SAIL of the operation		

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
	Comments	*N/A*	*N/A*	*N/A*
	Criterion #3 (UAS design)	Consider the criteria defined in section 9		
	Comments	*N/A*	*N/A*	*N/A*

OSO #20 - A Human Factors evaluation has been performed and the Human-Machine Interface (HMI) found appropriate for the mission

HUMAN ERROR		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #20 **A Human Factors evaluation has been performed and the HMI found appropriate for the mission**	Criteria	The UAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation.		
	Comments	If an electronic means is used to support potential Visual Observers in their role to maintain awareness of the position of the unmanned aircraft, its HMI: • is sufficient to allow the Visual Observers to determine the position of the UA during operation; • does not degrade the Visual Observer's ability to: ○ scan the airspace visually where the unmanned aircraft is operating for any potential collision hazard; and ○ maintain effective communication with the remote pilot at all times.		

HUMAN ERROR		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #20 **A Human Factors evaluation has been performed and the HMI found appropriate for the mission**	Criteria	The applicant conducts a human factors evaluation of the UAS to determine if the HMI is appropriate for the mission. The HMI evaluation is based on inspection or Analyses.	Same as Low but the HMI evaluation is based on demonstrations or simulations.[1]	Same as Medium. In addition, a competent third party witnesses the HMI evaluation.
	Comments	*N/A*	*[1] When simulation is used, the validity of the targeted environment used in the simulation needs to be justified.*	*N/A*

8. Adverse Operating Conditions

OSO #23 - Environmental conditions for safe operations defined, measurable and adhered to

ADVERSE OPERATING CONDITIONS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #23 Environmental conditions for safe operations defined, measurable and adhered to	Criterion #1 (Definition)	Environmental conditions for safe operations are defined and reflected in the flight manual or equivalent document.[1]		
	Comments	*[1]The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		
	Criterion #2 (Procedures)	Procedures to evaluate environmental conditions before and during the mission (i.e. real-time evaluation) are available and include assessment of meteorological conditions (METAR, TAFOR, etc.) with a simple recording system.[2]		
	Comments	*[2]The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		
	Criterion #3 (Training)	Training covers assessment of meteorological conditions.[3]		
	Comments	*[3]The distinction between a low, a medium and a high level of robustness for this criterion is achieved through the level of assurance (see table below).*		

ADVERSE OPERATING CONDITIONS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #23 Environmental conditions for safe operations defined, measurable and adhered to	Criterion #1 (Definition)	Consider the criteria defined in section 9		
	Comments	*N/A*		

	Criterion #2 (Procedures)	• Procedures do not require validation against either a standard or a means of compliance considered adequate by the competent authority.
		• The adequacy of the procedures and checklists is declared.
			• Procedures are validated against standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.
			• The adequacy of the procedures is proved through:
			  ○ Dedicated flight tests, or
			  ○ Simulation provided the simulation is proven valid for the intended purpose with positive results.
				Same as Medium. In addition:
				• Flight tests performed to validate the procedures cover the complete flight envelope or are proven to be conservative.
				• The procedures, flight tests and simulations are validated by a competent third party.

	Comments	*N/A*	*N/A*	*N/A*
	Criterion #3 (Training)	Training is self-declared (with evidence available).	• Training syllabus is available. • The operator provides competency-based, theoretical and practical training.	A competent third party: • Validates the training syllabus. • Verifies the remote crew competencies.
	Comments	*N/A*	*N/A*	*N/A*

OSO #24 - UAS designed and qualified for adverse environmental conditions (e.g. adequate sensors, DO-160 qualification)

(a) To assess the integrity of this OSO, the applicant determines:

- Can credit be taken for the equipment environmental qualification tests / declarations, e.g. by answering the following questions:
  i. *Is there a Declaration of Design and Performance (DDP) available to the applicant stating the environmental qualification levels to which the equipment was tested?*
  ii. *Did the environmental qualification tests follow a standard considered adequate by the competent authority (e.g. DO-160)?*
  iii. *Are the environmental qualification tests appropriate and sufficient to cover all environmental conditions related to the ConOps?*
  iv. *If the tests were not performed following a recognized standard, were the test performed by an organisation/entity being qualified or having experience in performing DO-160 like tests?*
- Can the suitability of the equipment for the intended/expected UAS environmental conditions be determined from either in-service experience or relevant test results?
- Any limitations which would affect the suitability of the equipment for the intended/expected UAS environment conditions.

(b) The lowest integrity level should be considered for those cases where a UAS equipment has only a partial environmental qualification and/or a partial demonstration by similarity and/or parts with no qualification at all.

ADVERSE OPERATING CONDITIONS		**LEVEL of INTEGRITY**		
		N/A	**Medium**	**High**
OSO #24 UAS designed and qualified for adverse environmental conditions	Criteria	N/A	The UAS is designed to limit the effect of environmental conditions.	The UAS is designed using environmental standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority.
	Comments	*N/A*	*N/A*	*National Aviation Authorities (NAAs) may define the standards and/or the means of compliance they consider adequate. The SORA Annex E will be updated at a later point in time with a list of adequate standards based on the feedback provided by the NAAs.*

ADVERSE OPERATING CONDITIONS		**LEVEL of ASSURANCE**		
		N/A	**Medium**	**High**
OSO #24 UAS designed and qualified for adverse environmental conditions	Criteria	N/A	Consider the criteria defined in section 9	
	Comments	*N/A*	*N/A*	

9. Assurance level criteria for technical OSO

		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
TECHNICAL OSO	Criteria	The applicant declares that the required level of integrity has been achieved[1].	The applicant has supporting evidence that the required level of integrity is achieved. This is typically done by testing, analysis, simulation[2], inspection, design review or through operational experience.	A competent third party validates the claimed level of integrity.
	Comments	*[1] Supporting evidence may or may not be available*	*[2] When simulation is used, the validity of the targeted environment used in the simulation needs to be justified.*	*N/A*

Bibliography

[1] W. Moskwa, "World Drone Market Seen Nearing $127 Billion in 2020, PwC Says," *Bloomberg*, 2016 (cit. on pp. 1, 9, 10).

[2] E. Yağdereli, C. Gemci, and A. Z. Aktaş, "A study on cyber-security of autonomous and unmanned vehicles," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 369–381, 2015 (cit. on pp. 1, 15, 75).

