12-2021

Airspace Integration of New Entrants and Safety Risk Management Models

Fadjimata Issoufou Anaroua
issoufof@my.erau.edu

AIRSPACE INTEGRATION OF NEW ENTRANTS AND SAFETY RISK MANAGEMENT MODELS

by

Fadjimata Issoufou Anaroua

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Systems Engineering
at Embry-Riddle Aeronautical University

Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach, Florida
December 2021

AIRSPACE INTEGRATION OF NEW ENTRANTS AND SAFETY RISK MANAGEMENT MODELS

by Fadjimata Issoufou Anaroua

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Radu F. Babiceanu, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the Degree of Master of Science in Systems Engineering.

Radu Babiceanu Digitally signed by Radu Babiceanu Date: 2021.12.09 10:07:48 -05'00'

Radu F. Babiceanu, Ph.D.
Committee Chair

Mustafa Ilhan Akbas Digitally signed by Mustafa Ilhan Akbas Date: 2021.12.09 17:04:37 -05'00'

M. Ilhan Akbas, Ph.D.
Committee Member

Omar Ochoa Digitally signed by Omar Ochoa Date: 2021.12.09 10:37:43 -05'00'

Omar Ochoa, Ph.D.
Committee Member

Radu Babiceanu Digitally signed by Radu Babiceanu Date: 2021.12.09 17:07:45 -05'00'

12/9/21

Radu F. Babiceanu, Ph.D. — Date
Interim Chair, Electrical Engineering and Computer Science

James W. Gregory Digitally signed by James W. Gregory Date: 2021.12.09 21:17:42 -05'00'

12/10/21

James W. Gregory, Ph.D. — Date
Dean, College of Engineering

Christopher Grant Digitally signed by Christopher Grant Date: 2021.12.10 14:25:36 -05'00'

12/10/21

Christopher D. Grant, Ph.D. — Date
Associate Provost of Academic Support

Acknowledgments

I would like to first and foremost thank all my family, and especially my mother who has always supported me and my projects. Thank you for always being there for me as such a brave and wonder woman. The encouragements to never give up whatever the obstacles helped me succeed. I thank my late father who has always been my role model in term of excellence. Even though he is no longer among us, I know he will be proud of the person I am today.

I would like to thank Dr Radu Babiceanu for advising my thesis and all the tremendous effort and assistance deployed from the beginning to the end of my master’s degree. The continued support was indeed much appreciated throughout the whole engineering process. I thank Dr. Omar Ochoa for the incredible teaching expertise. I gained valuable knowledge during my early stages. I thank Dr. Ilhan Akbas for giving me multiple opportunities to discuss and explore the Research/Technology area and learn new knowledge. I thank Dr Richard Stansbury for providing me a platform to put up my research abilities and skills in practice and contribute to his research lab.

Special appreciation to Amina I. Anaroua, who introduced me to the Aviation world and Embry-Riddle Aeronautical University and provided assistance during my integration.

Finally, I thank all the Riddle family for supporting me and providing me with all the necessary tools to make my research project an unforgettable and rich experience.

Table of Contents

List of Tables

List of Figures

Abstract

In the recent years, the demand for airspace access of Unmanned Aerial Systems (UAS) increased significantly and is continuously increasing for different altitude-types UAS. A similar evolution is expected from Commercial Space Operations (CSO) in the next years. These aviation/aerospace systems will need to be seamlessly integrated in the National Airspace System (NAS), at their operational altitude levels, and accounted for from all perspectives, including proactively addressing their safety hazards. This thesis captures the requirements for the new entrants' integration, and then identifies and analyzes the safety risks added to the NAS operations by its new entrants, the future omnipresent UAS on different NAS levels and the coming CSO age. Methodologies such as Functional Hazard Analysis, Subsystem and System Hazard Analysis, and Safety Risk Management are explored and integrated in the airspace new entrants' framework and models. In addition, techniques such as state-machine modeling and simulation are used on an identified use case of UAS operations in crowded airspace.

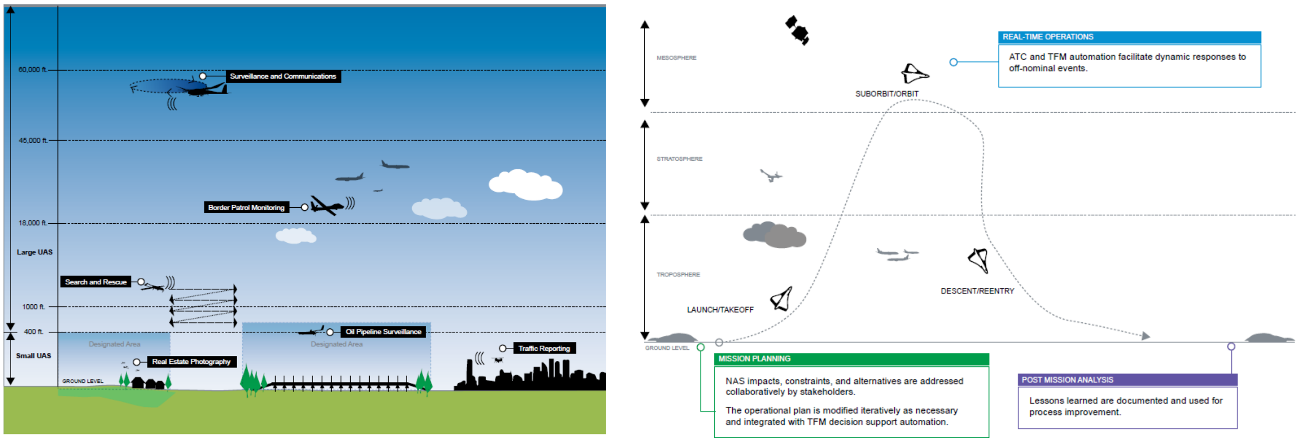
Chapter 1

Introduction

1.1 Unmanned Aerial Systems and Commercial Space Operations

In the recent years, the demand for airspace access of Unmanned Aerial Systems (UAS) increased significantly and is continuously increasing for different altitude-types UAS. A similar evolution is expected from Commercial Space Operations (CSO) in the next years. These aviation/aerospace systems, also called new entrants, will need to be seamlessly integrated in the National Airspace System (NAS), at their operational altitude levels, and accounted for from all perspectives, including proactively addressing their safety hazards. UAS can operate in both controlled and uncontrolled airspace and can be piloted by legitimate or malicious actors. Solutions to proactively address any safety risks need be developed and implemented based on the airspace they operate in. On the other hand, CSO require special considerations such as launch, reentry, landing, window duration, and trajectory. The biggest concerns related to the increased CSO activities are safety-related and minimizing the NAS operations impact.

The UAS and CSO as airspace new entrants were identified in a recent Federal Aviation Administration (FAA) report as one of the emerging NAS challenges that must be addressed in the near future (FAA, 2016). Solutions such as collaborative air traffic management and management of special activity airspace were proposed. Fig. 1 below presents the expected future NAS operational framework for the new entrants: UAS and CSO (FAA, 2016).



ATC and TFM automation facilitate dynamic responses to off-nominal events.

NAS impacts, constraints, and alternatives are addressed collaboratively by stakeholders.

The operational plan is modified iteratively as necessary and integrated with TFM decision support automation.

Lessons learned are documented and used for process improvement.

Fig. 1: Expected Future NAS Operational Framework for the UAS and CSO (FAA, 2016)

Besides air traffic management through flight/launch scheduling and divided airspace operations, the seamless integration of this new entrants requires a thorough risk analysis process. This thesis will initially capture requirements for the new entrants' integration, and then identify and analyze the safety risks added to the NAS operations by its new entrants, the future omnipresent UAS on different NAS levels and the coming CSO age.

1.2 Significance of the Study

Unmanned Aerial Systems (UAS) are employed in many areas such as military and law enforcement surveillance, environmental monitoring, logistics services, agriculture operations, and many other applications.

The 21st century has seen an exponential growth in the development and use of unmanned aircraft. It is a new emerging technology, said to be "a game-changing technology" like the automobile or the computer where back in their launching days. It is also the fastest growing area of aviation. In addition to providing economic benefits, UAS pose a range of issues, including the safety and management of airspace, as well as social, privacy, and security issues for the community in general (Arblaster, 2018).

Despite the efforts made by the UAS researchers, manufacturers, and operators, there is still a large public and private operators mistrust regarding UAS deployment. This mistrust acts as a big challenge for ubiquitous UAS deployment. Regulatory authorities require the presentation of a safety assessment process for UAS operations, which can help with overcoming these challenges and increase the level of confidence in the UAS and of their operations. The safety assessment process is usually developed in the design phase, which among other aspects identifies potential failure conditions in operation of a particular UAS. It also includes the potential consequences of failure and the proposed mitigation measures to be included in the design so that the resultant failure severity is reduced (Goncalves *et al.*, 2017).

Another domain affected by the rapid growth of UAS and CSO is the Air Traffic Management (ATM) operations. Appropriate safety measures and the management of increased unmanned aircraft traffic needs to be addressed through regulations and adoptions of safety assessment models. Flying systems operating without a pilot on board could lead to a series of safety hazards in the ATM domain. Identified risk range from UAS operations resulting in injuries of the public or property damage. Even more, unregulated UAS operations present the risk of collision between the unmanned system and another airspace user in any phase of flight (Arblaster, 2018). This study will identify the risks associated with the integration of UAS and capture the necessary safety measures to address and define appropriate requirements for the safe integration of unmanned vehicles in the airspace.

1.3 Problem Statement and Assumptions

Recent studies have identified that the coordination of the entire airspace system and the integration of UAS further require the need for a type of centralized management function to ensure safe integration within the NAS. The management needs to address different types of models such as air space sectors and unmanned traffic management, so that it can provide technologies and tools that allow all users fair and safe access for low-altitude airspace operations.

In addition, as stated above, UAS operations have increased safety risks to other aircraft, property, and people on the ground. Airports and areas surrounding airports in the vicinity of aircraft approach and departure are a particular concern. Current technology makes unmanned systems difficult to detect by air traffic controllers. For example, an increasing number of near misses between unmanned aircraft and manned aircraft have been recently reported in the United Kingdom.

To address the risks associated with the ever-increasing number of UAS, operating and technological developments are expected. Technological measures include equipping UAS with data transmission capabilities, so that they can be identified by ATM centers, and thus keeping them at a safe distance from commercial and other aircraft. Prohibiting entry in restricted areas through geofencing is another technological solution that will reduce safety risks. From these perspectives, capturing the requirements for the new entrants' integration, and then identify and analyze the safety risks associated is crucial in the event of NAS safe integration of different UAS. This study depicts the main requirements for a safe integration and identifies the relevant hazards and safety risks associated to UAS operations in national airspace.

Since UAS are being widely used for multiple purposes, and their integration addresses a large variety of safety related issues to NAS operations, it is important to define the assumptions related to the study. These assumptions originate from the following airspace operations safety and risk attributes.

- Potential that UAS operations will introduce additional risks into the NAS.
- Need to assess the dissimilarities for the different UAS-type operations.
- Requirement to have a comprehensive safety risk management for all UAS operations.
- Re-evaluation of the safety risk associated with the previously approved NAS operations.

Based on the above attributes, this study will use the following assumptions regarding UAS operations.

- Safety risk assessment covers all UAS types that may result in potential risks to current NAS operations.
- UAS operations uses current Air Traffic Control procedures, requirements, and instructions.
- UAS operations meets the performance requirements set for the airspace class or route in which they operate.

On the space operation side, it was examined that space traffic management will become a challenge as more and more small satellites enter near space and sub-orbital flights become a reality. The space traffic management should be approached in similar with low-altitude unmanned air traffic, so the above assumption remains valid.

Chapter 2

Relevant Literature Review

2.1 Technology Advancements

New technological developments have given rise to new entrants into airspace which are having a significant impact on the future profile of the ATM industry. There is a rapid development of new types of aircraft, primarily unmanned aircraft commonly known as “drones,” and additionally increased space transportation (Arblaster, 2018). UAS are similar to air vehicles and their associated equipment. But, at the difference with other air vehicles, UAS do not carry human operators. They are remotely piloted, or with an autopilot assistance, or they can completely fly autonomously. According to ICAO (2011) definition, unmanned aircraft are part of UAS where an aircraft can be “remotely and fully controlled from another place (ground, another aircraft, and space) or pre-programmed to conduct flight without intervention.

Globally, air navigation service providers (ANSPs) and civil aviation authorities (CAAs) agree that new approaches need to be launched that promote the use of unmanned systems while ensuring the safety of the existing airspace actors. Safety has always driven advancements in aviation and must continue to do so in the new era of unmanned platforms. UAS Traffic Management (UTM) for low-altitude airspace reinforces this need and provides a path forward for safe integration of all vehicles (Matus and Hedblom, 2018). The UTM core the authors study represents an intermediate approach that seeks to build on progress made towards large-scale UAS integration.

It is reported that the UTM core represents a solution that can maintain the level of safety that aviation operations currently exhibit.

In an environment with high traffic density, there will be conflicting UAS operations. Since traffic must be managed efficiently for low-altitude airspace, it will require to prioritize operations and address potential conflicts in the airspace (Matus and Hedblom, 2018).

Sanat (2019) examined and showed that space traffic management will become a challenge as more and more small satellites enter near space and sub-orbital flights become a reality. There are government efforts to examine potential rules for commercial space flights. The FAA and other federal agencies have the responsibility of providing the airspace operators with appropriate rules for commercial space flights up to Low Earth Orbit (LEO).

The safety critical systems used in domains such as nuclear power, transport, medical, and information systems are required to go through the formal process of certification. This process ensure that these systems will deliver the expected services to its users. To ensure the certification processes of large safety-critical systems follow the certification authority regulations, the systems, security, and software engineering departments needs a thorough knowledge of the process of providing the certification evidence, including the engineering analysis models and methods (Kaur *et al.*, 2018).

2.2 Unmanned Aerial Systems Integration

ICAO (2011) presents the principles for the introduction of unmanned aircraft into controlled airspace. It includes limitations on the risk to other aircraft, or third parties, and to accessing the airspace. Furthermore, the outlined procedures for handling unmanned aircraft are directed to mirror those for manned aircraft whenever possible.

Most of the researchers working on unmanned system integration focus on analyzing the reliability, safety, and dependability of systems without considering security. However, security is an essential prerequisite for all the above system characteristics. A secure system provides more confidence in its reliability, availability, safety, and the accomplishment of its performance metrics.

Gerdes *et al.* (2018) have introduced the dynamic airspace sectorization which allows for an efficient allocation of scarce resources considering operational, economic, and ecological constraints. The model accounts for the traffic conditions in both nominal and variable air traffic. The sectorization model considers the requirements of air traffic management (safety, capacity, and efficiency), the actors (which should unhindered access), and the environment (which may include restricted areas). The sectorization model is developed to account for different operational demands and performance. Due to the increase in air traffic of many types, the urban areas traffic management will become more and more challenging. Other authors introduced besides sectorization, a so-called dynamic airspace configuration with the objective to minimize air traffic controllers' effort while moving from one sector to another. It is reported that the approach also increases the stability of the airspace sectorization (Kopardekar *et al.*, 2007).

Arblaster (2018) contrasts the features of the unmanned and traditional manned aviation industry and emphasizes the need to adopt safety regulations for the unmanned operations that have the same high levels of performance as in the manned aviation industry. From regulatory agencies' perspectives this is well understood, and the steps are moving into the right direction. It is expected that more analysis will be conducted to determine the risks that result from unmanned aircraft integration into airspace operations. Specific areas that are needed for further research are the study of the safety risks at and around airports. Safety regulations covering the use of unmanned aircraft in and around airports are already in place all over the world, which in most cases are prohibiting any unmanned flights too close to airports. To enforce those regulations, technology that reliably detects small, unmanned systems have to be developed and made available for interested stakeholders. The federal government agencies have launched the UAS detection initiative involving testing technologies to detect unauthorized operations at around airports and unauthorized airspace (AUVSI, 2017). Other solutions include geofencing technology and virtual barriers that could be installed to prevent UAS from entering restricted areas (Arblaster, 2018).

