Document Version
Final published version

Citation (APA)
Salma, V. (2024). *Safety and Reliability of Commercial Airborne Wind Energy Systems*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:a917f333-dae7-4232-ab58-df216f3dee46

Safety and Reliability of Commercial Airborne Wind Energy Systems

Volkan Salma

SAFETY AND RELIABILITY OF COMMERCIAL AIRBORNE WIND ENERGY SYSTEMS

SAFETY AND RELIABILITY OF COMMERCIAL AIRBORNE WIND ENERGY SYSTEMS

Dissertation

for the purpose of obtaining the degree of doctor
at Delft University of Technology
by the authority of the Rector Magnificus Prof.dr. ir. T.H.J.J. van der Hagen
chair of the Board for Doctorates
to be defended publicly on
Tuesday 1 October 2024 at 12:30 o'clock

by

Volkan SALMA

Master of Science in Computer Engineering, Gazi University, Turkey
born in Kayseri, Turkey

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus,	chairman
Prof. Dr. Gerard J.W. van Bussel	Delft University of Technology, promotor
Dr.-Ing. Roland Schmehl	Delft University of Technology, promotor
Independent members:	
Prof.dr.ir. Henk .A.P. Blom	Delft University of Technology
Prof. Dr.-Ing. Dieter Moormann	RWTH Aachen University, Germany
Prof. Dr. Po Wen Cheng	University of Stuttgart, Germany
Dr.ir. M.M. (René) van Paassen	Delft University of Technology
Dr.ir. Delphine De Tavernier	Delft University of Technology
Prof.dr.ir. Axelle Viré	Delft University of Technology, reserve member

Keywords: Airborne Wind Energy, Safety, Reliability, Certification

ISBN 978-94-6366-919-1

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

CONTENTS

SUMMARY

Airborne wind energy (AWE) is a novel concept aiming to substantially reduce the material demand and environmental impact of wind energy generation. AWE systems can also access steadier and stronger wind at higher altitudes, which is inaccessible to conventional wind turbines. The lower material effort, the increased capacity factor, and the access to so-far unused wind resources render AWE a potential cornerstone in a future low-carbon energy economy. The new conversion concept is currently being demonstrated by several start-up companies using different technical implementations at different maturity levels. The unifying challenge for commercialization is the operational robustness of the technology. For a successful market acceptance, the introduced aviation and ground-related safety risks need to be mitigated.

The present work aims to bring AWE closer to commercial success through two main contributions. As a first contribution, well-established practices of reliability engineering are used to measure and then systematically improve the safety and reliability of AWES systems. Experience from other safety-critical domains such as aviation, space, automotive, and medical are used to achieve this objective. A fault tree analysis (FTA) and failure mode and effects analysis (FMEA) are applied to an existing demonstrator system. A common practice in the safety-critical domain is automatically monitoring the system's health and taking action in case of faults. In this regard, a systematic fault detection isolation and recovery (FDIR) model is proposed for AWES. This architecture is generally applicable and flexible and can be applied to different AWE systems.

After reaching the required reliability and safety levels, formalization by the certification authorities is required. As a second contribution, the current regulatory framework is reviewed, the relevant authorities identified and a roadmap for aviation certification is presented. The "Specific Operations Risk Assessment" (SORA) by the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is a comprehensive and well-structured framework. Therefore, following the SORA is considered the best way forward to get the flying permit for AWES, claiming the "specific" category from the European Union Aviation Safety Agency (EASA) regulation. This permit is applicable for commercial operations in Europe. Other civil aviation authorities may also recognize the EASA's flying permit. In this respect, the SORA is applied to a hypothetical commercial operation scenario, and requirements for the flying permit are discussed.

SAMENVATTING

Airborne wind energy (AWE) is een nieuwe technologie die tot doel heeft om stabielere en krachtigere windbronnen op grotere hoogten te benutten die niet bereikt kunnen worden met conventionele windturbines. AWE is ook goedkoper in de productie dan conventionele windturbines vanwege het lagere totale materiaalgebruik. Het lagere materiaalgebruik, het verhoogde vermogensrendement en de toegang tot tot nu toe ongebruikte windbronnen maken AWE tot een potentieel hoeksteen in een toekomstige, koolstofarme energie-economie. Het concept is vandaag de dag bewezen met verschillende soorten AWE die worden vervaardigd door universitaire onderzoeksgroepen en bedrijven. Deze prototypes bevinden zich op verschillende volwassenheidsniveaus. Vandaag de dag is de belangrijkste uitdaging voor de commercialisering van luchtgebonden windenergiesystemen (AWES) de robuustheid van de systemen. Naast robuustheid moeten ook de luchtvaart- en grondgerelateerde veiligheidsrisico's die door AWES worden geïntroduceerd worden verminderd voor marktaanvaarding.

Het huidige werk heeft tot doel om AWE dichter bij commercieel succes te brengen door middel van twee belangrijke bijdragen. Als eerste bijdrage worden goed ingeburgerde praktijken van betrouwbaarheidsengineering gebruikt om de veiligheid en betrouwbaarheid van AWES-systemen te meten en vervolgens systematisch te verbeteren. Ervaringen uit andere veiligheidskritieke domeinen zoals de luchtvaart, ruimtevaart, auto-industrie en medische sector worden gebruikt om dit doel te bereiken. Een foutenboomanalyse (FTA) en foutmodus- en effectenanalyse (FMEA) worden toegepast op een bestaand demonstratiesysteem. Een veelvoorkomende praktijk in het veiligheidskritieke domein is het automatisch monitoren van de gezondheid van het systeem en het nemen van actie in geval van fouten. In dit opzicht wordt een systematisch model voor foutdetectie, isolatie en herstel (FDIR) voorgesteld voor AWES. Deze architectuur is over het algemeen toepasbaar en flexibel en kan worden toegepast op verschillende AWE-systemen.

Na het bereiken van de vereiste betrouwbaarheids- en veiligheidsniveaus is formalisatie door de certificeringsautoriteiten vereist. Als tweede bijdrage wordt het huidige regelgevingskader beoordeeld, worden de relevante autoriteiten geïdentificeerd en wordt een routekaart voor luchtvaartcertificering gepresenteerd. De "Specifieke Operatie Risicoanalyse"(SORA) van de Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is een uitgebreid en goed gestructureerd kader. Daarom wordt het volgen van de SORA beschouwd als de beste manier om een vliegvergunning te krijgen voor AWES, waarbij de "specifieke"categorie wordt geclaimd van de regelgeving van het Europees Agentschap voor de Veiligheid van de Luchtvaart (EASA). Deze vergunning is van toepassing op commerciële operaties in Europa. Andere burgerluchtvaartautoriteiten kunnen ook de vliegvergunning van de EASA erkennen. In dit opzicht wordt de SORA toegepast op een hypothetisch commercieel bedrijfsscenario, en worden de vereisten voor de vliegvergunning besproken.

ABBREVIATIONS

AEC	Airspace encounter categories
AEH	Airborne electronic hardware
AHSS	Advanced high strength steel
ANSP	Air navigation service provider
ARC	Air risk class
ATC	Air traffic control
AWE	Airborne wind energy
AWES	Airborne wind energy system
AWT	Airborne wind turbine
BDD	Binary decision diagram
BVLOS	Beyond visual line of sight
CAA	Civil aviation authority
C2	Command and control
CFA	Controlled firing area
cFS	Core flight system
CMS	Change management system
CONOPS	Concept of operations
DAA	Detect and avoid
DAL	Design assurance level
EASA	European Union Aviation Safety Agency
ERP	Emergency response plan
ESA	European Space Agency
EVLOS	Extended visual line of sight
FAA	Federal Aviation Administration
FDIR	Fault detection, isolation and recovery
FL	Flight level
FMEA	Failure mode and effects analysis

GPS	Global Positioning System
GRC	Ground risk class
GNSS	Global navigation satellite system
GS	Ground station
GSE	Ground support equipment
HAV	Highly autonomous vehicles
IMU	Inertial measurement unit
IR	Infrared
KCU	Kite control unit
LCoE	Levelized cost of energy
LEI	Leading edge inflatable
LEO	Low-earth-orbit
LOS	Line of sight
JARUS	Joint Authority on Rule-making for Unmanned Systems
RTK	Real-time kinematic positioning
MAC	Mid-air Collision
MCS	Minimal cut sets
MSL	Mean sea level
MOA	Military operation area
NAA	National Aviation Authority
NASA	National Aeronautics and Space Administration
NOTAM	Notice to Airmen
OA	Operational approval
OSO	Operational safety objective
RPAS	Remote-piloted aircraft system
SAE	Society of Automotive Engineers
SAIL	Specific assurance and integrity level
SAVOIR	Space avionics open interface architecture
SORA	Specific operation risk assessment
SSG	Safety system for ground
SW	Software
TMPR	Tactical mitigation performance and robustness requirements

TMZ	Transponder mandatory zone
TRL	Technology readiness level
TU Delft	Delft University of Technology
UA	Unmanned aircraft
UAS	Unmanned aerial system
UTM	Unmanned aircraft system traffic management
VLOS	Visual line of sight

NOMENCLATURE

A	Availability, no unit
S_i	Severity of an incident, currency for cost risk, no unit
P_i	Probability of an incident, no unit
$Risk_\mathrm{i}$	Risk of an incident, no unit
$v_\mathrm{w,ref}$	Reference wind speed at 6m altitude, m/s
η	Characteristic life of an item, hours
β	The slope of the best-fit line through the data points on a Weibull plot, no unit
γ	The failure-free life, hours
v_w	Wind speed, m/s
$v_\mathrm{w,low}$	Low wind speed threshold for depower settings change, m/s
$v_\mathrm{w,high}$	High wind speed threshold for depower settings change, m/s
$\mathbf{g}_\mathrm{k}$	Gravitational acceleration vector, ms^{-2}
g	Magnitude of gravitational acceleration, ms^{-2}
v_a^n	Apparent wind velocity, m/s
u_S	Steering command, no unit
u_D	Depower command, no unit
r_k	Yaw-rate response of the kite, rad/s
E_k	Total kinetic energy of the kite, J
I_k	Moment of inertia for the kite, kgm^2
ω_k	Angular velocity of the kite, rad/s
m_k	Mass of the kite, kg
$\mathbf{v}_\mathrm{k}$	Velocity of the kite, m/s

1

INTRODUCTION

1.1. BACKGROUND

The increasing need for renewable energy has led to widespread deployment of wind turbines, initially only on-shore but for more than a decade also off-shore [1]. The trend goes to ever-larger turbines with increasing capacity factors [2]. On the other hand, the cost of structures scales unfavorably with a square-cube law, and modern wind turbines are approaching an economically feasible size limit [3]. Airborne wind energy (AWE) systems use tethered flying devices to harvest wind energy beyond the height range accessible to tower-based turbines [4–7]. For AWES, the wind is both the energy source and the means to keep the aircraft airborne via avionic and robotic technologies. The working principles of AWES and the state-of-the-art are explained by Schmehl [8]. Figure 1.1 shows some representative examples of AWES.

Using a tether allows the harvesting height to be adjusted continuously to optimize the availability of the wind resource. Compared to harvesting at the fixed hub height of wind turbines, the wind power that is available 95% of the time increases roughly by a factor of two [9]. A tower is, in principle, not needed for the system's operation. The tether attaches to the ground station at sea
land level, substantially reducing the structural loads and thus also the required material [6, 10]. The lower material use, the increased capacity factor, and the access to a so-far unused wind resource render AWE a potential cornerstone in a future low-carbon energy economy.

AWE technology can significantly reduce the levelized cost of energy (LCoE) by eliminating a large part of the rotor blades, the tower, and the foundation; these make up for about 50% of current turbine costs [11].

The complex interdisciplinary interactions of the system challenge the development of AWES. To name a few specific examples, one must accept the challenge of designing a complex flight control system to replace a conventional wind turbine's heavy tower and foundation with a lightweight tensile structure (i.e., the tether). AWE systems typically operate in crosswind maneuvers, where the flight speed is closely coupled with

Figure 1.1: Selected AWES concepts: Kitepower, EnerKite, TwingTec, Ampyx Power, Makani Power, Wind-Fisher, Skysails, Kitemill, Kitekraft, Mozaero (photos from AWEC conferences book of abstracts).

both the wind speed and the reeling speed of the tether. This interdependence presents a significant operational challenge. Without responsive control, a wind gust can rapidly accelerate the flying device, which amplifies the aerodynamic loads; this leads to potential rupture of the tether or other irreversible damage —and in the worst -case—loss of the flying device or harm to people. For comparison: wind turbines are less prone to this coupling problem due to the large inertia of their blades. This is why a highly dynamic and fault-tolerant winch control, at the physical limits of the actuating electrical drive system, is of critical importance for the successful operation of an AWES. Interlinked with the fundamental problem of tethered flight control are the physics of the wind environment, the aeroelastic response of a highly flexible flying vehicle and tether, and the electrical energy conversion system and grid integration characteristics. Take-off and landing are particularly challenging as they can occur in a wide range of conditions. Most implemented AWES concepts rely on an aerodynamic lift, and the tethered flying devices can thus not be stopped immediately when unexpected wind conditions or system failures occur. Exactly how critical an operational anomaly is depends on the specific AWE technology. Lightweight, flexible membrane wings fly slower and can generally be relaunched after an emergency landing or repaired and relaunched after a crash landing, while heavier rigid wings fly faster, and a crash landing most likely means a total loss. Next to the availability of the system and its maintenance cost, the safety of people or objects on the ground and other users of the airspace is another vital point.

As AWE systems operate at higher altitudes and their operations are not stationary, the interaction with the aviation system is potentially stronger. For these reasons, AWE systems introduce risks to third parties in the air and objects on the ground. Thus, besides addressing the safety issues for wind turbines, such as the risk of lightning or fire within the equipment, additional considerations are required for managing aviation-related risks.

The current state of AWES is the result of more than one decade of research and development mostly carried out by start-up companies under budget and schedule constraints. This pressure led to fast manufacturing and testing cycles. To reduce costs and mitigate system complexity, these mostly resorted to ‘off-the-shelf’ components;

addressed only several selected sub-systems at a time, neglecting interaction and operational analysis of the whole; and targeted incremental goals. Such an approach delivered small-scale demonstrators that could fly for a few hours or days. These demonstrators showed AWE's technical feasibility and economic potential in future energy networks. However, it led to relatively slow development overall due to the following:

- lack of a holistic view of the systems to be developed [12];
- lack of a comprehensive systems engineering approach [13];
- lack of effective knowledge sharing and access to results (both successes and failed attempts) [13]

Over the past decade, the airborne wind energy (AWE) sector has experienced steady growth, widely regarded as a potentially transformative solution [1, 14]. The significant potential of AWE technology has drawn numerous start-ups to the field. Figure 1.2 shows, as of 2023, academic and industrial entities actively working on AWE technology.

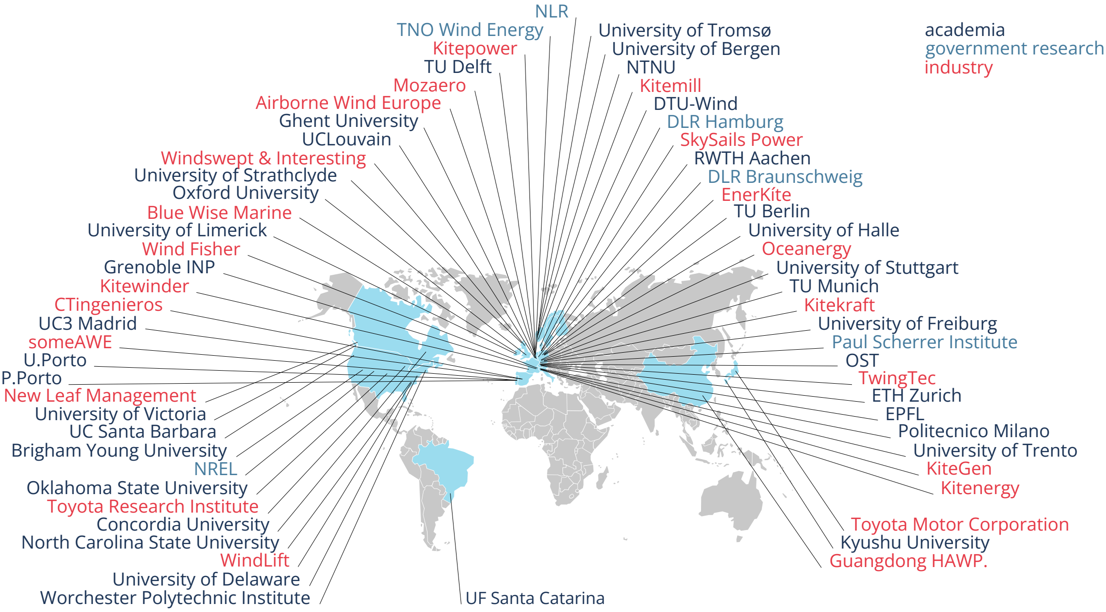


Figure 1.2: Organisations active in research and development of AWE in 2023 [15].

Business plans and purely economic aspects require these companies to work very fast toward demonstrators and prototypes. In this situation, a systematic systems engineering approach, with the crucial element of reliability analysis, is typically overlooked. Moreover, companies have yet to be able to afford all of the requisite competencies to understand the interdisciplinary aspects of the fully integrated system. Hence, development has focused mainly on parts of the system (e.g., components or modules); thus, many interacting and operational aspects, faults, and uncertainty in the system's performance have been neglected [12, 13, 16]. One of the main limitations of this technology is its lack of reliability. The significant impediments are interdisciplinary scientific challenges that such a trial-and-error approach or subsystem focus cannot be tackled. For example:

(i) understanding the most likely set of extreme events, failures, and uncertainties that an AWES must survive to achieve a certain level of reliability; and

(ii) interdisciplinary scientific understanding to adequately model the complete system during extreme events and failures.

Therefore, future AWES must be designed, implemented, and tested in a holistic and science-based manner such that they

- work robustly even under extreme/abnormal conditions and heavy system/model uncertainties;
- be fault-tolerant to guarantee essential operation or transition to a fail-safe state under faults until maintenance can be/is scheduled;
- interact and operate reliably inter-system-wide and with the environment (e.g., grid).

Even in the absence of faults, these systems can, in principle, cause damage due to a wrong decision. A long-standing major challenge is devising the most effective methodology to design a control logic that can guarantee safety for such systems. Solving this challenge thus implies advancing the knowledge in the safety-critical system. In this regard, innovative hierarchical and distributed control methods for safety-responsible systems are required, featuring a combination of exploitation, exploration, and safety aspects in the computation of any decision taken by the machine. The control design method will also include active fault management strategies and adaptive techniques that will increase performance and reliability over time, exploiting the collected operational data to continuously validate and improve an inner model (digital twin) of the system and its environment.

To improve reliability, one must comprehensively understand the sources of failure. The source of failure may start with an extreme weather event, a sudden component failure, or a logic failure in the control system. The most likely sources of failures must be quantified through uncertainty quantification to maximize reliability. However, a single fault or extreme event may not be enough to lead to failure; a fault-tolerant design can help AWES to mitigate failures. A system perspective must be applied to understand how these faults propagate through the system to achieve a fault-tolerant design. AWES have a great range of operations (e.g., the operational altitude, landing, taking-off, energy generation mode, and emergency actions in different altitudes). Thus, operational analysis is needed to understand how operating conditions affect reliability. For example, increased altitude can give these systems room to recover from unstable flight conditions. At the same time, the frequency of extreme weather (e.g., lightning) or icing events can also vary according to the operational altitude, so operation also affects the uncertainty quantification. Thus, this engineering challenge simplifies the complex phenomena leading to failure into a systematic design methodology aimed at enhancing reliability.

In 2017 the European Commission (EC) launched an independent study on the challenges of commercializing AWES [13]. The study concluded that:

- AWE can be a powerful instrument to decarbonize the energy system: it could supply 100% of EU electricity demand at competitive cost (compared to other power generation technologies) with solely 1% of land use and, if offshore deployment is included, even up to 300% of the total (2015) EU energy demand;
- A major barrier pertaining to technology readiness is the lack of reliability in available AWES. A solid track record (of operational hours, safety, and standards) is needed to become accepted by society and markets;
- More fundamental research and private-public collaboration(s) are required to remove development barriers through holistic science-based systems engineering approach.
- The companies regard their low-power generating prototypes as commercially uncompetitive. Consequently, they recognize the necessity of scaling up their systems to meet the demands of the target market. However, for many components, the Technology Readiness Levels (TRLs) achieved do not translate to scaled-up systems, which constrains most companies to a TRL of 4, with some approaching TRL 5.

Regarding the TRL, more recent reports by the National Renewable Energy Laboratory [12] and the U.S. Department of Energy to the U.S. Congress [17] state that the level went a step higher, with some companies reporting in the low TRL 7 range. We consider this rating TRL 7 for the systems that have already achieved long operation durations, such as those from Skysails and Kitepower.

To develop and produce large-scale AWES, with each unit providing several Megawatts of power—and where the AWES can reliably produce energy for years under many weather conditions—it is no longer feasible to continue the past 'trial-and-error' approach. A radical new vision addressing the above points is required.

Despite the differences between the various AWE concepts, the industry consensus is that safe and robust operation with sufficient autonomy is a prerequisite for successful market introduction and public acceptance [18]. To the author, the commercial prototypes have been operated continuously for only a few days. Nevertheless, to become economically viable, AWES must fly autonomously, safely, and reliably for many years.

1.2. THESIS OBJECTIVE

This thesis proposes broadly applicable engineering methods aimed at improving the reliability and safety of AWE technology in its path toward commercialization. This improvement is deemed necessary for the future of the AWE research. Once the technology reaches the required safety and reliability level, the provided airworthiness certification roadmap can be followed for commercial use and public acceptance.

To reach this main objective, the following side objectives are defined:

- to present the status of AWES prototypes from a safety and reliability engineering perspective. This point also includes operation permits in place and potentially required airworthiness certification in the future,
- to present failure mode examples from different AWE systems,
- to conduct a systematic safety and reliability assessment on an example AWE system, which may be used as a guideline for other systems,
- and to propose a generally applicable Fault Detection, Isolation, and Recovery (FDIR) system architecture to systematically improve the reliability, safety, and availability of AWES.

1.3. THESIS STRUCTURE

After introducing the AWE technology and the motivation of the work in Chapter 1, Chapter 2 presents the relevant fundamentals of safety and reliability engineering to provide the necessary background for the remaining of the work. Chapter 2 then presents the state of the literature on AWE safety and reliability topics. AWE field tests are carried out with ad hoc permits from different local authorities. Chapter 2 provides an overview of the flying permit status of current prototypes to grasp the variety of architectures currently considered. Finally, Chapter 2 concludes with the research questions to which this work aims to respond.

Chapter 3 describes the Kitepower system of Delft University of Technology (TU Delft), which is used as a demonstrator for the safety analysis. In addition to system components, operational aspects are crucial for the safety assessment. Therefore operation modes and the operation zone definitions are also described.

Chapter 4 describes the safety analysis systematically conducted on the Kitepower system, which was described in Chapter 3. FMEA (Failure mode and effect analysis) and FTA (Fault tree analysis) tools have been used for the analyses. Even though the mentioned methods are current practices in the industry, it is not easy to find a complete exercise that is publicly available. This chapter aims to provide a practical guideline to the AWES industry by presenting the method, implementation details, and the granularity level of the analyses.

Chapter 5 proposes a fault detection, isolation, and recovery (FDIR) system architecture generally applicable to AWE systems. The introduced system will be tuned and validated with the actual flight data of the Kitepower system. The aim is that lower layers of the FDIR can be directly applied to any AWE system. However, the up-most FDIR layer is system-specific and shall be customized according to the operational aspects of the particular system.

Chapter 6 discusses AWE systems' certification aspects and permitting status. Firstly the organizations that may have a role in the certification process have been identified. Then, the chapter summarizes the aviation rules that may apply to AWES. The chapter concludes with our view on the best possible approach for the regulatory process. Chapter 6 was the first chapter in this thesis by development order. Although many years passed since writing the chapter, the ICAO, FAA, and EASA regulations that may be relevant to AWES are still valid. There have been developments in the UAS certification field, which is considered applicable to AWES. These developments are in line with the expectations given in the chapter. Chapter 7 details the latest status of the UAS regulations and elaborates on the recommended way forward for the flying permit of AWES.

To complement the proposed way forward on the certification process in Chapter 6, Chapter 7 conducts the recommended specific operations risk assessment (SORA) on a hypothetical commercial AWE system. SORA was initially developed for unmanned spacecraft systems, which is now considered applicable by the European Union Aviation Safety Agency (EASA) for the flight permit of AWE systems.

2

STATE OF RESEARCH

The first part of the chapter describes the basic reliability engineering concepts used in the following chapters. Subsequently, the chapter reviews the relevant work on AWES's safety, reliability, and certification. The chapter then presents the different operation permit characteristics for various AWES prototypes. Within this scope, current operation permit details for several prototypes are presented. The information has been collected through a survey in which all the major AWE parties provided their status. Survey results also present companies' perspectives on commercial certification. Based on the status of the AWE industry and the literature, the research questions for this thesis are formulated.

2.1. FUNDAMENTALS OF RELIABILITY AND SAFETY ENGINEERING

Reliability is defined as the ability of a system or component to perform its required functions under stated conditions for a specified period [19]. Mathematically, reliability is defined as the probability P that the random variable time to failure (T) is greater or equal to mission time (t) [20].

$$R(t) = P(T \geq t)$$

Reliability values are quantitative measures, but these values should be considered relative rather than absolute. For example, reliability values give valuable metrics to compare the different alternatives of a design. Another area where the reliability numbers are standard is the reliability target requirements enforced by the certification bodies to ensure design performance. Reliability calculations are expressed in failure-related units such as mean time to failure, failure rate/frequency, or mean time between failures.

Reliability is a quantification of the failure concept, whereas safety deals with all hazards and the consequences of failure. Safety and reliability engineering offers methods for quantitatively assessing performance, identifying crucial factors, and gaining an understanding to enhance system reliability. This understanding includes actions to decrease the likelihood of failures and their hazardous outcomes, measures to address these failures, and establishing strategies for recovery in the event of a failure. System reliability and safety assessment studies characterize the failures and hazardous scenarios. Some examples of failure characterization by causes are the following:

- Weak or non-existing quality control process for the development
    - Design problems
    - Poor manufacturing methods
    - Using substandard components
- Weak or non-existing maintenance/operation protocols
    - Operator errors
    - Overuse, aging or wearing out
    - Stress-related problems on the materials

Industry often uses the Bathtub function (Figure 2.1) to model product failure rates. Failure means the instantaneous rate of failure for survivals until time t. Early hazard rates are generally high because some products fail quickly due to manufacturing defects or substandard components. After eliminating the weak products, the hazard rate decreases and becomes relatively constant. The hazard rate rises again depending on the product operation and maintenance characteristics. This rise is primarily because of wear-out, fatigue damage, and poor maintenance. Thus, the hazard rates of a product over its lifetime can be modeled as three distinct regions:

- 1- Early failure region (decreasing hazard rate)
- 2- Useful operation life region (constant hazard rate)
- 3- Wear-out failure region (increasing hazard rate)

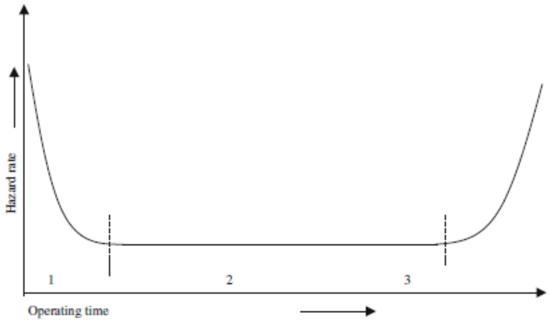


Figure 2.1: Bath-tub curve [20]

In the early failure region, products/items should be monitored carefully in operational use. It is common to apply burn-in tests to screen out early failures before supplying them to users. In this region, highly accelerated life tests or stress tests are helpful methods to identify and fix the root causes of the failures [21]. The useful operation life region is where random failures govern the hazard rate. This rate converges to a constant rate over time. The wear-out failure region is when the product should be replaced or removed from the operation.