[3] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, IEEE, 2017, pp. 194–199 (cit. on pp. 1, 75).

[4] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," en, in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, IEEE, Sep. 2016, pp. 216–221 (cit. on pp. 1, 4, 16, 75).

[5] W. Chen, Z. Duan, and Y. Dong, "False data injection on EKF-based navigation control," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2017, pp. 1608–1617 (cit. on p. 1).

[6] *Unmanned Aircraft Systems (UAS)*, International Civil Aviation Organization (ICAO), 2011 (cit. on pp. 4, 7).

[7] A. Zolich, T. A. Johansen, K. Cisek, and K. Klausen, "Unmanned aerial system architecture for maritime missions. Design & Hardware description," in *2015 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, IEEE, 2015, pp. 342–350 (cit. on pp. 4, 5, 7, 8).

[8] S. G. Gupta, D. Ghonge, P. M. Jawandhiya, *et al.*, "Review of unmanned aircraft system (UAS)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume*, vol. 2, 2013 (cit. on pp. 4, 5).

[9] P. Rudol, "Increasing autonomy of unmanned aircraft systems through the use of imaging sensors," Ph.D. dissertation, Linköping University Electronic Press, 2011 (cit. on p. 4).

[10] K. Nonami, F. Kendoul, S. Suzuki, W. Wang, and D. Nakazawa, *Autonomous flying robots: unmanned aerial vehicles and micro aerial vehicles*. Springer Science & Business Media, 2010 (cit. on p. 5).

[11] Z. Liu, D. Theilliol, L. Yang, Y. He, and J. Han, "Transition control of tilt rotor unmanned aerial vehicle based on multi-model adaptive method," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2017, pp. 560–566 (cit. on p. 5).

[12] B. Lee, P. Park, C. Kim, S. Yang, and S. Ahn, "Power managements of a hybrid electric propulsion system for UAVs," *Journal of mechanical science and technology*, vol. 26, no. 8, pp. 2291–2299, 2012 (cit. on p. 5).

[13] T. H. Bradley, B. A. Moffitt, D. N. Mavris, and D. E. Parekh, "Development and experimental characterization of a fuel cell powered aircraft," *Journal of Power sources*, vol. 171, no. 2, pp. 793–801, 2007 (cit. on p. 5).

[14] A. Gong, J. L. Palmer, G. Brian, J. R. Harvey, and D. Verstraete, "Performance of a hybrid, fuel-cell-based power system during simulated small unmanned aircraft missions," *International Journal of Hydrogen Energy*, vol. 41, no. 26, pp. 11 418–11 426, 2016 (cit. on p. 5).

[15] H González-Jorge, M Bueno, J Martínez-Sánchez, and P Arias, "Low-Altitude Long-Endurance Solar Unmanned Plane for Forest Fire Prevention: Application to the Natural Park of Serra do Xures (spain)," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 42, p. 135, 2017 (cit. on p. 5).

[16] P. Oettershagen, A. Melzer, T. Mantel, K. Rudin, T. Stastny, B. Wawrzacz, T. Hinzmann, K. Alexis, and R. Siegwart, "Perpetual flight with a small solar-powered UAV: Flight results, performance analysis and model validation," in *2016 IEEE Aerospace Conference*, IEEE, 2016, pp. 1–8 (cit. on p. 5).

[17] E. Baskaya, G. Manfredi, M. Bronz, and D. Delahaye, "Flexible open architecture for UASs integration into the airspace: Paparazzi autopilot system," in *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, IEEE, 2016, pp. 1–7 (cit. on p. 6).

[18] M Bryson and S Sukkarieh, "UAV Localization Using Inertial Sensors and Satellite Positioning Systems," in *Handbook of Unmanned Aerial Vehicles*, Springer, 2015, pp. 433–460 (cit. on p. 6).

[19] L. Mejias, J. Lai, and T. Bruggemann, "Sensors for missions," in *Handbook of Unmanned Aerial Vehicles*, Springer, 2015, pp. 385–399 (cit. on p. 6).

[20] M. S. Grewal, L. R. Weill, and A. P. Andrews, *Global positioning systems, inertial navigation, and integration*. John Wiley & Sons, 2007 (cit. on p. 6).

[21] D. Dusha and L. Mejias, "Error analysis and attitude observability of a monocular GPS/visual odometry integrated navigation filter," *The International Journal of Robotics Research*, vol. 31, no. 6, pp. 714–737, 2012 (cit. on p. 6).

[22] J. R. G. Braga, H. F. de Campos Velho, and E. H. Shiguemori, "Lidar and non-extensive particle filter for uav autonomous navigation," in *Computational Intelligence in Emerging Technologies for Engineering Applications*, Springer, 2020, pp. 227–238 (cit. on p. 6).

[23] N. Hallermann and G. Morgenthal, "From aerial photography to 3-dimensional inspection of bridges," in *Proceedings in the IABSE Conference*, 2016, pp. 8–11 (cit. on p. 7).

[24] I. Colomina and P. Molina, "Unmanned aerial systems for photogrammetry and remote sensing: A review," *ISPRS Journal of photogrammetry and remote sensing*, vol. 92, pp. 79–97, 2014 (cit. on p. 7).

[25] S. Kim and J. Irizarry, "Human performance in UAS operations in construction and infrastructure environments," *Journal of Management in Engineering*, vol. 35, no. 6, p. 04 019 026, 2019 (cit. on p. 7).

[26] S. W. Chen, G. V. Nardari, E. S. Lee, C. Qu, X. Liu, R. A. F. Romero, and V. Kumar, "Sloam: Semantic lidar odometry and mapping for forest inventory," *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 612–619, 2020 (cit. on p. 7).

[27] Y. Guo, *Lidar-based mapping method, device and system*, US Patent 10,578,742, Mar. 2020 (cit. on p. 7).

[28] R. Kestur, S. Omkar, and S Subhash, "Unmanned aerial system technologies for pesticide spraying," in *Innovative Pest Management Approaches for the 21st Century*, Springer, 2020, pp. 47–60 (cit. on p. 7).

[29] Y. A. Pederi and H. S. Cheporniuk, "Unmanned aerial vehicles and new technological methods of monitoring and crop protection in precision agriculture," in *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, 2015, pp. 298–301 (cit. on p. 7).