Advanced commercial UAS ask for more performant capabilities, requiring higher degrees of complexity and remote sensing to complete their missions. Search and Rescue (SAR) operations use UAS designed to operate in disaster scenarios, where beyond visual range and teleoperation are required and most of the control is performed by the given the current environment conditions (Polka, *et al.* 2017).

2.3 Safety Risk Modeling

Safety mishaps occurring in today's systems can have severe consequences in terms of financial loss, human losses, and environmental damage. Furthermore, the today's public tolerance to mishaps is lower than in the past, so the pressure on deploying safe systems is as high as it ever was. Safety is a key identified requirement for all airspace actors, where safety is defined as "freedom from those conditions that can cause death, injury, occupational illness and damage or loss of equipment or property" or as 'the freedom from unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly because of damage to the property or to the environment."

Aizpurua and Muxika (2013) reviewed the state-of-the-art safety assessment techniques, used for the design of generic systems. Kriaa *et al.* (2018) provided an overview of the methods for a combined assessment of the safety and security. De la Vara *et al.* (2019) offered an overview of the available safety standards, while Ivarsson and Gorschek (2009) reviewed the methods available for deriving requirements in safety-critical systems. In addition, the literature review identified the work of Nair *et al.* (2014) who carried out a systematic review on the evidence required for the safety certification. However, the authors did not focus on specific methods, even though these methods are necessary for evidence generation in the system safety case.

Each safety activity ensures the expected safety levels at a specific system design stage by considering the specific safety hazards of the system. Hazard identification considers fault scenarios development, and their risk assessment, and aims at predicting the failure scenarios occurrence and their severity (Bolbot *et al.*, 2019). Several identified approaches focus on the integration of hazard identification or similar methods and verification activities. Pereira *et al.* (2019) have combined the STPA and the model checking for ensuring safe software properties for an adaptive cruise speed control system. Rokseth *et al.* (2018) used the STPA for deriving test objectives for the ship power management system. Blackburn *et al.* (2018) used Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) to derive the requirements for the verification of a robot collision avoidance system through testing and theorem proving. Zhang *et al.* (2017) proposed to incorporate belief, uncertainty, and measurement profiles to enhance MBT with application to a smart home and the logistics of a manufacturing system. Finally, Sharvia and Papadopoulos (2015) combined FLSA with model checking for the safety assessment of the brake by wire system.

In the unmanned aerial systems arena, safe operations in the airspace ask for capabilities of situational awareness to derive avoidance solutions based on the environment actors to ensure safety in operations. Generally, UAS operations are divided in two types based on the actual available communications and decision models: collaborative and non-collaborative. Swarm models such as the one described by Wang *et al.* (2021) include multiple UAS that cooperate and share information through data networking. The capabilities result in enhanced perception of environmental situation, which ultimately improves mission success, such as cooperative search, reconnaissance and attacks.

Other technological advances that help with increased safe operations relate to the development of sensor and computing technologies. These technologies provide accurate information required for safe navigation. Moreover, automatic control and networking technologies, enabled by multi-sensory systems, is extensively present in UAS and it can provide fully automated aircraft guidance. Related to these efforts, the launch of Performance-Based Navigation (PBN), as an updated navigation technology from the existing Performance-Based Operations (PBO), provides the needed information for navigation systems performance requirements defined based on the safety, accuracy, integrity, and availability of the expected operations (Bolbot *et al.*, 2019). Patriarca *et al.* (2013) define the needed first steps for integrating UAS in non-segregated airspace through pilot skills comparison between autonomous unmanned and manned systems. The effort is performed within the current framework for civil aviation that includes safety at its core. Even with these steps, more data are needed to build probabilistic risk analysis models for UAS collision with other actors operating in non-segregated airspace.

All these advancements offer the means for UAS manufacturers, operators, and regulators to test new models for better data collection and analysis with the objective of improving overall safety.

Since data collection may be in some cases not an easy process, for hazards that have only a very low risk to activate into mishaps another solution to improve safety is to explore UAS simulated operations or data coming from similar applications. Accepting a final mishap risk is easier when the risk initial mishap risk is mitigated, and the risk mitigation and calculation is backed-up by relevant quantitative data. Also, uncertain risk does not always equate to high risk, and is most of the time encounter when new technology is launched. As more understanding on the hazard and its activation is obtained, the uncertainty is reduced and the risk can be better quantified, as well as mitigation solution can be better employed. Still, in uncertain environments such as UAS operating based on new technology, it is not always straight-forward to collect data, so the reduction of risk uncertainty is limited (NAS, 2018).

It is expected that in the future, certain UAS operations, as well as CSO operations, will be required to undergo a certification process similar to that for manned aircraft. The avionics equipment installed on UAS and CSO systems is a prime candidate for certification processes. However, standard creation must involve all interested stakeholders to ensure maximum safety and consequently lowest risk for UAS and CSO flight operations. Therefore, while the process may have already started it will take a certain time until the new standards or recommendations become available (Patriarca *et al.*, 2013).

Chapter 3

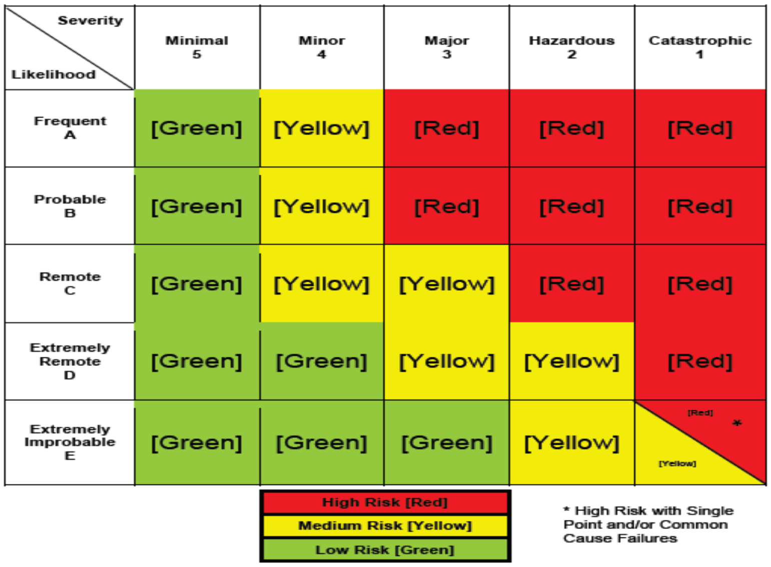
Safety Risk Methodology

3.1 Overview of the Safety Risk Process

The overall system requirements are captured in natural language format and use the requirements decomposition process, as well as identify derived requirements at the same level of decomposition. The safety risk process follows the five-step FAA Safety Risk Management Guidelines (FAA, 2018a), which includes system analysis, hazard identification, and safety risk modeling, analysis, assessment, and control, as depicted in Fig. 2 below.

Fig. 2: FAA Safety Risk Management Process (FAA, 2018a)

The modeling part uses techniques identified in the complementary FAA documentation to the five-step process that discusses the Safety Risk Management Tools (FAA, 2018b). These tools include Hazard and Risk Analysis directed towards system functionality, i.e., Functional Hazard Analysis (FHA), and system physical architecture of subsystems and components, System/subsystem Hazard Analysis (SHA). The results of the safety risk analysis will be summarized also using the color-coded FAA Risk Assessment Matrix presented in Fig. 3 below.



Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	[Green]	[Yellow]	[Red]	[Red]	[Red]
Probable B	[Green]	[Yellow]	[Red]	[Red]	[Red]
Remote C	[Green]	[Yellow]	[Yellow]	[Red]	[Red]
Extremely Remote D	[Green]	[Green]	[Yellow]	[Yellow]	[Red]
Extremely Improbable E	[Green]	[Green]	[Green]	[Yellow]	[Red] * [Yellow]

High Risk [Red]
Medium Risk [Yellow]
Low Risk [Green]

* High Risk with Single Point and/or Common Cause Failures

Fig. 3: FAA Risk Assessment Matrix (FAA, 2018a)

In addition, modeling and simulation techniques such as Petri-net and state-machine analysis are used in the use case depicted in Fig. 4. The use case, analyzed in a subsequent section, considers UAS operations in a crowded and obstacle-based airspace environment.

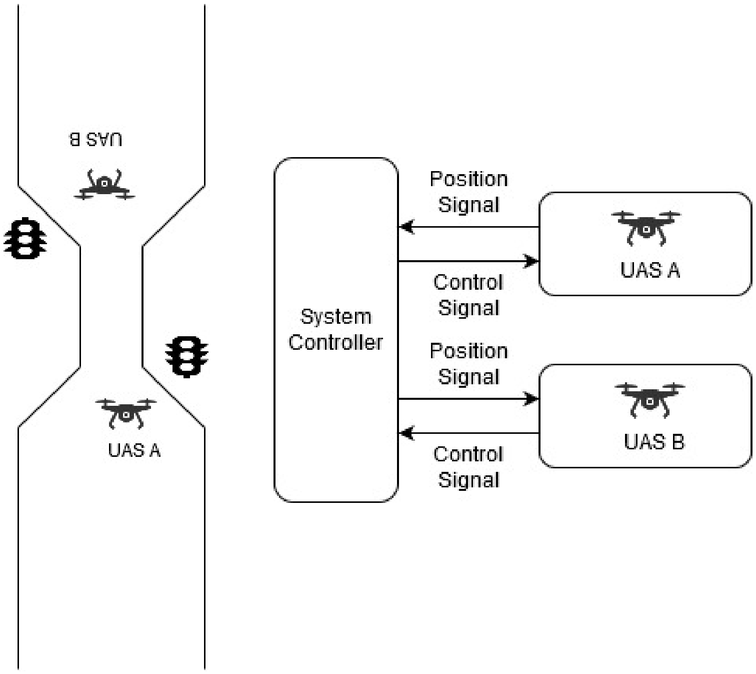


Fig. 4: UAS Use Case for Safety Risk Analysis and Mitigation Control

3.2 System Operational Concepts and Risk Modeling

3.2.1 UAS System Overview

Unmanned aerial systems are considered for systems analysis and requirements modeling. In aviation and in aerospace environments, an UAS refers to an unmanned aircraft or spacecraft. Literature and industry also refer to UAS as unmanned aerial vehicles (UAV), or in more popular terms, they are referred as drones. Government regulators or inter-governmental organization such as ICAO also name these systems as remotely piloted autonomous systems (RPAS). Practically, a drone is a flying robot that is piloted remotely, or it can fly autonomously by employing onboard software. Besides control software, drones include sensors and avionics equipment, such as GPS. The UAS degrees of autonomy range from remote control by a human operator to fully autonomous by an onboard computer.

In relation to UAS flying in open airspace, there are several safety concerns. UAS could crash into buildings, interfere with airspace, or cause many other problems, so government regulators are cautious when it comes to opening the airspace for all types of UAS. The FAA allowed limited operation of unmanned systems starting with 2016, and later on advised that operators can fly only during daylight or twilight, with altitude and speed restrictions. The flight permission is given subject to offering visual line of sight for their remote pilot.

UAS have many daily applications such as recreational, photography, commercial, and logistics. However, from the requirements engineering perspective, their two basic expectations are flight requirement and navigation requirement. Flight requirement is usually met by employing a power source, such as battery or fuel, rotors, propellers, and the frame, typically made of composite materials to reduce weight and increase maneuverability during flight. To meet the navigation requirement, UAS employ a software-hardware controller used for all navigation purposes, as well takeoff and landing. The controller communicates with the UAS through radio waves. Some of these characteristics and capabilities are provided in Table 1 UAS (FAA, 2018c).

Table 1: UAS Types and Capabilities UAS (FAA, 2018c)

UAS Capabilities	UAS Types
Degree of autonomy	Fully controlled by a remote pilot Fully autonomous
Mode of operation	Simple line of sight Beyond visual line of sight Swarm of UAS flying in formation
Size	Miniature (< 2 lbs) and as small as few inches Large (over 300 lbs) and several meters in length
Flight characteristic: height and range	Miniature: fly under 500 ft above ground and under 50 yards distance Large: fly at altitudes of 56,000 ft and distances of thousands of miles
Energy source	Battery cells Solar cells Traditional aircraft fuel
Communication	One-way communication from controller to UAS Two-way communication
Equipment	Basic equipment as in model aircraft Advanced equipment similar to manned aircraft
Capabilities	Similar to model aircraft Similar to manned aircraft

3.2.2 UAS System Operational Concepts

The operational concept of the UAS in space is schematically presented in Fig. 5. Three main components are needed for safe UAS operation in airspace:

- UAS pilot: the pilot is responsible for operating the unmanned system, which includes takeoff, flightpath, and landing. Pilots are also conducting safety tests, oversee and review the vehicle performance, and assess system's capabilities. They may also operate equipment installed on the systems, such as cameras and other sensors.

- ATM services providers: if possible, procedures should be similar to those for manned aircraft, and include separation services. RPAS are handled similarly to manned aircraft if their equipment, navigation, and two-way communications are comparable to those of a manned aircraft (ICAO, 2015).
- Airspace: unmanned traffic management can be considered as a collection of services intended to offer safe and efficient operations of UAS. In controlled airspace, the operations must be performed according to regulations in place at the time of flight.

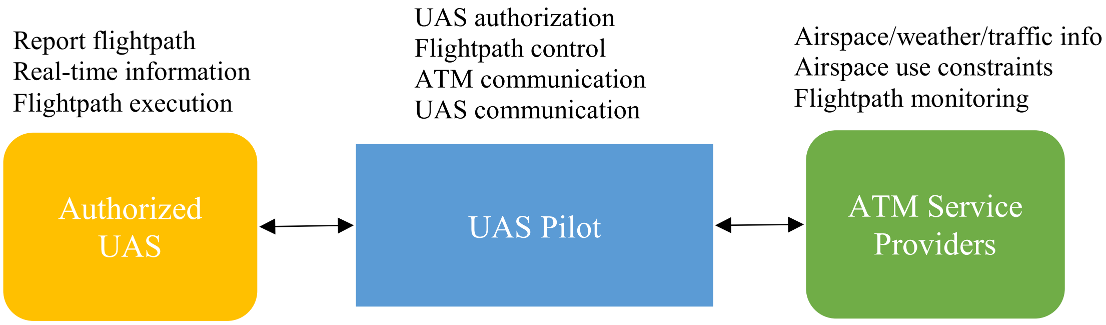


Fig. 5: Context Diagram for the UAS Operations (FAA, 2020a)

Recent regulations require registration of UAS weighing 55 lbs. or more only. To remotely fly UAS systems, the pilots must also be familiar with several rules such as the following:

- Safe operation includes both in the sky and on the ground UAS operations.
- Safe operation requires the UAD remains clear of all aircraft, people, and structures.
- Safe operation requires compliance to airspace operations and privacy laws.

ATM service providers should ensure the accomplishment of several processes and log in information such as the following:

- Times of operation, notification of beginning and ending of UAS operation.
- Route/altitude information understandable by air traffic controllers.
- Procedures covering lost communication link cases.
- Notification procedures in the event of an anomaly if it impacts the controlled airspace.