The first step to increase the reliability of a system first step is to measure the present level of reliability. Reliability engineering provides tools for the assessment of reliability levels. It is also essential to consider the trade-off between the required reliability and the available resources. Reliability improvement also depends on the stage of the system; if the system is in the design phase, design simplification or redundancy can improve reliability. If the system is in production, well-established quality control processes and suitable components can improve reliability. Good maintenance protocols are the best resort to improve reliability when the system is deployed and operation has already started.

Safety is a combination of reliability and managing hazardous situations. To achieve an acceptable level of safety, besides increasing reliability, the consequences of failure must be mitigated. Protection or safety mechanisms are examples of such mitigations.

Availability of a system means the probability of being operational at a specified time. Availability metric equals reliability for a non-repairable system. If repair is possible, it increases the availability, but this does not affect the reliability performance.

The most straightforward representation of availability (A) is the ratio of the system uptime to total time:

$$A = \frac{Uptime\_of\_system}{Uptime\_of\_system + Downtime\_of\_system}$$

Risk definitions in the literature are diverse. According to Kaplan and Garrick [22]. Risk is a function of answers to the following three questions:

- “What can go wrong?”;
- “How likely is it to go wrong?”;
- “If it goes wrong, what are the consequences?”

Quantitatively, the risk is calculated with Equation (2.1):

$$Risk_i = \langle S_i P_i \rangle \tag{2.1}$$

In Equation (2.1), i is the index for a specific scenario ($i = 1, 2, \ldots N$), which has a occurrence probability of P_i and has a severity (consequence) of S_i.

For an engineering system, higher risk means lower safety. Risk assessment has the same meaning as the safety assessment for engineering applications. This thesis will follow the "safety assessment" terminology.

Reliability and safety engineering emerged relatively late compared to other engineering disciplines. Pierce introduced the weakest link axiom: “a chain is no stronger than its weakest link” in 1926 [23]. The recordings of aircraft accidents started in the

1930s to form statistical failure models of various aircraft components [24]. Manufacturers then used the feedback to improve designs. Pugsley defined the first quantitative safety objective in 1939 that the accident rate of an aircraft should not exceed $10^{-5}/h$.

The *redundancy* concept to improve reliability was first introduced during the development of V1 missiles in Germany. The first rockets had poor reliability performance. The team was working based on the 'weakest link' axiom; however, they figured out that failures are caused by the weakest and the remaining components. Subsequently, mathematician Eric Pernchka developed the elements' survival probability formula, which is the basis of the reliability of a series of systems [24]. According to Pernchka, "if the survival probability of an element is $1/x$, the survival probability of system of n such similar components will be $1/x^n$". Later on, Wernher Von Braun practically applied this concept to improve the reliability of future missiles by using redundant components. Also, until World War II, reliability engineering developed progressively primarily because of the unreliability of vacuum tubes, which was causing over 50% of the defense equipment to be in a failed state already in storage [20].

One of the effective methods today for safety assessments, especially in nuclear and aerospace engineering, is the "Fault Tree Analysis (FTA)". FTA was first developed at Bell telephone laboratories to assess the safety of the launch control system of the Minuteman I Intercontinental Ballistic Missile (ICBM). FTA is a "top-down" deductive analysis aims to identify and analyze conditions that lead to a particular system failure, commonly a catastrophic event.

The second tool, which is also the central pillar that is not only used in safety-critical systems but almost all engineering systems, is the "Failure mode and effects analysis (FMEA)." FMEA is a "bottom-up" analytical method used in the design phase to map and examine individual component failures and trace the potential effects on the entire system's performance. The aerospace industry started to use FMEA in the early 1960s, and over the years, it became popular in many other domains, such as the automotive and medical industries. The method has also been adopted for wind turbines [25].

Another commonly used method for safety assessment is "Probabilistic Risk Assessment (PRA)." NASA developed PRA after the Apollo 1 disaster in 1967. PRA requires special but often necessary tools like human reliability analysis (HRA) and common-cause-failure analysis (CCF). HRA deals with methods for modeling human error [26].

Along with software becoming a critical component in safety-critical systems, another branch in reliability engineering focusing on software reliability has emerged. This field concerns a reliable software system's development, testing, and maintenance processes. Software reliability is different from hardware reliability in many aspects. Firstly, the software does not wear out. There are no random faults in software systems. Software flaws, which are systematic errors, are the source of the faults . Software reliability metric is the probability of operation in a given environment within the predefined range of inputs without failures.

The bathtub curve shown in Figure 2.1 does not reflect the failure characteristics of software systems because the software does not wear out over time. However, the early failure region of hardware has a similar failure model to the software validation phase. In this period, software bugs or requirement non-compliances are discovered and rectified. The probability of software failure in the valuable life period in practice is not similar to that of hardware. Typically, the failure rate is decreased with the subsequent releases during the lifetime of a software system. Figure 2.2 shows the failure-rate model of a software system. Spikes in the model represent the newly introduced bugs unrelated to the modifications in the release.

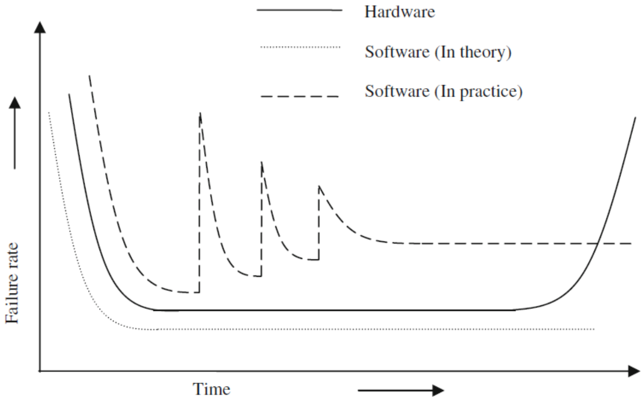


Figure 2.2: Comparison of hardware and software bathtub curves [20]

The term “Fault detection, isolation, and recovery” (FDIR) defines systematically monitoring the system during the operation, detecting the occurring faults and isolating it to prevent fault propagation and taking appropriate recovery actions if possible. This capability reduces the diagnostic time or downtime in general, thus increasing the system availability. Safety-critical systems make use of FDIR systems to reduce safety risks.

Improving the safety and reliability of a complex system requires identifying the risk in advance and taking active mitigation measures. In the literature, these implementations are called FDIR, health management, or fault management. Even though there is no standard methodology for FDIR among different domains due to different fault characteristics and recovery actions, the following classification can be made according to the fault detection approach [27]:

- Classical techniques
- Model-based and parameter estimation methods
- Knowledge and rule-based methods
- Machine learning-based methods

In the conventional wind turbine domain, there are few literature reviews for health management [28–30]. Lately, there has been an increasing trend of using model-based reasoning algorithms for fault detection. This shift in approach has brought attention to various techniques and indicators that can aid in identifying potential issues. One such indicator that has gained more attention is acoustic emission, particularly in detecting incipient wind turbine failures [31].

For the space domain, efforts are ongoing in NASA[32] and ESA to support the industry by providing guidelines for creating reusable and trustworthy fault detection, isolation, and recovery systems. As a result of the working groups, NASA published a draft version of the Fault Management Handbook [33]. Independently developed ESA FDIR guidelines will be published soon.

Different fault detection approaches exist depending on the complexity and criticality of systems. Depending on operating modes and availability requirements, a system fault can be detected manually or automatically. For a system that an operator operates in close proximity, system failures can be detected quickly by human visual and auditory senses. If, for example, a light is switched on and there is no illumination, one can visually detect a problem with the light switch, light bulb, power source, or circuitry. If no human is in the loop for the same system, additional monitoring elements are required to detect the faults. In general, these elements incur additional costs associated with complex system designs.

FDIR implementation often necessitates additional hardware beyond what is necessary for the system's primary function. This need, in turn, impacts both reliability and cost, necessitating careful consideration and trade-offs to achieve a well-balanced solution. Furthermore, FDIR systems should be meticulously designed with fail-safe measures and undergo thorough validation. In certain instances, the development of FDIR may incur higher costs than developing the system's primary functions.

The reliability of the FDIR system should be greater than that of the system under monitoring. This level of reliability can be reached by keeping the complexity of the FDIR low or using stricter design standards. If this rule is not applied, the failure probability of the FDIR becomes more significant than the primary system; thus, FDIR only decreases the reliability and availability of the primary system by generating false actions. As a general principle, the FDIR should be kept as simple as possible but effective in meeting operational needs.

FDIR can detect faults at a level where components are connected sequentially, but it cannot pinpoint the specific component that has failed in such cases. In order to keep the FDIR design simple, common practice is to use redundancy and take out the complete module or subsystem in case of its faults instead of determining the exact location of the fault.

One should design the recovery module of the FDIR, keeping simplicity in mind. One common approach is defining a recovery mode to preserve simplicity. The following three approaches are typical for the design of a recovery mode;

- 1- Complete (functional) recovery using redundancy
- 2- Functional recovery using alternative paths
- 3- Recovery with degraded functionality

FDIR replaces a failed part with a redundant identical to recover the system's functionality. This widespread approach is called reconfiguration for mission-critical or safety-critical systems such as satellites, spacecraft, or airplanes.

For most systems, complete (functional) redundancy is not commercially feasible; instead of having a redundant unit, an alternative path may be designed to recover faulty functionality. The alternative path usually only achieves the limited capabilities of the original function. For example, missing precise positioning data of an aircraft (e.g., RTK-GPS) can be derived from the auxiliary measurement units, such as inertial measurement units, for a period to allow emergency landing.

For some recovery actions, degraded functionality may offer the most cost-effective and less complex design. For example, in unmanned aerial vehicles, an exceptionally fundamental secondary flight computer with no automatic flight control but only allows the pilot control can be the safest design choice. Also, many earth observation satellites today have a degraded recovery mode, called barbeque, which does not do any attitude control but only turns the satellite to prevent sun exposure to only one side.

2.2. RESEARCH ON AWES RELIABILITY AND SAFETY

At the time of writing this dissertation, only a few studies have directly addressed the reliability, safety, and certification aspects of AWE systems.

At the airborne wind energy conference (AWEC 2015), Glass mentioned the unique challenge of airborne wind turbine (AWT) certification because of the combined elements of wind turbine together with aircraft and the additional tether considerations [34]. In addition, a unified framework for the certification of AWTs is suggested. This framework reviews the existing standards in related sectors, including wind turbine standards and aviation standards. Then, the AWT operation regime identification is required to see what must be addressed in the standards. Afterward, a conservative gap analysis has to be performed to identify the areas not adequately covered by the standards. Lastly, new requirements must be developed to fill the gaps. Glass recommends collaborating with the standards-developing organizations through the standard-making process.

At the same conference, Ruiterkamp[35] provided an overview of existing and expected rules and the standards for ensuring the safe operation of AWE applications. He further described possible risks introduced by AWE systems and supplemented his study with the expected legislation for a rigid wing concept.

Langley[36] investigated AWE systems from a legal perspective. In this study, he introduces the environmental impacts of AWE systems and the current legal landscape. Makani Power, which was a Google Alphabet subsidiary has published a detailed document about the operation of an AWE system [37], responding to the “Notification for Airborne Wind Energy Systems (AWES)” issued by the Federal Aviation Authority (FAA) [38].

Kruiff and Ruiterkamp[39] outline the civil aviation standards and design processes that are applied by Ampyx Power B.V. for rigid-wing AWE system development. Salma et al.[40] describe the aviation-related risks introduced by AWE systems and give an overview of existing and expected regulations for AWE systems. Friedl[41] and Friedl et al.[42] Investigate means to augment the flight control system using an algorithm that detects potentially hazardous situations and reconfigures the system to ensure safe operation. Glass[34] reviews the relevant wind turbine and aviation standards and suggests an initial framework for a set of standard wind conditions for the certification of airborne wind turbines[43].

Stoeckle[44] proposes an FDIR approach for autonomous parafoils, which are not AWE systems but conceptually very similar compared to AWE systems using flexible membrane wings with a suspended control unit.

Researchers working in the AWESCO doctoral training network addressed key technical challenges of wind energy generation using tethered wings. Rapp and Schmehl[45] proposed a robust control system for AWES, which can handle disturbances such as atmospheric turbulence and mismatches between the model used for control design and the actual plant while achieving the nominal control objectives. This work differs from other AWE control literature since the main objective of the proposed controller is to ensure the system's robustness during all operational phases and not for generating the maximum power.

Particularly the robustness levels of current prototypes during take-off and landing is low. Rapp et al.[46] propose a novel vertical take-off and landing methodology using a multi-copter to improve the robustness.

Thedens et al. [47] focus on the reliability of the flexible wing. To ensure the reliable structural performance of the wing, they proposed an optimization strategy to reduce profile deformation using additional fabric attached to the rib.

The fault-tolerant multi-phase controller design by Eldeeb et al.[48] aims to improve the reliability of the electrical drive to which the rigid or soft kite is coupled. It has pivotal importance on system reliability because electromechanical energy conversion control also controls the operational point of the kite.

Rapp and Schmehl [49] present a technique to enhance the resilience of flight operation of AWE systems by systematically avoiding upset conditions, such as sudden increases in tether force.

"AWE Safety and Technical Guidelines" working group of Airborne Wind Europe Association published Key Safety Principles for the operation of experimental and developmental Airborne Wind Energy Systems [50]. This publication is the commitment of the member organizations of Airborne Wind Europe to adhere to the safety principles of operations. These principles include; building a safety culture, avoiding harm and damage to third parties, avoiding mid-air collisions, conducting only safe and approved tests, training the test personnel, having test procedures, reporting incidents, and applying continuous improvement of safety processes. The same group then published a guideline on the Specific Operations Risk Assessment (SORA) process to support AWE organizations for their Concept of Operations (CONOPS) development [51].

In his master's thesis, Minderhoud adapted a risk model framework [52] to analyze the operations of the Kitepower system. He identifies hazardous scenarios in detail and proposes a model for quantifying the risks associated with these scenarios [53].

At present, no study has offered a complete methodology for improving AWE systems' safety and reliability to a level suitable for commercialization.

2.3. CURRENT OPERATION PERMIT STATUS OF AWE SYSTEMS

Airborne wind energy is currently in the development and testing phase. In this phase, companies and research groups conduct their tests with special permissions. Most of these permissions are issued by local civil aviation authorities. AWE application examples from different high-level architectures are shown in Figure 2.3.

Comprehensive information for each architecture and implementation details for practically demonstrated AWE systems can be found in [5].

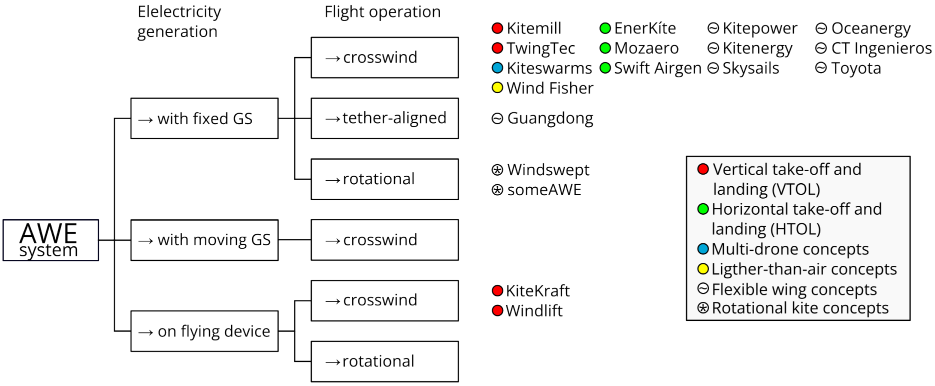


Figure 2.3: Selection of AWE applications and architectures in 2024

To develop a clear understanding of where the AWES industry stands today, as well as a vision of where it is heading in terms of operational safety and airspace integration, a survey is conducted by TwingTec, Airborne Wind Europe, and UASolutions with special financing by the Swiss Federal Office of Civil Aviation. AWES companies were invited to provide technical specifications and flight permit information for their prototypes. Figure 2.4 shows the companies that provided their systems' essential technical specifications and operational attributes. In addition to these companies, one anonymous participant provided their data to the survey.

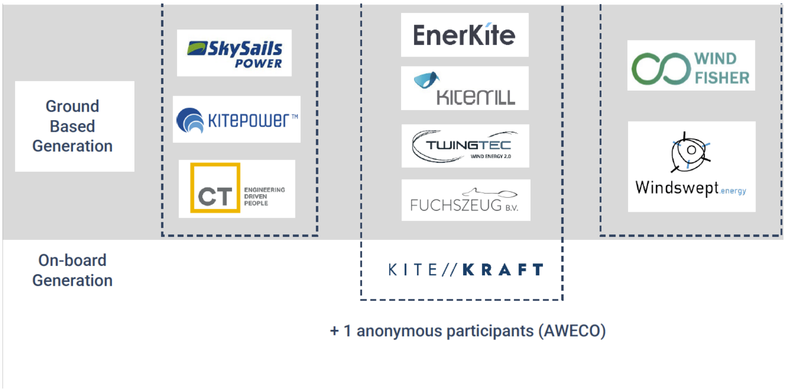


Figure 2.4: Participants of the survey [54].

Table 2.1 lists the current and expected common attributes of AWES systems. The analysis of this data shows that current prototypes have a small airborne mass and occupy only a tiny volume of the airspace. However, the final commercial products are expected to be significantly larger, with higher airborne mass occupying larger volumes of the airspace. Concerning operations, Figure 2.5 shows the main operational attributes of AWES.

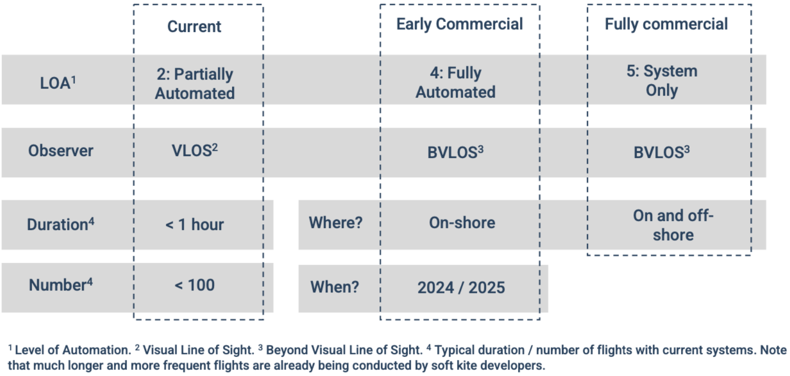
Table 2.1: Current and expected most common attributes of AWES systems [54].

	Current	Fully commercial (expected)
Wingspan	3-8 m	20-40 m [3]
Mass	<25 kg	600 - 5670 kg
Airspeed	25-30 m/s	25 - 75 m/s
Config	Rigid[1], GBG[2], single tether	Rigid, GBG, single tether
Power	<50 kW	1 - 2 MW

[1] First commercial operations are already underway based on soft kites with larger dimensions

[2] Ground-based generation

[3] >40m for soft kite



	Current		Early Commercial	Fully commercial
LOA[1]	2: Partially Automated		4: Fully Automated	5: System Only
Observer	VLOS[2]		BVLOS[3]	BVLOS[3]
Duration[4]	< 1 hour	Where?	On-shore	On and off-shore
Number[4]	< 100	When?	2024 / 2025	

[1] Level of Automation. [2] Visual Line of Sight. [3] Beyond Visual Line of Sight. [4] Typical duration / number of flights with current systems. Note that much longer and more frequent flights are already being conducted by soft kite developers.

Figure 2.5: Overview of the operational specifications of the tested prototypes of AWE developers [54].

Current systems generally have human pilots in the loop or supervising the system. They operate in a selected safe area to mitigate the risks to third parties. However, fully automatic commercial operation is expected. Moreover, the systems will ultimately have to comply with international airspace regulations. In this respect, reported current and planned air risk mitigations are shown in Figure 2.6.

Similarly, Figure 2.7 shows the expected ground risk mitigations.

There currently needs to be a consensus among the certification authorities. Some aviation authorities require personnel training for technically similar concepts, while others do not impose this requirement. Some prototypes need licensed personnel to operate. While most prototypes can operate at night, some can operate only during daylight hours. As an example, Appendix A presents the test flight permissions of Makani Power imposed by the FAA.

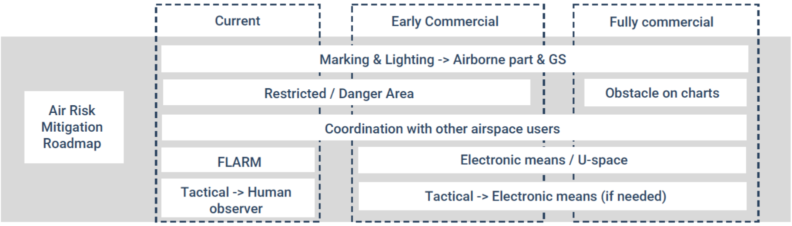


Figure 2.6: Implemented and expected air risk mitigations for AWES [54].

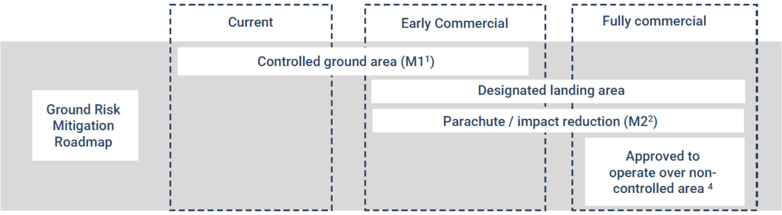


Figure 2.7: Implemented and expected ground risk mitigations for AWES [54].

Table 2.2: Overview of the technical specifications of the AWES prototypes as of 2022 [55].

Developer	Prototype Name	Kite System	Electricity Generation	Wing Span (m)	Wing Surface Area (m2)	Min.-Max. Altitude (m)	Rated Power (kW)
SkySails Power	SKN PN-14	soft-wing	ground-gen	15.6-22	90, 180	200-400	200
Kitepower	Falcon	soft-wing	ground-gen	13.3	47, 60	70-400	100
Kitenergy	KE60 Mark II	soft-wing	ground-gen	12.5	42, 50	100-400	60
EnerKite	EK30	hybrit-wing	ground-gen	8-14	4-8	50-300	30
Ampyx Power	AP3	fixed-wing	ground-gen	12	12	200-450	150
Kitemill	KM1	fixed-wing	ground-gen	7.4	3	200-500	20
TwingTec	Pilot System	fixed-wing	ground-gen	5.5	2	up to 300	10
Skypull	SP130	fixed-wing	ground-gen	2 x 1.3	2 x 0.5	up to 75	1.5
Windswept	Daisy Kite Turbine	fixed-wing	ground-gen	6 x 1 m (rotor dia. 4.48 m)	6 x 0.2 m2	10	1
someAWE	someAWE rotary kite	fixed-wing	ground-gen	4 x 1 m (rotor dia. 3.5 m)	4 x 0.15 m2	-	500 W
Kitekraft	SN7	fixed-wing	fly-gen	2.4	1.08	100	~12
Windlift	C1	fixed-wing	fly-gen	3.8	0.95	30-100	2

2.4. RESEARCH QUESTIONS

This thesis aims to answer the following research questions:

1. **How well are current AWES prototypes assessed in terms of safety and reliability?**
2. **How can the reliability and safety levels of an AWE system be determined systematically?**
3. **How to improve the current design and operation concepts to reach the commercially required safety and reliability levels?**
4. **How can a "Fault Detection isolation and recovery" (FDIR) system architecture be developed for AWES?**
5. **What is a suitable roadmap for AWES certification? Which technical and operational mitigations would facilitate the certification process?**

The chapters in this thesis respond to the research questions in detail. Additionally, a summary of the answers to the questions can be found in Chapter 8.

3

SYSTEM DEMONSTRATOR

3.1. ABSTRACT

After more than a decade of research and development, numerous AWES prototypes that have successfully demonstrated the concept of efficient electricity generation have emerged. Initially, the primary focus was on system development and flight testing to fine-tune the components and validate the concepts, with less emphasis on safety and reliability. However, today, many systems have reached a mature stage, and the main challenge lies in ensuring credible, safe, and continuous operation. This chapter provides an overview of the Kitepower system in 2016. Since then, systematic improvements have been implemented to enhance system reliability while accelerating commercialization activities. Although the chapter may not reflect the most recent advancements in commercial systems, it serves as an example to familiarize the reader with the main components and operation modes of a flexible kite AWE system. Safety analysis in Chapter 4 is conducted on the presented system. The fault detection, isolation, and recovery (FDIR) design given in Chapter 5 is also developed mainly for the kite power system described in this chapter.

3.2. THE KITE POWER SYSTEM

Part A describes the technology demonstrator which is developed and regularly operated from 2010 to 2015 by the Delft University of Technology [57, 58]. This platform has been designed for the pumping cycle operation of a lightweight flexible-membrane wing with an average traction power of 18 kW during the reel-out of the tether. Depending on the kite used, this platform achieved a net mechanical power of up to 7 kW [57]. From 2016 onwards, the spin-off company Kitepower B.V [59] used the technology base for the commercial development of a scaled-up version. The description mainly captures the development status when the technology was transferred from university labs to the commercial team. Since then, the development has progressed to second and

---

Parts of this chapter have been published in Ref. [56].

even third component generations to accommodate the stepwise scaling of the system to a net electrical power of 100 kW. The description includes the necessary adaptations of the commercial development.

3.3. FUNCTIONAL COMPONENTS

The system components are illustrated in Figure 3.1. The traction force is generated by a flexible-membrane wing steered by a kite control unit (KCU). This remote-controlled cable robot is suspended in the rear bridle line system and modulates the force level by adjusting the pitch angle of the wing. The airborne subsystem of the wing, bridle line system, and KCU is denoted as a kite and has been described in detail by Oehler and Schmehl [60]. The tether is deployed from the drum/generator module of the ground station. The system's positive net power output is achieved by operating the kite in pumping cycles, alternating between reel-out and reel-in of the tether. While reeling out, the kite is flown in crosswind maneuvers to maximize the traction force and the generated energy [61]. These figure-of-eight flight patterns are hinted at Figure 3.1. To reel in, the maneuvers are discontinued, and the kite is depowered by pitching the wing to lower its angle of attack, substantially reducing the traction force and the required energy to retract the kite. The part of the generated electrical energy used to retract the kite is buffered in a rechargeable battery. The operational success of the system depends significantly on actively controlling both tether reeling and the kite's flight path. The individual components of the system are detailed in the following paragraph.

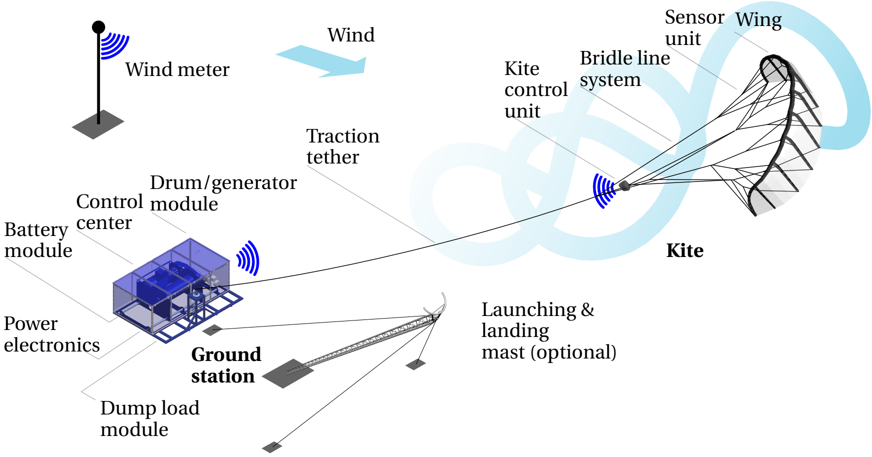
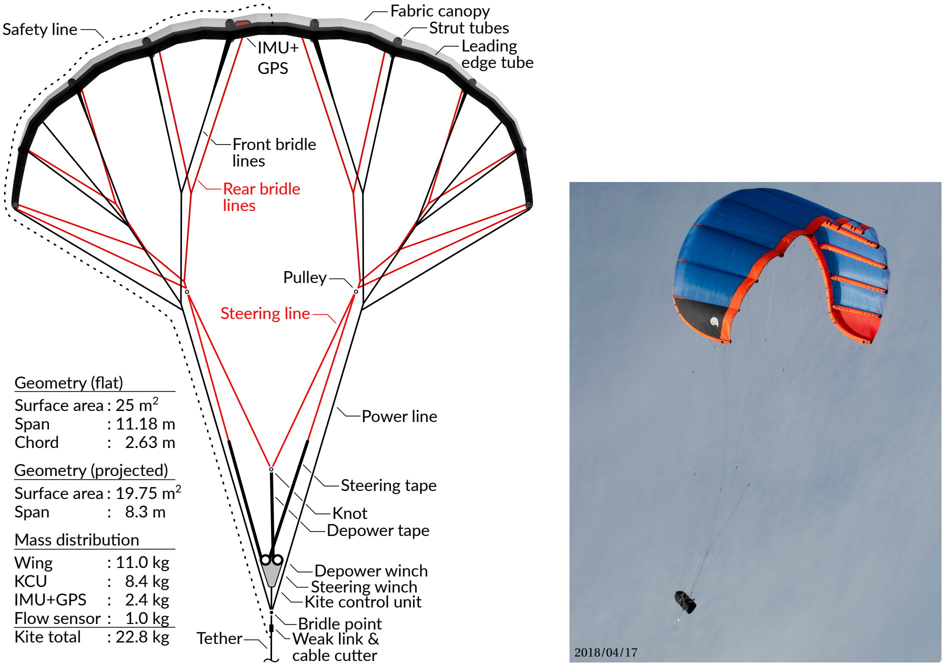


Figure 3.1: Components of the kite power system, equipped with 18 kW ground station and 25 m^2 leading-edge inflatable (LEI) V3 tube kite.