[30] H. Okcu, "Operational requirements of unmanned aircraft systems data link and communication systems," *Journal of Advances in Computer Networks*, vol. 4, no. 1, pp. 28–32, 2016 (cit. on p. 8).

[31] A Klimkowska, I Lee, and K Choi, "Possibilities of UAS for maritime monitoring," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 41, p. 885, 2016 (cit. on p. 8).

[32] *European Drones Outlook Study: Unlocking the value for Europe*, Single European Sky Atm Research Joint Undertaking (SESAR), Nov. 2016 (cit. on pp. 8, 10).

[33] F. Giones and A. Brem, "From toys to tools: The co-evolution of technological and entrepreneurial developments in the drone industry," *Business Horizons*, vol. 60, no. 6, pp. 875–884, 2017 (cit. on pp. 9, 10).

[34] G. Thibault and G. Aoude, "Companies are turning drones into a competitive advantage," *Harvard Business Review*, 2016 (cit. on p. 9).

[35] F. Veroustraete, "The rise of the drones in agriculture," *EC agriculture*, vol. 2, no. 2, pp. 325–327, 2015 (cit. on p. 9).

[36] M. Kulbacki, J. Segen, W. Knieć, R. Klempous, K. Kluwak, J. Nikodem, J. Kulbacka, and A. Serester, "Survey of drones for agriculture automation from planting to harvest," in *2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES)*, IEEE, 2018, pp. 000 353–000 358 (cit. on p. 9).

[37] K. Ghaffarzadeh, "Agricultural robots and drones 2017-2027: Technologies, markets, players," IDTechEx, Tech. Rep., 2017 (cit. on p. 9).

[38] *Drones in the energy industry*, Drone Industry Insights, Dec. 2018 (cit. on p. 9).

[39] *Drone market size and forecast 2019-2024*, Drone Industry Insights, Mar. 2019 (cit. on p. 10).

[40] *Drones market research report - forecast 2028*, Market Research Future, Jul. 2018 (cit. on p. 10).

[41] *Commercial drones in 2022*, Interact Analysis (cit. on p. 10).

[42] M. Huttunen, "The u-space concept," *Reprinted from Air & Space Law*, vol. 44, no. 1, pp. 69–89, 2019 (cit. on pp. 10, 11, 14).

[43] E. Baskaya, "Fault detection and diagnosis for drones using machine learning," Ph.D. dissertation, ENAC - Ecole Nationale de l'Aviation Civile, 2019 (cit. on p. 11).

[44] *Notice of Proposed Amendment 2017-05: Introduction of a regulatory framework for the operation of drones*, European Union Aviation Safety Agency, May 2017 (cit. on p. 11).

[45] J Kamienski and J Semanek, "ATC perspectives of UAS integration in controlled airspace," *Procedia Manufacturing*, vol. 3, pp. 1046–1051, 2015 (cit. on p. 11).

[46] *Notice of Proposed Amendment 2015-10: Introduction of a regulatory framework for the operation of drones*, European Union Aviation Safety Agency, Oct. 2015 (cit. on p. 11).

[47] *U-space: Blueprint*, SESAR Joint Undertaking, 2017 (cit. on pp. 13, 14).

[48] A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Spoofing countermeasure for GNSS receivers-a review of current and future research trends," *European Space Agency*, vol. 4, p. 6, 2013 (cit. on p. 15).

[49] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012 (cit. on pp. 15, 75, 154).

[50] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57–65, 2015 (cit. on pp. 15, 75).

[51] S. Yunmok, S. Hocheol, K. Dongkwan, P. Youngseok, N. Juhwan, C. Kibum, C. Jungwoo, and K. Yongdae, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th USENIX Security Symposium (USENIX Security 15)*, Washington, D.C.: USENIX Association, 2015, pp. 881–896 (cit. on pp. 15, 75).

[52] C.-Y. Lu, P. Guo, L.-H. Feng, A.-Y. Yang, J.-Y. Wang, and C.-Y. Xing, "An intentional acoustic interference approach to control output signals of MEMS gyroscope based on short-time Fourier analysis," in *2019 20th International Conference on Electronic Packaging Technology (ICEPT)*, IEEE, 2019, pp. 1–4 (cit. on pp. 15, 75).

[53] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *2017 IEEE European symposium on security and privacy (EuroS&P)*, IEEE, 2017, pp. 3–18 (cit. on pp. 15, 75).

[54] Z. Tu, F. Fei, M. Eagon, D. Xu, and X. Deng, "Flight recovery of mavs with compromised imu," *arXiv preprint arXiv:1812.00063*, 2018 (cit. on p. 15).

[55] M. Crispoltoni, M. L. Fravolini, F. Balzano, S. D'Urso, and M. R. Napolitano, "Interval fuzzy model for robust aircraft IMU sensors fault detection," *Sensors*, vol. 18, no. 8, p. 2488, 2018 (cit. on p. 16).

[56] A. A. Yaseen and M. Bayart, "Cyber-attack detection in the networked control system with faulty plant," in *2017 25th Mediterranean Conference on Control and Automation (MED)*, IEEE, 2017, pp. 980–985 (cit. on p. 16).

[57] G. Fournier, P. Audren De Kerdrel, P. Cotret, and V. Viet Triem Tong, "DroneJack: Kiss your drones goodbye!" In *SSTIC 2017 - Symposium sur la sécurité des technologies de l'information et des communications*, Rennes, France, Jun. 2017, pp. 1–8 (cit. on pp. 16, 75).

[58] *Mavlink developer guide*, Online (cit. on p. 16).

[59] J. A. Marty, "Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft," Air force institute of technology, Tech. Rep., 2013 (cit. on p. 16).

[60] C. Stracquodaine, A. Dolgikh, M. Davis, and V. Skormin, "Unmanned aerial system security using real-time autopilot software analysis," in *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, 2016, pp. 830–839 (cit. on p. 16).

[61] M. Heiges, R. Bever, and K. Carnahan, "How to Safely Flight Test a UAV Subject to Cyber-Attacks," Georgia Tech Research Institute, Tech. Rep., 2015 (cit. on pp. 16, 75).