FAA rules apply to the entire national airspace system (presented in Fig. 6). UAS pilots should be familiar with the definitions of controlled and uncontrolled airspace, so that they are aware the areas legally to fly UAS. Controlled airspace is located around airports and at specific heights, where air traffic controllers actively communicate, direct, and separate all air traffic. Other airspace is considered uncontrolled because it is not under direct control of air traffic controllers. According to Fig. 6, UAS can be flown in uncontrolled airspace up to 400 feet above the ground. Fort commercial operators, a license is required to fly in controlled airspace.

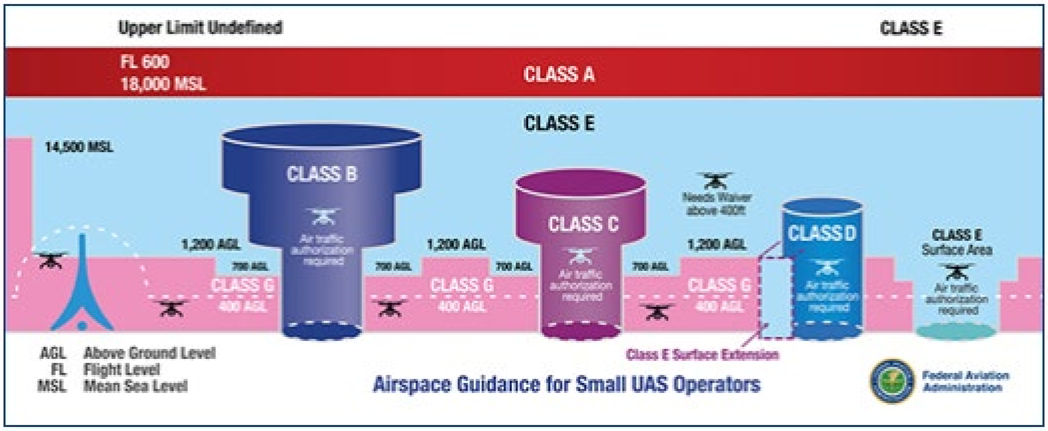


Fig. 6: Airspace Classification and Guidance for UAS operations (NAS, 2018)

3.2.3 UAS System Operational Goals

The high-level goals for the UAS integration into controlled and uncontrolled airspace are presented below. The goals may vary between controlled and uncontrolled airspace with more detailed information included for controlled airspace.

- G-1---UAS integration should address security and privacy risks.
- G-2---UAS integration should review operational concepts, including night operations, flight over people and beyond the pilot's line of sight, package delivery, detect-and-avoid technologies, and the reliability and security of data links between pilot and aircraft.
- G-3---UAS integration should consider a continued safety of all air traffic, manned and unmanned.
- G-4---UAS integration should ensure safety of persons on the ground.
- G-5---UAS integration should adhere to complex low-level unmanned aircraft operations.
- G-6---UAS integration should address the ongoing support of technological advancements.
- G-7--- UAS integration should address evaluation of security and environmental risks; and
- G-8--- UAS integration should address provision for a global, harmonized framework for air traffic management.

The high-level goals of the UAS system when flying in controlled and uncontrolled airspace are presented below.

- GS-1---UAS should be kept at a safe distance from other aircraft.
- GS-2---UAS should follow appropriate separation rules from other aircraft.
- GS-3---UAS should be able to be detected in case of promiscuity with other aircrafts.
- GS-4---UAS should fly at a safe distance from the ground.
- GS-5---UAS should not cause public safety issue or interfere with public.

- GS-6---UAS should strictly follow current regulation rules as specified by authorities.
- GS-7---UAS should fly within a specified airspace sector following airspace sectorization and traffic management systems.
- GS-8---UAS should be safely integrated within the airspace.
- GS-9---UAS should operate from designated airports.

3.2.4 New Airspace Entrants System Overview

The new-entrant technologies are being increasingly developed and commercialized in the recent years. This is asking for changes from the aviation and aerospace industries, which will have to adapt their operations towards increasing capacity, safety, and efficiency. As previously, the UTM was developed for unmanned traffic management, it is expected that a similar trend to come into play for space traffic management. The envisioned Space Traffic Management (STM) system will evolve from the current ground-based legacy systems with a significant involvement from the advanced global network of Communication, Navigation and Surveillance (CNS) technologies. (Hilton *et al.*, 2019).

Another important aspect of space vehicles is their vital launch and flight into orbit operations. These segments of flight characterized by critical dynamic, streamlined, and thermodynamic conditions. This influences to a large extent the planning and activities of the launch vehicles and their payload. Equally important are the re-entry operations. The essential goals during these stages of flight are: (1) to guide the orbiter along a path that minimizes the demands on the orbiter system design throughout the orbiter missions; and (2) to deliver the orbiter to a satisfactory energy state and vehicle altitude at the initiation of the terminal guidance system (Hilton *et al.*, 2019). The safety requirements for the new entrants must be explored separately from the safety requirements as applied to unmanned systems.

3.2.5 New Airspace Entrants Operational Concepts

Aviation and space flight safety regulations and standards have evolved over time as the more stringent rules were expected from the safety of flight perspective with the increase in number of space launches and traffic. Commercial Space Administration (AST) of the FAA has different safety criteria from Air Traffic Management (ATO) operations. The acceptance of public safety threats is expressed using different terminology and metrics. Aircraft hazard areas (AHA) is considered as metric during take-off and re-entry operations to keep launch vehicles separate from other NAS operations. AHA is an area of airspace where a person onboard an aircraft would be exposed to injury as a result of an abnormal event, including the fall of debris from a carrier (CFR Title 14. Chapter III). For take-off or re-entry operations, for a given location, extent, and duration of the AHA, the AST acceptable mishap probability of adverse events (death or serious injury) is 1×10^{-6} per aircraft. On the other hand, ATO imposes a probability of 1×10^{-9} for the same scenario. However, the two cannot be compared as they refer to different operational contexts and models.

Table 2: Acceptance Criteria for Public Safety (FAA, 2018c)

Element	AST Evaluation	ATO Evaluation
Safety Standard	1×10^{-6} For casualty-producing collisions	1×10^{-9} For catastrophic hazards
Period	Per aircraft, per launch/re-entry operation	Per affected flight hour or air traffic control operation
Consequence	Casualty of an aircraft occupant	Fatality of an aircraft occupant

ATO recently proposed the use of the Acceptable Risk Level (ALR) measure to temporarily fill the gap and accommodate the rise in NAS commercial space operations.

3.2.6 Acceptable Level of Risk Approach

ALR approach was developed as a need to identify solutions for air traffic operations associated with NAS new entrants that are not covered by existing ATO safety standards. As mentioned above, ATO safety standard considers a catastrophic probability of less than 1×10^{-9}. The ALR approach is more complex and requires several conditions to ensure the proposed acceptability level is obtained (FAA, 2018c). It defines an alternative method for accepting the catastrophic risk for air traffic when interactions with commercial space flights takes place. While the mishap probability is higher than for the traditional air traffic, ALR limits the number of exposed aircraft to the NAS infrastructure. The risk contours and levels and AHA for a given space launch are depicted din Fig. 7 below. It should be mentioned that there are specified restrictions related to flying within the risk contours and that no operations are permitted within the AHA. ALR is viewed as a temporary solution to enable commercial space activities for use when the individual hazard risk is greater than the in-use ATO standard. The FAA Order 8040.4 allows for a defined risk to be accepted for a limited period while new mitigations are developed and implemented, which is precisely the case for the new airspace entrants' operations [FAA, 2018c].

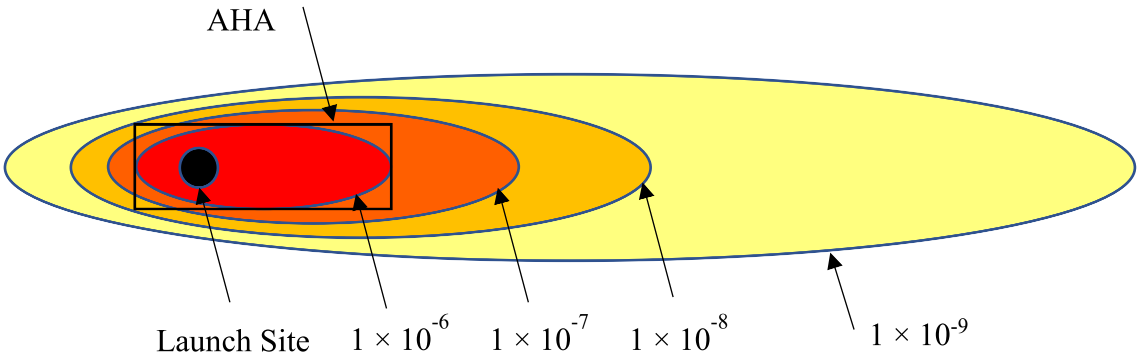


Fig. 7: Risk Contours and Levels and AHA for New Airspace Entrants (FAA, 2018c)

There are two approaches for ALR model depending on the risk level acceptance criteria. The first approach considers the individual risk as the probability that at least one passenger on an exposed flight experiences a fatality because of a space launch in the area. This individual risk has an upper limit equivalent to 1 × 10^{-7} probability. The second approach considers the collective risk as the number of fatal accidents due to space launch debris in the affected regions over a specified period. This collective risk is equivalent to 1 × 10^{-9} probability, or no fatal event occurring in an average person's lifetime [FAA, 2018c].

3.2.7 New Airspace Entrants Operational Models

The FAA guidance for ALR provides seven different use case scenarios for commercial space missions. These use cases are presented in Table 3 below along with their safety risk information based on the mission type.

Table 3: New Airspace Entrants Mission Models and Risk Contours (FAA, 2018c)

Mission Type	Mission Summary	System Examples	Risk Contours	Sites Impacted
Launch Barge Fly-Back	Liftoff, stage separation, ignition, boost-back burn/reentry/ soft touchdown, second stage engine cutoff, payload separation	SpaceX Falcon 9 Blue Origin New Glenn Ariane 5	Booster landing Width: 20-100 mi Length: 100s-1000s mi	Launch Landing
Launch Site Fly-Back	Similar to Launch Barge Fly-Back	Similar to Launch Barge Fly-Back	Debris landing Width: 100s mi Length: 100s-1000s mi	Launch Landing
Capsule Re-entry	Parachute or powered re-entry	Soyuz SpaceX Dragon Orbital Antares	Capsule landing Width: 100-150 mi Length: 200-400 mi	Landing

Captive Carry Orbital	Aircraft/space vehicle climb-to-launch altitude, space vehicle launch, space vehicle ascent to altitude, reentry, and return to spaceport	White Knight Two Carrying Virgin Galactic	Space vehicle landing Diameter: 20-50 mi	Landing
Horizontal Suborbital	Horizontal takeoff, powered ascent, coast to altitude, vehicle reentry, horizontal landing	XCOR Lynx	Space vehicle landing Diameter: 20-50 mi	Launch Landing
Winged Re-entry	Rocket powered winged reentry vehicle, horizontal landing	Dream Chaser Boeing	Vehicle landing: similar to aircraft	Landing
Point-to-Point	Takeoff or liftoff, ascent and transition to space, reentry, return to landing site	No known current examples	Two risk contours: departure and arrival, with sizes dependent on mission	Launch Landing

3.3 System Safety Requirements Modeling

3.3.1 UAS Systems Safety Hazards

The following main relevant hazards and corresponding risk were identified through the UAS initial safety requirement process.

- Air conflicts: cover the risk of a collision hazard in the air between an UAS and an airplane; it is calculated for medium air collision and navigation volumes and safety regulations in terms of ATM.
- Aircraft upsets: includes loss of control situations; relevant since UAS operate near ground and can result in hazards to people or other entities on the ground.
- Systems failure: power plant failures result in inability of the UAS to operate; non-power plant failures include both hardware and software errors.

- Third party conflict: UAS collisions with people or property resulting in injuries or damage.
- Near encounters: occur when UAS is sighted in the proximity of another aircraft; could result in the need of the aircraft to maneuver to maintain a safe distance from UAS.
- Terrain collisions: occurrence involves collisions with terrain that could result in loss of control; also, bird strikes are part of this category.

3.3.2 UAS Systems Functional Requirements

Safe integration and operation of UAS into NAS requires the accomplishment of a series of requirements. A high-end UAS existing on the market today will include the following functional requirements.

- REQ-UAS-1: UAS shall be equipped with different state-of-the-art technology such as infrared cameras, GPS, and laser.
- REQ-UAS-2: UAS shall be equipped with Obstacle Detection and Collision Avoidance Technology such as Vision Sensor, Ultrasonic, Infrared, and Lidar.
- REQ-UAS-3: UAS shall be controlled by remote Ground Control System (GSC) referred to as a ground cockpit.
- REQ-UAS-4: UAS equipment shall include an Internal Compass and Failsafe Function.
- REQ-UAS-5: UAS shall have an Intelligent Flight System for active tracking, waypoints, and others.
- REQ-UAS-6: UAS shall have a security and anti-hacking system.
- REQ-UAS-7: UAS shall have a radar positioning and return home system.

- REQ-UAS-8: UAS shall adhere to the dual Global Navigational Satellite Systems (GNSS) such as GPS and GLONASS.
- REQ-UAS-9: UAS shall fly in both GNSS and non-satellite mode.
- REQ-UAS-10: UAS shall exhibit highly accurate navigation system when flying, especially in applications such as surveying landscape and Search and Rescue missions.
- REQ-UAS-11: UAS shall have obstacles avoidance system and cameras to build a 3D map of surroundings, which will include trees, people, animals, cars, buildings, and more.
- REQ-UAS-12: UAS shall have an updated gyroscope stabilization and flight controllers.
- REQ-UAS-13: UAS propulsion systems shall include the following components: Motor Stator, Motor Bell (rotor), Windings, Bearings, Cooling System, Electronic Speed Controllers, ESC Updater, Propellers, Wiring, Arm.
- REQ-UAS-14: UAS shall have a Ground Station Controller (GSC) or a smartphone app, allowing them to fly and to keep track of the current flight telemetry.
- REQ-UAS-15: UAS telemetry data showing on the remote controller shall include range, height, speed, GNSS strength, remaining battery power, and warnings.
- REQ-UAS-16: UAS shall adhere to the latest “No Fly Zone Technology” to increase flight safety and prevent accidents in restricted areas.
- REQ-UAS-17: UAS shall be updated with the new “First Person View’’ technology; a video camera shall be mounted on the unmanned aerial vehicle to broadcast the live video to the pilot on the ground.
- REQ-UAS-18: UAS pilots shall be flying the aircraft as if they were on-board the aircraft instead of looking at the aircraft from the pilots’ actual ground position.

- REQ-UAS-19: UAS shall be equipped with firmware and flight assistant port; the flight control system communicates with a PC assistant through a micro-USB cable; this shall allow configuration of the UAS and to upgrade the drone firmware.
- REQ-UAS-20: UAS shall have LED flight indicators that are found at the front and the rear of the drone; generally, LEDs shall be green, yellow or red.
- REQ-UAS-21: UAS shall operate with Remote Control System; UAS and the ground control shall already be paired when it leaves the factory.
- REQ-UAS-22: UAS shall have an updated Remote Control Receiver; location of the receiver link button shall always be under the UAS.
- REQ-UAS-23: UAS shall follow the Range Extender Technology, which is a wireless communication device that generally operates within the 2.4 GHz frequency.
- REQ-UAS-24: UAS shall be equipped with an Anti-Drop Kit to help keep the stabilizer and camera connected to the aircraft.
- REQ-UAS-25: The UAS operating system shall be similar to most unmanned aircraft that use Linux and MS Windows.

3.3.2 UAS Systems Non-Functional Requirements

Safe integration and operation of UAS into NAS also requires the accomplishment of a series of non-functional and operational requirements. A high-end UAS existing on the market today will include the following non-functional requirements. The below list includes also operational requirements.