3.3.1. WING

As illustrated in Figures 3.1 and 3.2, the wing consists of a fabric canopy and an inflated tubular frame, which combines a bow-shaped leading edge tube with several connected strut chordwise tubes. The distributed aerodynamic load acting on the flying wing is



(A) **(B)**

Figure 3.2: A, Front view of the leading-edge inflatable (LEI) V3 kite [60]; B, Photo of the V5.40 with 40 m^2 wing surface area (courtesy of Kitepower B.V.).

transferred to the tether by a bridle line system. This particular design is derived from leading-edge inflatable (LEI) kites that, in smaller sizes, are popular for kiteboarding. The rigid chordwise reinforcements have been added to increase the maximum wing loading of the flexible membrane structure. The leading edge tube has both an aerodynamic and a structural function. On the one hand, the pressurized tube defines the radius of the leading edge, which substantially influences the aerodynamic characteristics of the wing [62]. On the other hand, the tubular frame defines the shape of the unloaded wing. During the flight, the wing deforms substantially, and the geometry of the bridle line system mainly controls its shape. Next to its primary function of generating the traction force, the wing also acts as a morphing aerodynamic control surface. An asymmetric actuation of the rear bridle lines leads to a twist deformation of the wing, which induces both a side force and a yaw moment that enables the kite to fly a turning maneuver [63, 64]. On the other hand, a symmetric actuation modulates the traction force by adjusting the pitch angle of the wing and, by that, its angle of attack. The power setting quantifies the degree of symmetric actuation. Because this also shifts the aerodynamic load in a chordwise direction, the entire kite pitches around the bridle point [60]. The depicted LEI V3 kite with 25 m^2 wing surface area can structurally support an aerodynamic load of up to 8 kN. The commercial development includes geometrically scaled wing prototypes of 25, 40, 60, and 100 m^2 surface area, intending to converge on a size below 80 m^2 for the 100 kW system. These kites use fabric materials with higher durability and UV coating for an extended lifetime.

3.3.2. BRIDLE LINE SYSTEM

The front bridle lines support the leading edge tube and the front sections of the strut tubes. The left and right line branches transfer a significant part of the aerodynamic load and connect to the left and right power lines. These bypass the KCU and attach directly to the tether at the bridle point. The rear bridle lines support the trailing edge of the wing and its tips. The two-line branches connect via pulleys to the two steering lines. Together with the steering and depower tapes deployed from the KCU, the two steering lines form two connected line loops used for asymmetric or symmetric wing actuation. The KCU is connected to the bridle point by a short line segment. Depending on the kite size, the bridle line system may include additional pulleys at bridle split points to allow the line geometry to passively adjust to varying load distribution and shape of the wing. The tether incorporates a weak link and a separate cable cutter just below the bridle point. While the weak link breaks at a predefined tether force to avoid overload and possible damage to the system, the cable cutter severs the tether in an emergency on command. In case of passive or active separation of the kite from the tether, the safety line is used to land the kite in tethered parachute or paraglide mode. This line is not tensioned during regular operation, directly connecting the center of the leading edge tube with the tether below the weak link. The kite is instantly depowered with the bridle point separated from the tether. The relatively heavy KCU swings below the wing, which can be retracted to the ground station in a stable payload configuration at relatively low flight speed [44].

3.3.3. KITE CONTROL UNIT

The central components of the KCU are the actuation drive trains, which comprise steering and depower motors, gearboxes, tape drums, and a depower break. Tapes are used instead of lines because of the better-reeling behavior and lower-layer build-up on the drums. The maximum unloaded reeling speed for both motors is 0.4 ms^{-1}. For redundant communication with the ground station, the KCU relies on three separate wireless links. The main link uses a 5 GHz dipolar directional antenna and is backed up by a slower 2.4 GHz serial link. The ground control can use both links interchangeably, retaining full automatic control functionality. A direct manual remote control of the KCU can also be established via a 2.4 GHz link. A rechargeable battery module provides the onboard power. The KCU uses two onboard computers. A COTS (commercial of the shelf) SBC (single board computer) is used for tasks that are not time-critical, like communications. At the same time, motor control is performed by a faster microcontroller board developed at the Delft University of Technology. The commercial development includes second and third-generation control units to meet the increased force levels of the 100 kW system [65, 66]. These units are equipped with an airborne wind turbine to power all onboard systems.

3.3.4. TETHER

The function of the tether is to transfer the traction force of the kite to the ground station. The 4 mm rope is made of Dyneema® SK75, has a total length of 1 km, a weight of 0.8 kg per 100 m, a mean breaking strength of 13 kN, and a special coating to enhance its lifetime under the cyclic bending load caused by the reeling on and off the drum [67]. The tether is a major safety-critical system component. Because it is not redundant, it is designed according to a safe-.life philosophy must be replaced when reaching a certain number of load cycles or age. The tether of the commercial 100 kW system has a diameter of 14 mm and transfers a nominal traction force of 50 kN.

3.3.5. GROUND STATION

The ground station uses a drum/generator module to convert the traction power of the outbound, powered kite into electrical energy and to retract the depowered kite, consuming some of the generated energy. The electrical machine of this regenerative winch has a nominal power of 18 kW and connects to the drum via a gearbox with a fixed transmission ratio. As shown in Figure 3.1, the tether enters the ground station through a fixed swivel head and pulley guiding system. For systematic, layer-by-layer reeling on and off the drum, the entire winch is mounted on a sled that is moved transverse to the incoming tether. The alternating linear motion of the sled is coupled directly to the rotational motion of the drum. Except for the separate measurement mast and optional launch mast, the ground station houses all other components, such as the control center, the rechargeable battery module, and the power electronics. The commercial system uses an electrical machine with a nominal power of 180 kW.

3.3.6. DISTRIBUTED SENSOR NETWORK

A network of distributed sensors is used to measure environmental conditions and operational parameters of the system [57]. However, only some of this information is required for automatic operation, and some are for research and development. It is concisely described the sensor data that is useful for fault detection. The wind speed and direction six meters above the ground are measured by a sensor mounted at the tip of a mast, which transfers its data to the control center wirelessly. The elevation and azimuth angles of the tether and the traction force are measured at the swivel head where the tether leaves the ground station. The KCU has potentiometers and temperature sensors for steering and depower motors. Also, the battery voltage is measured and recorded. As illustrated in Figure 3.2, the wing is equipped with a sensor unit comprising a global positioning system (GPS) receiver and inertial measurement unit (IMU). Because the wing deforms under load, these sensors may produce misleading data, although the sensors work fine.

3.3.7. WINCH CONTROLLER

The winch controller modulates the reeling speed of the tether to maximize the energy output while ensuring the reliable and safe operation of the system. A baseline strategy for AWE systems in pumping cycle operation using crosswind maneuvers is to reel out at roughly one-third of the wind speed [61] or slightly faster and reel in as fast as the depower capability of the specific kite design allows. For cost-competitive and resource-efficient system designs, the nominal tether force during reel out at the nominal wind speed is close to the maximum allowed value. To avoid overloading the system due to natural fluctuations of the wind speed, set values are used for both reeling speed and maximum tether force. During reel out, the set value for the speed is tracked unless the maximum tether force is exceeded. In this case, the reeling speed is increased to track the set value of the force. During reel-in, a different combination of set values is used. Of particular importance is to transition between the set values gradually when switching the reeling direction [68, 69].

3.3.8. FLIGHT CONTROLLER

The flight controller is responsible for the motion component transverse to the tether. It consists of three distinct functional components: flight path planner, flight path controller, and course controller. The flight path planner corresponds to an aircraft's guidance or navigation controller. It is not involved in the actual steering of the kite but maps out the future system states, using the path and course controllers to reach those states. Thus, the flight path planner exercises control of the pumping cycle level. Figure 3.3(A) illustrates the five individual flight phases of a pumping cycle. The flight phases correspond to specific system states: “Reel out” describes the figure-of-eight flight maneuvers, “PointToZenith” the termination of these crosswind maneuvers and redirection of the kite to point towards the zenith, “Depower” the retraction of the kite with a reduced angle of attack, “Power” the increase of the angle of attack and “Intermediate” a diving maneuver to adjust the elevation angle of the tether to its value during the traction phase. The system can only be in one state at a time. When reaching the switch criteria for a certain flight phase, the path planner updates the desired system state and initiates the next flight phase. When switching states, the flight path planner sets one or more new target points on the unit sphere around the ground station, adapts the desired de-power setting and issues a certain set force to the winch controller.

The flight path controller is only active during system states with more than one target point, for example, during the figure-of-eight maneuvers of the traction phase. Its task is to issue only one of those points at a time and to switch to the next one when certain conditions are met. The prevailing wind speed is measured to calculate the desired elevation angle to achieve the optimal pulling force in varying wind conditions. The flight path controller can add a specific offset elevation to the fixed target points to optimize the pulling force. With the flight path planner not only issuing settings for depower and winch control but also, assisted by the flight path controller, setting a target point on the unit sphere, it is the task of the course controller to steer the kite towards this target point. For this purpose, the course controller calculates the desired course using great-circle navigation on the unit sphere [41] and the heading required to fly this course. The actual heading, estimated or measured, is then compared to the desired heading, and an anti-windup PID controller is used to minimize the error.

3.3.9. DISTRIBUTED SOFTWARE ARCHITECTURE

The modular software architecture accounts for the fact that the hardware components of the control system are distributed over the different parts of the kite power system. For example, the two computers in the KCU are connected to the three computers in the ground station via wireless links. For this reason, the accurate timing of the communication between the distributed hardware components is crucial. During early flight tests, unstable control behavior is observed when the latency between a measurement and the corresponding reaction of an actor exceeds 100 ms [70]. An operating system tuned for low latency is chosen to address this latency. To stay within the maximum tolerable latency, the time budget of each component is precisely calculated based on its technical specifications. A typical example is an IMU signal from the sensor unit mounted on the wing. Such a measurement can take up to 20 ms, generating a signal that is transferred to the main computer of the KCU on a wire (5 ms), wirelessly sent to the ground station (15 ms), processed by the Kite State Estimator (5 ms) and the Flight Path Controller (15 ms), wirelessly sent back to the motor control motherboard of the KCU and transmitted to the steering motor controller (20 ms). Except for the winch control, which is subject to firm real-time requirements, communication between the distributed software components is realized via a middle-layer SW library. This library supports publish-subscribe pattern is well suited for distributed designs. The required time budget is met using a message serialization library.

3.4. MODES OF OPERATION

The fundamental operational phases of an AWE system are launching, energy harvesting, and landing. These phases are adjusted to the prevailing wind conditions. For example, the kite is launched only when a minimum wind speed is achieved. To maximize the net energy output and to ensure safe operation, the pumping operation is adjusted each cycle to the wind speed profile. When exceeding the maximum wind speed, the cut-out speed, the crosswind maneuvers are discontinued, and the kite is steered towards a static flight position. This parking mode can also be initiated due to potentially harmful weather conditions or other external influences. Parking is also one of the possible reactions to operational anomalies, which the system may detect while continuously monitoring its health state. To be consistent with the literature the following terminology is used[71]: A fault is a defect of a component or a system. A failure is a state of not meeting the defined objective. A hazard is any source of potential damage. A malfunction is functioning differently than aimed, and a mitigation measure is an action for reducing the severity or probability of an undesired event. The wind window is a quarter-spherical region downwind of an observer at the ground station in which the kite can be flown in a controlled way. In the following sections, a zoning concept for pumping kite power systems is proposed, and then the different modes of operation are detailed.

3.4.1. ZONING CONCEPT

How does the specific operation of two or more pumping kite power systems affect the use of airspace and land has been analyzed theoretically by Faggiani and Schmehl [72] for flexible wing systems and by Licitra [73] for rigid wing systems. The zoning concept for the commercial 100 kW system of Kitepower B.V. is depicted in Figure 3.4. The operational zone covers the volume swept by the kite and the tether during regular pumping cycle operation. The flight zone, on the other hand, covers the more significant volume in which the kite and tether may fly during launching, landing, and parking. The zone also includes a safety margin to cover deviations from the typical flight path. On the ground, the danger zone is accessible only to experienced personnel. People, animals, or light transportation are allowed in the surrounding safety zone, but there has to be an awareness of the flight operations above. Accordingly, the safety zone excludes busy roads, railways, or open water. Considering that this zoning concept is only the first proposal based on a decade of operational experience with a single system is important. The arrangement and joint operation of multiple systems in a park configuration are subject to continued research. The zoning concept will be affected majorly by the certification and regulation processes required for the commercial deployment of the kite power system [40].

3.4.2. LAUNCHING

The standard procedure to start the kite power system is a winch launch of the kite. For this purpose, the wing is placed with its trailing edge on the ground at some distance downwind of the ground station. For the technology demonstrator of the university research group with a maximum wing size of 25 m^2, this was done by a ground crew, which also held the wing in position until take-off. A ground anchoring system for the commercial system retains the wing. In a short prelaunch procedure, the tether and bridle line system is first tensioned by the winch, then the wing is released automatically and pulled against the wind direction to take off. To integrate launching and landing compactly with the ground station, experimental mast- and drone-based techniques have been investigated [46, 58].

3.4.3. NORMAL OPERATION

As long as the system does not detect any faults, failures, or malfunctions, the health state is set to normal operation, and the flight path planner commands pumping operation by cycling through the system states illustrated in Figure 3.3(A). As described in Section 3.3.8, the planned path is adjusted for each cycle, depending on the expected wind resource.

3.4.4. RESTRICTED OPERATION

Restricted operation is the only health state that allows pumping operation even after detecting a fault. The restriction can relate to different system components, depending on the fault. If, for example, the standard deviation of the wind speed exceeds a limiting value, the set force for the winch controller is reduced for safety reasons. In case of unusually high temperatures of the steering motors, the course controller gains can be adjusted so that the load on the motors is reduced. This reduction can be done, for example, by flying larger figure-of-eight maneuvers with a larger turning radius.

3.4.5. PARKING

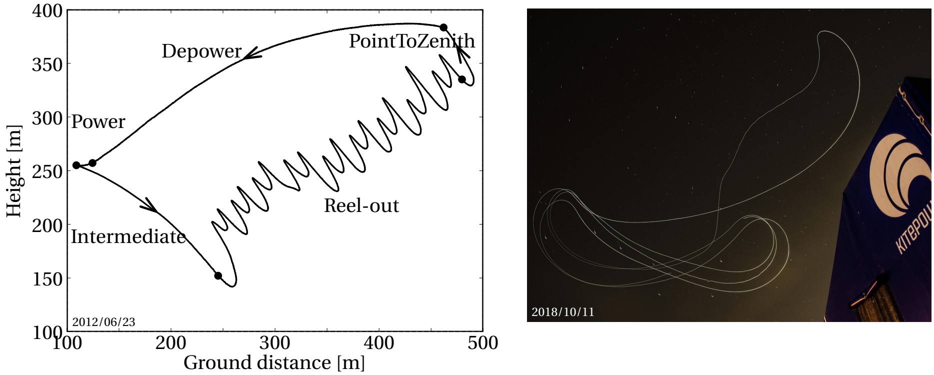
The kite is maneuvered into a parking position by terminating the crosswind maneuvers and steering the wing to point toward the zenith. With the flight speed dropping to zero, the traction force of the wing reduces substantially. This force and the elevation angle of the tether can be controlled with the depower setting of the kite. The parking maneuver is very similar to the maneuver executed during the system state “PointToZenith” that follows the reel-out phase of a pumping cycle, as described in Section 3.3.8. Temporarily parking the kite can be helpful, for example, to avoid landing and relaunching in case of a passing thunderstorm. Parking can also be triggered as a reaction to an anomaly. This reaction makes sense only for faults that can cause a system malfunction but not a failure. Because other than a failure, a malfunction disappears with time such that the pumping operation can be resumed. An example would be a failing dump load module of the ground station, which can cause the battery voltage to exceed a threshold. Another example would be a drop in the power level of the KCU below a threshold. Several options have been investigated to authorize the KCU to park the kite autonomously if no steering inputs are received from the ground station. This autonomous fall back into a "fail-safe" state would increase the overall safety by covering the worst case of losing the wireless connection to the control center.

3.4.6. IMMEDIATE LANDING

Extensive loss of operational safety or other situations requiring repair or maintenance on the ground causes the FDIR system to request an immediate landing. The following automatic landing procedure consists of three phases. First, the kite is parked and reeled-in to an altitude of around 100 m. To ensure that tether forces stay within acceptable limits and that the kite does not overfly the zenith, the depower setting during this flight phase is adjusted according to the wind speed. Once the set value of the tether length is reached and specific other requirements are met, the kite adapts its depower setting and dives into the wind window, passing three waypoints. Figure 3.5 shows the simulated flight path of this diving maneuver for three different wind speed ranges. The flattened spherical coordinate plane represents the wind window, and the three dots within this window are the waypoints that vary with the wind speed range. When arriving at a defined minimum height, the kite is powered up and navigates towards a final fourth waypoint on the edge of the wind window. In this last phase of the descent, the kite decelerates and eventually drops to the ground.

3.4.7. EMERGENCY LANDING

An emergency landing occurs when the flight control system has lost steering authority. This case can occur, for example, when a steering line ruptures and the fault detection algorithm detects a significant difference between the actual yaw rate of the wing, as estimated from GPS data, and the reference yaw rate, as derived from an empirical yaw rate correlation [74]. The cable cutter separates the KCU from the main tether to start the emergency landing. Consequently, the relatively heavy KCU, still attached to all bridle lines, swings below the wing so the kite can be retracted to the ground station in a paraglide/parachute mode using the additional safety line. This procedure has been described in detail in Section 3.3.2. After a few seconds of oscillations, the system reaches a new trim state, with the KCU stabilizing the flight like a parachuting pilot. The kite then descends towards the ground station with the fifth line connected to a central point on its leading-edge, retaining the system's steerability. However, as the wing loading during an emergency landing is orders of magnitude smaller than during reel-out operation, the steering input's effects are much smaller. Once the emergency landing is initiated, the flight path planner issues a single navigation point at the wind window zenith, and the winch starts reeling in the tether until the kite passes through a certain touchdown height. De-power is adjusted to ensure a soft landing. An emergency landing can also be initiated passively by a breaking weak link.



(A) **(B)**

Figure 3.3: A, Side view of the measured flight path of a representative pumping cycle with indicated flight phases between switch points[41]; Photographic visualization of a pumping cycle during night operation by tracing a marker light on the kite from the ground station (right) using long-term exposure (courtesy of Kitepower B.V.).

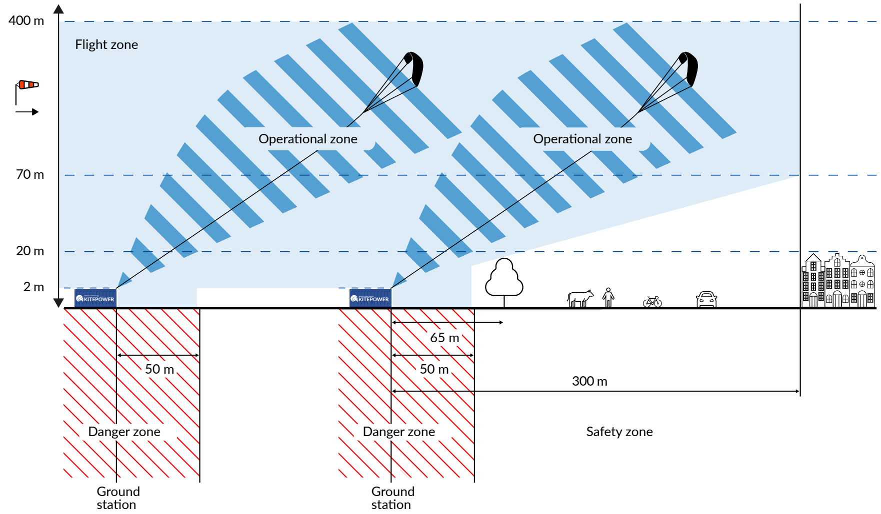


Figure 3.4: General spacial layout of pumping kite power systems (courtesy of Kitepower B.V.). *Note: AWE Europe safety working group proposes a more generally applicable zoning concept. See Chapter 7 Figure 7.3.*

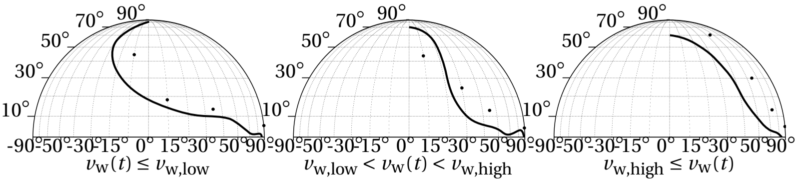


Figure 3.5: Observed landing paths of the kite on the flattened spherical coordinate plane for different wind speed ranges [41].

4

SYSTEM SAFETY AND RELIABILITY ASSESSMENT

4.1. ABSTRACT

In order to increase the robustness levels for commercial AWES, systematic safety analyses should be run iteratively during the development. This chapter presents the details of the systematic safety analysis of the Kitepower system. For the analyses, industry-proven reliability engineering methods, FMEA (Failure mode and effect analysis) and FTA (Fault tree analysis) are conducted. Interpretation of the results from the analyses is provided. The initiated measures from the analyses already show a clear impact on the Kitepower system, and the uptime of the development platform is continuously increasing. To our knowledge, this chapter is a unique study that details the followed methodology for airborne wind energy systems (AWES). The presented method and implementation details can be considered a practical guideline for conducting systematic safety analyses.

4.2. INTRODUCTION

Reliability engineering provides several methods to systematically improve the availability and safety of complex technical systems [33, 53, 75, 76].

In this work, FMEA and FTA, which are common in aircraft industry, has been conducted. Failure mode and effects analysis (FMEA) is a “bottom-up” analytical method used in the design phase to map and examine individual components’ failures and trace the potential effects on the entire system’s performance. FMEA is widely used in automotive and aerospace engineering and many other domains. The method has also been adopted for wind turbines [25]. Fault tree analysis (FTA) is the reverse of FMEA, a “top-down” deductive analysis aiming to identify and analyze conditions that lead to a particular system failure, commonly the catastrophic event.

Parts of this chapter have been published in Ref. [56].

The outcome of the analyses helps improve the reliability and safety levels of AWES by proposing engineering design changes, development process improvements, or methodological changes in the operation of AWES. In addition, these analyses provide a foundation for the FDIR architecture by pointing out which faults need to be detected and how they can be mitigated. Thus, safety analyses derive the requirements for an FDIR system. Although the methodology presented here is for a specific AWE system, the flexible-wing kite power system of the Delft University of Technology and Kitepower B.V., it is generic. It can be applied to different types of AWE systems. The chapter is organized as follows. Section 4.3 describes the systematic safety assessment and improvement using FMEA and FTA, considering FDIR system components as an integral part of the fault management strategy. The achieved results are presented in Section 4.4 and Section 4.5 finalizes the chapter with conclusions.

4.3. SYSTEM SAFETY ASSESSMENT AND IMPROVEMENT

One of the first steps to improve the reliability and safety of a complex technical product like an AWE system is a systematic and comprehensive assessment of its architecture, design, installation, and maintenance to ensure that the relevant safety requirements are met. In the following, failure mode and effect analysis (FMEA) together with fault tree analysis (FTA) are used to assess and systematically improve the reliability and safety of the technology development platform described in Chapter 3. Because FMEA and FTA depend strongly on the mix of people contributing to them, team members with different professional backgrounds, such as system design, operations, safety, legal, and finances, have been involved to ensure high quality. A fault detection, isolation, and recovery (FDIR) system has been proposed as an integral part of the fault management strategy. The operation target for this reliability analysis is one week of flight without human intervention, except for launching and landing.

4.3.1. FAILURE MODE AND EFFECT ANALYSIS

The FMEA analysis method was developed by NASA in the 1960s, first used within the Apollo program and later adapted for aerospace, nuclear, and other applications with high severity in case of failure. Nowadays, FMEA is used in various fields, such as automotive engineering, for quality management to identify and overcome weak points during the early design phases of a product. The highly structured approach assesses all possible failure modes and their effects for all system components. For each failure mode, the worst consequence is taken into account. Mitigation measures are proposed for these failures with high severity or high probability. However, the process considers only one failure at a time, not a combined occurrence of failures and their effects. The quality of the analysis essentially depends on the available practical experience with the system and its different components [77].

For the FMEA, the system is first divided into subsystems, which are then broken down into components, as shown in Table 4.1. The present study distinguishes mechanical, electronic hardware (HW), and software (SW) components. Software malfunctions (i.e., wrong calculations, data corruption, processing delays) and failures (i.e., crashes) are investigated separately. Depending on the operation mode, a failure mode can have

Table 4.1: Breakdown of the kite power system for the FMEA into subsystems and components.

Subsystem	**Components**
Traction power system	Wing, bridle line system and tether.
Communication system	Data communication software, remote controller (RC) data communication firmware, data-link hardware, RC data-link hardware, message forwarder software.
Sensing system	Inertial measurement unit (IMU) communication software, IMU hardware, global positioning system (GPS) communication software, GPS hardware.
Actuation system	Steering motor hardware, depower motor hardware, motor driver microcontroller hardware, motor driver microcontroller software.
Control system	Kite state estimator software, flight path controller software, flight path controller steering software, flight path controller destination software, kite control software, message forwarder software, central processing unit hardware, microcontroller unit hardware.
Onboard power system	Airborne wind turbine (AWT) hardware, maximum power point tracking hardware, batteries hardware, power board hardware.
Ground control system	System state controller software, ground state estimator software, winch control software, clock software, message forwarder software, ground control computer.
Ground sensing system	Sensor software, GPS hardware, wind sensor hardware, force sensor hardware.
Ground power system	Generator, gear box, sled and secondary electrical drive, tether guidance mechanism, low-level winch control, batteries hardware, dump load module, inverter, grid connection (optional).

different effects. The failure mode is duplicated whenever this happens to investigate its effect on different operation modes, such as energy harvesting, launching, or landing. The FMEA is conducted with a spreadsheet, listing one failure mode per row and grouping these rows into subsystems. Columns are the following investigated properties;

1. the potential fault mode (software malfunction, software fault, hardware fault, wrong configuration, data corruption or data delay),
2. causes of the fault and mechanisms,
3. the foreseeable sequence of post-failure events,
4. the hazardous situation,
5. the worst case harm (physical injury or damage to the health of people, or damage to property or the environment),
6. the corresponding severity
7. the corresponding probability
8. the proposed mitigation measure
9. the residual post-mitigation worst-case harm
10. the residual severity and
11. the residual probability.

The probability definitions used in the analysis are listed in Table 4.2, while Table 4.3 lists the severity definitions and the associated global harm.

Table 4.2: Probability definitions for the failure modes [78].