[62] S. Nas, "The definitions of safety and security," *Journal of ETA Maritime Science*, vol. 3, no. 2, pp. 53–54, 2015 (cit. on p. 20).

[63] A. Burns, J. McDermid, and J Dobson, "On the meaning of safety and security," *The Computer Journal*, vol. 35, no. 1, pp. 3–15, 1992 (cit. on p. 20).

[64] *Glossary of Terms*, Version 1, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Jun. 2017 (cit. on p. 20).

[65] Y. Li and F. W. Guldenmund, "Safety management systems: A broad overview of the literature," *Safety science*, vol. 103, pp. 94–123, 2018 (cit. on p. 20).

[66] *ISO/IEC 27032: 2012–Information technology—Security techniques—Guidelines for cybersecurity*, International Organization for Standardization, International Electrotechnical Commission, ISO/IEC Geneva, 2012 (cit. on p. 20).

[67] David Kleidermacher, Mike Kleidermacher and Mike Kleidermacher, *Embedded system security*. Newes, 2012 (cit. on p. 20).

[68] L. Piètre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," *Reliability Engineering & System Safety*, vol. 110, pp. 110–126, 2013 (cit. on pp. 20, 24–26, 40).

[69] D Delves, "International Atomic Energy Agency. IAEA safety glossary: terminology used in nuclear safety and radiation protection. 2007," *Vienna: International Atomic Energy Agency*, p. 227, 2007 (cit. on pp. 20, 22).

[70] L. Piètre-Cambacédès and C. Chaudet, "The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 2, pp. 55–66, 2010 (cit. on p. 20).

[71] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015 (cit. on p. 20).

[72] C. Raspotnig and A. Opdahl, "Comparing risk identification techniques for safety and security requirements," *Journal of Systems and Software*, vol. 86, no. 4, pp. 1124–1151, 2013 (cit. on p. 20).

[73] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security Application of Failure Mode and Effect Analysis (FMEA)," en, in *Computer Safety, Reliability, and Security*, A. Bondavalli and F. Di Giandomenico, Eds., vol. 8666, Springer International Publishing, 2014, pp. 310–325 (cit. on pp. 20, 41).

[74] D. R. Steve Kremer Ludovic Mé and V. Roca, "Cybersecurity - Current challenges and Inria's research directions," INRIA, Tech. Rep., 2019 (cit. on p. 20).

[75] *Guidelines for Development of Civil Aircraft and Systems - ARP4754*, SAE International Group (cit. on pp. 22, 26).

[76] *Ccps process safety glossary*, Centre for Chemical Process Safety (cit. on p. 22).

[77] *ISO 14971:2019 Medical devices — Application of risk management to medical device*, The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (cit. on p. 22).

[78] R Ask, R Røisli, S Johnsen, M Line, A Ueland, B Hovland, L Groteide, B Birkeland, A Steinbakk, E Hagelsteen, *et al.*, *Information security baseline requirements for process control, safety and support ict systems. isbr, olf104 (2006)* (cit. on p. 22).

[79] R. Kissel, "Glossary of key information security terms," en, National Institute of Standards and Technology, Tech. Rep. NIST IR 7298r2, May 2013 (cit. on p. 22).

[80] *ISO/IEC 27000 glossary standard*, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). (cit. on p. 22).

[81] R. Shirey, "Internet security glossary, version 2," RFC 4949, August, Tech. Rep., 2007 (cit. on p. 22).

[82] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011 (cit. on p. 23).

[83] M. Kabir-Querrec, "Cyber security of smart-grid control systems: intrusion detection in IEC 61850 communication networks," Ph.D. dissertation, Université Grenoble Alpes, 2017 (cit. on pp. 23, 25, 28).

[84] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, *Fault Tree Handbook with Aerospace Applications*. nasa Washington, DC, 2002 (cit. on p. 23).

[85] *Iso/guide 73:2009 risk management — vocabulary*, the International Organization for Standardization (ISO) (cit. on p. 23).

[86] F. Khan, S. Rathnayaka, and S. Ahmed, "Methods and models in process safety and risk management: Past, present and future," *Process safety and environmental protection*, vol. 98, pp. 116–147, 2015 (cit. on pp. 23, 32).

[87] P. Kobes, "Zoom sur la norme internationale IEC 62443 pour la cybersécurité des systèmes numériques industriels," in *Cybersécurité des installations industrielles*, Cépaduès, 2016 (cit. on pp. 23, 39).

[88] J. Mcdonald, N. Oualha, A. Puccetti, A. Hecker, and F. Planchon, "Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations," in *2013 IEEE Grenoble Conference*, IEEE, 2013, pp. 1–6 (cit. on p. 25).

[89] V. Agrawal, "A framework for the information classification in ISO 27005 standard," in *2017 ieee 4th international conference on cyber security and cloud computing (cscloud)*, IEEE, 2017, pp. 264–269 (cit. on p. 25).

[90] S. Ariyani and M. Sudarma, "Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System," *vol*, vol. 6, pp. 1–6, 2016 (cit. on pp. 25, 27).

[91] R. A. Clothier and R. A. Walker, "Safety Risk Management of Unmanned Aircraft Systems," *Handbook of unmanned aerial vehicles*, pp. 2229–2275, 2015 (cit. on p. 25).

[92] J. Jalouneix, P. Cousinou, J. Couturier, and D. Winter, "Approche comparative entre sûreté et sécurité nucléaires," *Rapport Technique*, vol. 117, 2009 (cit. on pp. 25, 26).

[93] C. A. Ericson *et al.*, *Hazard analysis techniques for system safety*. John Wiley & Sons, 2015 (cit. on pp. 25, 32, 34, 36–38).

[94] *DO-326a/ED-202a:AIRWORTHINESS SECURITY PROCESS SPECIFICATION*, EUROCAE, Jun. 2014 (cit. on p. 25).

[95] D. Vasseur, *Risques industriels: complexité, incertitude et décision: une approche interdisciplinaire*. Tec & doc-Lavoisier, 2006 (cit. on p. 26).

[96] S. Tom, D. Christiansen, and D. Berrett, "Recommended practice for patch management of control systems," Idaho National Laboratory (INL), Tech. Rep., 2008 (cit. on p. 26).

[97] *Manuel de référence des service de sécurité*, CLUSIF, 30 rue Pierre Sémard, 75009 Paris, France, 2010 (cit. on p. 26).