- REQ-UAS-26: UAS shall be kept within sight (an observer may aid with this task; Pilot (or observer) cannot be responsible for more than one UAS at a time.

- REQ-UAS-27: UAS shall not be operated in any careless or reckless manner.
- REQ-UAS-28: UAS shall be flown during daylight or in twilight with appropriate anti-collision lighting.
- REQ-UAS-29: UAS shall fly with minimum weather visibility is three miles from the control station.
- REQ-UAS-30: UAS shall have the maximum allowable altitude of 400 feet above the ground, and higher if the drone remains within 400 feet of a structure.
- REQ-UAS-31: UAS maximum speed shall be 100 mph (87 knots).
- REQ-UAS-32: UAS shall not be flown over anyone who is not directly participating in the operation, under a covered structure, or inside a covered stationary vehicle.
- REQ-UAS-33: UAS operation from a moving vehicle shall not be allowed unless flying over a sparsely populated area.
- REQ-UAS-34: UAS operation in Class G airspace shall be allowed without air traffic control permission.
- REQ-UAS-35: UAS operation in Class B, C, D and E airspace shall need ATC approval.
- REQ-UAS-36: UAS shall carry an external load only if it is securely attached and does not adversely affect the flight characteristics or controllability of the aircraft.
- REQ-UAS-37: UAS shall be made available to the FAA for inspection or testing on request; any operation that results in serious injury, loss of consciousness, or property damage must be reported to the FAA.
- REQ-UAS-38: UAS pilot shall ensure safe operation both in the sky and on the ground and maintain separation at any time.
- REQ-UAS-39: UAS shall remain always clear of all aircraft, people, and structures.

- REQ-UAS-40: UAS shall adhere to airspace, aircraft operations, and privacy laws always.
- REQ-UAS-41: UAS shall maintain minimum separation with all obstacles on ground.
- REQ-UAS-42: UAS deployment shall be in safe distance from observers.
- REQ-UAS-43: UAS shall fly with approved flight plans unless below 400 ft where there is no obligation for approval.
- REQ-UAS-44: UAS shall be operated by operators certified by the local authorities.

3.3.3 Recreational UAS Requirements

A series of new requirements are considered below for recreational type UAS (FAA, 2021a; 2021b).

- REQ-UAS-45: Recreational UAS shall fly only for recreational purposes (enjoyment).
- REQ-UAS-46: Recreational UAS shall follow the safety guidelines of an FAA-recognized Community Based Organization (CBO).
- REQ-UAS-47: Recreational UAS shall be kept within the visual line of sight or use a visual observer who is co-located (physically next to) and in direct communication with them.
- REQ-UAS-48: Recreational UAS shall give way to and do not interfere with manned aircraft.
- REQ-UAS-49: Recreational UAS shall fly at or below 400 ft in controlled airspace (Class B, C, D, and E) only with prior authorization.
- REQ-UAS-50: Recreational UAS shall fly at or below 400 feet in Class G (uncontrolled) airspace.
- REQ-UAS-51: Recreational UAS pilots shall take The Recreational UAS Safety Test and carry proof of test passage.

- REQ-UAS-52: Recreational UAS pilots shall have a current registration, marked on the outside with the registration number, and carry proof of registration.
- REQ-UAS-53: Recreational UAS shall not operate systems in a dangerous manner.
- REQ-UAS-54: Recreational UAS shall not interfere with emergency response or law enforcement activities.
- REQ-UAS-55: Recreational UAS pilots shall not fly under the influence of drugs or alcohol.
- REQ-UAS-56: Recreational UAS pilots shall not violate any of these rules, and/or operating in a dangerous manner.
- REQ-UAS-57: In case of violation, recreational UAS pilots shall be subject to FAA enforcement action.

3.3.4 UAS Certified Remote Operators Requirements

Additional requirements were identified for UAS certified remote operators and must be considered for commercial operations. The requirements add more safety concerns and hazards with potential risks if they are not followed properly as specified.

- REQ-UAS-58: UAS operators shall not fly around airports because it is difficult for manned aircraft to see and avoid a drone while flying.
- REQ-UAS-59: UAS operators shall avoid manned aircraft and are responsible for any safety hazard their system creates in an airport environment.
- REQ-UAS-60: UAS operators shall not enter a runway without any prior clearance or approval.
- REQ-UAS-61: UAS operators shall be in good physical and mental condition to safely fly their aircraft.

- REQ-UAS-62: UAS operators shall not pilot more than one aircraft at a time.
- REQ-UAS-63: UAS operators shall a have a remote pilot certificate or be under the direct supervision of a person who holds the certificate type.
- REQ-UAS-64: UAS operators shall confirm that aircraft is in good condition for safe operation before each flight.
- REQ-UAS-65: UAS operators shall immediately notify NTSB of any accident or incident.
- REQ-UAS-66: UAS operators shall not fly over public roads, nor take off or land on roads.
- REQ-UAS-67: UAS operators shall not expand existing privacy threats and create new methods of invading privacy in any manner.

3.4 System Safety Hazard and Risk Modeling

3.4.1 Hazard Identification

One of the first steps performed for system safety assessment is hazard identification and analysis. Review of the literature identified a new taxonomy for hazard analysis called Hazard Analysis and Classification System (HCAS), which considers four main hazard system sources: Airmen, UAS, Operations, and Environment (Luxhoj, 2013). To perform hazard analysis, safety engineers define first a preliminary hazard list, which is further refined with new hazards and more details to the initially identified ones. To make the hazard analysis a comprehensive process, the identified hazards correspond to the high-end type of UAS, which are practically equipped with similar systems as a manned small aircraft. For example, high-end UAS are equipped with ADS-B Out system. The same approach is considered for the subsequent risk analysis, where to provide a comprehensive analysis, the processes included for risk control and mitigation are similar to the ones the UAS manufacturer and pilot as well as the aviation safety body are similar or the same as those for a manned small aircraft. FAA info is used throughout the section (FAA, 2019, 2020a, 2020b).

3.4.2 Preliminary Hazard List

The following hazards were identified during the initial steps of the safety risk assessment process and are included in the list below. For each of the hazards their description, system state, and effects are presented.

Hazard 1 (H-1): Potential RF communication issues

- Description: Radio frequency interference, electromagnetic interference, simultaneous transmissions, and congestion.
- System state: Inability to establish radio communication, loss of communication between the UAS and the radio station.
- Hazard effects if activated: Collision with a manned aircraft in air; in the worst cases, fatalities.

Hazard 2 (H-2): Communication link failure

- Description: The command and control (C2) communication link may fail.
- System state: Loss of real-time C2 communication data link between the Pilot in Command (PIC) and the UAS.
- Hazard effects if activated: Fatalities or injury to persons other than the UAS, mid-air collision.

Hazard 3 (H-3): Loss of navigation capabilities

- Description: UAS may loss navigation capabilities.

- System state: Reduced separation between aircraft with operational errors of high severity, i.e., an unsafe state is built from operational mistakes; failures in the communication between remote pilot and aircraft, i.e., UAS losses piloting capability.
- Hazard effects if activated: Possibility of collision occurs because of proximity of less than 500 feet to another aircraft, catastrophic damage, mid-air collision, and death.

Hazard 4 (H-4): UAS fly away

- Description: UAS may fly away, loss of remote pilot control.
- System state: Interruption or loss of the remote control, pilot is unable to affect control of the aircraft and, as a result, the UAS is not operating in a predicable or planned manner, reduction of separation between UAS and other aircraft.
- Hazard effects if activated: Discomfort to those on ground, serious injury to persons on ground, mid-air collision, infrastructures/building damage.

Hazard 5 (H-5): Avionics failure

- Description: Avionics instruments may fail.
- System state: GPS stabilizer defect, altitude indicator with the rate-of-turn indicator and vertical speed indicator malfunction, pilot not familiar with area.
- Hazard effects if activated: Harm to people/other aircraft, damage of UAS, damage of infrastructure.

Hazard 6 (H-6): Power Failure/Mechanical/Battery issues

- Description: Loss of power, mechanical issues and or battery life may decrease.

- System state: UAS motor failed, hardware failed, battery or power failed, software crashed, GPS fail, lost link, avionics fail, pilot command lost.
- Hazard effects if activated: Collision between UAS and aircrafts/other persons and infrastructures, ground or mid-air collisions.

Hazard 7 (H-7): Wildlife issues

- Description: Birds may strike UAS, stuck in UAS parts (wings, engine etc.)
- System state: Aircraft deviates with birds on air, struck and unstable UAS, conflict during takeoff, approach, and landing, conflicting state with terrestrial animals on the ground during the takeoff, roll, or landing, take off/landing aborted, changed path, flight aborted.
- Hazard effects if activated: Damage to UAS, crash, discomfort to those on ground, striking a person on the ground causing injury or fatality, collision with aircraft on air, damage to infrastructures.

Hazard 8 (H-8): Runway conflicts

- Description: Hazardous things/persons/objects on runway, obstacles may appear during approach and landing, blocked traffic, people on runway, runway excursions, contaminated runways or flooded.
- System state: high approach speeds, unstable approaches and go-around decision making, deviation of UAS.
- Hazard effects if activated: Collison with people, infrastructures and objects on the runway and ground, damage to UAS systems, UAS crash/fatalities, injury to people.

Hazard 9 (H-9): External systems failure

- Description: External systems supporting UAS operations may fail, malfunctions of system components that are not part of UAS, but support safety and operations may occur.
- System state: ADS-B lost signal, losses of station GPS signal, radio station fail, UTM failure, cyber-attack, ATC station power failure, screen black out, no traffic advisories.
- Hazard effects if activated: Mid-air collision, ground collisions, near misses, lost communication and interference, which will cause confusions, reduction of separation between aircrafts, delays, damage, injury, and/or fatalities.

Hazard 10 (H-10): Human error

- Description: Remote pilot or ATC mistake that causes deviation and unsafe state with other aircraft, maintenance errors, improper handling of traffic advisories and information, confused traffic information.
- System state: UAS on unplanned route and wrong path, conflicting state and reduced separation, conflict with traffic in visual line and path.
- Hazard effects if activated: Near misses, collisions with other manned aircraft, discomfort to UAS and pilot, planned route deviation in hazardous conditions.

Hazard 11 (H-11): Adverse weather and operating conditions

- Description: Un-forecasted weather conditions, reduced or low visibility, topography unique weather.
- System state: UAS unable to fly planned route, flight operation abortion and deviation to unplanned routes, losses of navigation capabilities, loss of control and visual line.

- Hazard effects if activated: Collison between UAS and other manned aircraft, ground collision, damage to UAS and other buildings/infrastructures.

Hazard 12 (H-12): Loss of UAS detection and control

- Description: UAS may be lost without noticing, remote UAS detector failed, remote pilot losses control over crashed UAS.
- System state: failed UAS detector, loss of situational awareness and control of the UAS during conditions of low speed, high pitch and high bank angle, weight and balance issues, lost trajectory, crashed UAS.
- Hazard effects if activated: crash into a building or obstacle resulting in secondary injury from UAS debris or building damage, mid-air collision with other unmanned or manned aircraft, and potentially one or more injuries or fatalities.

Hazard 13 (H-13): Detect and avoid system failure

- Description: Loss of visual line of sight, UAS limited ability to sense intruding aircraft, detect and avoid system error.
- System state: Traffic conflicts, UAS failed to detect intruders due to size, detection errors, unexpected low altitude operations.
- Hazard effects if activated: Collison between UAS and other manned aircraft, catastrophic damage and fatalities to people and infrastructures.

3.4.3 Functional Hazard and Risk Modeling

The functionality of a system determines what the system must do to deliver the required system behavior, broken down into functions with input, output, and transformation rules. The following functional hazards were identified during the safety risk assessment process, and were present among the hazards included in the Preliminary Hazard List. For each of the functional hazards their description, effects, system state, causes, existing controls and justification are presented. In addition, all the elements of the risk analysis are included for all identified functional hazards, which include the resulting risk severity and its rationale, risk likelihood and rationale, initial mishap risk, safety recommendations and organizations responsible for their implementation, and predicted residual risk and the prediction rationale are presented. To make the functional hazard analysis a comprehensive process, the identified hazards correspond to the high-end type of UAS, which are practically equipped with similar systems as a manned small aircraft. For example, high-end UAS are equipped with ADS-B Out system. The same approach is considered for the subsequent risk analysis, where to provide a comprehensive analysis, the processes included for risk control and mitigation are similar to the ones the UAS manufacturer and pilot as well as the aviation safety body are similar or the same as those for a manned small aircraft.

Functional Hazard 1 (FH-1): Command and control of remote pilot failure

- Function: Command and control (C2) UAS (between UAS and control station).
- Hazard Description: loss of command and control over UAS operations, malfunction of technical component of the UAS, transponder may fail, geofencing may fail, data may be lost, software may fail, remote communications may fail.
- Effects: UAS may undertake an unpredictable and unnecessary maneuver, it may result in uncontrolled conflicts and crashes, and possibly causing injury and/or death.
- System State: Fly away, total loss of C2 data link, UAS leaves planned route that may cause a deviation from planned operations, pilot unable to monitor UAS, pilot unable to maintain command during all phases of flight.

- Cause: C2 system failed, adverse conditions occurred, loss of power, intruder attacked system, network system error and disconnected.
- Existing Controls: integrated and monitored C2 link with appropriate performance in place, competent and more trained applicant/operator to back up, technical containment in place and effective.
- Control Justification: Performance testing to avoid unnecessary operational error of high severity, UAS operator training to maintain control and follow procedures in case of command loss, external entities support such ATC report, nearby aircraft situation report and monitoring, emergency stations.
- Severity: Catastrophic (1).
- Severity Rationale: There is the consequence of reaching an unsafe and dangerous state, therefore, this risk is deemed catastrophic.
- Likelihood: Remote (C).
- Likelihood Rationale: There is the dependency of a combination of events due to control loss, multiple UAS systems may fail but the probability of this event is considered remote since C2 system is tested and inspected before any flight_operations.
- Initial Mishap Risk: 1C
- Safety Recommendations: Redundancy of technical systems, C2 link performance appropriate, safe recovery from technical issue, improve new ways of technical containment, provide alternative or manual systems in case of command loss.
- Organization Responsible for Implementing Safety Recommendations: UAS manufacturer and/or Civil Aviation Authority.

- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., catastrophic (1) and remote (C). Based on the classification presented, this is considered a Medium-Risk event.
- Predicted Residual Risk Rationale: There are many options for autonomy that may be deployed in case of C2 system loss, e.g., UAS are guided to a specific location/waypoint and fly a pattern waiting for new commands; there is also the autonomous return option; therefore, this risk is categorized as Medium-Risk event.

Functional Hazard 2 (FH-2): Communication and data system (C2) link failure

- Function: Establishes (C2) link communication.
- Hazard Description: C2 data link may be lost, cyclic and transient transmissions may fail, UAS may be unable to send and receive data in specified areas by networks parameters cyclically and automatically, communication and connectivity may be completely lost.
- Effects: increased pilot and ATC workload, call sign confusion, collision with a manned aircraft or obstacle in air, in the worst cases, fatalities.
- System State: UAS loses control, control link between the aircraft and the pilot is lost, communication C2 link system is deteriorated.
- Cause: Dysfunctional data link, UAS module not operational, maintenance or setting error, wiring of C2 cable not properly working, no power supplying to the module.
- Existing Controls: Stand-by master which is a local station that substitutes the functionality of the master station to allow data link to continue, the auto replication and two-pieces terminal block as back-up.
- Control Justification: The master data link station plays a crucial role in communication; data may link stops if that station stops abnormally; by preparing a stand-by master, auto-

replication and two-pieces terminal block in order to enhance the reliability of the network and avoid impact to the lines of systems caused by a C2 link stoppage.