Code	P value	P definition
A	1	Extremely unlikely (virtually impossible or no known occurrences on similar products or processes, with many running hours)
B	2	Remote (relatively few failures)
C	3	Occasional (occasional failures)
D	4	Reasonably possible (repeated failures)
E	5	Frequent (failure is almost inevitable)

Table 4.3: Severity definitions and harm of the failure modes (Adapted from [78]).

Code	S value	S definition	Harm
I	1	No relevant effect on reliability or safety	No harm
II	2	Very minor, no damage, no injuries[1]	Maintenance
III	3	Minor, low damage, no injuries[2]	Harm to environment
IV	4	Moderate, moderate damage, injuries possible[3]	Financial loss Injury from fire, smoke, explosion (operator harm) Injury by tether (operator harm) Injury by tether (3rd person harm)
V	5	Critical[4]	Damage to infrastructure Injury by electric shock (operator harm) Injury by kite crash (operator harm) Injury by kite crash (third-person harm) Injury from fire, smoke explosion (third-person harm)
VI	6	Catastrophic[5]	Injury by kite collision or crash (many people)[6]

[1] Only results in a maintenance action, noticed by alert customers.
[2] Affects very little of the system, noticed by average customers.
[3] Most customers are annoyed, mostly financial damage.
[4] Causes a loss of primary function; loss of all safety margins, severe damage, severe injuries, maximum one possible death.
[5] Product becomes inoperative; failure may result in complete unsafe operation and possible multiple deaths.
[6] Only possible if kite leaves the operation zone, which is also the top event for the FTA discussed in Section 4.3.2.

For each failure mode, a risk number R is calculated as the product of severity S and probability P.

$$R = S \cdot P \tag{4.1}$$

Properly assigning severity and probability values is crucial for the risk evaluation of the specific failure mode. For this reason, the values for S and R are evaluated closely with the engineering team of Kitepower B.V. working on the 100 kW system.

The investigated failure modes are prioritized in the next step based on the calculated risk numbers and corresponding mitigation measures proposed. The FDIR system presented in Chapter 5 can mitigate most failure modes. However, for some modes, the risk can be effectively lowered only by decreasing the failure probability of the component, which requires a stricter development or verification process or purchasing a higher quality component. In Section 4.4, the result of the FMEA is presented and two specific failure modes are presented as examples.

4.3.2. FAULT TREE ANALYSIS

As mentioned in the previous section, an FMEA does not consider combined occurrences of faults and their effects. However, faults with low individual risk factors can cause hazardous situations simultaneously. To consider this, FMEA is complemented with FTA [77]. The method was developed in the 1960s to analyze a ballistic missile system and has subsequently been applied in a broader context to analyze the risks related to safety and economically critical assets [76, 79]. A fault tree is a logic diagram describing the relationships between a particular system failure and the individual faults, failures, and malfunctions on component and subcomponent levels that contribute to this particular failure. The fault tree follows a top-down structure using logic gates and events to model how the component states relate to the entire system's state. The top event corresponds to the particular system failure that is investigated. The logic diagram is extended for quantitative failure analysis by quantitative information about component reliability, such as failure probabilities.

Most AWE systems crucially rely on active control of several distributed subsystems that are mechanically and electronically coupled, each consisting of several components. Each component can have several failure modes depending on the failure's operation phase or physical characteristics. Thus, considering the entire AWE system, the number of possible combinations of these failure modes is enormous. A common practice for FTA is to address only those combinations with catastrophic consequences. Once the fault tree is defined and failure models assigned to all involved system components, FTA software tools can be used to calculate the probability of catastrophic consequences and prioritize the different contributors to the top event with catastrophic consequences. Contributors with high priority are then improved to decrease their impact on the failure. This process of FTA and subsequent design modifications are repeated iteratively until the computed probability of the catastrophic event has been decreased below a certain threshold.

For the kite power system investigated in this study, an utterly unsafe operation with possible deaths and damage to critical infrastructure is defined as the catastrophic event. This would be the case if the kite leaves the operation zone, which could entail the following catastrophic consequences

- entering forbidden airspace and collision with other users of the airspace[40],
- crashing into a critical infrastructure on the ground,
- crashing on a highway,
- crashing outside of the operation zone which is not free of people.

Because of the severity of these consequences, the case of the kite leaving the operation zone is defined as the top event (see also Table 4.3). Only these events which bring the system to the specific top event are analyzed. Crashes or other undesired events *within* the operation zone are not included in the FTA because their consequences are not considered catastrophic. The fault tree is created and the component failures are modeled for the same operational target as the FMEA: a one-week flight without pilot intervention. Figure 4.1 depicts the complete fault tree, with 31 basic events and two undeveloped events populating the leaf nodes. The undeveloped events "winch system problem" and "kite damaged, not steerable" could have been broken down further to the component level; however, within the frame of this study, instead integral probability models are assigned to both events. The parts of the fault tree highlighted in different colors are further detailed in Figures 4.2 to 4.5. The top event with one abstracted branch represented by a triangle symbol is shown in Figure 4.2. The intermediate event "mal-

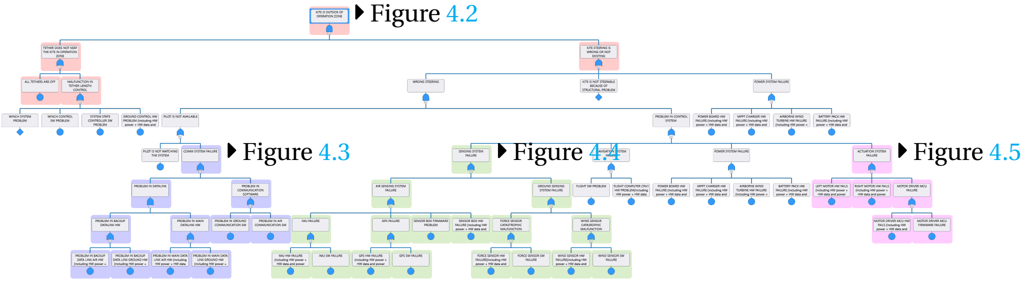


Figure 4.1: Complete fault tree (see Figure 4.2 for symbol legend).

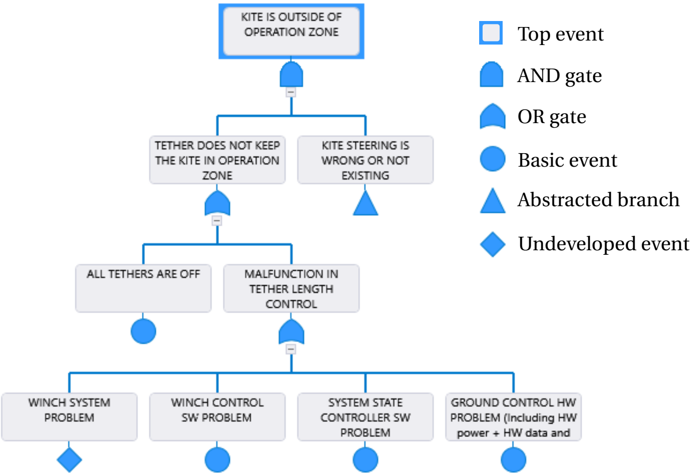


Figure 4.2: Fault tree for the top event “Kite is outside of operation zone”.

function in tether length control” is caused by any of the four events at a lower level, i.e., “ground control HW problem”, “system state controller SW problem”, “winch control SW problem” or “winch system problem”. The undeveloped event includes all other ground components that cause a malfunction of the tether length control. A “malfunction in tether length control” or the basic event “all tethers off” causes the intermediate event “tether does not keep the kite in operation zone”. If this occurs with the condition “kite steering wrong or not existing”, the top event “kite outside operation zone” is caused. Figures 4.3 to 4.5 show fully detailed branches, ending at basic events, which are the leaf nodes of the fault tree.

The investigated failure events and the corresponding probability density functions are listed in Table 4.4. For all software and firmware components in the system, a constant failure rate of 10^{-3}/h is used. This value corresponds to software developed according to DO-178C (Software Considerations in Airborne Systems and Equipment Certification) with Development Assurance Level (DAL) D [80]. Even though no formal standard was followed during the development of the current software, DAL-D level failure rate is

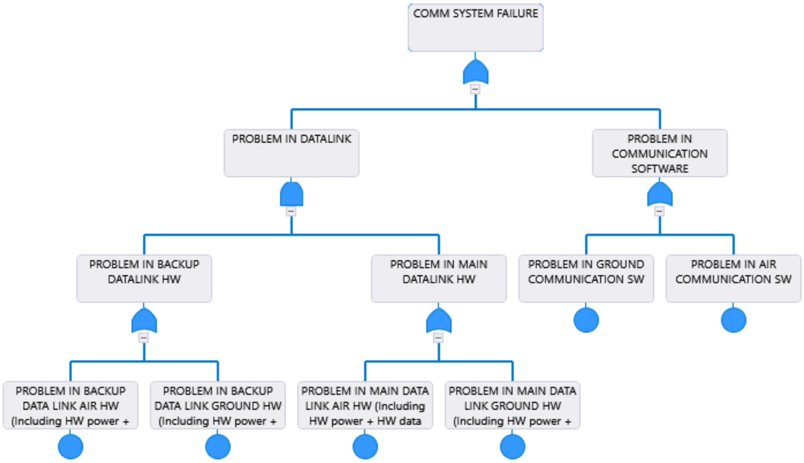


Figure 4.3: Fault tree for the intermediate event “Communication system failure”.

considered reasonable based on the generated artifacts, test intensity, and flight hours of the software components. Failure databases provide generic failure data collected from a variety of sources. Weibull failure coefficients from Barringer & Associates, Inc. [81] are a starting point for some hardware components. Some of the basic events in the fault tree data were not available in the failure databases. For such events, expert opinion and engineering judgment were used to estimate the failure probability. The expected mean time to failure for a non-repairable system is abbreviated as MTTF. The Weibull probability density function is parametrized by the characteristic life (hours) η, the slope β, and the failure-free life (hours) γ.

4.4. RESULTS

Within the scope of the FMEA, eighty different failure modes of electronic hardware and software components are investigated. Based on the risk number calculated from Equation (4.1), a prioritized list of failure modes that could lead to potentially hazardous situations is compiled. To increase system-wide reliability and safety, the modes that can be mitigated by an FDIR system and the modes that require a redesign of the involved components are distinguished to meet stricter reliability standards. For example, Table 4.5 details a flight path controller software malfunction that FDIR can mitigate. The rows listing the residual severity, probability, and risk number indicate the improvement the proposed mitigation measure can achieve. The specific operational target impacts the foreseeable sequence of events and the suitable mitigation measures. For example, certain sensor failures may be tolerable for short flights when the pilot is in the loop. However, for one week of flight, the intervention of a pilot can not be proposed as a mitigation measure.

Table 4.6 shows an example of reducing the risk of a failing motor driver microcon-

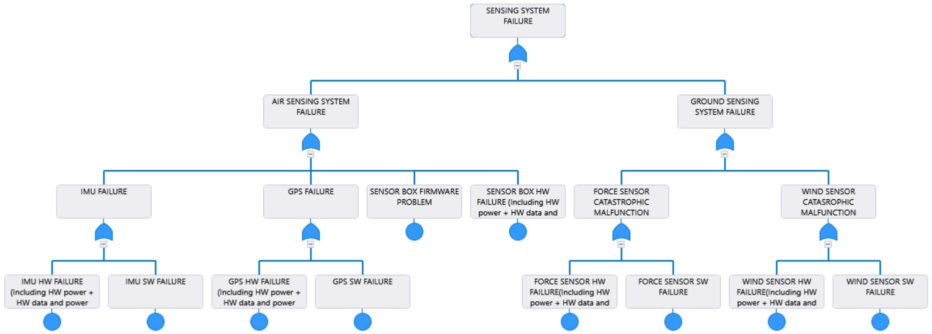


Figure 4.4: Fault tree for the intermediate event “Sensing system failure”.

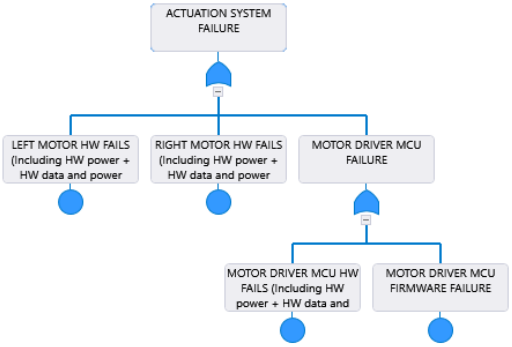


Figure 4.5: Fault tree for the intermediate event “Actuation system failure”.

troller software by defining a stricter software standard, such as changing the design assurance level (DAL) from D to C.

The total risk number of the technology development platform calculated by the FMEA is 569. The risk number can be decreased to 370 by applying the proposed mitigation measures. The maximum risk number of a single failure mode is calculated as 15, which can be reduced by mitigation to 10. The residual severity of all individual failure modes is below 6, which means that the proposed mitigation measures effectively prevent any single failure causing the catastrophic event, which is defined as the kite leaving the operation zone and potentially colliding with other users of the airspace or crashing on the ground.

With the FTA, combinations of failures that cause the catastrophic event are in the focus. Based on the fault tree illustrated in Figure 4.1, 33 different component failure events are defined that may trigger the catastrophic event in combination. A probability model is assigned to each of these failure events. Then, the exact probability of the catastrophic event is determined using the binary decision diagram (BDD) method [82] and considering Boolean logical relationships of the failure events. Minimal cut sets (MCS)

Table 4.4: Failure events and probability density functions used for the FTA. Hardware (HW) includes HW power, HW data, and power cabling.

Subsystem	**Failure event**	**Probability density function**
	Pilot offline[1]	MTTF(MTTF=5)
Traction power system	All tethers off[2], kite mechanically detached from ground station	Constant($q = 0.01$)
	Kite not steerable because of structural problem	Weibull($\eta = 200, \beta = 2, \gamma = 0$)
Communication system	Communication software (SW) airborne component fails	Constant($q = 0.001$)
	Communication SW ground component fails	Constant($q = 0.001$)
	Main data-link HW airborne component fails	Weibull($\eta = 100000, \beta = 1, \gamma = 0$)
	Backup data-link HW airborne component fails	Weibull($\eta = 100000, \beta = 1, \gamma = 0$)
	Main data-link HW ground component	Weibull($\eta = 100000, \beta = 1, \gamma = 0$)
	Backup data-link HW ground component fails	Weibull($\eta = 100000, \beta = 1, \gamma = 0$)
Sensing system	Inertial measurement unit (IMU) HW fails	Weibull($\eta = 75000, \beta = 0.7, \gamma = 0$)
	IMU SW fails	Constant($q = 0.001$)
	Global positioning system (GPS) HW fails	Weibull($\eta = 75000, \beta = 0.7, \gamma = 0$)
	GPS SW fails	Constant($q = 0.001$)
	Sensor box SW problem	Weibull($\eta = 100000, \beta = 0.7, \gamma = 0$)
	Sensor box HW fails	Weibull($\eta = 100000, \beta = 0.7, \gamma = 0$)
Actuation system	Left motor HW fails	Weibull($\eta = 50000, \beta = 1.2, \gamma = 0$)
	Right motor HW fails	Weibull($\eta = 50000, \beta = 1.2, \gamma = 0$)
	Motor driver microcontroller unit (MCU) HW fails	Weibull($\eta = 100000, \beta = 0.7, \gamma = 0$)
	Motor driver MCU SW fails	Constant($q = 0.001$)
Control system	Flight SW problem	Constant($q = 0.001$)
	Primary CPU HW problem	Weibull($\eta = 25000, \beta = 0.7, \gamma = 0$)
	System state controller SW problem	Constant($q = 0.001$)
Onboard power system	Power board HW fails	Weibull($\eta = 75000, \beta = 0.7, \gamma = 0$)
	Maximum power point tracker (MPPT) charger HW fails	Weibull($\eta = 100000, \beta = 0.7, \gamma = 0$)
	Airborne wind turbine HW fails	Weibull($\eta = 50000, \beta = 1.2, \gamma = 0$)
	Battery pack HW fails	Weibull($\eta = 8000, \beta = 2, \gamma = 0$)
Ground control system	Winch system problem	Weibull($\eta = 25000, \beta = 1, \gamma = 0$)
	Winch control SW problem	Constant($q = 0.001$)
	Ground control HW problem	Weibull($\eta = 25000, \beta = 0.7, \gamma = 0$)
Ground sensing system	Wind sensor HW fails	Weibull($\eta = 50000, \beta = 1.2, \gamma = 0$)
	Wind sensor SW fails	Constant($q = 0.001$)
	Force sensor HW fails	Weibull($\eta = 100000, \beta = 0.7, \gamma = 0$)
	Force sensor SW fails	Constant($q = 0.001$)

[1] Only applicable during launching and landing, which at present state of development still requires a pilot.

[2] Includes safety line.

are also extracted during the probability calculation.

In a fault tree, an MCS is the smallest combination of basic events causing the system failure. Unlike the classical minimal cut set method, the BDD method provides exact values for the cut set unavailability and relative importance. Unavailability is defined as the probability that a specific cut set is in a failed state at time t, and the Vesely-Fussell importance factor is used which is defined as the fraction of system unavailability contributed by a specific cut set [79]. Table 4.7 lists the minimal cut sets, their unavailability, and their relative importance for the technology development platform.

Figure 4.6 shows the computed unavailability of the investigated system as a function of the days in operation.

After one week of operation, the computed unavailability is 2.75%, equivalent to a system failure rate of 0.163×10^{-3}/h. The minimal cut sets listed in Table 4.7 amount to joint unavailability after one week of 2.70%, which means that these first ten cut sets practically describe the catastrophic system failure behavior resulting from simultaneous component failures. At the time of writing, the commercial technology development platform was continuously further developed, applying the insight gained from the re-

Table 4.5: Example for the FMEA of a failure mode forming a requirement for the FDIR system.

Properties	**Definition**
Subsystem	Control system
Item	Flight path controller software
Mission phase	Energy harvesting
Fault mode	Malfunction
Cause(s)/Mechanism short sentence about	Bug in software, operating system fault, insufficient system resources, wrong task priority assignment, wrong configuration of the operating system
The foreseeable sequence of events	Motors stop functioning or wrong commands to the motors, loss of flight control
Hazardous situation	Uncontrolled crash of kite inside operational zone
Harm (worst case)	Injury by kite crash (operator harm)
Severity	5
Probability	3
Calculated risk number	15
Mitigation measure	At FDIR Level 3, the model implemented in health supervisor detects substantial deviations from planned flight path, overrule commanded state to “kite safe state”, kite goes into parking (see Section 3.4.5)
Residual harm (worst case)	Maintenance required
Residual severity	2
Residual probability	3
Residual risk number	6

Table 4.6: Example for the FMEA of a failure mode pointing out a necessity for a stricter standard.

Properties	**Definition**
Subsystem	Actuation system
Item	Motor driver microcontroller software
Mission phase	Energy harvesting/landing/launching
Fault mode	Failure
Cause(s)/mechanism	Bug in motor driver software
The foreseeable sequence of events	Loss of steering authority, tether tension can be controlled by the depower motor, controlled immediate landing within operational zone (see Section 3.4.6)
Hazardous situation	Uncontrolled crash of kite inside operational zone
Harm (worst case)	Injury by kite crash (operator harm)
Severity	5
Probability	2
Calculated risk number	10
Mitigation measure	Define more stringent design/development/test software standard to increase reliability
Residual harm (worst case)	Injury by kite crash (operator harm)
Residual severity	5
Residual probability	1
Residual risk number	5

liability analysis step by step. As a result, some of the critical components’ design was improved, and some FDIR system modules were implemented. Even with the partial implementation of these measures, a reliability improvement can be recognized from the flight logs. Figure 4.7 illustrates the increasing number of flight days per quarter and the total accumulated number of flight days. The dashed line indicates the limit of continuous operation at around 90 days per quarter.

Table 4.7: First ten minimal cut sets with unavailability and Vesely-Fussell (VF) importance factor calculated for one week of operation.

Minimal Cut Set	**Unavailability** [%]	**VF Importance** [%]
Ground control HW problem Kite damaged, not steerable	1.5	48.14
All tethers off Kite damaged, not steerable	0.51	16.21
Winch system problem Kite damaged, not steerable	0.34	10.86
Primary CPU HW problem Ground control HW problem Pilot offline	0.08816	2.82
Winch control SW problem Kite damaged, not steerable	0.05062	1.62
System state controller SW problem Kite damaged, not steerable	0.05062	1.62
Ground control HW problem Power board HW failure	0.04119	1.32
Ground control HW problem IMU HW failure Pilot offline	0.04119	1.32
GPS HW failure Ground control HW problem Pilot offline	0.04119	1.32
Ground control HW problem MPPT HW failure	0.03372	1.08
$\sum_{n=10}$	2.69669	86.31

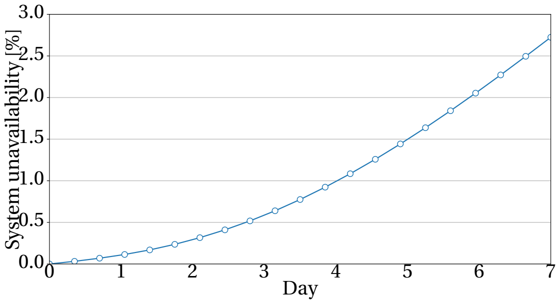


Figure 4.6: Unavailability of the kite power system.

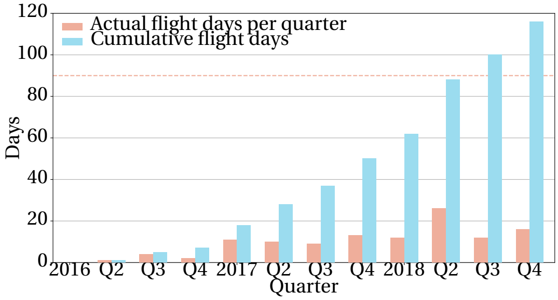


Figure 4.7: Number of flight days for Kitepower B.V. from 2016 until 2019.

4.5. CONCLUSIONS

System reliability, operational robustness, and safety are crucial for successfully commercializing airborne wind energy (AWE). Given the technology's inherent complexity, these aspects must be considered early in the system design process. In this study, a failure mode and effects analysis (FMEA) and a fault tree analysis (FTA) are combined to assess and systematically improve the reliability and safety of a 100 kW technology development platform, which has been derived from a well-documented technology demonstrator with 18 kW electrical machine. Potentially hazardous situations are mitigated by failure detection, isolation, and recovery (FDIR) using a hierarchical architecture from the space industry that fits well with the design of AWE systems.

In the FMEA, only single failure modes are considered, one by one, proposing mitigation measures for each mode to increase the system-wide reliability and safety. With the FTA, simultaneous failures are focused and the resulting probability of the worst-case event is defined, The worst-case event is defined as the kite leaving the operation zone in an uncontrolled way. The underlying fault mechanisms that can cause this event are revealed and this information is provided to the engineering team for iterative improvement of the system design. The computed probability will later be used to prove to a certification body that the probability of harming people is below a specific limit.

At the time of writing, the commercial technology development platform was continuously further developed, and the proposed mitigation measures were only partially implemented. For example, the holistic model-based technique at FDIR Level 3 was not yet validated for different flight conditions, and the redesign of critical components was not completed. Nevertheless, the initiated measures already show a clear impact, and the uptime of the development platform is continuously increasing.

5

FAULT DETECTION, ISOLATION, AND RECOVERY (FDIR) SYSTEM FOR AIRBORNE WIND ENERGY SYSTEMS

5.1. ABSTRACT

Safety-critical systems are systems whose failure or malfunction may result in death, serious injury of the people, loss or damage of the system, or environmental harm. Fault detection, isolation, and recovery (FDIR) is a technique to monitor the system during operation, identify faults that occur, pinpoint the type of fault and its location, isolate it, and take appropriate recovery actions. An FDIR system is a significant component of today's safety-critical systems to mitigate the hazardous consequences of faults. This chapter proposes a general FDIR architecture that applies to different AWES. In addition, the chapter presents the details of a fuzzy-logic-based flight anomaly detection layer developed for flexible wing AWES. The initial flight data shows that the proposed system can detect critical flight anomalies without generating false alarms. A similar systematic health management system is needed to reach commercial AWES's required reliability and safety levels. To our knowledge, this study is the first to offer a methodology for AWES's health management.

5.2. INTRODUCTION

The present chapter proposes a multilayered architecture for the health management of AWES to reach the required reliability and safety levels for commercialization. Like space missions, AWES must perform their tasks with high autonomy under severe environmental conditions. To achieve commercially required robustness levels, we tailored

---

Parts of this chapter have been published in Ref. [83].

a hierarchical FDIR architecture for AWES, initially developed for European earth observation satellites [84]. Firstly, a set of requirements for an FDIR system is defined. These requirements are gathered by a reliability analysis using the FMEA and FTA methods detailed in Chapter 4. The obtained requirements mitigate the system failure cases. Although we present the methodology for a specific AWE system, the flexible-wing kite power system of the Kitepower/TuDelft (see. Chapter 3), it is generic in its setup, and it can hence be applied to other types of AWE systems.

After presenting the high-level architecture of the AWES-tailored FDIR in Sections 5.3.1, this work details the "flight anomaly detection" layer of the FDIR, which consists of three decision engines. One is for checking if the kite is still under control, the second is to ensure that the kinetic energy level of the airborne part is below a predefined safety limit, and the third engine is for confirming that the kite's position is still within the operation envelope. It is considered that the proposed "flight anomaly detection system" is an essential contribution to the AWE literature for the commercialization and certification processes.

To our knowledge, no study to date has offered a methodology on the health management of AWES. Stoeckle[44] proposes an FDIR approach for autonomous parafoils that resemble kites with the suspended control unit. Friedl [41] and Friedl et al. [42] investigated means to augment the flight control system using an algorithm that detects potentially hazardous situations and reconfigures the system to ensure safe operation.

5.3. OBJECTIVES

Objective of this chapter is to propose an FDIR approach for airborne wind energy systems to reach publicly acceptable and commercially feasible reliability and safety levels. Maximum acceptable failure probabilities are;

- catastrophic failure condition of 10^{-8} per flight hour (pfh),
- and hazardous failure condition of 10^{-7} pfh

assumed according to Salma et al. [40]. These requirements are further discussed in later chapters (See Section 6.7).

These safety and reliability requirements need to be breakdown for sub-systems and reliability scheme designed accordingly. In practice, FDIR requirements are derived from the safety analyses of the systems. As a case study, safety analyses for the flexible-wing kite power system of the Delft University of Technology and Kitepower B.V is conducted. This chapter elaborates on implementing and validating the proposed FDIR architecture.

The first three layers of the proposed FDIR are to increase the availability and robustness of the system. The safety design target of FDIR is to prevent the catastrophic failure scenarios that are identified by FTA (Fault tree analysis) and FMEA (Failure mode and effect analysis) in Chapter 4.

5.3.1. FAULT DETECTION, ISOLATION AND RECOVERY

Fault detection, isolation, and recovery are integral parts of the fault management strategy because they implement the mitigation measures proposed by the reliability analyses. A generic high-level FDIR functionality for AWE systems is outlined in Table 5.1.

Table 5.1: Generic high-level FDIR functionality required for AWE systems.

Fault Detection	**Isolation**	**Recovery**
HW/SW interface communication problems	Detach faulty sensor	Reconfigure SW modules
SW faults	Detach faulty actuator	Reconfigure HW modules
Flight pattern tracking anomalies	Stop recurring faults	Generate safe winch command
Winch command anomalies		Generate safe flight trajectory
Tether force anomalies		Generate safe steering command
Onboard power system anomalies		Generate safe kite state
Ground-to-air communication anomalies		Generate safe steering command and immediate landing
Reaction to steering command anomalies		Cut safety line and emergency landing
HW faults		Acquire data from redundant or different sensors
Sensor data anomalies		

A minimal implementation complexity should be chosen for several reasons. Firstly, this generally reduces the effort to validate the implemented FDIR system. In most cases, physical models that can be part of such a system are validated only for nominal operation, with often insufficient prediction quality for off-design scenarios resulting from anomalies. An example is the inability to predict the behavior of the wing because of the damaged bridle line system.

Secondly, the system's overall complexity has to be manageable, and the reliability of the FDIR system should be greater than the system under monitoring. Therefore, detection mechanisms are designed only for failure modes identified by the FMEA and FTA. For the same reason, the mitigation measures are grouped as much as possible, using a joint FDIR implementation per group.