[98] *Annex E of SORA - integrity and assurance levels for the Operation Safety Objectives (oso)*, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Jan. 2019 (cit. on pp. 26, 66, 92, 95).

[99] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003 (cit. on p. 26).

[100] R. Bell, "Introduction to IEC 61508," in *ACM International Conference Proceeding Series*, vol. 162, 2006, pp. 3–12 (cit. on p. 27).

[101] *Functional safety essential to overall safety - an introduction to functional safety and the iec 61508 series*, International Electrotechnical Commission (IEC), 2015 (cit. on p. 27).

[102] S. ARP4761, "Guidelines and methods for conducting the safety assessment process on airborne systems and equipments," *USA: The Engineering Society for Advancing Mobility Land Sea Air and Space*, 1996 (cit. on p. 27).

[103] *JARUS guidelines on Specific Operations Risk Assessment (SORA)*, Version 1, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Jun. 2017 (cit. on pp. 27, 62, 64, 66, 67, 69).

[104] *Jarus guidelines on Specific Operations Risk Assessment (SORA)*, Version 2, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Oct. 2019 (cit. on pp. 27, 62, 66, 86, 87).

[105] B. Leander, A. Čaušević, and H. Hansson, "Applicability of the IEC 62443 standard in Industry 4.0/IIoT," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–8 (cit. on p. 28).

[106] *Airworthiness security process specification ed-202 / do-326*, EUROCAE, 102 rue Etienne Dolet, 92240 MALAKOFF, France, Jun. 2014 (cit. on p. 28).

[107] J. P. Jouas, J. L. Roule, D. Buc, O. Corbier, M. Gagné, M. Hazzan, G. Molines, C. Pineault, L. Poulin, P. Sasseville, C. Jolivet, and M. Touboul, *MEHARI Overview*, Club de la sécurité de l'information français (CLUSIF), Apr. 2010 (cit. on p. 28).

[108] *Guide de développement d'une base de connaissances d'analyse de risque de MEHARI*, Club de la sécurité de l'information français(CLUSIF), 11 Rue de Mogador, 75009 Paris, 2011 (cit. on p. 28).

[109] E. Kelling, M. Friedewald, T. Leimbach, M. Menzel, P. Säger, H. Seudié, and B. Weyl, "Specification and evaluation of e-security relevant use cases," E-safety vehicle intrusion protected applications project, Tech. Rep., Dec. 2009 (cit. on p. 28).

[110] S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, F. Andreas, G. Sigrid, H. Olaf, R. Roland, R. Matthias, B. Henrik, A. Ludovic, P. Renaud, P. Gabriel, R. Alastair, W. David, and W. Benjamin, "Security requirements for automotive on-board networks based on dark-side scenarios," EVITA, Tech. Rep., 2009 (cit. on p. 28).

[111] *Training Guide: Hazard & Operability Analysis (HAZOP)*, Product Quality Research Institute, May 2015 (cit. on p. 29).

[112] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (hazop) analysis. a literature review," *Journal of hazardous materials*, vol. 173, no. 1-3, pp. 19–32, 2010 (cit. on p. 29).

[113] D. P. Nolan, *Safety and security review for the process industries: Application of HAZOP, PHA, what-if and SVA reviews*. William Andrew, 2011 (cit. on p. 29).

[114] M. Sallak, C. Simon, and J.-F. Aubry, "A fuzzy probabilistic approach for determining safety integrity level," *IEEE Transactions on Fuzzy Systems*, vol. 16, no. 1, pp. 239–248, 2008 (cit. on pp. 29–32).

[115] A. E. Summers, "Techniques for assigning a target safety integrity level," *ISA transactions*, vol. 37, no. 2, pp. 95–104, 1998 (cit. on pp. 30, 31).

[116] A. A. Baig, R. Ruzli, and A. B. Buang, "Reliability analysis using fault tree analysis: A review," *International Journal of Chemical Engineering and Applications*, vol. 4, no. 3, p. 169, 2013 (cit. on p. 32).

[117] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Transactions on reliability*, vol. 41, no. 3, pp. 363–377, 1992 (cit. on p. 33).

[118] H. Boudali, A. Nijmeijer, and M. I. Stoelinga, "Dftsim: A simulation tool for extended dynamic fault trees," in *Proceedings of the 2009 Spring Simulation Multiconference*, Citeseer, 2009, pp. 1–8 (cit. on p. 33).

[119] G. Merle, J.-M. Roussel, and J.-J. Lesage, "Quantitative analysis of dynamic fault trees based on the structure function," *Quality and Reliability Engineering International*, vol. 30, no. 1, pp. 143–156, 2014 (cit. on p. 33).

[120] G. Merle, J.-M. Roussel, J.-J. Lesage, V. Perchet, and N. Vayatis, "Quantitative analysis of dynamic fault trees based on the coupling of structure functions and monte carlo simulation," *Quality and Reliability Engineering International*, vol. 32, no. 1, pp. 7–18, 2016 (cit. on p. 33).

[121] H. Tanaka, L. Fan, F. Lai, and K Toguchi, "Fault-tree analysis by fuzzy probability," *IEEE Transactions on reliability*, vol. 32, no. 5, pp. 453–457, 1983 (cit. on p. 33).

[122] U. Hauptmanns, "Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges," *Journal of Loss Prevention in the Process Industries*, vol. 17, no. 5, pp. 339–345, 2004 (cit. on p. 33).

[123] R. Ferdous, F. Khan, B. Veitch, and P. R. Amyotte, "Methodology for computer aided fuzzy fault tree analysis," *Process safety and environmental protection*, vol. 87, no. 4, pp. 217–226, 2009 (cit. on p. 33).

[124] M. Yazdi, F. Nikfar, and M. Nasrabadi, "Failure probability analysis by employing fuzzy fault tree analysis," *International Journal of System Assurance Engineering and Management*, vol. 8, no. 2, pp. 1177–1193, 2017 (cit. on p. 33).

[125] J Andrews, "Tutorial fault tree analysis," in *Proceeding of the 16th International System Safety Conference, Loughborough*, 1998 (cit. on p. 33).