- Severity: Major (3).
- Severity Rationale: There is the consequence of reaching an unsafe and dangerous state, pilot unable to establish communication parameters to C2 network, there may be a substantial damage to UAS, therefore this risk is deemed major.
- Likelihood: Probable (B).
- Likelihood Rationale: With all available functions to prevent data link stoppage and enhance network reliability, there is still a probability to be determined for this event to occur at some point, therefore the hazard likelihood is probable.
- Initial Mishap Risk: 3B
- Safety Recommendations: Have all the functions systems available any time. Frequent inspection and testing of the data link communication, adoption, and implementation of the link controller model with high speed and reliability is recommended, combination with other systems to reduce likelihood of the hazard.
- Organization Responsible for Implementing Safety Recommendations: C2 link manufacturers, FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Major (3) and Probable (B). Based on the classification presented, this is considered a Low-Risk event.
- Predicted Residual Risk Rationale: C2 link is reliable for data with retrying and resending data transmissions in case of loss due to noises. Many options as alternative were

implemented such as stand-by master, slave station disconnection, auto replication, two-piece terminal block, therefore the risk is deemed low

Functional Hazard 3 (FH-3): Detect and avoid system failure

- Function: Detect and avoid air traffic.
- Hazard Description: Detect and avoid system function may fail, UAS may fail to detect intruder aircraft.
- Effects: Possibility of collision as a result of proximity of less than 500 feet to another aircraft, conflict with another aircraft, crash occurrence, aircraft intruder is not detected when there is a threat, traffic on a collision course is tracked incorrectly as a non-threat, intruder detected but system failed avoidance rule.
- System State: UAS loses of control and/or failed to detect conflict with another aircraft. Situation result in unnecessary avoidance maneuver that endangered other aircraft.
- Cause: Pilot error, detect and avoid system failure, deterioration of weather conditions where system unable to detect and avoid, technical systems failure.
- Existing Controls: Use "see and avoid" concept at all times regardless of whether the operation is Instrument Flight Rules or Visual Flight Rules, appropriate procedures for flight operations, traffic advisory, radar and ADS-B integration, monitoring of frequency, ATC support.
- Control Justification: See and avoid is necessary as ATC cannot always keep all aircraft separated, executing appropriate clearing procedures is necessary before all climbs, descents, turns, training maneuvers, or aerobatics, awareness for type of airspace to operate within, monitor of frequency if unable to initiate contact and detect and avoid system has failed.

- Severity: Hazardous (2).
- Severity Rationale: There is the consequence of reaching an unsafe and conflicting state, UAS may follow conflicting route with other aircraft, and therefore this risk is deemed hazardous.
- Likelihood: Extremely remote (D).
- Likelihood Rationale: The hazard likelihood is extremely remote for this event due current technology most aircraft must be equipped with detect and avoid system, while UAS detect and avoid system fail, conflicting aircraft may still avoid the UAS.
- Initial Mishap Risk: 2D.
- Safety Recommendations: Practice of visual separation always in case of conflict in low altitude, all aircraft must have their detect and avoid system properly inspected and tested, ATC notification of all conflicting aircraft in case detect and avoid system failed.
- Organization Responsible for Implementing Safety Recommendations: UAS manufacturers, FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Hazardous (2) and Extremely Remote (D). Based on the classification presented, this is considered a Medium-Risk event.
- Predicted Residual Risk Rationale: Following the recommendations and appropriate procedures, the command with alternate options such as visual rules in case of detect and avoid system failure reduce the risk of mid-air collision and ground collision with people or obstacles. This is a medium risk event.

Functional Hazard 4 (FH-4): Dysfunctional flight plan command

- Function: Execute flight plan command.
- Hazard Description: flight route and information may be lost, transponder may fail, undetected flight path, incorrect operations may be performed, inappropriate command followed, UAS following different route than the one in flight plan.
- Effects: conflict with other manned aircraft, possibility of soft landing reduces the risk of fatalities, but discomfort to people on air and on ground.
- System State: loss of piloting capability, UAS is uncontrollable, UAS flying on totally different route than planned, UAS fly away.
- Cause: Dysfunctional flight plan command, power failure, slower response from flight command, maintenance error, unresponsive command button, and undetectable flight route and path.
- Existing Controls: Manual and cartographic procedures and flight route and path development, pilot training to read flight route in map in case of flight command system failure, possibility of soft landing and waiting areas based on waypoints.
- Control Justification: Manual procedures are proven to be effective in case of automatic flight plan dysfunction, pilot training is necessary to control route and aircraft path and redirect UAS to soft landing or waiting area.
- Severity: Minor (4).
- Severity Rationale: In case of lost flight path, some procedures are to be followed to avoid possible conflict and or collision, pilot will likely request earlier a soft landing and or proceed to a waiting area, therefore the severity is minor for this hazard.
- Likelihood: Remote (C).

- Likelihood Rationale: The hazard likelihood is remote because pilot will have various options to test their flight plan systems before subsequent operations, the situation occurrence may be remote since corrective action may be taken while on ground.
- Initial Mishap Risk: 4C.
- Safety Recommendations: Having alternatives option ready all the time, ensuring UAS is checked and inspected, flight plan command must be functional before any flight, familiarity with operating environments is recommended, guidance by external systems such ATC and nearby aircraft traffic advisories in case of lost flight path.
- Organization Responsible for Implementing Safety Recommendations: UAS operators and Civil Aviation Authority.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Minor (4) and Remote (C). Based on the classification presented, this is considered a Low-Risk event.
- Predicted Residual Risk Rationale: In case of flight plan command loss, pilot have many alternatives to maintain safety and avoid hazard occurrence, also the knowledge and familiarity with operational environment is an advantage in this situation and reduce the risk of high severity. It is a low-risk event.

Functional Hazard 5 (FH-5): Electrical system function failure

- Function: Control power system (electrical).
- Hazard Description: loss of power, failure of UAS electrical system and battery life, engine may fail, hardware and software may fail, navigation may fail, technical components may fail.

- Effects: Loss of the power subsystem result in loss of control of the UAS and multiple out of control operation, unsafe state is built, collision and or fatalities, communication and data is lost.
- System State: UAS operating in unsafe margins, unable to detect and avoid, loss of communication and following incorrect flight route and path.
- Cause: Low electricity or complete loss of UAS electrical system, wires deterioration and power connection failed, maintenance error or mishap, low battery life, system black-out.
- Existing Controls: Manual and cartographic procedures and flight path developed, pilot training to read flight path in case of system failure, possibility of soft landing and waiting areas based on waypoints.
- Control Justification: Manual procedures are proven to be effective in case of automatic flight plan dysfunction, pilot training is necessary to control path and redirect aircraft to soft landing or waiting area.
- Severity: Catastrophic (1).
- Severity Rationale: In case of lost flight path, some procedures in place are to be followed to avoid possible conflict and or collision, pilot will likely request earlier a soft landing and or proceed to a waiting area, therefore the severity is minor for this hazard.
- Likelihood: Extremely Remote (D).
- Likelihood Rationale: The hazard likelihood is remote because pilot will have various options to test their flight plan systems before subsequent operations, the situation occurrence may be remote since corrective action may be taken while on ground.
- Initial Mishap Risk: 1D.

- Safety Recommendations: Having alternatives option ready all the time, ensuring check and inspection of flight plan command before any flight, familiarity with operating environments, guidance by external systems such ATC and nearby aircraft traffic advisories in case of lost flight path.
- Organization Responsible for Implementing Safety Recommendations: UAS operators, Civil Aviation Authority.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Catastrophic (1) and Extremely Remote (D). Based on the classification presented, this is considered a High-Risk event.
- Predicted Residual Risk Rationale: In case of flight plan command loss, pilot have many alternatives to maintain safety and avoid hazard occurrence, also the knowledge and familiarity with operational environment is an advantage in this situation and reduce the risk of high severity. It is a low-risk event.

Functional Hazard 6 (FH-6): Transponder failure

- Function: Monitor communications.
- Hazard Description: Voice communication may fail, radio frequency interference, electromagnetic interference, simultaneous transmissions may occur, congestion.
- Effects: Pilot not familiar with area and unable to monitor frequency and operations, unsafe flying state, UAS unable to communicate with stations.
- System State: The pilot detected loss of voice communication, UAS unable to pursue flight operations, pilot not aware of meteorological and weather conditions, UAS unable to receive traffic advisories and information.

- Cause: Atmospheric conditions that deteriorates communications, bad weather, large discharges of static electricity, damage to sensitive solid-state microelectronics found in avionics, unauthorized transmissions, malicious transmissions, unresponsive transponder.
- Existing Controls: use of secondary/rescue frequency, adjustments of the radio, interference cases report, investigation of malicious interference, reported sources of interference are detected and arranged to prevent recurrence, flights operations abortion.
- Control Justification: All cases of radio interference must be reported according to the national mandatory occurrence reporting scheme, malicious interference must be investigated by the police, with the objective of identifying and prosecuting the culprit, operations abortion and return reduce the risk of collision and path interference.
- Severity: Minor (4).
- Severity Rationale: The pilot detects the loss of voice communication, may not end the mission and abort flight if alternate ATC communication link exists. There is also a secondary and rescue frequency always available. The severity of this event is minor.
- Likelihood: Frequent (A).
- Likelihood Rationale: Operation of large numbers of aircraft in the same airspace increases the likelihood of simultaneous transmission, especially when the volume of traffic approaches the maximum handling capacity of the controller, therefore the event is considered frequent.
- Initial Mishap Risk: 4A.
- Safety Recommendations: review the RTF communication equipment and operating procedures, ATC must have detailed information on RTF cross-coupling and BSS functionality. Transponder testing before any flight, proper maintenance required.

- Organization Responsible for Implementing Safety Recommendations: Civil Aviation Authority/ FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Minor (4) and Frequent (A). Based on the classification presented, this is considered a Low-Risk event.
- Predicted Residual Risk Rationale: Communication monitor refers often to voice transfer, and in case of failure command and control data link remains operable. But ATC or other air traffic instructions will not be received. Therefore, this risk is considered low in the event of piloting capabilities remains with visual detect & avoid of all traffic.

Functional Hazard 7 (FH-7): Failure of weather conditions detector

- Function: Detect adverse weather/environmental conditions.
- Hazard Description: Weather conditions detection function may fail, inoperable system, adverse weather condition exists but system failed to detect.
- Effects: UAS control and operation outside of performance envelope is lost. Possibility of conflict with other aircraft on air or encounter with people on ground or ground structures.
- System State: UAS in dense traffic environment with no weather information, miscalculated path, and route/angles, landing or approach system failed due to bad weather.
- Cause: Weather detection system failure, network and connectivity issues, lower visibility.
- Existing Controls: Notification to ATC, traffic advisories and meteorological info, report of adverse conditions and further conditions by ATC, attempt to provide instructions to UAS operator to mitigate effects of failure, practice of visual separation.

- Control Justification: ATC instructions are crucial in term of weather and environmental conditions. The reporting of the current conditions by ATC if UAS is unable to detect adverse weather will prevent damage and UAS operations failure.
- Severity: Hazardous (2).
- Severity Rationale: There is the possibility of total loss of UAS control in case adverse weather conditions were not detected, UAS operator and ATC may not prevent this occurrence in a loop due to system failure and that make the severity as hazardous.
- Likelihood: Probable (B).
- Likelihood Rationale: Weather conditions deteriorates often, and predictions are not always accurate in terms of environment, if UAS weather detection system failed, there is probability of brusque conditions deterioration and changes at any time, therefore the likelihood is probable.
- Initial Mishap Risk: 2B.
- Safety Recommendations: ATC must establish immediate communication, immediate report to ATC of weather system failure, request of traffic advisories and current weather with possibility to abort operations, maintain detect and avoid system operational, practice visual line of sight separation.
- Organization Responsible for Implementing Safety Recommendations: FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Hazardous (4) and Probable (A). Based on the classification presented, this is considered a Medium-Risk event.

- Predicted Residual Risk Rationale: In most cases, there is a backup weather information source. In worst cases, major consequences could be severe if UAS operate in a high-density traffic environment. Elsewhere the risk is considered medium.

3.4.4 System/Subsystem Hazard and Risk Modeling

The architecture of a system determines what the system is able to do to deliver the required system behavior, broken down into subsystem and components with input, output, and internal system process. The following system/subsystem hazards were identified during the safety risk assessment process, and were present among the hazards included in the Preliminary Hazard List. For each of the system/subsystem hazards their description, effects, system state, causes, existing controls and justification are presented. In addition, all the elements of the risk analysis are included for all identified system/subsystem hazards, which include the resulting risk severity and its rationale, risk likelihood and rationale, initial mishap risk, safety recommendations and organizations responsible for their implementation, and predicted residual risk and the prediction rationale are presented. To make the system/subsystem hazard analysis a comprehensive process, the identified hazards correspond to the high-end type of UAS, which are practically equipped with similar systems as a manned small aircraft. For example, high-end UAS are equipped with ADS-B Out system. The same approach is considered for the subsequent risk analysis, where to provide a comprehensive analysis, the processes included for risk control and mitigation are similar to the ones the UAS manufacturer and pilot as well as the aviation safety body are similar or the same as those for a manned small aircraft.

System/Subsystem Hazard 1 (SSH-1): Radio failure

- Hazard Description: communication system may fail, radio frequency may interfere with other systems, electromagnetic discharges, simultaneous transmissions may occur, traffic congestion.
- Cause: Establishment of radio communication failed, communication system failed between the UAS and the radio station.
- System State: Pilot unable to communicate or receive proper traffic instructions, confused and errored information reception.
- Existing Controls: Use of secondary frequency and radio station, back-up frequency and emergency radio station available, use of nearby stations or other aircrafts radio frequency to communicate, operations on rescue frequency.
- Control Justification: The back-up and rescue frequency are necessary control to mitigate the risk of call interference and confusion on ATC instructions. Immediate switch to rescue frequency is necessary to avoid risk of misinformation and collecting other traffic intended traffic information.
- Effects: Confused states causing deviation from intended route, improper traffic information that can lead to collision with a manned aircraft in air, lost UAS in the worst cases, fatalities.
- Severity: Hazardous (2).
- Severity Rationale: The radio frequency failure or interference represent a major hazard because of misleading traffic info and therefore risk of collision or path interference with other aircraft.
- Likelihood: Probable (B).

- Likelihood Rationale: Due to large numbers of aircraft in the same airspace the likelihood of simultaneous transmission, especially when the volume of traffic approaches the maximum handling capacity of the ATC, therefore the event is considered probable.
- Initial Mishap Risk: 2B.
- Safety Recommendations: Awareness for blocked transmissions, strict observance of standard RTF procedures and phraseology, including rigorous application of the read-back, hear-back process.
- Organizations Responsible for Implementing Safety Recommendations: Civil Aviation Authority, FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Hazardous (2) and Probable (B). Based on the classification presented, this is considered a Medium-Risk event.
- Predicted Residual Risk Rationale: Radio communication refers often to voice transfer between ATC and UAS pilot, in case of failure, UAS is still operable but ATC or other air traffic instructions will not be received. Therefore, the risk of collision occurs, so this is considered a Medium Risk event.

System/Subsystem Hazard 2 (SSH-2): Loss of network connectivity

- Hazard Description: Data and communication (C2 link) system failure, navigation may fail, UAS may loses control, remote network station may deteriorate.
- Cause: Data link system may fail to connect, network and connectivity issues, module not operational, pilot error or setting error, deterioration of wiring cables, power or connectivity to network is lost, bad weather conditions occurrence.