A hierarchical FDIR architecture is adopted from the space domain[84] because it fits well with the investigated AWE system. Satellites, for example, have high-reliability requirements, incorporate a safe mode, and use holistic anomaly detection. The layered structure supports a clear organization of tasks and helps in the identification of all possible failures. The modular and distributed architecture at low levels is straightforward to maintain in case of design changes. We implement this architecture with five hierarchical levels where each level represents a different way of monitoring and detection, as illustrated in Figure 5.1.

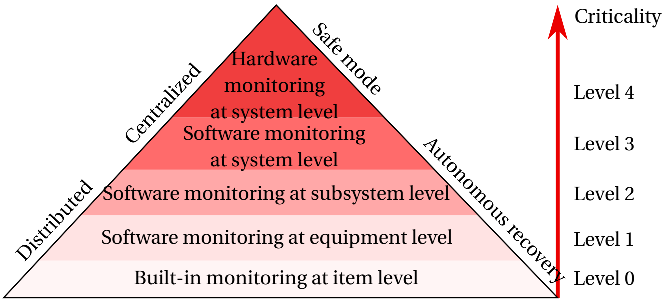


Figure 5.1: Hierarchical FDIR architecture.

Items represent the smallest functional units associated with the lowest FDIR level, followed by equipment, subsystems, and the entire system at successively higher levels. With the FDIR level, the criticality of the inspected faults increases. Fault monitoring and detection start at the lowest level. Higher levels are triggered only after activating the lower level several times without correcting the fault. The five levels are introduced in the following.

- Level 0 performs built-in monitoring at the item level. Some functional units must be capable of recovering autonomously from faults without affecting the system's performance. This autonomy is necessary, especially if the recovery time for a specific defect is critical. Software and hardware watchdogs in microcontroller boards are typical examples of Level 0 FDIR.

- Level 1 monitors the system at the equipment level for units that can not detect and recover autonomously from faults. At this level, the subsystem performs detection, recovery, and isolation (if required). Switching from a faulty sensor to a redundant one or deriving the data from a different sensor(s) are examples of Level 1 FDIR. For the subsystems, inputs and outputs are checked by the Level 1 FDIR concerning data consistency (continuity and frequency checks), measurement consistency (range check, rate check, comparison with a redundant sensor), and command consistency(command timing and feedback).

- Level 2 monitors the system performance at the subsystem level. Faults that cannot be localized at lower levels are caught at this level. The total current flow monitoring from the KCU onboard power subsystem and reconfiguring the subsystem in case of a fault is an example of Level 2 FDIR.

- Level 3 monitors the system performance at the system level. One or more faults that could not be recovered at the lower levels are caught by the Level 3 FDIR if it affect the system's performance. Heuristic methods [85] or model-based methods [86] are used for detecting such a system-wide anomaly. In general, the flight dynamics response of the kite to steering commands is a good indicator of the overall health status of the airborne subsystem. In our study, an empirical correlation [74] between the turn rate of the kite and the steering actuation is used for the Level 3 FDIR implementation. This correlation has to be determined by system identification for each kite, also considering the dependency on the depower setting.

- Level 4 performs hardware-only monitoring at the system level to protect the system from catastrophic events. There are no recovery or isolation actions at this level. An example of such a hardwired system-level alarm is cutting the tether for a controlled landing in the event of losing control.

Levels 3 and 4 are centralized and monitor the entire system by applying a holistic perspective. For example, the failure event "kite leaves operation zone but causing fault not identified" is handled at Level 3. In contrast, Levels 0, 1, and 2 are decentralized. Each subsystem has its FDIR component, which may consist of levels 1 and 2. Similarly, items may have their Level 0. FDIRs for each subsystem do not necessarily include all three levels. The composition of the levels, including the fault detection sensitivity, shall be determined according to the risk coefficient of the fault, which the FMEA determines. Thus, detection mechanisms only at higher levels, e.g., Levels 3 and 4, may be sufficient for non-critical faults.

FDIR Level 3 and FDIR Level 4 run independently from the flight software because these layers directly affect the system safety factor. Data to be used for flight anomaly detection have to be trustworthy. As inputs, angular and linear acceleration measurements, position data, and steering motor commands are considered sufficient for the proposed system.

In the kite power system, there is more than one accelerometer for redundancy purposes. The anomaly detection system uses the same consolidated acceleration data as the flight control system. Critical sensor data loss recovery is handled in the lower levels of FDIR. If the critical sensor's recovery is not possible, a flight anomaly alarm is triggered to terminate the flight.

A "false positive FDIR alarm" means FDIR wrongly reports an error even if there is no fault in the system. And, a "false negative FDIR status" means the FDIR misses a fault that should have been detected by the FDIR. Low false alarm rates are critical for FDIR Level 3 and Level 4 because false-positive alarms may decrease the system's availability by triggering an emergency landing when unnecessary. On the other hand, false negatives may cause hazardous consequences if the FDIR system does not command an emergency landing when it has to.

Three main criteria have been defined to decide whether the operation is safe during the flight. These are; (i) Kite shall be under control, (ii) the kinetic energy of the kite shall not exceed a predefined limit (iii) the kite shall be in the allowed operation zone.

Violating any of the abovementioned criteria is sufficient for triggering the anomaly detection alarm. A time-triggered filter is used to filter out false alarms. Thus, the violation should last a predefined period of time to raise the anomaly flag. The high-level architecture of the flight anomaly detection system is shown in Figure 5.2.

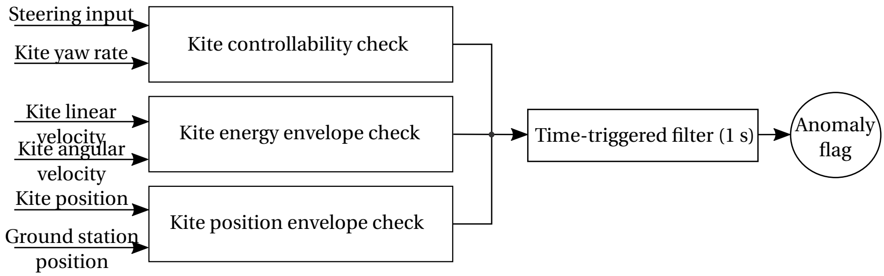


Figure 5.2: High-level architecture of the kite anomaly detection system.

1. **Kite controllability:**
   Steering, altitude, and the attitude of the kite need to be controllable at any moment under any environmental condition. An independent system is considered necessary to check if the flight control system can control the system as expected. This detection module is system-specific and should be designed considering the dynamics of AWES. As an example controllability check, a fuzzy logic expert sys-

tem using a Mamdani fuzzy inference engine is presented [87] for steering anomaly detection. Mamdani systems incorporate expert knowledge in the form of IF-THEN rules expressed in natural language. The proposed fuzzy engine uses the steering motor command and the yaw-rate response of the kite to decide whether the kite is still under control. The positive correlation between the steering input and the yaw-rate measurement is presented in [74].

Implementation and working details of the proposed fuzzy interference system can be found in [88]. In the scope of this work, the following essential application-specific definitions are provided.

(a) **Definitions of the fuzzy rules considering the relationship between the inputs and outputs**

As detailed in [74], the correlation given in Equation (5.1) was found using system identification methods. While C_1 and C_2 are kite specific parameters dependent on mass, geometry and power setting, the term $\mathbf{g}\cdot\mathbf{y}_{(K)}$ relates to the angle between the gravity vector and the $y_{(K)}$ axis.

$$r_K = C_1 v_\mathrm{a}^n u_\mathrm{S} + C_2 \frac{\mathbf{g}\cdot\mathbf{y}_{(K)}}{g} \tag{5.1}$$

Considering the correlation between steering input and corresponding yaw rate response, the fuzzy relationship shown in Table 5.2 is defined between the input variables and the output variable “steeringAnomalyDegree”:

(b) **Definition of the input membership functions, to fuzzify the inputs**

Five triangular membership functions are defined both for the steering and yaw-rate inputs. These inputs are “negative high”, “negative medium”, “low”, “positive medium”, and “positive high”. Membership functions against the input values are defined as shown in Figure 5.3 and Figure 5.4.

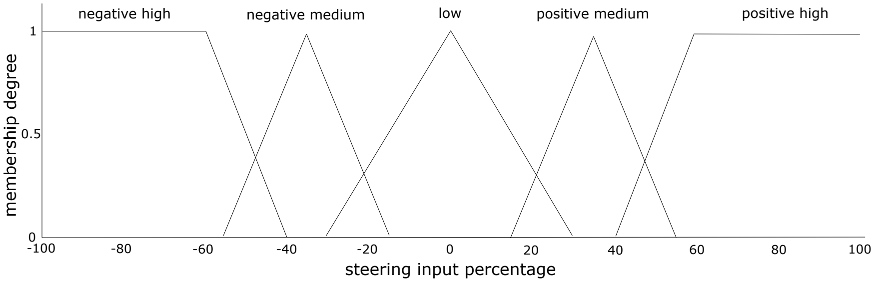


Figure 5.3: Membership functions for the fuzzification of steering input.

(c) **Definition of the output membership functions, to de-fuzzify the output**

To acquire the real anomaly value, the defuzzification of the “steeringAnomalyDegree” is implemented with the membership function shown in Figure 5.5.

Table 5.2: Mamdani fuzzy interference engine rules between the inputs and outputs.

IF (steering command)	AND (yaw rate measurement)	THEN: (anomaly result)
negative high	negative high	normal
negative high	low	anomaly
negative high	positive high	anomaly
negative high	negative medium	warning
negative high	positive medium	anomaly
negative medium	negative high	warning
negative medium	low	warning
negative medium	positive high	anomaly
negative medium	negative medium	normal
negative medium	positive medium	anomaly
low	negative high	anomaly
low	low	normal
low	positive high	anomaly
low	negative medium	warning
low	positive medium	warning
positive medium	negative high	anomaly
positive medium	low	warning
positive medium	positive high	warning
positive medium	negative medium	anomaly
positive medium	positive medium	normal
positive high	negative high	anomaly
positive high	low	anomaly
positive high	positive high	normal
positive high	negative medium	anomaly
positive high	positive medium	warning

Anomaly degree values of 0.8 or greater are set as alarm-triggering conditions for flight anomaly.

2. **Safe position envelope:**
   Tether length limits the operation volume of the kite. A kite must always be connected to the ground to have a safe operation. In the case of tether rapture, the kite can fly away and may cause catastrophic consequences 4. Position control to ensure that the kite is always in the operation zone is implemented to mitigate the risk of catastrophic events.

3. **Safe energy envelope:**
   If the kite is "out of control", the possible damage level is directly proportional to the kinetic energy of the kite. Therefore, the kite shall have an energy level below a predefined threshold to operate safely. If total kinetic energy exceeds the limit, immediate actions must be taken. The total kinetic energy of the kite is defined as the sum of translational and rotational contributions

$$E_\mathrm{k} = \frac{1}{2} m_\mathrm{k} v_\mathrm{k}^2 + \frac{1}{2} \boldsymbol{\omega}_\mathrm{k}^\top \cdot \mathbf{I}_\mathrm{k} \cdot \boldsymbol{\omega}_\mathrm{k}, \tag{5.2}$$

   where $\boldsymbol{\omega}_\mathrm{k}$ is the angular velocity of the kite and $\mathbf{I}_\mathrm{k}$ the constant inertia tensor.

5.4. RESULTS

Calibration and validation of the proposed anomaly detection system are done with accurate flight data. At the time of this work, the system is tested with five flight logs with

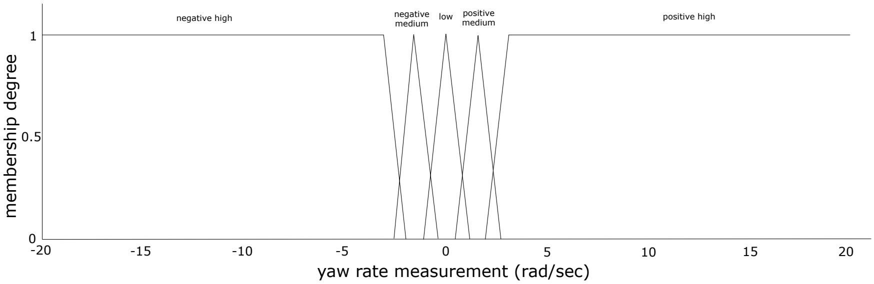


Figure 5.4: Membership functions for the fuzzification of yaw-rate measurement.

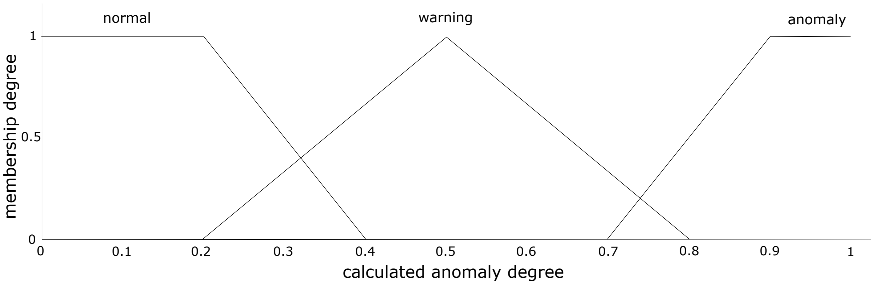


Figure 5.5: Membership functions for the defuzzification of anomaly degree output.

a total flight time of approximately 14 hours. The system is designed to work only in power generation mode. Since the mode of operation data was not recorded in the flight logs, only the data that the kite had an altitude of 100 m or above was considered valid. When the kite's altitude is below 100 m, it is considered either on the ground or in take-off/landing mode, so anomaly detection is not enabled.

Two of the five flight logs are selected from nominal flights. The other three test flight logs have stall events. Stall event cases are selected to verify the fuzzy logic engine developed for checking the kite controllability criteria. Meaningful results for two nominal flights and stall events are similar. Therefore, only one of the nominal flight cases and one of the non-nominal flight cases are presented.

5.4.1. RESULTS FOR THE NOMINAL FLIGHT CONDUCTED ON 2019.11.29:

KITE CONTROLLABILITY:

The anomaly detection system is fed with recorded original flight data. System-wide anomaly detection is never triggered for the given nominal flight test case. The output of the fuzzy engine exceeded the predefined threshold value(0.8) 12 times in the total of 3 hours and 17 minutes of flight time. However, these overshoots never lasted longer than 1 second. Consequently, values over the thresholds were considered false alarms and filtered out by the time trigger filter, set to one second. Table 5.3 shows eliminated false alarms with the highest anomaly scores. It is assessed that unexpectedly high anomaly scores were because of the latency between the steering input and its corresponding

Table 5.3: Highest anomaly scores in the nominal flight which are filtered out by time trigger filter. r

Simulation time stamp (ms)	**Steering input [-100,100]**	**Yaw rate (rad/sec)**	**Anomaly degree [0,1]**
4402.92	65.13	0	0.8943
4403.02	64.22	0	0.8943
4480.42	64.98	0	0.8943
4480.52	64.00	0	0.8943
3833.83	-65.82	5.1816e-07	0.8943
1331.37	-64.00	-1.9129e-05	0.8943
1331.47	64.00	-1.9129e-05	0.8943

Table 5.4: Maximum observed kinetic energy levels for nominal flight case.

	maximum observed value (kJ)
Transitional kinetic energy	46.18
Rotational kinetic energy	1.25

yaw-rate feedback.

The histogram of the fuzzy engine output values for the conducted nominal flight is shown in Figure 5.6.

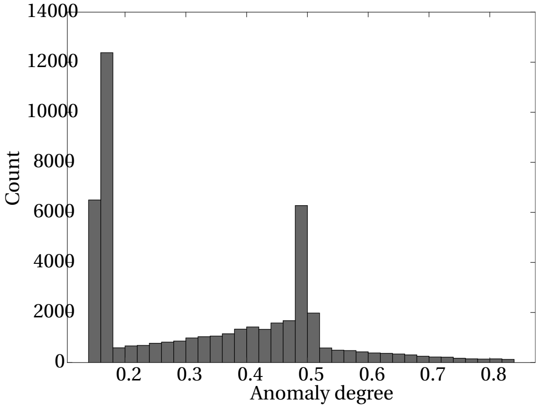


Figure 5.6: Anomaly degree level distribution for a nominal flight case.

ENERGY ENVELOPE:

The maximum allowed kinetic energy is set to 100 kJ considering the potential damage impact of an AWES for the worst-case scenario [40, 83] and the energy-based airworthiness categorization for civil unmanned aircraft systems proposed in [89].

Table 5.4 shows the observed maximum translational and rotational kinetic energy levels. Even in the worst case, the total energy level is still in the allowed range with a tolerance of 52 percent. It is also observed that even with a cautious inertia tensor assumption, rotational kinetic energy is negligible compared to translational kinetic energy in the nominal flight case.

POSITION ENVELOPE:

Considering only the data which kite has an altitude of 100 m or above, the calculated kite distance to the ground station varies between 362 and 201 m. Given that the maximum allowed distance was set to 495 m, considering 450 m of tether length and 10 percent measurement error tolerance, the kite was always in the "safe" operation zone. Thus, an anomaly alarm due to position envelope violation is never triggered.

5.4.2. RESULTS FOR NON-NOMINAL FLIGHT CONDUCTED ON 2019.09.03:

KITE CONTROLLABILITY:

According to the flight logs written by the test team, an unexpected flight anomaly occurred. Later investigations show that this was due to testing new power parameters in the control system. The operator reported that the kite was almost going to the front stall, but it managed to recover itself after causing an overshooting of the tether. Figure 5.7 shows the steering command input, corresponding yaw rate response, and simulated output of the kite controllability check during the anomaly. The control loss alarm was triggered three times, and all alarms lasted longer than 1 second. Thus, these three alarms pass the time trigger filter and generate system-wide anomaly alarms to take emergency actions. As seen in the graphic, the first alarm lasted about 5 seconds. Moreover, the second detection lasted about 7 seconds, and the final one lasted about 15 seconds s until the system recovered itself.

Nineteen s after the recovery, the kite goes to the front stall again, which triggers the existing safety release mechanism for a smooth kite landing. Figure 5.8 shows the data of the second stall case. As expected, the controllability anomaly detection system was triggered many times over one second, sufficient to enable system-wide anomaly actions.

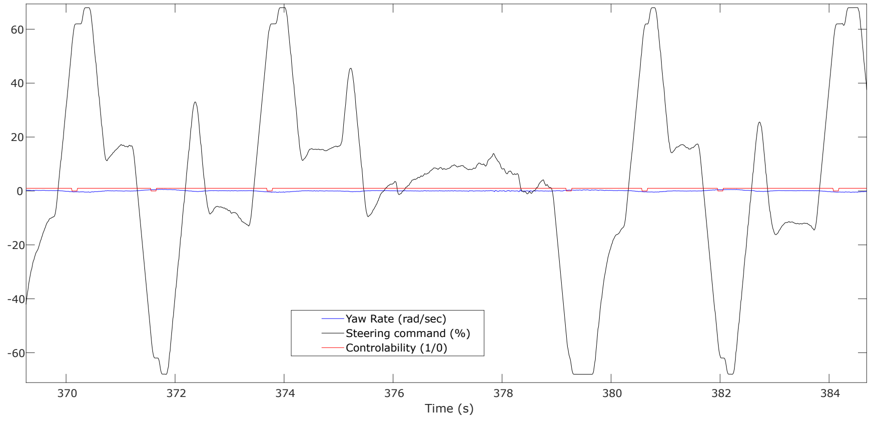


Figure 5.7: Steering input command (%), yaw-rate response (rad/sec), and simulated controllability anomaly result (1/0) during the first stall case.

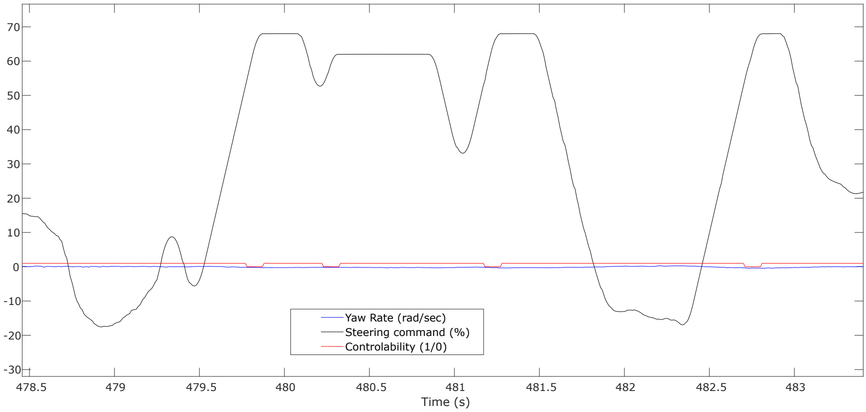


Figure 5.8: Steering input command (%), yaw-rate response (rad/sec), and simulated controllability anomaly result (1/0) during the second stall case.

ENERGY ENVELOPE:

Rotational and translational energy levels are shown in Figure 5.9. Since the total energy level is below the allowed kinetic energy threshold(100K Joule), an anomaly alarm is never triggered because of kinetic energy envelope violation.

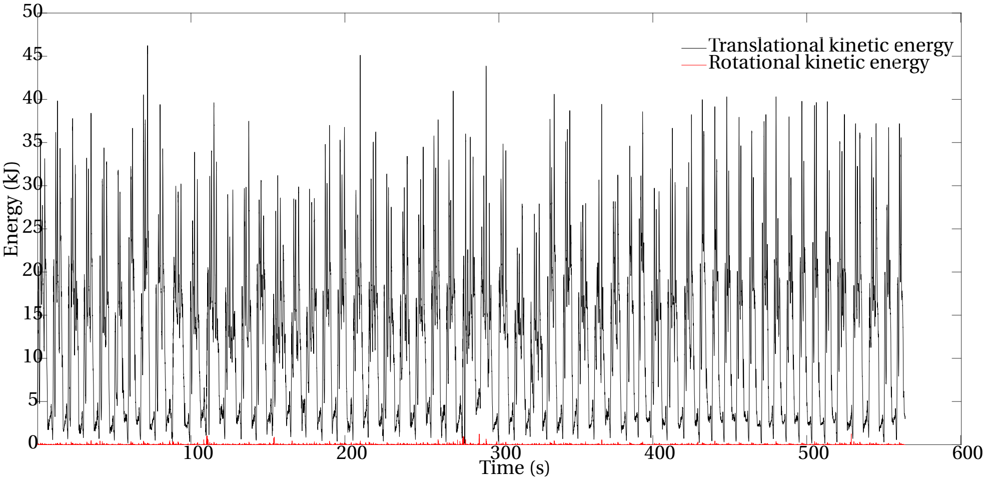


Figure 5.9: Rotational and translational kinetic energy levels for the non-nominal flight case.

POSITION ENVELOPE:

Kite distance to the ground station varies between 128 and 344 m. No anomaly alarm was triggered because of the violation of the position envelope.

5.5. CONCLUSIONS

AWE systems are operationally more complex than conventional wind turbines. Therefore, a systematic safety engineering approach is necessary to reach the required safety and reliability levels. In this chapter, we have presented a multi-layered fault detection, isolation, and recovery (FDIR) architecture that is specifically tailored to AWES. The first results of the flight anomaly detection layer of FDIR have been presented in this work. At the time of this work, the "flight anomaly detection" layer of the proposed architecture is tuned and tested with limited flight data with promising results. The data shows that the proposed system can detect critical flight anomalies without generating false alarms. However, the target is well-tuning the system with more flight data until the expected confidence level for the anomaly detection rates is reached.

6

REGULATORY PROCESS AND PERMITTING OF AIRBORNE WIND ENERGY SYSTEMS

6.1. ABSTRACT

Safety is a major factor in the permitting process for airborne wind energy systems. To successfully commercialize the technologies, safety, and reliability must be ensured by the design methodology and must meet accepted standards. Current prototypes operate with special temporary permits, usually issued by local aviation authorities and based on ad-hoc safety assessments. There is no standard view on regulation at the national or international levels. This chapter investigates the place of airborne wind energy systems in the airspace and possible aviation-related risks. Then, the required reliability level for commercial AWES has been discussed quantitatively. Then, the parties that may have a role in the airworthiness certification are investigated. Current and expected international airspace regulations are reviewed that can be used to find a starting point to evidence the safety of airborne wind energy systems. The chapter concludes with a recommended way forward for the certification of commercial AWES.

6.2. INTRODUCTION

The main system components are one or more flying devices, tethers, and the energy conversion system, which can be part of the flying device or a ground station. The flight control system can be either part of the flying device, a separate airborne device, or part of the ground station. Implemented prototypes are thoroughly classified in [5]. Although existing standards can be partially applied to some of the components, such as the low voltage directive (LVD) 2006/95/EC for electrical installation and machine directives 2006/42/EC or IEC 61400 for wind turbines, there are no standards for the

---

Parts of this chapter have been published in Ref. [40].

tether and the flying devices. This chapter investigates the applicability of existing rules and standards whose objective is to manage aviation-related risks. In essence, these standards define the acceptable risks to other airspace users, people, and property on the ground, often denominated as third-party risks. This chapter aims to provide an overview of the current situation of AWE applications from the aviation perspective and outline a permitting and certification approach for different AWE systems.

Ampyx Power was one of the early movers in this area and pursued the European Aviation Safety Agency (EASA) the certification of a utility-scale, grid-connected rigid glider. This chapter aims to position the experience of Ampyx Power in the broader context of commercial-scale AWE systems of any design. This study is restricted to systems whose operation requires permitting by aviation authorities and takes place near populated areas and critical infrastructure. In other words, this chapter considers only deployment scenarios which create an actual safety risk. It is assumed that the commercial operations for which a permit is sought initially occur over land restricted to qualified personnel. The focus is on the European regulatory framework and those AWE systems for which the current unmanned aerial vehicle (UAV) regulations seem most appropriate as a starting point. We merely provide the basic context for other cases.

The chapter is structured as follows. Section 6.3 describes the commonly used terms in the study, such as “regulation”, “certification” and “flying permit”. In Sect. 6.4, it is explored the perspective for a large-scale deployment of such prototypes, and for this, the place of the AWE applications in the airspace is studied. Possible interference between AWE systems and current aviation activities is described. In Section 6.5, the civil aviation authorities, which would most likely be important in the regulation-making process, are introduced. The Section 6.6 highlights three possible starting points to obtain operation permits for AWE prototypes. The first is unmanned aerial vehicle (UAV) registration, the second is air navigation obstacle registration, and the third is tethered gas balloon registration. Concerning UAV regulations, the current certification framework and future expectations are described, highlighting different views of aviation authorities on tethered aircraft. Concerning air traffic obstacle regulation, ICAO rules for air traffic obstacles that might apply to AWE applications are referenced. Lastly, yet importantly, we assess in Section 6.7 different permitting and certification paths for AWE systems in the light of current regulations and future projections.

6.3. CONCEPTS OF REGULATION, CERTIFICATION AND FLYING PERMIT

As a starting point, how regulation, certification, permitting, and standards related to each other are described in the European context. The relevant overarching European laws are the Regulation (EC) No. 216/2008 [90], which distributes the responsibilities between EASA and the national aviation authorities (NAA), defines the mechanism of certification and lists the high-level airworthiness requirements, as well as Commission Regulation (EU) No. 748/2012 [91], which implements Part 21, the globally agreed requirements for certification in aviation. The Certification Specification (CS) and Special Conditions (SC) are type-specific soft regulations for airworthiness (incl. safety through the respective articles 1309), and suitable starting points for tailoring. Certification is done concerning a certification basis agreed between the applicant and aviation authority: a selection and tailoring of the appropriate CS/SC and definition of an acceptable means of compliance, using e.g., ARP/ED standards.[1] A Permit to Fly is given by the NAA for small, experimental, or developmental systems. The necessary airworthiness and safety evidence shall be approved by a certification body or a qualified entity (this may be as part of a certification trajectory but does not have to be). The key question addressed here is: can the system be flown safely? The NAA, in addition, considers local constraints and operational safety.