[126] J. D. Andrews and S. J. Dunnett, "Event-tree analysis using binary decision diagrams," *IEEE Transactions on Reliability*, vol. 49, no. 2, pp. 230–238, 2000 (cit. on p. 34).

[127] *Reactor safety study: An assessment of accident risks in US commercial nuclear power plants*, US Nuclear Regulatory Commission, 1975 (cit. on p. 34).

[128] A. de Ruijter and F. Guldenmund, "The bowtie method: A review," *Safety science*, vol. 88, pp. 211–218, 2016 (cit. on pp. 35, 36).

[129] S. Sklet, "Safety barriers: Definition, classification, and performance," *Journal of loss prevention in the process industries*, vol. 19, no. 5, pp. 494–506, 2006 (cit. on p. 35).

[130] A. Badreddine, T. B. Romdhane, M. A. B. HajKacem, and N. B. Amor, "A new multi-objectives approach to implement preventive and protective barriers in bow tie diagram," *Journal of Loss Prevention in the Process Industries*, vol. 32, pp. 238–253, 2014 (cit. on p. 36).

[131] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, "Handling and updating uncertain information in bow-tie analysis," *Journal of Loss Prevention in the Process Industries*, vol. 25, no. 1, pp. 8–19, 2012 (cit. on p. 36).

[132] O. Salvi and B. Debray, "A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive," *Journal of hazardous materials*, vol. 130, no. 3, pp. 187–199, 2006 (cit. on p. 36).

[133] C. Jacinto and C. Silva, "A semi-quantitative assessment of occupational risks using bow-tie representation," *Safety Science*, vol. 48, no. 8, pp. 973–979, 2010 (cit. on p. 36).

[134] N. Paltrinieri, F. Khan, P. Amyotte, and V. Cozzani, "Dynamic approach to risk management: Application to the hoeganaes metal dust accidents," *Process Safety and Environmental Protection*, vol. 92, no. 6, pp. 669–679, 2014 (cit. on p. 36).

[135] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, "Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach," *Process Safety and Environmental Protection*, vol. 91, no. 1-2, pp. 1–18, 2013 (cit. on p. 36).

[136] N. J. Duijm, "Safety-barrier diagrams as a safety management tool," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 332–341, 2009 (cit. on p. 36).

[137] *ISO 17776:2000 Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment*, International Organization for Standardization, 2000 (cit. on p. 36).

[138] J. L. Rouvroye and E. G. van den Bliek, "Comparing safety analysis techniques," *Reliability Engineering & System Safety*, vol. 75, no. 3, pp. 289–294, 2002 (cit. on pp. 36, 38).

[139] M. Bouissou and J.-L. Bon, "A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes," *Reliability Engineering & System Safety*, vol. 82, no. 2, pp. 149–163, 2003 (cit. on p. 36).

[140] H.-C. Liu, L. Liu, and N. Liu, "Risk evaluation approaches in failure mode and effects analysis: A literature review," *Expert systems with applications*, vol. 40, no. 2, pp. 828–838, 2013 (cit. on p. 37).

[141] P. David, V. Idasiak, and F. Kratz, "Towards a better interaction between design and dependability analysis: FMEA derived from UML/SysML models," *Proceedings of ESREL 2008 and 17th SRA-EUROPE annual conference*, vol. 3, Sep. 2008 (cit. on p. 37).

[142] S. Kmenta and K. Ishii, "Advanced FMEA using meta behavior modeling for concurrent design of products and controls," in *Proceedings of the 1998 ASME design engineering technical conferences*, 1998 (cit. on p. 38).

[143] M Nicholson and J McDermid, "Extending PSSA for Complex Systems," in *Proceedings of the 21st International System Safety Conference (ISSC)*, 2003 (cit. on p. 39).

[144] N. Kube and B Singer, "Security assurance levels: a SIL approach to security," in *Procdeedings of the 2nd SCADA Security Scientific Symposium (S4)*, 2008 (cit. on p. 39).

[145] J. D. Gilsinn and R. Schierholz, "Security assurance levels: A vector approach to describing security requirements," *NIST*, 2010 (cit. on p. 39).

[146] R. Winther, O.-A. Johnsen, and B. A. Gran, "Security assessments of safety critical systems using HAZOPs," in *International Conference on Computer Safety, Reliability, and Security*, Springer, 2001, pp. 14–24 (cit. on p. 40).

[147] J. Wei, Y. Matsubara, and H. Takada, "Hazop-based security analysis for embedded systems: Case study of open," in *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, IEEE, 2015, SSS–1 (cit. on p. 40).

[148] T. Srivatanakul, J. A. Clark, and F. Polack, "Effective security requirements analysis: Hazop and use cases," in *International Conference on Information Security*, Springer, 2004, pp. 416–427 (cit. on p. 40).

[149] B. Daruwala, S. Mandujano, N. K. Mangipudi, and H.-c. Wong, "Threat analysis for hardware and software products using HazOP," in *Proceedings of the international Conference on Computational and information Science.*, 2009, pp. 446–453 (cit. on p. 40).

[150] B. Schneier, "Modeling security threats," *Dr. Dobb's Journal*, 1999 (cit. on p. 40).

[151] V. Nagaraju, L. Fiondella, and T. Wandji, "A survey of fault and attack tree modeling and analysis for cyber risk management," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE, 2017, pp. 1–6 (cit. on p. 40).

[152] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *2009 9th International Conference on Intelligent Transport Systems Telecommunications,(ITST)*, IEEE, 2009, pp. 641–646 (cit. on pp. 40, 75).

[153] J. Xu, K. K. Venkatasubramanian, and V. Sfyrla, "A methodology for systematic attack trees generation for interoperable medical devices," in *2016 Annual IEEE Systems Conference (SysCon)*, 2016, pp. 1–7 (cit. on p. 40).

[154] E. J. Byres, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," in *Proceedings of the international infrastructure survivability workshop*, Citeseer, 2004, pp. 3–10 (cit. on p. 40).

[155] K. Edge, R. Raines, M. Grimaila, R. Baldwin, R. Bennington, and C. Reuter, "The use of attack and protection trees to analyze security for an online banking system," in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, IEEE, 2007, 144b–144b (cit. on p. 40).

[156] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," in *2009 IEEE/PES Power Systems Conference and Exposition*, IEEE, 2009, pp. 1–6 (cit. on p. 40).