- System State: UAS losses real-time command and control data link, link between the Pilot in Command (PIC) and the UAS is lost, connectivity to remote station is lost.
- Existing Controls: Back up functions and systems that maintain communication such as local station that substitutes the functionality of the master station to allow data link to continue, secondary network connectivity.
- Control Justification: The back-up data link station will easily replace data link structure if it stops, and the network station stops abnormally. These functions enhance network reliability and avoid impact caused by a C2 link stoppage; secondary network selection is proven effective in case the main network is lost.
- Effects: UAS is inoperable, loss of control, possibility of divergence and collision occurs because of proximity of less than 500 feet to another aircraft, catastrophic damage.
- Severity: Major (3).
- Severity Rationale: There is the consequence of reaching an unsafe and dangerous state if pilot losses UAS control while unable to establish communication and connectivity parameters to C2 network, substantial damage to UAS, therefore this risk is deemed major.
- Likelihood: Remote (C).
- Likelihood Rationale: This hazard likelihood is probable even though C2 link has integrated multiple back-up systems, cannot completely rely on network connectivity, and eliminates the risk of immediate loss of UAS control.
- Initial Mishap Risk: 3C.
- Safety Recommendations: Network reliability, frequent inspection and testing of the data link communication and back-up network functions, implementation of the most

performant link controller model with high speed and reliability is recommended, combination with other systems to reduce parameters errors.

- Organizations Responsible for Implementing Safety Recommendations: Network operators, C2 link manufacturers, FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Major (3) and remote(C). Based on the classification presented, this is considered a Medium-Risk event.
- Predicted Residual Risk Rationale: C2 link system is proven to be reliable for data connection with multiple options to retry and resend data transmissions in case of loss. Many alternatives are available onboard to allow connection and data transmission and reception from stations, therefore the risk is deemed Medium.

System/Subsystem Hazard 3 (SSH-3): Navigation systems failure

- Hazard Description: Loss of navigation capabilities, navigation system and subsystems failure may fail.
- Cause: lack of network connectivity, navigation subsystem command failure or broken, power failure, slower response from flight command, board panel deterioration.
- System State: loss of piloting and orientation capability; pilot unable to control UAS route and craft, UAS deviation to conflicting path with other aircraft.
- Existing Controls: Manual and written procedures for flight path and route developed, pilot training to read and understand flight path in case of navigation system issue, possibility to perform a soft landing or wait on specific areas based on waypoints, familiarity with operating areas.

- Control Justification: Written manual navigation procedures are proven to be effective in case of navigation issues, pilot training is necessary to control path and redirect aircraft to soft landing or waiting area, and familiarity with area will reduce risk of collision with unknown obstacles.
- Effects: an unsafe state is built from operational mistakes. C2 link failure, failures in the communication between remote pilot and aircraft, loss of piloting capability, fatal injury to persons other than the UAS, mid-air collision.
- Severity: Hazardous (2).
- Severity Rationale: In case of navigation system failure, alternative procedures may be followed to avoid conflict and or collision, pilot may request immediate soft landing and or proceed to a waiting area, but in high density traffic area the risk of path interference with other aircraft is high, which is a hazardous severity.
- Likelihood: Extremely remote (D).
- Likelihood Rationale: This hazard likelihood is extremely remote because pilot many inspections and test of UAS flying capabilities before operations, the hazard occurrence may be extremely remote since corrective action are performed while on ground.
- Initial Mishap Risk: 2D.
- Safety Recommendations: Alternate options must be ready within time, the check and inspection of navigation command must be performed before any flight, familiarity with operating environments, guidance by external systems such ATC and nearby aircraft traffic advisories in case of lost flight path.
- Organizations Responsible for Implementing Safety Recommendations: UAS manufacturers, FAA office of aviation safety.

- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Catastrophic (1) and Extremely Remote (D). Based on the classification presented, this is considered a Medium-Risk event.
- Predicted Residual Risk Rationale: Loss of navigation capabilities have direct consequences to UAS and operations. It is important to maintain UAS control at any time for safety reasons, failure of navigation capabilities in the worst cases fatalities in high density traffic area, therefore this is a high-risk event.

System/Subsystem Hazard 4 (SSH-4): Avionics system failure

- Hazard Description: Electronics may fail, engine controls, flight control systems, weather radar, navigation and communications, flight recorders, lighting systems, threat detection, fuel systems, electro-optic systems, performance monitors may fail.
- Cause: Power plant defect, display and management failure, software/hardware failure, communication or navigation failure, GPS stabilizer defect, avionics components and subsystems error, avionics maintenance error.
- System State: Pilot loses control of UAS operating capabilities, UAS in unstable state, safety margins decreasing, UAS unable to detect and avoid, lost navigation and communication.
- Existing Controls: Manual pilot activation, emergency call for ATC assistance and other nearby stations is possible, flight abortion and immediate soft-landing request, if power loss is detected, operation may be aborted, rerouting and landing procedures in place.
- Control Justification: Integrated avionics modules are safety critical and software intensive systems, failure of these systems may have catastrophic consequences. Therefore, drastic

controls such emergency rescue and ATC assistance are needed to mitigate potential hazard resulting in avionics failure.

- Effects: Loss of control of the UAS and multiple out of control operation, unsafe state, collision and or fatalities, harm to people/buildings, damage of UAS, damage of infrastructure.
- Severity: Catastrophic (1).
- Severity Rationale: Since integrated avionics modules are safety critical and software intensive systems, these systems are necessary for all phases of UAS operations and ensure safety, therefore failure of these systems may have catastrophic severity.
- Likelihood: Remote (C).
- Likelihood Rationale: This hazard likelihood is considered remote as research and development have improved efficiency by reducing weight and power consumption through different resources. The likelihood is often mitigated by reliable and high-definition systems.
- Initial Mishap Risk: 1C.
- Safety Recommendations: Preventive maintenance, external back-up system capable of taking remote control, smart cockpit technology, emergency management technology, improved training for maintenance professionals.
- Organizations Responsible for Implementing Safety Recommendations: UAS manufacturers, FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Catastrophic (1) and Remote (C). Based on the classification presented, this is considered a High-Risk event.

- Predicted Residual Risk Rationale: The hazard related to avionics components failure are considered high risk event because they have the combination of all systems supporting the UAS function and operations, failure of one system may cause all component to fail and the consequences may be fatal.

System/Subsystem Hazard 5 (SSH-5): Engine system failure

- Hazard Description: Engine may fail, mechanical, power, battery subsystems issues may arise.
- Cause: Loss of electrical coupling, battery or power loss resulting in engine failure, loss of power, failure of UAS electrical system and battery life.
- System State: UAS operating in unsafe margins, unable to detect and avoid, loss of communication, failed engine in flight, undetected UAS location, UAS loss of control in flight, aircraft crashes.
- Existing Controls: Secondary power system available, use of battery, emergency response, flight abortion and control under minimal operations by ATC, soft landing.
- Control Justification: In case of primary system power loss, secondary backup power system is available to prevent UAS from losing total control and pursue minimal operations, abortion of flight and emergency response and control exist if engine fails to avoid unnecessary risks that decrease safety margin of UAS and other aircraft accident.
- Effects: Collision between UAS and aircrafts/other persons/infrastructures, Ground/midair collisions.
- Severity: Catastrophic (1).

- Severity Rationale: Power failure if not properly detected may cause fatal accidents because UAS may lose control over operations and crash onto building/people or cause mid-air collision, this hazard category is catastrophic.
- Likelihood: Frequent (A).
- Likelihood Rationale: There are around 40% engine failure/power loss per 10,000 sport and recreational aircraft. Those cases refer to piston which are less reliable with a frequent occurrence, but it should be considered as well for UAS electric motors.
- Initial Mishap Risk: 1A.
- Safety Recommendations: Immediate action items, maintain battery power for emergency landing, use of high reliable batteries, report engine failure to ATC for assistance, flight under visual flight rules mode, landing as soon as possible in safe area.
- Organizations Responsible for Implementing Safety Recommendations: UAS manufacturers, operators, and FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Catastrophic (1) and Frequent (A). Based on the classification presented, this is considered a High-Risk event.
- Predicted Residual Risk Rationale: Engine failure due to power loss represent the second leading cause of fatal accidents, behind the loss of control-inflight, the consequences are drastic with collision on air, on ground, approach/landing. This is a high-risk event based on those issues.

System/Subsystem Hazard 6 (SSH-6): Traffic detection systems failure

- Hazard Description: Detect and avoid system may fail, UAS may have limited ability to sense intruding aircraft.

- Cause: Pilot error, detect and avoid system failure, lower visibility and deterioration of weather conditions, technical systems failure, maintenance error.
- System State: UAS in conflict with traffic. Situation may result in UAS performing unnecessary avoidance maneuver that will endanger other aircraft, UAS detection failed due to size, unexpected low altitude operations, UAS in high density traffic.
- Existing Controls: The "see and avoid" rule exists regardless of flight operation under instrument flight rules or visual flight rules, appropriate procedures for visual flight operations, traffic advisory, radar and ADS-B integration, frequency monitoring by pilot.
- Control Justification: See and avoid may keep UAS away from conflicting path. ATC cannot always keep all aircraft from each other's, Following appropriate clearing procedures is necessary before all climbs, descents, turns, training maneuvers, or aerobatics, awareness, monitor of frequency if unable to initiate contact to know surrounding aircraft.
- Effects: Collison between UAS and other manned aircraft on Air, catastrophic damage, and fatalities.
- Severity: Hazardous (2).
- Severity Rationale: There is the consequence of reaching an unsafe and conflicting state, UAS may follow conflicting route with other aircraft, perform dangerous maneuver or near misses, therefore this risk is deemed hazardous.
- Likelihood: Remote (C).
- Likelihood Rationale: The hazard likelihood is remote for this event due to current technology and alternative to detect and avoid most aircraft may fly under visual rules in

case of detection failure, while UAS detect and avoid system fail, conflicting aircraft may still avoid the UAS also. This is classified as remote.

- Initial Mishap Risk: 2C.
- Safety Recommendations: Visual separation rule appliance, in case of low altitude conflict, all aircraft must have their detect and avoid system properly inspected and tested, ATC must provide traffic information and advisories to all conflicting aircraft in case of loss detection, emergency landing if bad weather conditions.
- Organizations Responsible for Implementing Safety Recommendations: UAS manufacturers, operators, and FAA office of aviation safety.
- Predicted Residual Risk: The initial risk is based on the combination of severity and probability, i.e., Hazardous (2) and Remote(C). Based on the classification presented, this is considered a Low-Risk event.
- Predicted Residual Risk Rationale: Multiple alternate options are available for UAS unable to automatically detect and avoid, visual flight rules, ATC assistance with traffic information and advisories, flight abortion and landing are applicable in this state to mitigate safety risk with other aircraft. This may be defined as a low-risk hazard.

Chapter 4

Safety Risk Analysis and Implementation

4.1 Safety Risk Levels

The Safety Risk Management Framework (FAA, 2018a) presents the severity and likelihood of mishap events used for aviation operations, which can be used for UAS operations as well. Given that flying UAS in controlled airspace or by violating operational requirements may result in hazards to commercial aviation, property and the general public, the aviation severity and likelihood models apply for UAS operations as well as new airspace entrants' operations.

It is well established that an identified hazard can result in more than one outcome and that these outcomes may have different levels of severity and likelihoods of occurrence. It is also well established that the qualitative measure not only vary across categories but can also vary in a specific category within a certain range. The severity and likelihood categories used in safety risk management are presented in Tables 4-5 below. The mishap risk severity caries from Minimal to Minor, Major, Hazardous, and to Catastrophic, while the mishap risk likelihood varies from Frequent to Probable, Remote, Extremely Remote, and to Extremely Improbable. The intersection of risk likelihood and severity defines the risk index, which is used both as initial risk/mishap index and final/predicted risk/mishap index after the mitigation implementations.

Table 4: Mishap Risk Severity Levels and Evaluations (FAA, 2018a)

Minimal 1	Minor 2	Major 3	Hazardous 4	Catastrophic 5
Negligible safety effect	Physical discomfort to persons Slight damage to aircraft or vehicle	Physical distress or injuries to persons Substantial damage to aircraft or vehicle	Multiple serious injuries; fatal injury to a relatively small number of persons (one or two); or a hull loss without fatalities	Multiple fatalities (or fatality to all on board) usually with the loss of aircraft or vehicle

Table 5: Mishap Risk Likelihood Levels and Evaluations (FAA, 2018a)

Likelihood	Qualitative Evaluation	Quantitative Evaluation
Frequent A	Expected to occur routinely	Expected to occur more than 100 times per year (or more than approximately 10 times a month)
Probable B	Expected to occur often	Expected to occur between 10 and 100 times per year (or approximately 1-10 times a month)
Remote C	Expected to occur infrequently	Expected to occur one time every 1 month to 1 year
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 1 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than one time every 10 years

The color coded risk management matrix of Fig. 3 is used for the safety risk analysis process, levels used in the process are defined below. A high risk, where severity and likelihood evaluations map to the red cells cannot be accepted. Mitigation and monitoring techniques should be put in place to reduce the risk to an acceptable level. However, in operational environments, high risk may exist for a short time, and short-term risk acceptance guidance are established for such cases. Medium risk, which maps to the yellow cells in the matrix of Fig. 3, can be accepted without mitigation, but tracking and monitoring are required. This does not mean that efforts should not be directed towards potentially reducing this medium risk to lower levels. The green cells of Fig. 3 represent those operational scenarios in which the risk is evaluated as low. The low risk is acceptable without restriction or limitation, and hazards are not actively monitored. Still, documentation is needed to demonstrate the reported risk level.

The overall risk matrix, obtained by combining the hazards types altogether should be used to describe the effectiveness of proposed mitigation measures. Mitigations models described in the literature (Weibel and Hansman, 2005) cover aspects such as UAS airworthiness. Through mitigation, the UAS likelihood of entering a hazardous state can be reduced, UAS likelihood of avoiding failure states can be increased, and the UAS mishap events severity can be reduced. Generally, a successful mitigation strategy may result in reduction in the expected level of loss, reduction in the potential of loss, or a combination of both. Graphically, an improvement in the expected level of loss moves the risk horizontally and to the left, an improvement in the potential of loss moves the risk vertically and to the bottom, while their combination moves the risk diagonally towards the lower left corner.

4.2 Functional Hazard Analysis Resulting Risk Levels

Section 3.4.3 identified a series of functional hazards and processed them through mitigation solution from the Initial Mishap Risk to the Predicted Mishap Risk. These final, or residual, risk levels are used to plot the Functional Hazard Analysis Risk Matrix of Fig. 8. The resulting data is used for operational scenarios decision-making. Further mitigation may be needed based on the levels of residual risk to reduce it to acceptable levels.

Severity Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A		4A			
Probable B			3B	2B	
Remote C		4C			1C
Extremely Remote D				2D	1D
Extremely Improbable E					

Fig. 8: Resultant Functional Hazard Analysis Risk Matrix

As primary UAS operational hazards, the functional hazards are both internal and external to the system. Therefore, there are ample opportunities for UAS operators to deploy a range of mitigation strategies. Those mitigations could be both operational and technical, and once employed may reduce the risk to acceptable levels and provide safe UAS operation. The reviewed literature identified mitigation examples such as parachute recovery systems, frangible systems, autonomous recovery, and autonomous flight-termination guidance systems (Clothier *et al.*, 2011; Mejias *et al.*, 2009). The analysis also includes the development of a risk matrix chart that shows the risk using risk level bubbles that differ in size and color. Fig. 9 shows the highest functional risks of

1C and 1D, which correspond to the functional hazards: (FH-1) Command and control of remote pilot failure, and (FH-5) Electrical system function failure, respectively. As a general rule, the upper right quadrant gives the highest risks in terms of severity and likelihood of occurrence.