6.4. AWE SYSTEMS IN THE AIRSPACE

Aviation authorities divide the airspace into segments. These segments are called classes and labeled with the letters A through G. Each class has its own rules. For example, in Class A, all operations must be conducted under instrument flight rules (IFR) and air traffic control (ATC) clearance is required for flights. Even though most countries adhere to ICAO standard rules for classes, individual nations can adapt the rules to their own needs. Current AWE system prototypes operate in Class G airspace, usually near the ground. Figure 6.1 shows the separation and Class G airspace. Class G is typically up to 1200 feet above ground level (AGL). However, Class G can be limited to 700 feet AGL if there is an airport close by, which requires Class B airspace in its vicinity, as shown in Fig. 6.1. Class G is known as uncontrolled air space. There are no specific aircraft equipment or pilot specifications to enter Class G. Moreover, no ATC communication is required to fly in Class G. Although Class G is uncontrolled, civil aviation rules remain valid. There are visibility and cloud clearance requirements for flights in Class G, and most flights operate under visual flight rules, meaning that separation is based on the "see and avoid" principle. Since class G airspace is open to all users; AWE systems and aircraft interference is possible.

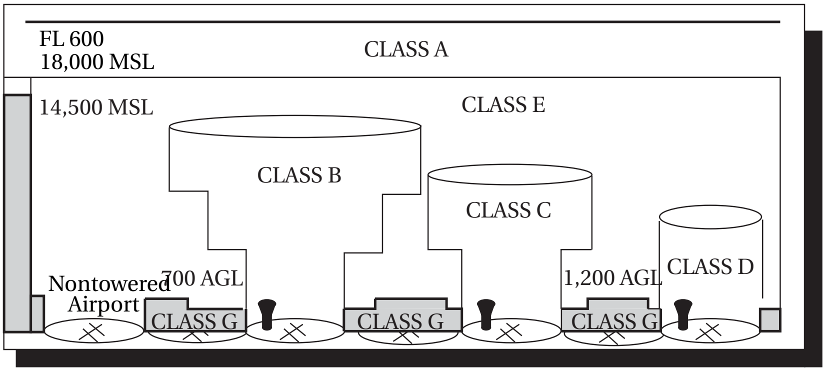


Figure 6.1: Airspace separation and Class G airspace by FAA. [92]

In addition to interference risk, there are other aviation-related risks posed by AWE systems. For example, uncontrolled crash (while the tether is attached or not) or uncon-

---

[1] The acronym ARP stands for Aerospace Recommended Practices and the acronym ED stands for EUROCAE (European Organisation for Civil Aviation Equipment) Document.

trolled departure from the designated flight area (with the tether partly attached or also detached) are the aviation risks that have to be managed.

6.5. RELEVANT AVIATION CERTIFICATION BODIES

This section discusses the regulatory bodies that provide safe aviation and civil airspace rules. There are national aviation organizations as well as international aviation organizations that strive to harmonize aviation rules in order to facilitate international air travel. These organizations all could have a role in the AWE-relevant rule-making process.

6.5.1. INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)

The ICAO was founded in 1944 upon the signing of the Convention on International Civil Aviation, commonly known as the Chicago Convention. Since 1947, the organization has worked with the Convention's 191 Member States and global aviation organizations as specialized United Nations (UN) agency. ICAO develops International Member states use standards and Recommended Practices (SARPs) as a framework for their aviation law-making processes.

6.5.2. FEDERAL AVIATION AUTHORITY (FAA)

The FAA is the civil aviation agency of the United States Department of Transportation. The agency makes Federal Aviation Regulations (FARs) and puts them into practice to ensure the safety of civil aviation within the United States. The FAA is authorized to certify a civil aircraft for international use.

6.5.3. EUROPEAN AVIATION SAFETY AGENCY (EASA)

The EASA was established in 2002 by the European Commission (EC) to ensure the safety of civil aviation operations. The agency advises the EC and European Union member states (EU) regarding new legislation. EASA, next to the FAA, is a second agency authorized to certify civil aircraft for international use.

6.5.4. NATIONAL AVIATION AUTHORITY (NAA)

The national regulatory body responsible for aviation is denoted as NAA or Civil Aviation Authority (CAA). These authorities make national legislation in compliance with ICAO SARPs.

6.5.5. JOINT AUTHORITIES FOR RULEMAKING ON UNMANNED SYSTEMS (JARUS)

The JARUS is a group that consists of experts from national aviation authorities or regional aviation safety organizations that aim to define the certification requirements for UAVs to integrate them safely to the current aviation system. JARUS defines its objective for UAVs as follows [93]:

> ...to provide guidance material aiming to facilitate each authority to write their own requirements and to avoid duplicate efforts.

Working groups in JARUS publish recommended certification specifications for interested parties such as ICAO, EASA, and NAAs.

6.5.6. AIRBORNE WIND EUROPE

Airborne Wind Europe is the association of the European airborne wind energy industry. It aims to represent the interests of the airborne wind energy industry and academia to decision-makers in politics and business, to provide reliable and high-quality information and data on airborne wind energy. It coordinates the industry at all levels. It consists of different working groups. Relevant to this chapter, the working group “AWE Safety and Technical Guidelines” aims to define ways to conduct the permitting process in cooperation with airspace authorities efficiently. "AWE Safety and Technical Guidelines" working group recently published agreed Key Safety Principles for operation [50]. Working group works also on defining Concept of Operations (CONOPS) [51] according to the "Specific Operations Risk Assessment" (SORA) Guidelines by JARUS [94]. This work can be considered a starting point for Chapter 7 in this thesis.

6.6. REGULATIONS FOR AIRBORNE WIND ENERGY SYSTEMS

At the time of this study, there is no directly applicable regulation for AWE technologies. However, regulations for UAVs, air traffic obstacles, or unmanned balloons are available as a starting point for tailoring to the specifics of a selected AWE architecture. This section summarizes current regulations for unmanned aerial vehicles from different regulatory bodies, air traffic obstacle regulations, and tethered gas balloon regulations. Similar-looking AWE systems can be categorized differently depending on the modes of operation, the inherent safety measures, and the proper starting point should be selected accordingly, together with the responsible aviation authority. Note that our focus is mainly on the developing UAV regulation since we expect that most tethered aircraft that will have the ability to (aerodynamically) leave their restricted safe area as a result of a single tether failure will be considered unmanned aircraft. Hence, for those systems, the UAV regulation seems the most appropriate starting point.

6.6.1. REGULATIONS FOR THE UNMANNED AERIAL VEHICLE CATEGORY

Unmanned aerial vehicles were first used in the military sector. The technology then evolved also for civil applications, and nowadays, there are already many commercial products on the market, such as UAVs for high-quality aerial photography or 3D mapping. However, the increasing interest in UAVs has also led to a rise in safety concerns. Consequently, national aviation agencies and international organizations have directed their attention to developing certification processes, regulations, and standards for UAVs, including those related to airworthiness. One of the main challenging factors for UAV regulation is the wide variety of systems in the UAV domain. For instance, the UAV concept includes devices from micro UAVs, which are extremely lightweight (e.g., 16 grams [95]) to High Altitude Long Endurance (HALE) class UAVs up to 14 tons [96]. Consequently, there is no consensus on a classification method which is able to cover this broad range yet. Several different classification approaches have been proposed for UAVs, such as classification according to aircraft weight, avionics complexity level, aircraft configuration (number and type of engines, etc.), aircraft speed, operation purpose (e.g., aerial work), operation airspace (segregated, non-segregated), overflown area, kinetic energy, operational failure consequence, and operation altitude.

The first publicly accepted standardization agreement, the STANAG 4671 [97] compiled by the North Atlantic Treaty Organization (NATO), was a significant step forward in UAV registration, even though it is limited to military UAVs. The standard is based on EASA's CS-23 [98] civil airworthiness code. In addition to CS-23, STANAG 4671 includes subparts specific to UAVs, such as ground control stations and datalink. The standard provides a broad range of requirements for flight, aircraft structure, design, construction, power plant, equipment, command and control, and the control station. However, the standard only addresses fixed-wing UAVs weighing 150 and 20,000 kg. As a result, a considerable number of UAV types are not covered by the standard, among which the designs that are not structurally similar to conventional aircraft. With the following STANAG 4703 [99], the NATO Standardization Agency (NSA) defined the airworthiness requirements also for lighter military UAVs whose take-off weight does not exceed 150 kg.

As of 2022, required rules for integrating UAVs in civil airspace are still subject to change, and different certification proposals from different certification authorities exist. In addition, it is known that a limited number of UAV applications are certified for civil operations by FAA and EASA with a case-by-case risk evaluation and only for specific operations. Depending on the definition of UAV in the upcoming regulations by different aviation authorities, some of the AWE applications may fall into the UAV category. In the following, the possibilities in the light of current regulations, known regulatory views, and the published regulatory proposals will be explored.

For AWE applications falling in the UAV category, an airworthiness certificate would be sought for commercial operation. Currently, two types of airworthiness certificates are typical for manned aviation namely standard airworthiness certificate and restricted airworthiness certificate. In contrast to the standard airworthiness certificate, the restricted airworthiness certificate has operational limitations, such as restrictions on maneuvers, speed, activities undertaken, or where the flights may be conducted. According to the first drafts of the UAV certification method proposals, a similar type scheme (standard and restricted airworthiness) will be used for UAVs. Considering that current AWE applications have particular characteristics, such as being tethered to a ground station or operating in a specific area, it can be expected that the restricted type-certificate will apply.

ICAO REGULATIONS FOR UNMANNED AERIAL VEHICLES

On 7 March 2012, ICAO adopted Amendment 6 to the International Standards and Recommended Practices, Aircraft Nationality, and Registration Marks are identical to Annex 7 to the Convention on International Civil Aviation (also known as the Chicago Convention). This revision included UAVs as remotely piloted aircraft (RPA), defining an RPA as “an unmanned aircraft which is piloted from a remote pilot station” [100]. At the same time, Amendment 43 to Annex 2 “Rules of the Air” to the Chicago Convention was adopted. This amendment stipulates that an RPA shall be operated in such a manner as to minimize hazards to persons, property, or other aircraft. Amendment 43 is the first regulation by ICAO that introduces the operation of remotely piloted aircraft systems (RPAS) in the Chicago Convention.

The current regulation [101] requires certification of all types of aircraft that intend to fly in controlled and uncontrolled airspace, even though the certification framework for UAVs is not clear in Chicago Convention yet. In March 2011, ICAO published Circular 328 specifically addresses "Unmanned Aircraft Systems (UAS)." [102]. This circular aims to establish a basis by properly defining the new technology clarifying the differences between unmanned and manned aircraft. In March 2015, Circular 328 was superseded by the "Manual on Remotely Piloted Aircraft Systems (Doc 10019)" [103]. The following excerpts from this document are deemed representative of ICAO's current perspective on UAVs [103, Chap. 1, Sect. 6]

> 1.6.3 These hazards relate to all RPAS operations irrespective of the purpose of the operation. Therefore, unless specified otherwise, the recommendations in this manual apply equally to commercial air transport and general aviation, including aerial work operations conducted by RPAS.
> 1.6.4 In order for RPAS to be widely accepted, they will have to be integrated into the existing aviation system without negatively affecting manned aviation (e.g., safety or capacity reduction). If this cannot be achieved (e.g., due to intrinsic limitations of RPAS design), the RPA may be accommodated by being restricted to specific conditions or areas (e.g., visual line-of-sight (VLOS), segregated airspace or away from heavily populated areas).

and further [103, Chap. 2, Sect. 2]

> 2.2.7 Categorization of RPA may be useful for a proportionate application of safety risk management, certification, operational, and licensing requirements. RPA may be categorized according to maximum take-off mass (MTOM), kinetic energy, various performance criteria, type/area of operations, and capabilities. Work is underway in many forums to develop a categorization scheme.

Autonomous unmanned aircraft and their operations, including unmanned free balloons or other types of aircraft which cannot be managed on a real-time basis during flight is not in the scope of Doc 10019. At the time of writing, there are no rules for AWE applications or tethered aircraft in the ICAO regulations.

EASA REGULATIONS FOR UNMANNED AERIAL VEHICLES

EC-2008 is the European Union's law that converts the ICAO SARPs to the EU structure, describing the responsibilities of EASA and NAAs [90]. Annex II of EC-2008 defines the exceptional cases which are outside EASA's area of responsibility. For example, the following cases do not lie within the responsibility of EASA[2]:

> (b) aircraft, specifically **designed or modified for research**, experimental or **scientific purposes**, and likely **to be produced in very limited numbers**...
> ...(I) unmanned aircraft with an operational mass of **no more than 150 kg**

---

[2] In this and the following quotations, the emphasis is added by the authors

NAAs of member states are responsible for the regulation of these cases. Apart from the exception mentioned above cases, EASA makes common European rules for UAV certification.

One of the important steps in civil UAV airworthiness certification is the interim Policy Statement EASA E.Y013-01 [104], which is still in use and aims at protecting people and property on the ground but not the UAV itself. The policy provides a kinetic energy-based classification method and a systematic certification guideline that suggests tailoring fixed manned aircraft certification regulations. According to the tailoring principle, class determination has to be done as a first step using the kinetic energy evaluation method defined in the regulation. Then, a tailoring process is required, adjusting an existing certification specification for a conventional aircraft in the same kinetic energy class as the new type intended to be certified. During this process, each requirement of the existing certification specification has to be reviewed, and its applicability to the new type has to be evaluated. Depending on the new type, special conditions may be added. These conditions may provide a starting point for future applicants. It is further stated in the policy [104, Paragraph 21A.17]

> At an applicant's request, the Agency may accept USAR version 3, STANAG 4671, or later updates, as the reference airworthiness code used in setting the type certification basis

It should be noted that Ampyx Power and EASA have concluded that the tethered aircraft of Ampyx Power resembles more an unmanned glider than the typical tactical UAV that STANAG 4671 is templating. Therefore, the company has chosen to tailor CS-22 for its airworthiness baseline. These examples show EASA's willingness to accept the most suitable pre-existing airworthiness certification standard as a starting point for the tailoring process. The EASA E.Y013-01 has been amended regarding system safety to cover the class of very light aircraft (VLA) by Special Condition SC-RPAS.1309 [105], leaning on CS23.1309 [98]. Ampyx Power also adopted this amendment as a starting point for the system safety.

The EASA E.Y013-01 guides restricted-type certificates and standard type certificates for UAVs. However, it does not regulate public operations such as UAVs used by the military, police, or firefighting departments. Regarding mass criteria, EASA advises the NAAs of member states to develop their regulations for UAVs lighter than 150 kg. Due to this rule, current laws for light UAVs in European countries are not harmonized, and some countries do not yet have regulations.

EASA publishes the drafts of amendments to ICAO regulations as Notice of Proposed Amendment (NPA) to collect member states' comments. In September 2014, the agency published the NPA-2014-09 with the first mention of operations of tethered aircraft [106]. In this notice, EASA identifies the tethering of the aircraft as a recognized mode of operation for remotely piloted aircraft

> **TAXONOMY OF OPERATIONS**
>
> RPA typical flight pattern may comprise a wide range of scenarios, which could be categorized into the following types of operations:

> (a) Very low level (VLL) operations below the minimum heights prescribed for normal IFR or VFR operations: for instance, below 500 ft (≈ 150 m) above ground level (AGL); they comprise:
>
> (1) **operations of tethered aircraft**;
>
> (2) Visual line of sight (VLOS) within a range from the remote pilot in which the remote pilot maintains a direct, unaided visual contract with the RPA and which is not greater than 500 m;
>
> (3) Extended visual line of sight (E-VLOS) where the remote pilot is supported by one or more observers and in which the remote crew maintains a direct, unaided visual contract with the RPA;
>
> (4) Beyond VLOS (B-VLOS), where neither the remote pilot nor the observer maintain a direct, unaided visual contract with the RPA.
>
> (b) **Operations of tethered aircraft**, above the minimum height in (a); ...

This statement can bring rigid-wing AWE systems under Amendment 43 to Annex II of the Chicago Convention. Annex II covers other aspects related to RPAS besides their integration in airspace, namely the principles that RPAS shall be airworthy, the remote pilots licensed, and the RPAS operator certified. However, specific ICAO standards and recommended practices—the SARPs—for the airworthiness and operation of RPAS, as well as for licensing of the remote pilot, have not been developed yet.

In addition to the EASA E.Y013-01 and NPA 2014-09, EASA has published a "Concept of Operations for Drones" [105]. This new proposal starts from the application rather than the aircraft used, applying a risk-based classification and regulation scheme for UAV operation. With this new scheme, EASA aims to cover a broad range of types and operations of UAVs, applying the three categories "Open", "Specific" and "Certified". Operations in the "Open" category would not require any certification as long as they operate within a defined boundary, for example, not close to aerodromes, not in populated areas, and being very small. The boundary conditions are not defined in the proposal. However, it is mentioned that conditions for the "Open" category are expected to be clarified in collaboration with member states and the industry. The "Specific" category is for UAVs whose conditions will not fit the "Open" category. These will require a risk assessment process specific to the planned operations. Depending on the risk assessment process output, they might be certified case by case with specific limitations adapted to the operations. Permitting for the "Specific" category would be delegated to the NAAs. If the risk assessment shows that the UAV introduces a very high risk, then the "Certified" category would be applicable. This requires multiple certificates similar to those for the manned aviation system, such as pilot license approvals for design and manufacturer organizations. In addition to the certificates which are currently in use for manned aviation industry, the "Specific" category may also require new additional certifications that are specific to UAV operations, such as command and control link certification.

The operation-specific, case-by-case safety assessment method for the "specific" category provides a mechanism to cover unconventional machines flying in civil airspace. If these machines have sufficient risk mitigation factors, such as being connected to the ground or being operated away from populated areas, an operation-specific a certificate could be sought. Current AWE applications would fall most likely into the "Specific" category, whereas utility-scale commercial systems would fall into the "Certified" category.

FAA REGULATIONS FOR UNMANNED AERIAL VEHICLES

The Title 14 of the Code of Federal Regulation [107] regulates the aeronautics and space operations conducted within the boundaries of the USA. According to the current version [107, Part 91, Sect. 2031]

> ...every civil aircraft that operates in the US must have a valid airworthiness certificate.

Currently, unmanned aircraft systems can be certified by the FAA to operate in the national airspace (NAS) with a special airworthiness certificate in the experimental category [107, Part 21, Sect. 191]. However, the FAA regards the aircraft as a part of a system, which includes command and control links, ground control systems, and ground crew, and accordingly, the entire system has to be certified. Nevertheless, the subsystems that do not exist in conventional aircraft, such as command and control links, ground control systems, or sense and avoid systems, do not have any regulations yet. As a result, the general use of commercial UAVs for civil use is currently highly restricted in US airspace.

Title 14 of the Code of Federal Regulation (14 CFR) classifies the operation purpose of UAVs at a very high level [108]. In this classification, the first category is “Civil use”, which refers to operation by a company or individual. The second category is “Public use” includes the operations for scientific research and governmental purposes such as military operations. The last category is the recreational use of model aircraft, which the FAA Advisory covers Circular 91-57 [109]. Currently, UAVs used for public operations require a Certificate of Waiver or Authorization (COA) from the FAA that permits public agencies and organizations to operate in a particular airspace. There are many COAs in use today by several organizations, such as the Departments of Agriculture (USDA), Commerce (DOC), Defense (DOD), Energy (DOE), Homeland Security (DHS), Interior (DOI), Justice (DOJ) as well as NASA, State Universities, and lastly State/Local Law Enforcement [110]. UAVs in the “Civil use” category can only operate with a special airworthiness certificate in the experimental category with limits on the operation to not create any risk for other airspace users or for people on the ground [107].

In February 2012, the United States Congress enacted the Federal Aviation Administration Reauthorization Legislation, which seeks to provide a framework for integrating UAVs safely into American airspace [111]. Following this action, the Next Generation Air Transportation System (NextGen) partner agencies, which are the Department of Transportation (DOT), DOD, DOC, and DHS, as well as NASA and FAA, started to work together to develop the Unmanned Aircraft Systems (UAS) Comprehensive Plan [112]. This report defines the interagency goals, objectives, and approach to integrating UAS into the national airspace. Following the release of this report, the FAA published a UAS roadmap [113], which includes a timeline for tasks required for integration of UAVs into the current aviation system. By this roadmap, FAA, together with NexGen agencies, established test sites for UAV research and development and study new UAV-specific technologies, such as detect-and-avoid systems.

While the FAA works on new regulations, the interim policy “Special Rules for Certain Unmanned Aircraft Systems” [111] has been enacted in 2012. Briefly, the Section 333 law authorizes the Secretary of Transportation to permit civil operations of UAVs after an evaluation.

Regarding AWE applications, there is a discrepancy between EASA and FAA. On the one hand, EASA recognizes the tethered aircraft as unmanned aircraft; on the other hand, FAA clearly excludes the tethered aircraft from the unmanned aircraft category [114, Appendix A];

> **41. Unmanned Aircraft (UA).** A device used or intended to be used for flight in the air that has no onboard pilot. This device excludes missiles, weapons, or exploding warheads but includes all classes of aircraft, helicopters, airships, and powered-lift aircraft without an onboard pilot. UA do not include traditional balloons (see 14 CFR part 101), rockets, tethered aircraft, and un-powered gliders

In December 2011, the FAA issued a “Notification for Airborne Wind Energy Systems” [38], according to which each deployment of an AWE system needs to be assessed on a case-by-case basis, accounting for the surrounding aviation environment to ensure aviation safety. Makani Power submitted a detailed response to this notification in February 2012 [37].

In December 2022, the FAA published a new statement that states that the FAA is finalizing its policy on the applicability of regulations concerning the safe, efficient use, and preservation of the navigable airspace to all airborne wind energy systems (AWES) [115].

In 2022, FAA issued the AWES "Policy Statement" following the "Notification" call in 2011.

6.6.2. REGULATIONS FOR AIR TRAFFIC OBSTACLE CATEGORY

Air navigation obstacles can impede civil air traffic. Some AWE companies registered their current AWE prototypes as air navigation obstacles. Such a registration aims to inform the aviation system to prevent incidents. For example, masts and wind turbines must be registered as air traffic obstacles. This information is visualized in aviation charts and is considered during flight route planning or emergencies. If we consider the typical operation altitudes of AWE systems, obstacle registration might be sought in the future. ICAO defines “obstacle” in the Chicago Convention, Annex 4 [116] as follows

> All fixed (whether temporary or permanent) and mobile objects, or parts thereof, that:
>
> a) are located on an area intended for the surface movement of aircraft; or
>
> b) extend above a defined surface intended to protect aircraft in flight; or
>
> c) stand outside those defined surfaces and that have been assessed as being a hazard to air navigation.

According to this definition, air traffic obstacles can be mobile as many AWE systems are.

The Chicago Convention, Annex 14 [117] is about aerodromes and includes the definition of the surrounding zones. Obstacle limitation surfaces are zones that must be free of obstacles to permit regular civil use of the airspace. However, many AWE applications will potentially operate outside of these zones, about which the ICAO recommends to the civil aviation authorities the following in Annex 14 [117]

> 4.3 Objects outside the obstacle limitation surfaces
>
> 4.3.1 Recommendation.— Arrangements should be made to enable the appropriate authority to be consulted concerning the proposed construction beyond the limits of the obstacle limitation surfaces that extend above a height established by that authority in order to permit an aeronautical study of the effect of such construction on the operation of aeroplanes.
>
> 4.3.2 Recommendation.— In areas beyond the limits of the obstacle limitation surfaces, at least those objects which extend to **a height of 150 m or more above ground elevation** should be regarded as obstacles unless a special aeronautical study indicates that they do not constitute a hazard to airplanes.

According to Annex 14, obstacles have to be conspicuous to air vehicles. Chapter. 6 on “Visual aids for denoting obstacles” describes the required marking and lighting scheme for different obstacles. Regarding marking methods for increasing visibility, the following is recommended

> 6.1.2.2 Recommendation –Other objects outside the obstacle limitation surfaces should be marked and/or lighted if an aeronautical study indicates that the object could constitute a hazard to aircraft (this includes objects adjacent to visual routes e.g. waterway, highway).

Similarly, Article 6.2.2 defines marking requirements for mobile objects, and Article 6.2.3 defines lighting requirements for objects with a height exceeding 150 m above ground. Article 6.2.4 addresses wind turbines separately, which is crucial because it defines the required marking for a wind farm setup. A similar or hybrid approach might be sought for future AWE farms.

6.6.3. REGULATIONS FOR TETHERED GAS BALLOONS CATEGORY

For static AWE systems that resemble the system developed by Altaeros Energies [118] a more applicable basis is the EASA certification specification for tethered gas balloons, CS-31TGB [119]. The lack of a complex control system which is required for the crosswind AWE systems, in conjunction with the self-stabilizing nature of a tethered lighter-than-air gas balloon will probably be sufficient to make CS-31TGB applicable.

We note here that the certification specification provides two more essential inputs for the generic safety requirements and certification basis of AWE systems:

1. CS 31TGB.25 where the required tether safety factor of 3.5 is given.

2. AMC 31TGB.53(a) where it is stated that acceptable means of compliance to CS 31TGB.25(a) can be shown by a certificate of compliance to the Machinery Directive 2006/42/EC [120]. This means that a winch system can be certified to the Machinery Directive 2006/42/EC , thereby showing compliance with an airspace certification specification. For AWE systems that use a winch as part of the ground station, limiting the certification efforts for non-flying parts can be important.

6.7. DISCUSSION

Since no unified legal framework for AWE systems exists to the present day, the categories mentioned above are just starting points for a discussion with the authorities. They are references from which deviations can be defined systematically on a case-by-case basis. Nevertheless, some generally valid considerations can be derived.

AWE systems introduce potential hazards for other airspace users and people or critical infrastructure on the ground. These inherent risks have to be mitigated to commercialize AWE technologies successfully. It should be noted that this risk mitigation is not only sensible for saving lives but also, from a commercial perspective, to reduce the costs resulting from accidents and crashes. It may well be a property of AWE that the commercial requirement for reliability is even more stringent than that coming from aviation regulations.[3]

If we define “normal operation” of the AWE system as the expected continuous operation within a limited airspace, with limited altitude and horizontal boundaries, we have to account for potential situations in which the AWE system interacts with the current civil aviation system. To prevent such undesirable interactions, regardless of the type of AWE system, some form of airspace segregation has to be arranged.

Furthermore, independent of the selected regulatory starting point, as UAV, obstacle or otherwise, and independent of the degree of permitting or certification sought, it will be fundamental that any risk of one or multiple fatalities as a result of a single functional failure is mitigated. The aviation approach to safe systems design is based on the presumption that

- any single function can fail, so it must be assumed that the tether can rupture,

---

[3] Consider, as an example, a fully autonomous utility-scale system that has a design lifetime of 20 years Moreover, it is in operation 5000 hours per year. Suppose that the airborne element replacement cost represents 10% of the levelized cost of energy (LCOE). As a a complex system, the airborne element may have 100 failure conditions that would lead to the loss of the aircraft (“hazardous”). If any of those failure conditions occur during the design lifetime, the energy cost would be driven up by 10%, say 0.5 euro cent per kWh, which is more than significant and will negatively affect the commercial viability. It is commonly argued that the probability of a failure condition that might lead to the death of someone from the general public (“catastrophic failure”) must be at least ten times less than a hazardous failure, leading to a required probability level per catastrophic failure condition of 10^{-8} per flight hour (pfh), which is once every $5000 \times 20 \times 100 \times 10$ flight hours. This number is two orders of magnitude more stringent than the 10^{-6} pfh requirement of Special Condition SC-RPAS.1309 [105] regarding UAVs or Certification Specification CS-23.1309 [98, Paragraph 23.1309] regarding general aviation.

To make the argument more vivid, one can also turn it around. For general aviation, a catastrophic incident is accepted every 10,000 flight hours. Yet, this number of flight hours is reached every other year by a single utility-scale AWE system and every week for a park of 100 systems. This is clearly something the general public would not accept. Note that utility-scale AWE cannot be installed too far away from the population since they are supposed to provide the population with electricity, and the long-distance cabling cost is forbiddingly expensive, so part of the solution has to come from additional design for safety. Still, even with the 10^{-8} pfh reliability level calculated above, in a park of 100 systems, nearly every two months, an aircraft would be expected to crash within the park, which hardly seems economically viable. So, a further reduction of the number of hazardous failure conditions and/or a further improvement in reliability and, accordingly, in design rigor, may be recommendable for this example.