[157] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, "Attack–defense trees and two-player binary zero-sum extensive form games are equivalent," in *International Conference on Decision and Game Theory for Security*, Springer, 2010, pp. 245–256 (cit. on p. 40).

[158] A. Jürgenson and J. Willemson, "Processing Multi-Parameter Attacktrees with Estimated Parameter Values," in *International Workshop on Security*, Springer, 2007, pp. 308–319 (cit. on p. 40).

[159] R. R. Yager, "OWA trees and their role in security modeling using attack trees," *Information Sciences*, vol. 176, no. 20, pp. 2933–2959, 2006 (cit. on p. 40).

[160] S. Garg and G. S. Aujla, "An attack tree based comprehensive framework for the risk and security assessment of vanet using the concepts of game theory and fuzzy logic," *Journal of Emerging Technologies in Web Intelligence*, vol. 6, no. 2, pp. 247–252, 2014 (cit. on p. 40).

[161] J. O. Aagedal, F. Den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stolen, "Model-based risk assessment to improve enterprise security," in *Proceedings. Sixth International Enterprise Distributed Object Computing*, IEEE, 2002, pp. 51–62 (cit. on p. 41).

[162] A. Gorbenko, V. Kharchenko, O. Tarasyuk, and A. Furmanov, "F(I)MEA-technique of web services analysis and dependability ensuring," in *Rigorous Development of Complex Fault-Tolerant Systems*, Springer, 2006, pp. 153–167 (cit. on p. 41).

[163] C. Schmittner, Z. Ma, and P. Smith, "FMVEA for safety and security analysis of intelligent and cooperative vehicles," in *International Conference on Computer Safety, Reliability, and Security*, Springer, 2014, pp. 282–288 (cit. on p. 41).

[164] J. B. Bowles and W. Hanczaryk, "Threat effects analysis: Applying FMEA to model computer system threats," in *2008 Annual Reliability and Maintainability Symposium*, IEEE, 2008, pp. 463–468 (cit. on p. 41).

[165] M. Rebekah, "Evaluating cyber risk in engineering environments: A proposed framework and methodology," SANS Institute, Tech. Rep., 2016 (cit. on p. 41).

[166] A. E. Tucci, "Cyber risks in the marine transportation system," in *Cyber-Physical Security*, Springer, 2017, pp. 113–131 (cit. on p. 41).

[167] P. Harry, "Bow Tie for Cyber Security (0x01): How to Tie a Cyber Bow Tie," PI Square, Tech. Rep., 2016 (cit. on p. 41).

[168] K. Bernsmed, C. Frøystad, P. H. Meland, D. A. Nesheim, and Ø. J. Rødseth, "Visualizing cyber security risks with bow-tie diagrams," in *International Workshop on Graphical Models for Security*, Springer, 2017, pp. 38–56 (cit. on p. 41).

[169] H. Abdo, "Dealing with uncertainty in risk analysis : combining safety and security," Theses, Université Grenoble Alpes, Dec. 2017 (cit. on pp. 41, 43).

[170] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the Markov-chain model for cyber-attack detection," *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116–123, 2004 (cit. on p. 42).

[171] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A Markov game theory-based risk assessment model for network information system," in *2008 International Conference on Computer Science and Software Engineering*, IEEE, vol. 3, 2008, pp. 1057–1061 (cit. on p. 42).

[172] V. Lakhno, D. Kasatkin, and A. Blozva, "Modeling Cyber Security of Information Systems Smart City Based on the Theory of Games and Markov Processes," in *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, IEEE, 2019, pp. 497–501 (cit. on p. 42).

[173] L. Piètre-Cambacédès and M. Bouissou, "Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)," in *2010 European Dependable Computing Conference*, IEEE, 2010, pp. 199–208 (cit. on p. 42).

[174] L. Piètre-Cambacédès and M. Bouissou, "Attack and defense modeling with BDMP," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, Springer, 2010, pp. 86–101 (cit. on p. 42).

[175] J. P. McDermott, "Attack net penetration testing," in *Proceedings of the 2000 workshop on New security paradigms*, 2001, pp. 15–21 (cit. on p. 42).

[176] S. Zhou, Z. Qin, F. Zhang, X. Zhang, W. Chen, and J. Liu, "Colored petri net based attack modeling," in *International Workshop on Rough Sets, Fuzzy Sets, Data Mining, and Granular-Soft Computing*, Springer, 2003, pp. 715–718 (cit. on p. 42).

[177] Y. Fu, J. Zhu, and S. Gao, "CPS information security risk evaluation system based on Petri Net," in *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, IEEE, 2017, pp. 541–548 (cit. on p. 42).

[178] J. Zhou, G. Reniers, and L. Zhang, "Petri-net based attack time analysis in the context of chemical process security," *Computers & Chemical Engineering*, vol. 130, p. 106 546, 2019 (cit. on p. 42).

[179] E. Lisova, I. Šljivo, and A. Čaušević, "Safety and security co-analyses: A systematic literature review," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2189–2200, 2018 (cit. on p. 43).

[180] F. Reichenbach, J. Endresen, M. M. Chowdhury, and J. Rossebø, "A pragmatic approach on combined safety and security risk analysis," in *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, IEEE, 2012, pp. 239–244 (cit. on p. 43).

[181] S. Plósz, C. Schmittner, and P. Varga, "Combining safety and security analysis for industrial collaborative automation systems," in *International Conference on Computer Safety, Reliability, and Security*, Springer, 2017, pp. 187–198 (cit. on p. 43).

[182] I. N. Fovino, M. Masera, and A. De Cian, "Integrating cyber attacks within fault trees," *Reliability Engineering & System Safety*, vol. 94, no. 9, pp. 1394–1402, 2009 (cit. on p. 43).

[183] M. Puys, M.-L. Potet, and A. Khaled, "Generation of applicative attacks scenarios against industrial systems," in *International Symposium on Foundations and Practice of Security*, Springer, 2017, pp. 127–143 (cit. on p. 43).

[184] *Juras guideline on sora*, Annex A : Guideline on collecting and presenting system and operation information for a specific UAS operation, Joint Authorities for Rulemaking on Unmanned Systems, 2017 (cit. on pp. 47, 98, 101).