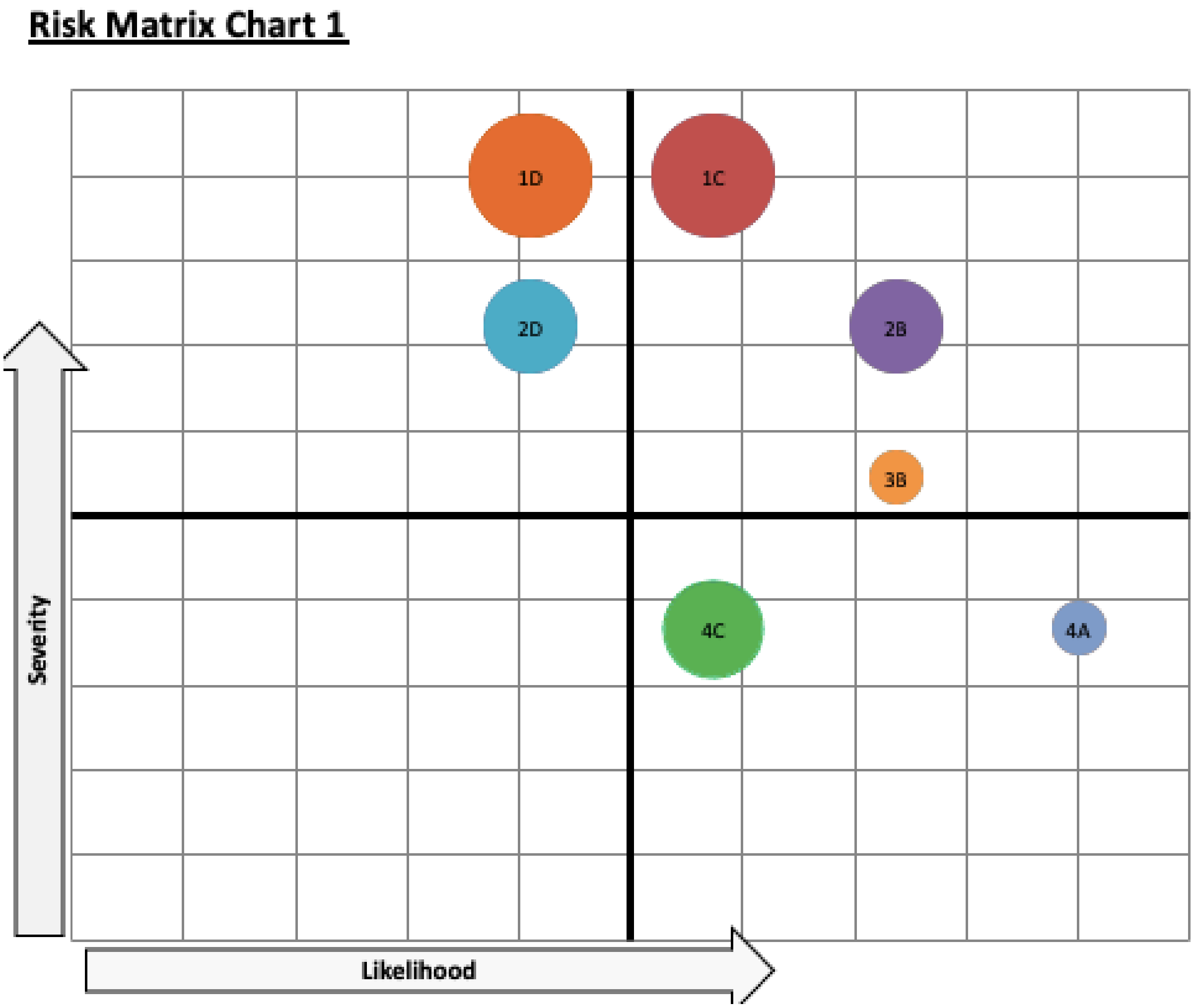


Fig. 9: Risk Matrix Bubble Chart for Identified Functional Hazards

4.3 System/Subsystem Hazard Analysis Resulting Risk Levels

Section 3.4.4 identified a series of physical architecture hazards, such as system, subsystem, and components hazards, and processed them through mitigation solution from the Initial Mishap Risk to the Predicted Mishap Risk. These final, or residual, risk levels are used to plot the System/Subsystem Hazard Analysis Risk Matrix of Fig. 10. The resulting data is used for operational scenarios decision-making. Further mitigation may be needed based on the levels of residual risk to reduce it to acceptable levels.

Severity Likelihood	Minimal 5 2	Minor 44	Major 36	Hazardous 28	Catastrophic 110
Frequent A5					1A
Probable B4				2B	
Remote C3			3C	2C	1C
Extremely Remote D2				2D	
Extremely Improbable E2					

Fig. 10: Resultant System/Subsystem Hazard Analysis Risk Matrix

For system, subsystem, and components related hazard a range of technologies could be used to provide safe implementations of physical architectures. The reviewed literature identified approaches that include the use of the risk matrix models to provide insights into mitigation needs and potential solutions to reduce the risk to acceptable levels. As for the functional hazard analysis, the current system/subsystem hazards analysis includes also the development of a risk matrix chart that depicts the identified risk using risk level bubbles that differ in size and color based on the identified risk. Fig. 11 shows the highest functional risks of 1A and 1C, which correspond to the system/subsystem hazards: (SSH-5): Engine system failure, and (SSH-4): Avionics system failure, respectively. As before, the upper right quadrant gives the highest risks in terms of severity and likelihood of occurrence.

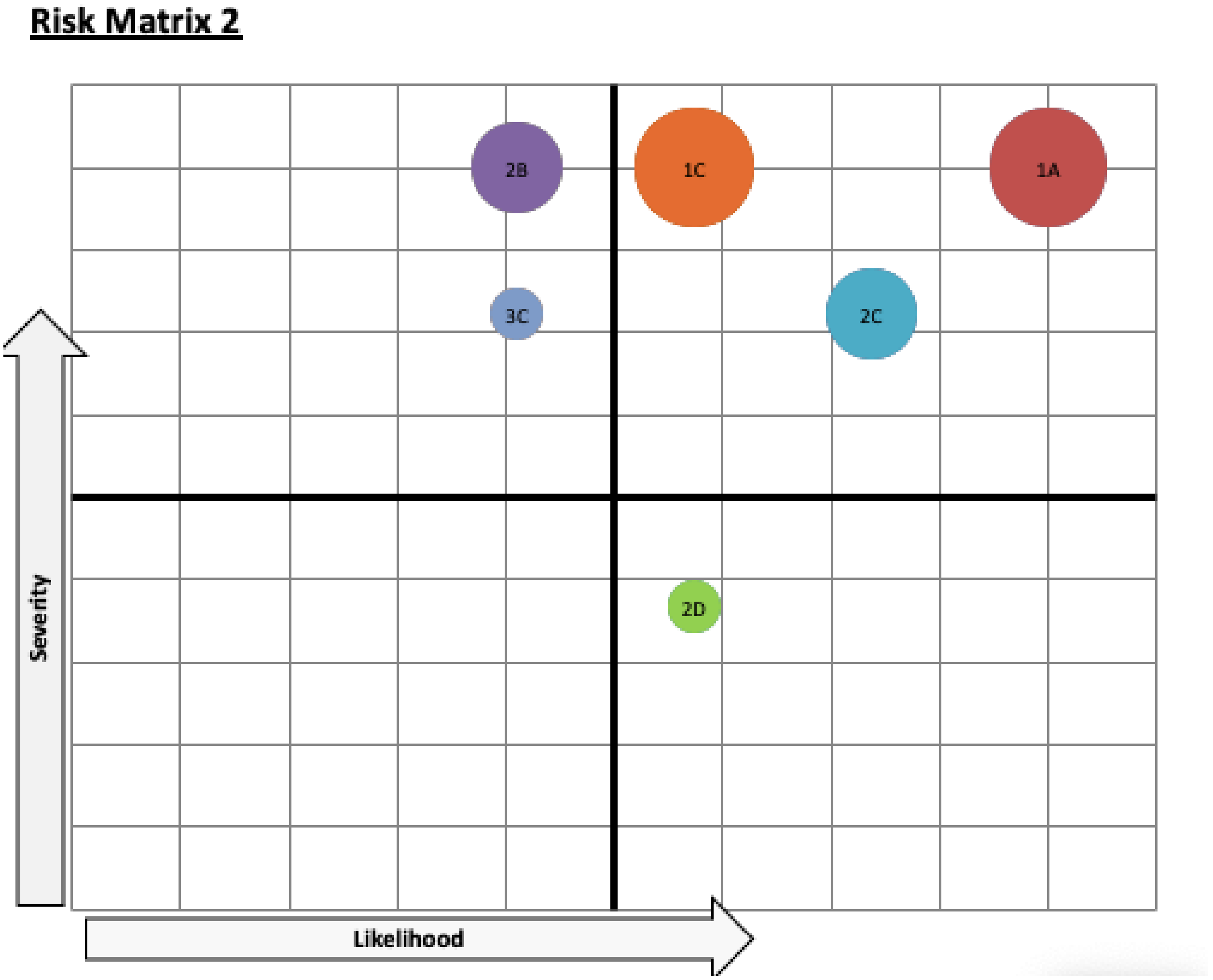


Fig. 11: Risk Matrix Bubble Chart for Identified System/Subsystem Hazards

4.4 Overall Hazard Analysis Resulting Risk Levels

To evaluate the overall hazard assessment, there is a need to identify the most significant hazards either in functionality or due to subsystems or components limitations. The two risk matrices of Fig. 8 and 10 are combined in an overall risk matrix, shown in Fig. 12.

Severity Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A		4A			1A
Probable B			3B	2B	
Remote C		4C	3C	2C	1C
Extremely Remote D				2D	1D
Extremely Improbable E					

Fig. 12: Resultant System/Subsystem Hazard Analysis Risk Matrix

Using the risk level bubble chart, all identified risks during functional hazard analysis, as well as the system/subsystem hazards analysis are shown in Fig. 13. Risk level bubbles of different size and color show the identified risk, the larger the bubble the higher the risk. Risks in the upper right quadrant are higher in terms of severity and likelihood of occurrence than in other quadrants. The highest overall risk (1A) results from the system/subsystem hazard analysis process and refers to UAS motor failure: (SSH-5): Engine system failure.

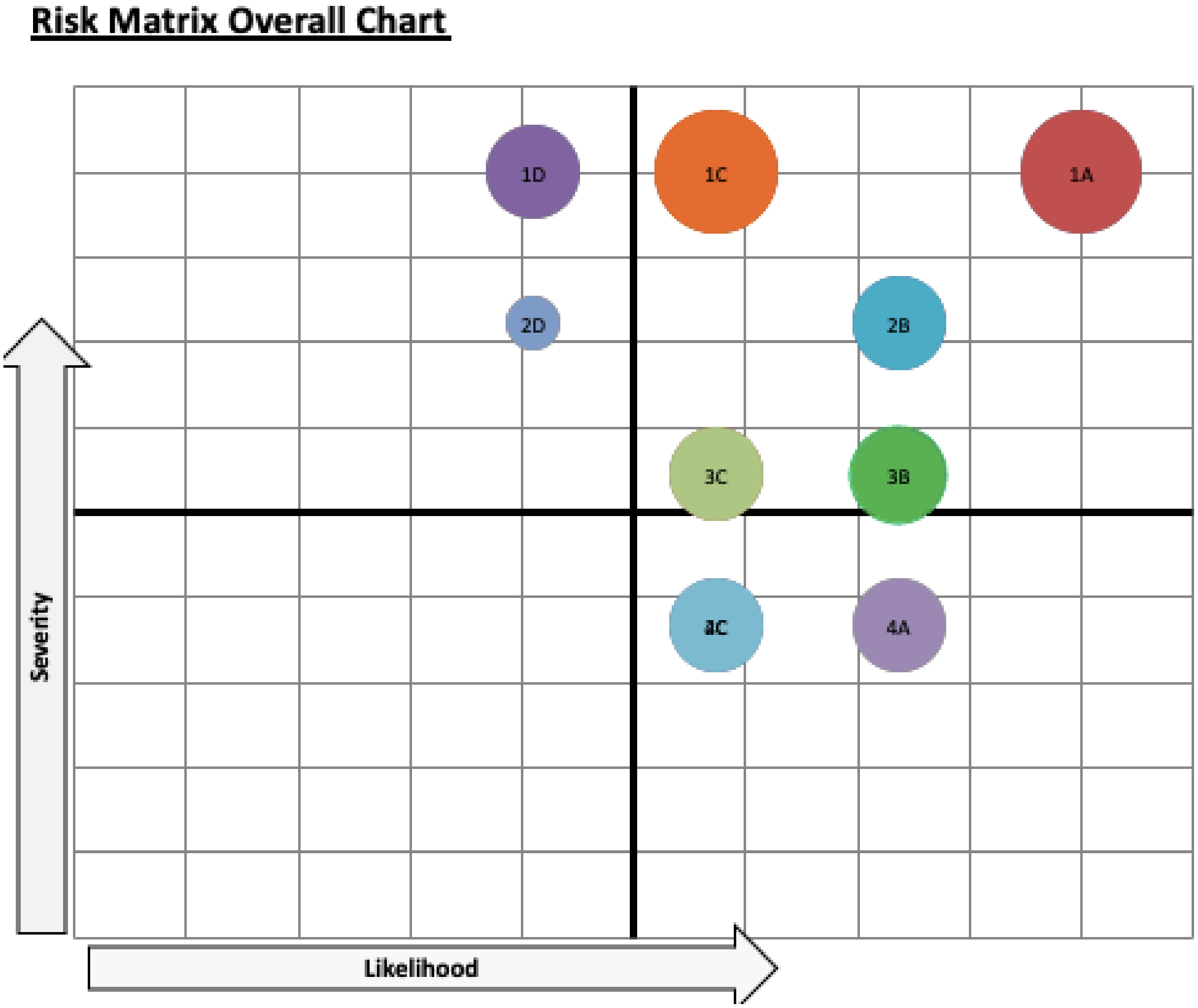


Fig. 13: Risk Matrix Bubble Chart for All Identified Hazards

4.5 Safety Risk Analysis Use Case

Consider the model in the figure below with two UAS performing their mission in a defined environment (e.g., between two high-rise buildings). The UAS flight environment is relatively uniform (i.e., it has the same width for most of its length) so that there is enough space to include two flight paths most of the time. However, it does include a narrow section, where the UAS flight paths overlap over the narrow section. To avoid collision, a stop light system is proposed to be designed, and the UAS equipped with image processing capabilities must obey to the stop light signals. The model is shown in Fig. 14 below.