What sets utility-scale AWE systems apart from general aviation aircraft and typical RPAS is the number of flight hours and the complexity, which determines the number of failure conditions. The challenge is that AWE systems are, in this regard, more in the direction of commercial airliners, albeit not quite as critical or complex, and an intermediate reliability approach and design rigor are to be pursued.

- any single failure with potential catastrophic consequence shall be demonstrably mitigated.[4]

Thus, assuming that the commercial AWE system is operated near a populated area—the consumer of the generated electricity—the risk of uncontrolled flight outside of the designated safe zone shall be mitigated in case of tether rupture or intentional release of the aircraft. Having a controlled flight following a mechanical disconnection is one possible option to mitigate such an event. Having a second, structurally independent tether is another option. Or one could otherwise, demonstrate that the detached kite is not able to reach people or critical infrastructure on the ground.

It should be noted that if one aims to operate a kite with significant kinetic energy directly above people, the tether solution alone cannot act as sufficient mitigation, for example, in case of a faulty flight controller that would lead to a crash in a populated area. It shall then be shown that there are independent means of overcoming a single failure of any flight control function.

Factors that will affect the authorities' assessment of the overall risk posed by the system furthermore includes the kinetic energy, the availability of onboard propulsion, which determines the flight range, and the complexity, including autonomy, with which AWE aims to enter new territory.

The above review is interpreted so that single-tether AWE systems that can still (aerodynamically) reach populated areas after tether failure or release are likely to be considered UAVs. Therefore, the certification approach for UAVs seems to be a suitable starting point, and the level of certification will depend on the risk factor that the system presents [105]. A different approach, such as obstacle registration, may arguably be followed, for example, for kites steered from the ground above a restricted area using two structurally independent tethers.

In any case, certification of design and operation to some defined standard will be necessary for commercial deployment. Apart from the expected positive impact of the introduction of rigorous processes on system reliability and maintenance, design certification enables the concept of similarity as evidence for quality and safety. This is a proven way to cost-effectively deploy the large numbers of complex systems the AWE industry aspires to. This means that production and maintenance aspects shall be standardized. Such certifications are outside the scope of this study. It should be noted that

---

[4] The certification requirement for catastrophic failure probability applies to the accidental death of someone from the general public during commercial operation. This is not to be confused with examples that may come to mind, such as the unfortunate recent SpaceShipTwo incident [121] that illustrate the higher level of acceptance for accidents during development affecting flight crew only. Secondly, the Certification Specification CS-23.1309 [98, Paragraph 23.1309] for mitigation of catastrophic failures applies to the functions of aviation systems, such as avionics, complex mechanisms, not to structures. For structures, it is recognized that redundancy could make the aircraft too heavy. The accepted approach here is to include the proper design safety factor and design for damage tolerance, for example, due to fatigue following barely visible tooling damage, hail, bird strike.

We argue that the tether is more than a structural element but a functional part of a complex mechanism. It is used to control and restrict the dynamics of the airborne element and is subject to wear during reeling; its integrity is affected by weather, salt spray, dirt, and lightning, and it is subject to complex loading dynamics, such as jerks, shocks, etc. At the same time, the tether is designed for minimal drag, so the design safety factor may be limited. Hence, we must assume its incidental failure as part of a safety analysis.

only aviation-related risks and the regulation aspects of the AWE systems are considered from an aviation perspective.

AWE systems are complex systems that consist of many components. There are additional regulations requirements, such as electric machinery regulations, grid connection regulations, noise emission regulations, environmental regulations and lighting regulations for the subcomponents which should be taken into consideration. It is noted here that those system elements and operations certified by an aviation authority are generally not required to comply with machine standards, but these Standards may support guidance for the design or verification.

6.8. CONCLUSIONS

AWE systems must be regulated for a successful commercial introduction and broad public acceptance. Ultimately, AWE systems are expected to be larger and heavier than current prototypes. They are expected to operate in Class G airspace where interaction with other users is possible. In addition, AWE systems introduce risks to the people on the ground. Therefore, it is expected that commercial AWE systems will have to comply with international airspace regulations.

The regulation framework for AWE systems is not yet mature. Current prototypes operate with special permits. Local aviation authorities issue these operation permits, and there is little commonality among the permits. Registration of the prototype as an air traffic obstacle or unmanned aerial vehicle (UAV) is the primary approach followed by AWE companies and academic research groups. Classifying the AWE systems as UAVs is a controversial topic: on the one hand, the current EASA view recognizes the tethered unmanned aircraft as UAV; on the other hand, the FAA excludes the tethered aircraft from the UAV category.

Each AWE system category has its operation characteristics. The path for flight permitting and product certification goes through hazard analysis and mitigation independently from the category into which the system falls.

A regulation set that is specific to AWE systems will be built up over time, based on the specifically negotiated cases of first movers. As long as such a regulation is not in place, the most appropriate existing certification specifications and standards will have to be selected with authorities and tailored as necessary. Certification is not an unnecessary burden but provides both a prudent and a necessary approach to large-scale commercial deployment near populated areas.

Lastly, yet importantly, AWE developers should accept the shared responsibility to avoid any incidents involving other airspace users, people on the ground or critical infrastructure. Such an incident, if no proper prevention or mitigation approach was in place, could well put the entire AWE industry under the most stringent aviation rules, which would jeopardize its commercial viability and eventual success.

7

OPERATION APPROVAL FOR COMMERCIAL AWES

7.1. ABSTRACT

Integrating the operation of airborne wind energy systems safely into the airspace requires a systematic qualification process. The EASA will likely approve commercial systems as unmanned aircraft systems within the “specific” category, requiring risk-based operational authorization. In this chapter, the risk assessment methodology is interpreted for airborne wind energy systems, going through the recommended procedure’s ten steps and discussing the particularities of tethered energy-harvesting systems. Although the described process applies to the entire field of airborne wind energy, it is detailed for a commercial flexible-wing airborne wind energy system. Analysis shows that, with the proposed air and ground risk mitigations, the level of confidence that the AWES operation will stay under control is increased by a factor of two. The framework is expected to increase the safety level of commercial airborne wind energy systems and ultimately lead to commercial operation approval.

7.2. INTRODUCTION

Airborne wind energy systems (AWES) employ kites or tethered aircraft to harvest wind energy at heights beyond the reach of conventional wind turbines. The access to this so-far unused wind resource, the substantially decreased material use, and the increased capacity factor render the technology a potentially important candidate for a future low-carbon energy economy [123, 124].

On the other hand, the development faces technical and non-technical challenges. The mechanical connection to the ground couples the flight speed with the wind speed and the tether reeling speed. For AWES operated in crosswind mode, this coupling is particularly strong. Without responsive feedback control, wind gusts can rapidly accelerate

---

Parts of this chapter have been published in Ref. [122].

the flying devices, increasing the aerodynamic loading and potentially causing a rupture of the tether or other irreversible damage. In the worst case, such events can result in a loss of the main component of the AWES or harm to people [125]. Most implemented AWES are based on aerodynamic lift, so the flight operation can not be terminated immediately to react to unexpected situations. It depends on the specific AWE technology exactly how critical an operational anomaly is [56]. Inflatable kites fly slower and can usually be relaunched after emergency or crash landings. Heavier fixed-wing kites fly faster, and a crash landing typically amounts to a loss of the kite. Another essential aspect next to the availability and maintenance cost is the safety of persons, properties, and critical infrastructures on the ground and other airspace users [55].

As AWES operate at higher altitudes than conventional wind turbines and their operations are not stationary, the interaction with the aviation system is potentially more intricate. AWES introduces risks to third parties in the air, which need to be considered in addition to the risks introduced by wind turbines, such as lightning or fire within the equipment.

Despite the various conceptual differences, the consensus in the industry is that safe and robust operation with a sufficient degree of autonomy is an important prerequisite for a successful market introduction of AWES and acceptance by the public [18, 55]. This target has not yet been achieved as none of the commercial prototypes has been operated continuously for over a few days. AWES must fly autonomously, safely, and reliably to become economically viable.

Even though AWES has no directly applicable functional and safety standards, relevant experience from other domains can provide additional insights into AWE and help reach the required level of robustness and safety. However, a traditional consensus-based standard approach is complex when the technology is not yet mature. To be viable, any standard will need unprecedented flexibility [126]. AWE sector can benefit from the experience of aviation, conventional wind turbine, satellite, and autonomous car industries. Similar to conventional wind turbines, commercial AWES must operate fully automated, day and night; they must be tolerant to unfavorable weather conditions. Marking regulations for wind turbines can be the starting point for the visibility marking of AWES [40].

Most LEO satellites do not have a permanent data connection with the ground. They transmit data (telemetry) and accept commands (telecommand) only during their passes over the ground stations. Their limited connectivity requires sufficient autonomy to conduct their nominal operations without ground intervention. In addition to the nominal operations, satellites have the autonomy to cope with faults in their subsystems. During the faults that the satellite cannot fix, the autonomous system keeps the satellite safe until the ground operator takes corrective actions. Even though the working environment and the disturbances for a spacecraft are different from AWES, a similar level of operational autonomy and fault detection, isolation, and recovery (FDIR) is required for the robust operation of commercial AWES. Space companies have their proprietary flight frameworks [127], and there has yet to be an agreed approach for the autonomy of satellites.

Recently, NASA released their flight software framework cFS (core flight system) to the public [128]. This framework is used in many NASA missions and will be the baseline of the Lunar Gateway project, a NASA and ESA cooperation. cFS should not be considered a good flight software framework only for space applications but also for any application that needs to be robust and highly autonomous. cFS may be considered a well-designed, flight-proven flight software framework alternative for AWES. Using cFS may increase the quality of flight software and speed up the certification process thanks to the provided development artifacts of the framework. There is no standard approach for the FDIR systems. Different missions apply their specific FDIR architecture. A publicly available FDIR architecture for AWES is presented in [83], building on an architecture initially developed for space applications [84]. The SAVOIR-FDIR working group at ESA is working on an FDIR guideline for the system level [129]. Similarly, NASA has its guideline for the design of FDIR denoted as Fault Management Handbook [33], which can help the design of FDIR for AWES.

The required autonomy level for AWES is comparable with the Society of Automotive Engineers (SAE) Levels 4 and 5 in autonomous driving terminology. Vehicles that fall into these levels are denoted as highly autonomous vehicles (HAVs). Similar to satellites, HAVs manage subsystem faults autonomously. Even though automotive standards address computer-based system safety, a development standard for SAE levels 4 and 5 has yet to be developed. Underwriters Laboratories and partners from the industry are currently working on a standard called ANSI/UL 4600, the standard for safety for the evaluation of autonomous products [130].

EASA's new regulation for UAS certification has three categories: ”open”, for low risk, “specific”, for increased risk, and “certified”, for the same risk as manned aviation. The “specific” category, defined in EASA's prototype drone regulation [105], is considered more appropriate for AWES because of its flexibility and holistic approach to various types of unmanned aircraft systems. To facilitate the applications for the “specific” UAS category, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) working group 6 provided a systematic methodology to define the operation concepts and evaluate the air and ground risks introduced by UAS [94].

The specific operations risk assessment (SORA) is a methodology for classifying the risk posed by a drone flight in the “specific” category. SORA provides a framework for identifying mitigations and safety objectives [131]. The methodology provides a systematic starting point for risk assessment and a foundation for communication with the certification authority. It requires agreeing on each assessment step with the certification authority because of the qualitative nature of the process. Depending on their knowledge of the system and expectations, different parties may interpret the criteria differently. The SORA framework guides the applicant and the authority while performing the risk assessment. Responsible authorities can decide to adopt the methodology into their regulations. The categorization of UAS as “open”, “certified”, and “specific” was first proposed by JARUS and then became a norm of EASA. Therefore, the expectation is that the SORA will eventually become the norm of EASA for assessing the airworthiness of “specific” UAS.

An application of the SORA process to UAS for crisis and disaster management is presented in [132]. It is concluded that the methodology for determining the risk level of UAS operations is not entirely suitable for disaster management UAS without prior adaptations. A point of criticism is that the SORA does not account for the particular threats that can occur in individual rescue operations. This is much less an issue for AWE because the operation of the flying devices follows a more regular and, thus, predictable pattern.

As most UAS operations today are conducted with a pilot in command, the remote-piloted aircraft systems (RPAS) term be regarded interchangeably with UAS. There is no “pilot in control” expected for the commercial AWES. Therefore, pilot or remote crew-related concepts in the SORA, such as “line of sight (LOS) flight” or “see and avoid maneuvers”, are not applicable for commercial AWES. Many mitigations for the air and ground-related risks can be proposed if an operator is involved. As this does not apply to commercial AWES operations, other mechanisms that replace the human safety factor are required for the AWES airworthiness certification.

This chapter is structured as follows. Section 7.3 introduces the relevant SORA terminology and its interpretation for AWES. Section 7.5 defines the coverage of the work according to the risk categories. Section 7.6 (SORA step 1) introduces a flexible-wing kite system with a hypothetical organization and operation scenario. Sections 7.7 to 7.15 go through the SORA steps 2 to 10, interpreting each step for AWES in general and this specific AWES in particular. Section 7.16 concludes the chapter by providing the main contributions and findings of the study.

7.3. METHODOLOGY

The SORA model classifies the system into one of six Specific Assurance and Integrity Levels (SAIL), following a series of well-defined steps outlined in Table 7.1. According to the SORA guidelines, the SAIL number represents ’the level of confidence that the defined UAS operation will remain under control within the boundaries of the intended operation’ [94]. More precisely, the resulting SAIL number reflects the combined assessment of both air and ground risks. Based on the calculated SAIL category, the operator is required to meet certain requirements to ensure a safe flight.

The SORA does not contain prescriptive requirements but safety objectives to be met at various levels of robustness that commensurate with risk. However, this chapter aims to follow the SORA steps and offer generally applicable prescriptive design considerations for AWES. These considerations are intended to identify the optimal balance in the safety/cost trade-off while taking into account the priorities and resources of AWE companies. The goal of this study is to develop a better understanding of the risks posed by these systems and to propose risk mitigation measures that enable AWES to be placed in the lowest SAIL category during the commercialization phase.

In the SORA ground risk assessment step, mitigations are proposed to reduce the resulting ground risk. However, it is important to note that sensitivity in assessing potential damage to critical infrastructure varies from country to country [94]. The SORA does not specify exact measures for ensuring infrastructure safety regarding residual ground risk. Consequently, additional requirements may be necessary to safeguard critical infrastructure, depending on the location of the operation site. Recently, JARUS published a new annex for SORA supporting developers on the theoretical basis for ground risk classification [133]. In this annex, it has been made explicit that developers of novel UAS are welcome to develop and apply further improved safety analysis methods. For more comprehensive ground risk modeling and quantification, developers may refer to [52,

Table 7.1: Subprocesses and steps in the SORA process, compiled from [94].

Step 1	CONOPS description
	Ground risk process
Step 2	Determination of the intrinsic UAS ground risk class (GRC)
Step 3	Final GRC determination
	Air-risk process
Step 4	Determination of the initial air risk class (ARC)
Step 5	Application of strategic mitigations to determine residual risk
Step 6	Tactical mitigation performance requirement (TMPR) and robustness levels
	Final specific assurance and integrity levels (SAIL) and operational safety objectives (OSO) assignment
Step 7	SAIL determination
Step 8	Identification of operational safety objectives (OSO)
Step 9	Adjacent area/airspace considerations
Step 10	**Comprehensive safety portfolio**

53, 134–137].

One of SORA's main goals is to guide operators and authorities by demonstrating the benefits of a standardized risk assessment methodology. To support this, Airborne Wind Europe collaborates with AWES developers to create a Concept of Operations (CONOPS) for AWES. This collaboration has produced, a guideline for the safe testing and demonstration of currently developed AWES [138] and an introduction to the SORA for AWE [51]. The Airborne Wind Europe safety working group expects the developed CONOPS to evolve for AWES during the commercialization.

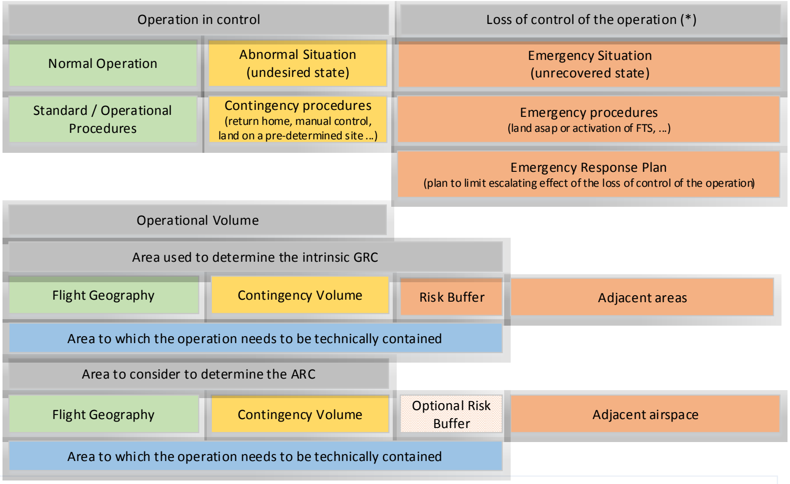
In contrast to the CONOPS and SORA work of Airborne Wind Europe, the present study aims for the operation approval of a future commercial use case rather than test operation during the development of the technology.

7.4. TERMINOLOGY

The SORA recommends standardizing the operation terminology using the semantic models and definitions illustrated in Figures 7.1 and 7.2.

The safety working group of Airborne Wind Europe extended the original SORA semantic model to better represent AWES' operational space. The new model is illustrated in Figure 7.3 with additional definitions in [139].

The terminology proposed in the figures is used as-is in this work as they cover the proposed commercial AWES operations.



(*) The Loss of control of operation corresponds to situations:

- where the outcome of the situation highly relies on providence; or
- which could not be handled by a contingency procedure; or
- when there is grave and imminent danger of fatalities.

Figure 7.1: SORA semantic model illustrates the required operational concept definitions for a new application [94].

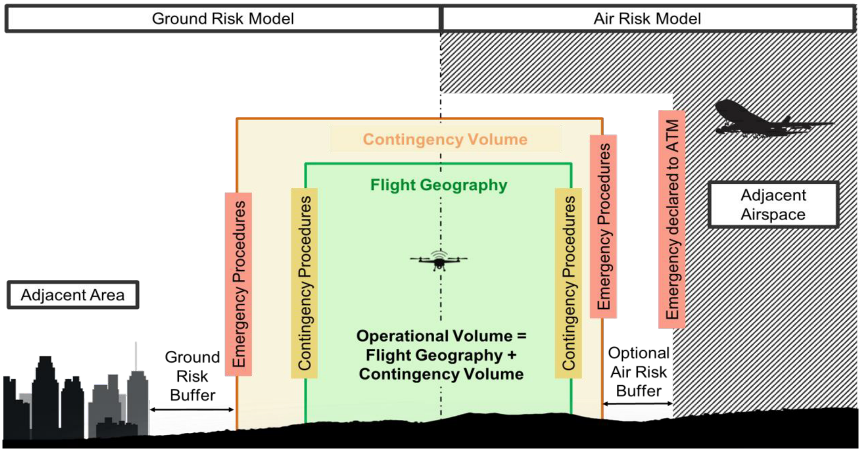


Figure 7.2: Graphical representation of the SORA semantic model [94].

7.5. RISK INTRODUCTION

To be consistent with the SORA, the risk categories that may cause the following harms are in the scope of the assessment:

- Fatal injuries to third parties on the ground,

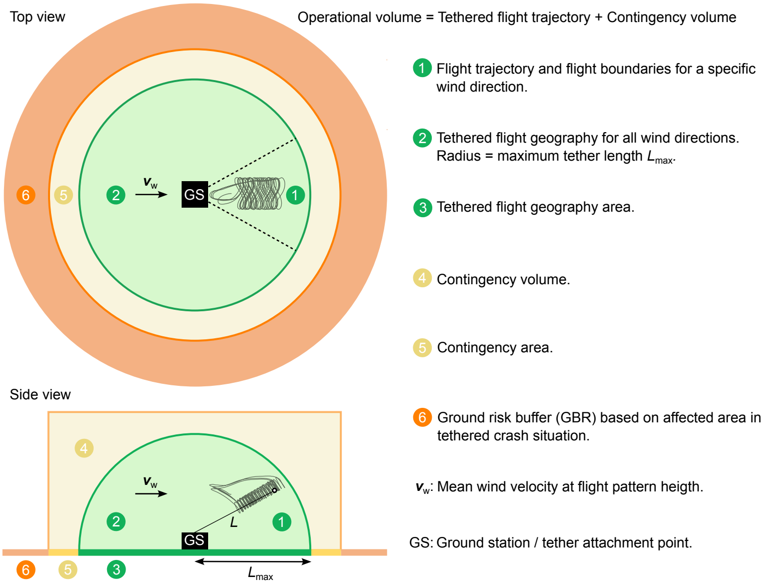


Figure 7.3: Definition of the operational volume for AWES and related terminology

- fatal injuries to third parties in the air,
- and, damage to critical infrastructure.

For the commercial operation scenario, the energy level of the airborne component is significantly higher than the amount of energy needed to cause fatal injuries in the case of a direct hit. Therefore, all crash cases are assumed to be potentially fatal.

7.6. SORA Step 1: CONOPS description

The starting point for the SORA is developing the “Concept of Operation” (CONOPS), describing the system, defining the operation concept, and providing the operator’s safety culture. Annex A of the SORA [140] is intended to support the operators in collecting and presenting the operational information for the applicant system. The following sections need to be developed by the applicant:

1. **Operation relevant information**
    (a) Organization
        i. Safety
        ii. Design and production

        iii. Training of staff involved in operations
        iv. Maintenance
        v. Crew
        vi. Configuration management
    (b) Operations
        i. Types of operations
        ii. Standard operating procedures
        iii. Normal operational strategy
        iv. Abnormal and emergency operation
        v. Accidents, incidents, and mishaps
        vi. Emergency response plan
    (c) Training
        i. General information
        ii. Initial training and qualification
        iii. Procedures for maintenance of currency
        iv. Flight simulation training devices
        v. Training program

2. **Technical relevant information**
    (a) UAS description
        i. Unmanned aircraft (UA) segment
        ii. UAS control segment
        iii. Geo fencing
        iv. Ground support equipment (GSE) segment
        v. Command and Control (C2) link segment
        vi. C2 link degradation
        vii. C2 link lost
        viii. Safety features

For the SORA Step 1, it is expected that the following requirements are covered by the AWE developer/operator.

- A safety management system is in place and is documented.
- The organization uses “industry best practices” to design and produce its AWES.
- The organization has training procedures in place, and they are documented.
- The organization has maintenance procedures in place, and they are documented.
- The organization has a description of the responsibilities and duties of personnel involved in test operations, and it is documented.

- The organization has a change management system (CMS) defined, and it is documented.
- The organization has a description of the responsibilities and duties of personnel involved in test operations, and it is documented.
- Normal operations consist of an airborne system connected to a ground station with a tether.
- The operator has documented their standard operating procedures, which are appropriate for the operations.
- The operator has documented their normal operating strategy, which is appropriate for the operations.
- The operator has documented their contingency procedures to be implemented in case of a system malfunction, abnormal operation, or an emergency. The critical failure modes of the system for all flight modes (i.e., launch, power production, land,...) have been analyzed by means of a failure mode and effects analysis (FMEA). At a minimum, this should include tether, ground station, and airborne system failure. An emergency landing procedure should be defined and documented. The tether release procedure should include provisions to ensure that the airborne part of the system does not leave the operational zone and that it results in an overall increase in safety and gives the operator a chance to minimize damage to their airborne system.
- The operator has a documented incident reporting procedure which is known to all operation personnel. At a minimum, any event involving the airborne system leaving the operational zone is expected to be reported to the local police and the certification authority.
- The operator has an emergency response plan documented and known to all operation personnel. The following scenarios should be covered: crash inside the operational zone, landing/crash outside of the operational zone, and collision with a manned aircraft.
- Description of the physical characteristics of the airborne system (mass, center of mass, dimensions,..) including photos, diagrams, and schematics; the materials used; the capability of the airborne system to withstand expected flight loads; the dimensioning of the tether; the airborne system performance characteristics (i.e., maximum altitude, endurance, accelerations, air-speeds, maximum ground speed,..); performance limits due to environmental and meteorological conditions (i.e., wind speed limitations, harsh weather conditions, minimum visibility conditions, temperatures limits,...); the propulsion system, on-board power generation, flight control surfaces and actuators, sensors, and payloads (if applicable) have been documented and provided.
- Description of overall system architecture, navigation concept, autopilot, flight control system, detect and avoid (DAA) system (if applicable) has been documented and provided.

- Description of the principles of the system or equipment used to perform geofencing functions has been provided. All AWES are connected to the ground by their tether. However, the tether can not be claimed for the 'geo-fence' requirement, considering the energy level of the AWES during the operation. The developer should have a documentation system by which they can ensure that the airborne part of the system stays within the operational zone even in the tether rapture or release case.
- Description of all the support equipment used on the ground, such as launch or recovery systems, generators, or power supplies; how the AWES is transported on the ground has been provided.
- Description of the highly autonomous nature of the system. Therefore, the inapplicability of the C2 link should be documented.
- Description of the system's single failure modes and recovery modes. Describe the emergency recovery capability to prevent third-party risk (i.e., flight termination or automatic recovery system). A functional and physical diagram of the overall system needs to be provided.

During the testing phase of AWES operations, the system operates at an automation level that allows a remote pilot to take control when necessary, such as initiating an emergency landing. Consequently, the CONOPS for AWES flight testing closely resembles the operation of Unmanned Aerial Systems (UAS). As a result, issues related to remote crew training and command and control (C2) radio links are relevant for AWES prototypes. Additionally, AWES has not yet achieved the reliability and robustness necessary for continuous 24/7 operation of large airborne devices in varied wind conditions [56, 141]. Given the relatively high probability of crashes at this developmental stage, operations depend on the remote crew to implement and execute risk mitigation procedures.

In contrast, commercial operations are expected to exhibit different characteristics. For example, human-controlled or human-supervised operation is not economically feasible for the ultimate commercial AWES. Therefore, the commercial AWES certification is irrelevant to emergency training, ground support equipment, ground control operators, and the command-and-control link. In order to make the separation clear, we outline a hypothetical AWE system in a commercial operation scenario as follows:

1. The airborne component is a single-unit flexible-wing kite with an area of 60 m^2.
2. Mechanical energy is transferred to the ground via one tether.
3. The airborne component can land and take off without human intervention.
4. The flight controller design is robust to weather conditions such as strong wind, heavy rain, or snow. (These conditions are considered abnormal operating conditions. Automatic procedures are in place in the flight control system, bringing the system to a safe state if the operation is unsafe or not feasible. Undesirable states are not considered an anomaly but a part of an operation where the system is still under control.)

The operation concept is the following:

1. The operation of the system is entirely autonomous. No ground intervention is required for the operation. There is no pilot or remote crew in the loop. Human intervention may be required only for maintenance purposes or emergencies.
2. Operation is continuous, both during the daytime and the nighttime.
3. Airborne component visibility cannot be guaranteed from the ground station due to the weather and light conditions.
4. Operations are conducted on a controlled ground area. Thus, only active participants with the training for the operation-relevant risks and emergency procedures may be present in the defined area.
5. The maximum allowed wind speed for the operation is 30 m/s (measured at ground level). For higher wind speeds, operations are terminated by the flight control system to protect the system and third parties.
6. Operations are conducted with a single system.
7. The operation volume is always free of local events and special circumstances.
8. Adjacent areas of the operation area are classified as sparsely populated.

Risk assessment in the following sections will be based on the assumed system. Some features of the system and operation definitions that may affect the risk assessment are left open for further discussion in the following sections. Thus, it will be possible to see the effect of the different design options on the risk assessment and, ultimately, on the SAIL level.

7.7. SORA STEP 2: DETERMINATION OF THE INTRINSIC GROUND RISK CLASS

SORA Step 2 relates to determining the initial risk of a person being struck by the airborne component according to Table 7.2.

As shown in Table 7.2, the initial risk highly depends on the characteristics of the AWES. To limit the scope following operational constraints are assumed:

- The airborne component consists of a 60 m^2 flexible-wing kite and a suspended kite control unit (KCU),
- The operation is over a controlled ground area,
- The operation is at a maximum altitude of 600 m. Therefore, a ground risk buffer of 600 m is assumed.