[185] *Airworthiness security methods and considerations*, EUROCAE, 102 rue Etienne Dolet, 92240 MALAKOFF, France, Sep. 2015 (cit. on p. 53).

[186] O. Gadyatskaya, R. Jhawar, P. Kordy, K. Lounis, S. Mauw, and R. Trujillo-Rasua, "Attack Trees for Practical Security Assessment: Ranking of Attack Scenarios with ADTool 2.0," in *Quantitative Evaluation of Systems*, G. Agha and B. Van Houdt, Eds., Cham: Springer International Publishing, 2016, pp. 159–162 (cit. on p. 55).

[187] F. Nikodem, A. Bierig, and J. S. Dittrich, "The New Specific Operations Risk Assessment Approach for UAS Regulation Compared to Common Civil Aviation Risk Assessment," in *DLRK 2018*, 2018 (cit. on p. 62).

[188] *Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (eu) 2019/947*, European Union Aviation Safety Agency (EASA), Oct. 2019 (cit. on p. 62).

[189] *Introduction of a regulatory framework for the operation of unmanned aircraft*, European Union Aviation Safety Agency (EASA), Dec. 2015 (cit. on pp. 62, 67).

[190] *A-NPA 2015-10: Introduction of a regulatory framework for the operation of drones*, European Union Aviation Safety Agency (EASA), Oct. 2015 (cit. on p. 67).

[191] C. Pauner, I. Kamara, and J. Viguri, "Drones. Current challenges and standardisation solutions in the field of privacy and data protection," in *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*, 2015, pp. 1–7 (cit. on pp. 67, 69, 71).

[192] S. Winkler, S. Zeadally, and K. Evans, "Privacy and Civilian Drone Use: The Need for Further Regulation," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 72–80, 2018 (cit. on p. 67).

[193] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," *Mobile Networks and Applications*, pp. 95–101, 2019 (cit. on p. 69).

[194] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European data protection: coming of age*, Springer, 2013, pp. 3–32 (cit. on p. 69).

[195] Z. Li, C. Gao, Q. Yue, and X. Fu, "Toward drone privacy via regulating altitude and payload," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 562–566 (cit. on p. 69).

[196] J. Villasenor, "Observations from above: Unmanned aircraft systems and privacy," *Harvard Journal of Law Public Policy*, 2013 (cit. on p. 69).

[197] S. Park and K. Lee, "Developing Criteria for Invasion of Privacy by Personal Drone," in *2017 International Conference on Platform Technology and Service (PlatCon)*, 2017, pp. 1–7 (cit. on pp. 69, 71).

[198] M. Bonetto, P. Korshunov, G. Ramponi, and T. Ebrahimi, "Privacy in mini-drone based video surveillance," in *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, vol. 04, 2015, pp. 1–6 (cit. on pp. 69, 71, 72).

[199] R. F. Babiceanu, P. Bojda, R. Seker, and M. A. Alghumgham, "An onboard UAS visual privacy guard system," in *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, 2015, pp. 1–8 (cit. on p. 69).

[200] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-Aware Restricted Areas for Unmanned Aerial Systems," *IEEE Security Privacy*, vol. 16, no. 2, pp. 70–79, 2018 (cit. on pp. 70, 72).

[201] *Planning, design, installation and operation of cctv surveillance systems. code of practice and associated guidance*, British Security Industry Association (BSIA), Jul. 2014 (cit. on p. 71).

[202] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, IEEE, 2012, pp. 585–590 (cit. on p. 75).

[203] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016 (cit. on p. 75).

[204] C. Capitán, J. Capitán, A. R. Castano, and A. Ollero, "Risk Assessment based on SORA Methodology for a UAS Media Production Application," in *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, 2019, pp. 451–459 (cit. on pp. 84, 90).

[205] *Deliverable d2.1: Multidrone media production requirements*, MULTIDRONE project - University of Bristol, Jul. 2017 (cit. on p. 84).

[206] R. Chevalier, M. Villatel, D. Plaquin, and G. Hiet, "Co-processor-based behavior monitoring: Application to the detection of attacks against the system management mode," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 399–411 (cit. on p. 106).

[207] X. Ruan, *Platform Embedded Security Technology Revealed*. Springer Nature, 2014 (cit. on p. 106).

[208] S. Krishnamurthy, J. R. O'donoghue, and N. Bhatia, *Methods for providing anti-rollback protection of a firmware version in a device which has no internal non-volatile memory*, US Patent 9,910,659, 2018 (cit. on p. 106).

[209] P. Raju, "Fundamentals of gps," *Satellite Remote Sensing and GIS Applications in Agricultural Meteorology*, p. 121, 2004 (cit. on p. 152).

[210] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005 (cit. on p. 152).

[211] M. Ahmad, M. A. Farid, S. Ahmed, K. Saeed, M Asharf, and U. Akhtar, "Impact and detection of GPS spoofing and countermeasures against spoofing," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, 2019, pp. 1–8 (cit. on p. 153).

[212] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012 (cit. on p. 153).

[213] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016 (cit. on p. 154).

[214] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *ION GNSS*, vol. 5, 2005, pp. 13–16 (cit. on p. 154).

[215] D. Shepard, "Characterization of receiver response to spoofing attacks," Ph.D. dissertation, The University of Texas at Austin, 2011 (cit. on p. 154).

[216] A. Jovanovic, C. Botteron, and P.-A. Fariné, "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, IEEE, 2014, pp. 1258–1271 (cit. on p. 154).

[217] C. E. McDowell, *GPS spoofer and repeater mitigation system using digital spatial nulling*, US Patent 7,250,903, 2007 (cit. on p. 154).

[218] P. Y. Montgomery, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2011 (cit. on p. 154).

[219] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," *Navigation*, vol. 58, no. 4, pp. 335–344, 2011 (cit. on pp. 154, 155).

[220] Y. Qiao, Y. Zhang, and X. Du, "A vision-based GPS-spoofing detection method for small UAVs," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*, IEEE, 2017, pp. 312–316 (cit. on p. 154).

[221] G Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *2017 23rd International Conference on Automation and Computing (ICAC)*, IEEE, 2017, pp. 1–11 (cit. on p. 155).

[222] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "Efficient drone hijacking detection using onboard motion sensors," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, IEEE, 2017, pp. 1414–1419 (cit. on p. 155).