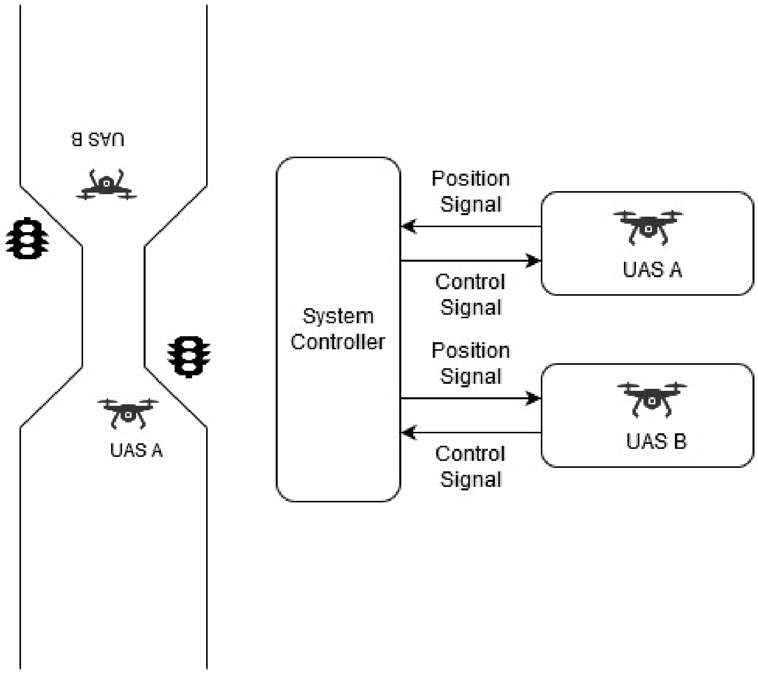


Fig. 14: UAS Safety Risk Analysis Use Case

4.5.1 Petri-Net Modeling

The first proposed solution for the use case is to use Petri-Net modeling approach to design the system controller to address the safety risk assessment of the model. The start-up sequence is not represented in the model, the two UAS are considered that they are already in flight in either direction and eventually will meet at the narrow section coming from the opposite directions. The solution includes the system controller to be installed for the stop light control of the narrow section and the Petri-Net model for the flight path of the two UAS outside and inside the narrow section of their flight paths. Since it is considered that the two UAS are already in flight, the transition states from the take-off to in-flight and from in-flight to landing are not represented in the model shown in Fig. 15. The model considers three places each for both UAS represented by the entry and exit points to the narrow sections, and the travel through it. The two stop lights are represented by another two places. The position signals and control signals are sent to the two stop lights and collision is avoided. The model does not allow the two UAS to enter and travel through the narrow sections at the same time.

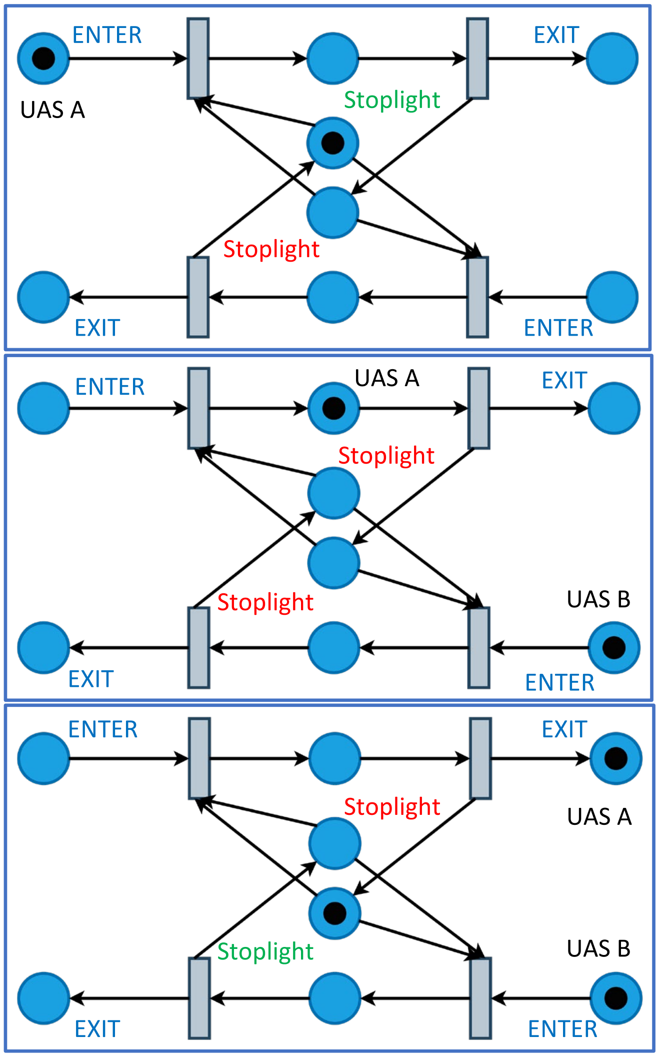


Fig. 15: UAS Safety Risk Analysis Use Case: Petri-Net Diagram

4.5.2 State Machine Modeling

The second proposed solution is to use state-machine modeling and linear temporal logic (LTL) to design the system controller to address the safety risk assessment of the model. As for the previous model, the start-up sequence is not represented in the model. The two UAS are considered already in flight in either direction and eventually will meet at the narrow section coming from the opposite directions. This second solution includes another type of system controller to be installed for the stop light control of the narrow section and the state-machine model for the flight path of the two UAS outside and inside the narrow section of their flight paths.

Since it is considered that the two UAS are already in flight, the transition states from the take-off to in-flight and from in-flight to landing are not represented in the state machine model depicted in Fig. 16. The model considers four states for each of the UAS, as well as a common collision state.

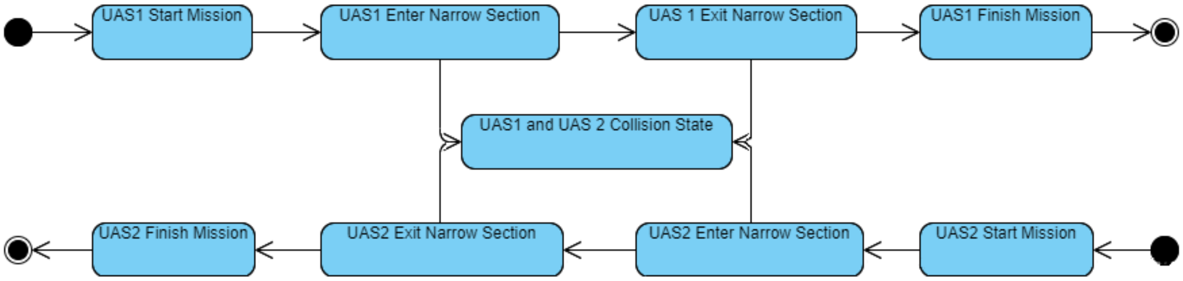

UAS1 Start Mission
UAS1 Enter Narrow Section
UAS 1 Exit Narrow Section
UAS1 Finish Mission
UAS1 and UAS 2 Collision State
UAS2 Finish Mission
UAS2 Exit Narrow Section
UAS2 Enter Narrow Section
UAS2 Start Mission

Fig. 16: UAS Safety Risk Analysis Use Case: State-Machine Diagram

- UAS Start Mission, where the UAS are following their initial calculated flight path.
- UAS Enter Narrow Section, where the UAS advance into the narrow section and only one of them can be in the section at any time.

- UAS Exit Narrow Section, where the UAS advance into the larger flight section and they can fly simultaneously.
- UAS Finish Mission, where the UAS resume following their initial calculated flight path.
- UAS Collision State, which may hold true only if the condition that only one UAS can fly within the narrow section is violated.

Therefore, an invariant for the model can be defined, and the defined invariant must not change at any time (i.e., it must remain in the false state). Environments such as Event-B model are used for defining invariants and state transitions given that they offer formal verification for design correctness by theorem proving (Abrial, 2010). A model is developed for the state transitions between the four distinct UAS states for each of the two UAS and for the common collision state.

```
MACHINE UAS
VARIABLES Position_Signal, Control_Signal
INVARIANT
   inv: ¬((mode := UAS_Start_Mission) ∧ (Position_Signal = GO) ∧ (Control_Signal = GO))
EVENTS
   Monitor = …
   Processing = …
   Correction = …
END
```

Fig. 17: UAS Safety Risk Analysis Use Case: State Machine Event-B Model

The execution of the state machine model is represented in Table 6 below, with the unsafe cases that violate the invariant highlighted. Through verification, it is assured that the invariant defined previously will always evaluate to `True`. This is equivalent to having `False` only Collision evaluations represented in the state-machine execution rows of Table 6.

Table 6: UAS Safety Risk Analysis Use Case: State-Machine Execution

UAS A Operation				UAS	UAS B Operation			
Start	**Enter**	**Exit**	**Finish**	**Collision**	**Finish**	**Exit**	**Enter**	**Start**
False	False	False	False	False	False	False	False	False
True	False	False	False	False	False	False	False	False
False	True	False	False	False	False	False	False	True
False	False	True	False	False	False	False	False	True
False	False	False	True	False	False	False	True	False
True	False	False	False	False	False	False	False	True
False	True	False	False	True	False	False	True	False
False	False	True	False	True	False	False	True	False
False	True	False	False	True	False	True	False	False
False	False	True	False	True	False	True	False	False

Chapter 5

Conclusions and Recommendations

The identified hazards exposed through the NAS integration of UAS were analyzed from the safety risks perspective. Risk mitigation can be performed since there is no uncertainty related to the UAS functionality and physical architecture and component design. The risk matrix provides a valuable tool for risk evaluation and mitigation needs. The same cannot be said for the new airspace entrants, where uncertainties may result in reduced potential for mitigation solutions.

Safety assurance recommendations include to the extent possible the employment of the safety risk assessment process, the use of quantitative risk metrics, continuously monitor the acceptable levels of risk, use of advanced airborne equipment, and reduced uncertainty in design, development, and operations of existing and new airspace entrants. Last, but not the least, safety assurance is dependent on the availability of regulations and guidelines for all air traffic actors, including UAS and new entrants.

References

Abrial, J.-R., *Modeling in Event-B: System and Software Engineering*, Cambridge University Press, 2010.

Aizpurua, J. I., Muxika, E., Model-Based Design of Dependable Systems: Limitations and Evolution of Analysis and Verification Approaches, *International Journal on Advances in Security* 6 (1-2), 12-31, 2013.

Arblaster, M. *Air Traffic Management: Economics, Regulation, and Governance*, Elsevier, 2018.

AUVSI, *Statement on FAA Expansion of Drone Detection Pathfinder Initiative*, Available at: https://www.auvsi.org/auvsi-statement-faa-expansion-drone-detection-pathfinder-initiative, 2016.

Blackburn, M. R., Austin, M. A., Coelho. M., Modeling and Cross-Domain Dependability Analysis of Cyber-Physical Systems, *IEEE International Systems Conference*, 2018.

Bolbot, V., Theotokatos, G., Bujorianu, L. M., Boulougouris, E., Vassalos, D., Vulnerabilities and Safety Assurance Methods in Cyber-Physical Systems: A Comprehensive Review, *Reliability Engineering and System Safety* 182, 179-193, 2019.

Clothier, R. A., Williams, B. P., Fulton, N. L., Definition of an Airworthiness Certification Framework for Civil Unmanned Aircraft Systems, *Safety Science* 49 (6), 871-885, 2011.

de la Vara, J.L., Ruiz, A., Gallina, B., Blondelle, G., Alana, E., Herrero, J., Warg, F., Skoglung, M., Bramberger, R., The AMASS Approach for Assurance and Certification of Critical Systems. *Embedded World Conference*, 2019.

FAA, *The Future of the NAS*, U.S. Department of Transportation, Federal Aviation Administration, 2016.

FAA, *Safety Risk Management Guidance: The 5 Step Process*, Federal Aviation Administration, 2018a.

FAA, *Safety Risk Management Guidance: SRM Tools*, Federal Aviation Administration, 2018b.

FAA, *Safety Risk Management Guidance: Applying the Acceptable Level of Risk (ALR) Approach to Commercial Space Missions in the National Airspace System (NAS)*, Federal Aviation Administration, 2018c.

FAA, *Unmanned Aircraft Systems Safety Management Policy (Order 8040.6)*, Federal Aviation Administration, 2019.

FAA, *Unmanned Aircraft Systems (UAS) Traffic Management, Concept of Operations v2.0*, Federal Aviation Administration, 2020a.

FAA, *EmpireDrone: Small Unmanned Aircraft Systems (sUAS) Aviation Training/Safety Manual*, Federal Aviation Administration, 2020b.

FAA, *Airspace 101 – Rules of the Sky*, Federal Aviation Administration 2021a. Available at: https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_101/

FAA, *Recreational Flyers & Modeler Community-Based Organizations*, Federal Aviation Administration 2021b. Available at: https://www.faa.gov/uas/recreational_fliers/

Goncalves, P., Sobral, J., Ferreira, L. A., Unmanned Aerial Vehicle Safety Assessment Modelling through Petri Nets, *Reliability Engineering and System Safety* 167, 383-393, 2017.

Hilton, S., Sabatini, R., Fardi, A., Agawa, H., Teofilatto, P., Space Traffic Management: Towards Safe and Unsegregated Space Transport Operations, *Progress in Aerospace Sciences* 105, 98-125, 2019.

ICAO, *Manual on Remotely Piloted Aircraft Systems (RPAS)*, International Civil Aviation Organization, 2015.

ICAO, *Unmanned Aircraft Systems (UAS)*, International Civil Aviation Organization, 2011.

Ivarsson, M., Gorschek, T., Technology Transfer Decision Support in Requirements Engineering Research: A Systematic Review of REj, *Requirements Engineering* 14, 155-175, 2009.

Kaur, R. K. Pandey, B., Singh, L. K., Dependability Analysis of Safety Critical Systems: Issues and Challenges, *Annals of Nuclear Energy* 120, 127-154, 2018.

Kopardekar, P., Schwartz, A., Magyarits, S., Young, J. Kriaa, S., Boissou, M., Laarouchi, Y., A New Safety and Security Risk Analysis Framework for Industrial Control Systems, *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 2018.

Kriaa, S., Boissou, M., Laarouchi, Y., A New Safety and Security Risk Analysis Framework for Industrial Control Systems, *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 2018.

Luxhoj, J. T. (2013). Predictive Analytics for Modeling UAS Safety Risks. *SAE International Journal of Aerospace* 6 (1), 128-138, 2013.

Matus, F., Hedblom, B., Addressing the Low-Altitude Airspace Integration Challenge -- USS or UTM Core? *Integrated Communications, Navigations Surveillance Conference*, 2018.

Mejias, L. Fitzgerald, D. L., Eng, P. C., Xi, L., *Forced Landing Technologies for Unmanned Aerial Vehicles Towards Safer Operations*, In: Aerial Vehicles, Thanh Mung, L. (Eds.), 2009.

Nair, S., De La Vara, J. L., Sabetzadeh, M., Bri, L., An Extended Systematic Literature Review on Provision of Evidence for Safety Certification, *Information Software Technology* 56 (7), 689-717, 2014.

Patriarca, R., Costantino, F., Di Gravio, G., Risk, Safety, Reliability and Satellites: Chronicles of a Fragmented Research Field, *Journal of Space Safety Engineering* 6, 201-211, 2019.

Pereira, D. P., Hirata, C., Nadjim-Tehrani, S., A STAMP-based Ontology Approach to Support Safety and Security Analyses, *Journal of Information Security and Applications* 47, 302-319, 2019.

Polka, M., Ptak, S., Kuziora, L., *The Use of UAV's doe Search and Rescue Operations*, Procedia Engineering 192, 748-752, 2017.

Rokseth, B., Haugen, O. I., Utne, I. B., Safety Verification for Autonomous Ships, *MATEC Web of Conferences* 273, 2019.

Sanat, K., Integrating Air and Near Space Traffic Management for Aviation and Near Space, *Journal of Space Safety Engineering* 6, 150-155, 2019.

Temme, A., Schultz, M., Dynamic Airspace Sectorisation for Flight-centric Operations, *Transportation Research Part C: Emerging Technologies* 95, 460-480, 2018.

Wang, L., Zhao, X., Zhang, Y., Wang, X., Ma, T, Gao, X., Unmanned Aerial Vehicle Swarm Mission Reliability Modeling and Evaluation Method Oriented to Systematic and Networked Mission, *Chinese Journal of Aeronautics* 34(2), 466-478, 2021.

Weibel, R. E., Hansman, Jr., R. J., Safety Considerations for Operation of Different Classes of UAVs in the NAS, *AIAA Aviation Technology, Integration, and Operations Forum*, 2014.