For a typical free-fall case, the drag coefficient of the kite wing does not let the kite have significant kinetic energy. However, the kite can have higher kinetic energy levels if the control unit loses control when flying in strong wind conditions. The maximum UA

Table 7.2: Determination of the intrinsic ground risk classes (GRC) [94].

Intrinsic UAS Ground Risk				
Max UAS characteristic dimension	1 m	3 m	8 m	>8 m
Typical kinetic energy expected	<700 J	<34 KJ	<1084 KJ	>1084 KJ
Operational scenarios				
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS in sparsely populated environment	2	3	4	5
BVLOS in sparsely populated environment	3	4	5	6
VLOS in populated environment	4	5	6	8
BVLOS in populated environment	5	6	8	10
VLOS over gathering of people	7			
BVLOS over gathering of people	8			

characteristic of the kite is (such as wingspan for fixed-wing or maximum dimension for multi-copters) the maximum length of the kite. For a 60 m^2 kite, it is assumed that the maximum length is more than eight meters. The operation scenario is VLOS (Visual Line of Sight) or BVLOS (Beyond Visual Line of Sight) over a controlled area, as mentioned in the operation definition.

Following the system definitions on Table 7.2, the resulting initial ground risk class is "GRC:4"

7.8. SORA STEP 3: FINAL GROUND RISK CLASS DETERMINATION

In the final GRC determination step, applicants should offer mitigations to reduce the initial risk of a person being struck by the airborne component for a "loss of control" case. Table 7.3 is used to modify the calculated GRC. A negative number in the table denotes the decrease of GRC, while a positive number means a risk increment.

Table 7.3: Mitigations for final GRC determination [94].

		Robustness		
Mitigation Sequence	**Mitigations for ground risk**	Low/None	Medium	High
1	M1 - Strategic mitigations for ground risk	0: None -1: Low	-2	-4
2	M2 - Effects of ground impacts are reduced	0	-1	-2
3	M3 - An emergency response plan (ERP) is in place, operator validated, and effective	1	0	-1

For Table 7.3, SORA defines M1, M2 and, M3 as the following:
M1: Strategic mitigations are to reduce the number of people at risk.
M2: This mitigation category aims to reduce the energy absorbed by people on the ground upon impact. These mitigations can be applied by reducing the UA impact dynamics (i.e., area, energy, impulse, transfer energy). One example of the M2 category is using an emergency parachute.

M3: Emergency response plan mitigations.
Furthermore, the SORA determines the robustness level of the mitigations considering their “level of integrity” and the claimed safety gain with a “level of assurance”. Table 7.4 guides the “level of assurance” value selection according to the criteria.

Table 7.4: Required criteria for integrity levels.

Level of integrity	**Criteria definition**
Low	Only the applicants’ declaration which states that the required level of integrity has been achieved is applicable.
Medium	Where the applicant provides supporting evidence regarding the level of integrity. This is typically achieved by means of testing.
High	Achieved integrity has been found acceptable by a competent third party.

Table 7.5: Determination of robustness level [94].

	Low assurance	**Medium assurance**	**High assurance**
Low integrity	Low robustness	Low robustness	Low robustness
Medium integrity	Low robustness	Medium robustness	Medium robustness
High integrity	Low robustness	Medium robustness	High robustness

Table 7.5 presents the outcome “Level of robustness” according to the provided “Level of assurance” and “Level of integrity” values.

For a flexible-wing kite system operating over a controlled area, further M1 mitigation is not applicable (Operating over a controlled area already has the lowest risk value). M3 mitigations do not apply to defined commercial kite operations. Since systems deployed in rural areas function autonomously, the operation and maintenance crew can not respond to an incident on short notice. Therefore, M3 increases the ground risk class factor by one.
M2 category mitigations are considered technically feasible to reduce the initial ground risk class. A safety system for ground (SSG), which detects the loss of control of the kite and reduces the kinetic energy of the kite immediately, can provide a reduction of risk class by a factor of two. The proposed SSG also reduces the risk of critical infrastructure harm. Therefore, such a system is considered a necessity for commercial AWES.

According to Table 7.5, for a “Highly robust” SSG, both the “Level of integrity” and the “Level of assurance” values have to be ‘High”. Therefore, the following requirements have to be met:

1. The activation of the SSG is automated.

2. The effects of impact dynamics and post-impact hazards are reduced to a level where it can be reasonably assumed that a fatality will not occur.

3. SSG used to reduce the effect of the UA impact dynamics are installed and maintained under manufacturer instructions.

4. Personnel responsible for the installation and maintenance of the SSG to reduce the effect of the UA impact dynamics are identified and trained by the applicant. A competent third party validates the claimed level of integrity against a standard considered adequate by the competent authority and through compliance acceptable to that authority.

Even though applicable standards for claiming technical compliance for SSG are not clear yet, it is considered safe to rely on civil aviation development standards.

Assuming that the described SSG system is in place, GRC for the defined commercial AWES operation is reduced by two points and determined as “GRC:2”.

7.9. SORA STEP 4: DETERMINATION OF THE INITIAL AIR RISK CLASS

The SORA Step 4 determines the Air Risk Class by evaluating the inherent risk of a mid-air collision. This qualitative category represents the rate of the AWE would encounter with a crewed aircraft before implementing any further tactical and strategic mitigations. The initial air risk class can be directly derived from the maps of the airspace characterization studies by the competent authority. If available, the applicant should use the dynamic or static air collision risk maps, These maps can be provided by the local aviation authority, air navigation service provider (ANSP), or UTM/U-Space service providers. Typically, the following factors affect the initial ARC determination;

- operation altitude,
- operating in controlled airspace or uncontrolled airspace,
- operating in an environment that has an airport or heliport,
- operating in airspace over urban or rural environment,
- operating in typical airspace or atypical (e.g., segregated) airspace.

When the risk maps are not available for the operation zone, SORA proposes the decision tree illustrated in Figure 7.4 to determine the initial ARC [1] .

---

[1] ARC-A represents the lowest risk category, and ARC-D represents the highest risk category.

“atypical airspace” is [142]:

- restricted airspace or danger areas,
- airspace where normal manned aircraft cannot go (e.g. airspace within 100 ft of buildings or structures),
- airspace characterization where the encounter rate of manned aircraft (encounter is defined as proximity of 3000 ft horizontally and ± 350 ft vertically) can be shown to be less than 1E-6 per flight hour during the operation),
- airspace not covered in Airspace Encounter Categories (AEC) 1 through 12.

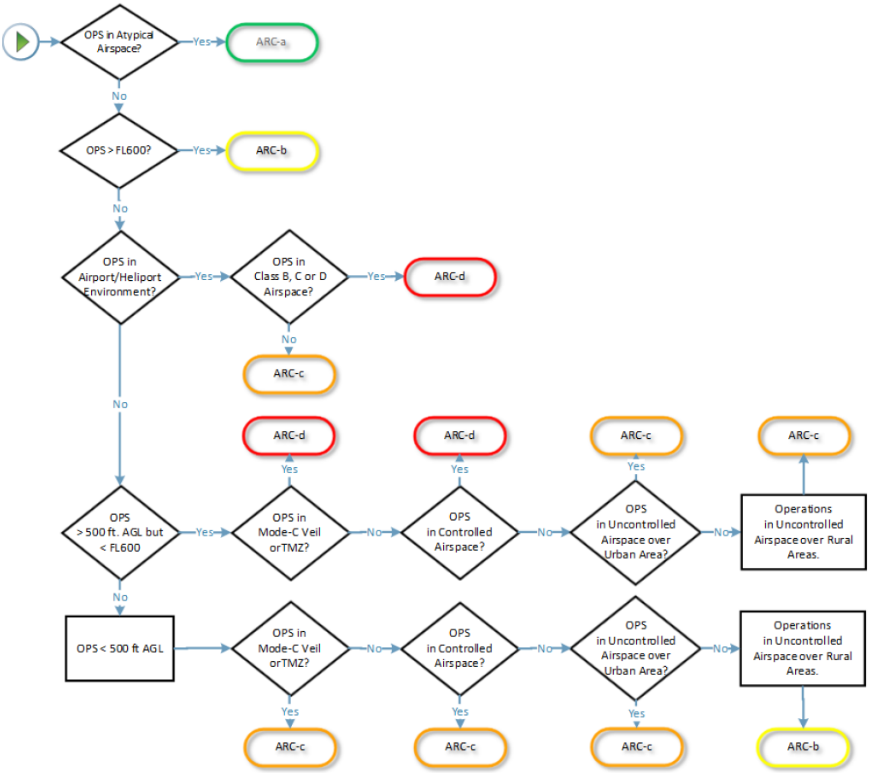


Figure 7.4: ARC assignment process [94]

Operations of the first commercial AWES are assumed to be conducted in uncontrolled airspace where an air traffic control (ATC) service is not deemed necessary or cannot be provided for practical reasons. Thus, defined commercial AWES will not operate in “atypical airspace”. More specifically, operations are expected to be in airspace class G, where the ATC has no authority for the separation. The operation altitude of the assumed system will be higher than 500 ft but less than the FL600 level.
For the future of AWES, operations may be located in special airspace, which limits the

---

The flight level (FL) is an aircraft’s altitude at the standard air pressure in aviation and aviation meteorology, expressed in hundreds of feet. Flight levels are usually designated in writing as FLxxx, where xxx is a two- or three-digit number indicating the pressure altitude in units of 100 ft (30 m) [143]. FL600 means the top of class A airspace corresponding to 60000 ft pressure altitude, the approximate top of the troposphere. This altitude is above commercial airliner operations.

“Mode C veil” refers to a kind of airspace that currently surrounds all primary Class B airports. This airspace extends horizontally to a circle of 30 NM radius centered on the airport and extends vertically from the surface up to 10000 ft MSL (mean sea level) [144]. The name refers to the mode of transponder operation required within this airspace — that is, with minimal exceptions, all aircraft operating within this airspace must have an altitude-reporting Mode C transponder in operation.

A transponder mandatory zone (TMZ) is an airspace of defined dimensions wherein the carriage and operation of transponder equipment are mandatory.

pilot operation in certain areas. Currently, special airspace consists of prohibited areas, restricted areas, warning areas, military operation areas (MOAs), alert areas, and controlled firing areas (CFAs), none of which are on the flight charts. The “Mode C veil” is considered unnecessary for the commercial AWES operation. Similarly, it is not expected to operate in TMZ for the assumed commercial AWES.
Being in uncontrolled airspace class G does not exclude nearby airports and heliports. Therefore, it is required to ensure that there is no airport or heliport in the vicinity of the operation area or that the operations are coordinated.
From the air risk category (ARC) point of view, there is no difference between operating over rural and urban areas. Nevertheless, this has a significant impact on GRC. Therefore, the recommendation for the first AWES commercial scenario is to operate over controlled ground areas only.

By executing the SORA decision tree for the initial ARC determination with the inputs from the representative operation scenario above, the initial air risk category for the commercial AWES is ARC-C.

The SORA states that the competent authority may raise the operation volume ARC to a higher level considering the circumstances, which could invalidate the decisions taken. Therefore, to agree with the competent authority on the same initial ARC, it is the applicant’s responsibility to ensure the decisions on the decision tree are always valid, even in undesired operational events such as losing control. We consider that, for commercial AWES, a holistic health monitoring system is required to cover the safety operational envelope requirements which are agreed with the certification authority. This system can be realized as proposed in Chapter 5.

7.10. SORA STEP 5: APPLICATION OF STRATEGIC MITIGATIONS TO DETERMINE RESIDUAL ARC (OPTIONAL)

After determining the initial air risk class, tactical and strategic mitigations may be proposed to reduce the risk category. Operating during certain times or within certain boundaries may be an example of strategic mitigations. Some form of detect-and-avoid system is a tactical mitigation example.
According to [145], the most common strategic mitigations by operational restriction are:

- Mitigation(s) that bound the geographical volume in which the UAS operates (e.g., certain boundaries or airspace volumes)
- Mitigation(s) that bound the operational time frame (e.g., restricted to certain times of day, such as flying only at night)

The geographic volume restriction is typically for claiming a lower ARC despite the high encounter risk. For example, a UAS operation in Class B airspace has a high rate of encountering a crewed aircraft. However, the UAS system can operate at the outer reaches of the Class B airspace where crewed aircraft do not routinely fly and can claim ARC reduction for its operation volume.

The selected operation volume for the representative commercial AWE is already the safest option (Class G, uncontrolled airspace, not being close to the Airport and heliport). Restriction on the timeframe is not a commercially feasible mitigation for AWES operations. Therefore, no strategic air risk mitigation applies to the proposed scenario.

7.11. SORA STEP 6: TACTICAL MITIGATIONS PERFORMANCE REQUIREMENT(TMPR) AND ROBUSTNESS LEVELS

Tactical mitigations are employed to address any remaining risk of mid-air collisions in order to meet the required airspace safety objectives. These mitigations may involve 'See and Avoid' strategies (e.g., operations within visual line of sight (VLOS)) or the use of systems that provide alternative methods to achieve the airspace safety objective, such as operations supported by one or more detect-and-avoid (DAA) systems.

VLOS operation for commercial AWES is not feasible considering 24/7 operation under various weather conditions at the operation altitudes of AWES. In addition to the operation conditions, a continuous "pilot in control" is considered not feasible. Therefore, the "see and avoid" maneuver can not be proposed for the commercial AWES. However, to further reduce the ARC of commercial AWES, DAA systems for triggering a passive separation maneuver (e.g., activating an emergency landing) can be implemented as a tactical mitigation.

Table 7.6: SAIL determination [94].

	Residual ARC			
Final GRC	A	B	C	D
≤ 2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Category C operation			

"According to Table 7.6, reducing the ARC level from C to B significantly impacts the resulting SAIL category for an ARC-3 UAS system. Therefore, to facilitate airworthiness certification, commercial AWES should incorporate a Detect and Avoid (DAA) system, as well as a separation maneuver designed specifically for emergencies involving crewed aircraft. The separation maneuver is tailored to the AWES design; however, the DAA system must monitor the environment surrounding the AWES to determine if a collision is imminent.

DAA systems are not only designed to detect and avoid other aircraft but also to make AWES visible to other aircraft or UAS, allowing them to detect and avoid AWES. Following advancements in drone airworthiness requirements, companies have begun offering DAA systems for drones, which could be adapted for AWES. In particular, the DAA system for AWES must account for the possibility of tether collision and plan the 'avoid maneuver' accordingly. The DAA system should function for both cooperative and non-cooperative aerial vehicles. Given the operational altitudes and commercial use of AWES, the likelihood of encountering non-cooperative aircraft is higher than that of encountering cooperative aircraft.

DAA system sensors can be classified as passive or active. Active sensors, such as radar, lidar, or ultrasonic sensors, emit signals and use their reflection for detection, while passive sensors rely on signals emitted by the target. For example, infrared (IR) and visual cameras are passive sensors. An example of a passive system uses cameras and a computer-vision system with artificial intelligence methods to mimic pilot perception, thereby replacing traditional 'see and avoid' capabilities [146]. These systems are lightweight and consume little power, making them strong candidates for integration into the airborne component of an AWES. However, their ability to estimate obstacle distances is less accurate, and their detection performance may be compromised by adverse weather conditions. Active sensor systems provide more precise distance measurements by utilizing time-of-flight data from emitted signals. However, these systems are heavier and consume more power, making them less suitable for integration into the airborne component of AWES. They may, however, be integrated into the ground component, considering the proximity of the airborne component to the ground station. In this configuration, the position of the airborne component would be transmitted to the ground-based system to accurately calculate crash probabilities and avoidance maneuvers. Although this approach requires modifications to existing DAA systems, which may necessitate re-qualification, it is considered the most viable long-term solution."

Assuming that the described DAA system is implemented for the hypothetical AWES system, the ARC level is reduced to ARC-B.

7.12. SORA STEP 7: FINAL SPECIFIC ASSURANCE AND INTEGRITY LEVELS (SAIL) AND OPERATIONAL SAFETY OBJECTIVES (OSO) ASSIGNMENT

SORA Step 7 consolidates the determined GRC and ARC to acquire the final SAIL value according to Table 7.6. Resulting SAIL category represents the confidence level that the system will stay under control.

Considering the discussions in the previous steps, the consolidated SAIL parameter for proposed commercial AWES is determined as “SAIL: II”, with the calculated “GRC:2” and “ARC-B”.

7.13. SORA STEP 8: IDENTIFICATION OF OPERATIONAL SAFETY OBJECTIVES (OSO)

SORA step 8 gives the expected levels for safety objectives according to the SAIL number in three qualitative categories. These are Low(L), Medium(M), and High(H). If a safety objective is not mandatory for the given SAIL, it is marked as Optional(O). It is the operators' responsibility to provide evidence showing that the objectives are satisfied with the associated level of robustness.

For the SAIL: II category, which is the determined SAIL category for the representative commercial AWES, the highest expected robustness level for the safety objectives is “Medium”.

Tables 7.7, 7.8, 7.9 and 7.10 lists the required objectives for SAIL: II. These lists should be considered the minimum set of requirements that was asked historically for the safety of similarly categorized UAS. The competent authority may extend the list or may change the associated robustness levels.

Table 7.7: Recommended operational safety objectives (OSO) in the SORA and their applicability to commercial AWES, compiled from [94]

OSO number	Technical issue with the UAS	Required robustness level for SAIL II	AWES applicability
1	Ensure the operator is competent and/or proven	L	Yes
3	UAS maintained by competent and/or proven entity	L	Yes
6	C3 link performance is appropriate for the operation	L	No
7	Inspection of the UAS (product inspection) to ensure consistency with CONOPS	L	Yes
8	Operational procedures are defined, validated and adhered to	L	Yes
9	Remote crew trained and current and able to control the abnormal situation	L	No
10	Safe recovery from technical issue	L	Yes

Table 7.8: Recommended operational safety objectives (OSO) in the SORA and their applicability to commercial AWES, compiled from [94]

OSO number	Deterioration of external systems supporting UAS operation	Required robustness level for SAIL II	AWES applicability
11	Procedures are in place to handle the deterioration of external systems supporting UAS operation	M	Yes
12	The UAS is designed to manage the deterioration of external systems supporting UAS operation	L	Yes
13	External services supporting UAS operations are adequate to the operation	L	No

Table 7.9: Recommended operational safety objectives (OSO) in the SORA and their applicability to commercial AWES, compiled from [94]

OSO number	Human error	Required robustness level for SAIL II	AWES applicability
14	Operational procedures are defined, validated and adhered to	M	No
15	Remote crew trained and current and able to control the abnormal situation	L	No
16	Multi-crew coordination	L	No
17	Remote crew is fit to operate	L	No
20	A human factors evaluation has been performed and the HMI found appropriate for the mission	L	No

7.14. SORA STEP 9: ADJACENT AREA/AIRSPACE CONSIDERATIONS

SORA step 9 addresses the risk of UAS control loss and, consequently, the infringement of the adjacent airspace or ground areas. Accordingly following requirements are enforced:

Table 7.10: Recommended operational safety objectives (OSO) in the SORA and their applicability to commercial AWES, compiled from [94]

OSO number	**Adverse operating conditions**	**Required robustness level for SAIL II**	**AWES applicability**
21	Operational procedures are defined, validated and adhered to	M	Yes
22	The remote crew is trained to identify critical environmental conditions and to avoid them	L	No
23	Environmental conditions for safe operations defined, measurable and adhered to	L	Yes

1. The probability of leaving the operational volume per flight hour shall be less than 1×10^{-4}.

2. No single failure of the UAS or any external system supporting the operation shall lead to operation outside the ground risk buffer. Compliance with the requirements above shall be substantiated by analysis or test data with supporting evidence.

3. Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to operations outside of the ground risk buffer shall be developed to an industry standard or methodology recognized as adequate by the competent authority.

However, these safety requirements are only applicable if the adjacent operation areas are:

1. Gatherings of people unless already approved for operations over gatherings of people OR

2. ARC-D unless the residual ARC is ARC-D

or in populated environments where:

1. M1 mitigation has been applied to lower the GRC

2. Operating in a controlled ground area

Because none of these adjacent conditions are met for the defined operational scenario of commercial AWES, we conclude that the requirements are not applicable.

SORA step 9 has another requirement for the operation containment which is defined as the following:

"No probable[2] failure of the UAS or any external system supporting the operation shall lead to operation outside of the operational volume. Compliance with the requirement above shall be substantiated by a design and installation appraisal and shall minimally include:

---

[2] The term "Probable" in the requirement means "Anticipated to occur one or more times during the entire system/operational life of an item" [94].

- design and installation features (independence, separation, and redundancy);
- relevant particular risk (e.g., hail, ice, snow, electro-magnetic interference) associated with the CONOPS”

The abovementioned containment requirement applies to the commercial AWES. In the defined system, the flight control system keeps the airborne component in the operation volume by processing the inputs such as position, wind speed, and tether tension from various subsystems. All these inputs are critical for keeping the system in operation volume. There are two possible approaches to cover the operation containment requirement:

1. Developing and qualifying the entire flight control system and all flight-relevant subsystems with a credible development standard,
2. or developing and qualifying an independent system that keeps the airborne component always in the operation zone in a failure case

Considering the technology maturity level and ongoing improvement of current AWES flight control systems (and subsystems), the second option considered more reasonable for the time being is to keep the technology development ongoing. Qualifying an entire system costs significantly more than qualifying a system with a dedicated task. Therefore, this study derives the following high-level requirements of an independent system that ensures that the airborne component is always in the operation zone:

- The fault detection system shall detect the position-keeping failure of the flight control system using independent algorithms/sensors.
- All critical hardware, sensors, and software should meet the reliability metric requirements, or redundancy should ensure reliability. The system’s hardware and software shall be qualified with a credible standard.
- If position control is lost, the system shall have the mechanism to conduct a controlled landing or crash in the operation zone. The components of this emergency system should have the same quality level as the detection module.

7.15. SORA STEP 10: COMPREHENSIVE SAFETY PORTFOLIO

SORA Step 10 summarizes the following objectives and mitigations:

- Mitigations used to modify the intrinsic GRC
- Strategic mitigations for the initial ARC
- Tactical mitigations for the Residual ARC
- Adjacent Area/Airspace considerations
- Operational safety objectives

Proper implementation of these claimed mitigations and satisfactory evidence are needed for a sufficient confidence level in the system. The operator should address additional requirements such as security and environmental requirements. The activities for the SORA may address some of these additional requirements, but the operator should ensure to cover them all. Then, the operator is responsible for ensuring the consistency between the documented SORA safety case and the actual operational conditions.

7.16. CONCLUSIONS

The airborne wind energy (AWE) sector has grown steadily in the last decade, and the technology is increasingly attracting the attention of governments, policymakers, and industry. The main barrier to commercialization is reaching the reliability and safety levels required for long-term operation in relevant wind environments. Because of the flying energy-harvesting devices, airborne wind energy systems (AWES) are closer to highly autonomous vehicles, drones, and robots than wind turbines. Despite many prototypes today, there has yet to be an agreed way forward for the commercial operation approval of AWES.

For a decade, much effort was invested in safely integrating unmanned aerial systems (UAS) into airspace. The European Union Aviation Safety Agency (EASA) has created a regulation for the flight approval of UAS with three categories. One of the categories, denoted as “specific”, is for non-regular UAS, which requires ad-hoc risk assessment and risk mitigations for the flying permits.

In this study, we propose that commercial AWES can be certified as a ’specific’ type of UAS by adhering to the risk assessment framework established by JARUS (The Joint Authorities for Rulemaking on Unmanned Systems). The selected framework, SORA (Specific Operations Risk Assessment), is considered to provide the most comprehensive and mature process for assessing the risks associated with commercial AWES operations. This chapter applies the SORA process step by step to a hypothetical commercial AWES operation, in order to identify potential ground and air risks posed by the system. For each identified risk, possible mitigation measures are discussed in detail.

In SORA terminology, the initial Ground Risk Class (GRC) is determined as ’GRC 4’ and is subsequently reduced to ’GRC 2’ by introducing a Safety System for Ground (SSG). This system detects the airborne component’s loss of control and immediately reduces the kite’s kinetic energy. The proposed system also mitigates risks to critical infrastructure, which are not fully addressed by SORA.

For the assumed operational scenario, the initial Air Risk Class (ARC) is identified as ’ARC C,’ representing the qualitative risk of encountering other aircraft during the operation. To further reduce this risk, a tactical mitigation is proposed, involving both a safety system to monitor the system’s position and a Detect and Avoid (DAA) system for emergency separation. These mitigations reduce the ARC to ’ARC B.’

With these GRC and ARC mitigations in place, the consolidated Specific Assurance and Integrity Level (SAIL)—the level of confidence that the UAS operation will remain under control—is increased twofold, resulting in a ’SAIL II’ classification.

The proposed mitigations are expected to significantly enhance the safety of commercial AWES operations. We believe that applying the steps outlined in this chapter will facilitate the approval process for commercial operations.

8

CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the most important findings of this work then further research directions are proposed.

8.1. CONCLUSIONS

To develop and commercialize large-scale AWES, with each unit providing several megawatts of power—and where the AWES can reliably produce energy for years under varying weather conditions, the safety and reliability of the systems need to be ensured and formally certified. Toward this objective, the following research questions are answered in this thesis;

1. How well are current AWES prototypes assessed in terms of safety and reliability?

   The exact levels of the AWES prototypes are not open to the public. However, with the provided survey responses by 11 sector representatives, the following conclusions can be drawn; Most of the systems are passing through a phase between prototyping and commercialization called early commercialization. Six systems are in the research and development phase and occasionally operate to finalize technology development. These systems' technology Readiness Levels (TRL) can be considered TRL5 or less. The remaining five systems are in Pilot/Demo, which flies frequently with a converged prototype to measure power output and demonstrate reliability and safety. TRL levels of these five systems can be considered between TRL6 and TRL7. Except for one system, there is an operator in the loop, a major mitigation for catastrophic events. However, systems are expected to be fully automatic for the commercialization phase, which is expected to start around 2025, which may significantly impact safety analyses and certification aspects. In terms of reliability, one system is reported as operated for three days, the maximum operation time of the other systems is in the levels of hours. All the systems operate over the dedicated ground areas, and notifications are sent to the other airspace users. 5 out of 11 systems intend to apply for SORA for airworthiness. Five systems are engaged with the aviation authority for SORA for their current operations already. 6 of the entities have an emergency response plan in place. The sector's average work effort for certification-related topics is 60 hours per month.

2. How can the reliability and safety levels of an AWE system be determined systematically?

   In order to determine the levels of reliability and safety levels precisely, statistics of extensive testing and use history should be examined. This approach may not be feasible for newly developed safety-critical complex systems such as AWES.

   The other approach is to derive the required levels of robustness and safety by considering commercial interests, certification needs, and public acceptance. Then, safety analyses, design and manufacturing artifacts, operation manuals, and test and simulation results should be used to claim that the targeted levels are met.

   For commercial AWES operation, the following targets are concluded in the previous chapters.

   The probability of catastrophic failure should be less than 10^{-8} per flight hour. The probability of hazardous failure condition should be less than 10^{-7} per flight hour. The probability of encountering a manned aircraft should be less than 10^{-6} per flight hour. The probability of leaving the operational volume should be less than 10^{-4} per flight hour.

3. How to improve the current design and operation concepts to reach the commercially required safety and reliability levels?

   In order to reach the required levels of safety and reliability, risks and failure cases need to be well extracted using safety analyses and then these risks are mitigated with design and operational mitigations. This study executed Failure Mode and Effect Analysis (FMEA) and Fault Tree analyses for the analysis step. The former analyzes the failure cases individually, and the latter considers the simultaneous fault cases that may bring the system to catastrophic conditions. These two industry-proven tools should be used if it is aimed to reach the targeted levels and claim the system's safety. Analyses should be executed iteratively until the design and operational scenarios reach the targeted safety and reliability level.

4. How can a “Fault Detection isolation and recovery” (FDIR) system architecture be developed for AWES?

   For commercial AWES, system monitoring should be completely automatic during the operation. This monitoring is achieved with a "Fault detection isolation and recovery" (FDIR) system. The requirements of the FDIR system are derived from the mitigations, which are populated from safety analyses and certification needs. In this thesis, a multilayered systematic FDIR architecture is proposed and detailed for commercial AWES. In order to reach the required safety and reliability levels for commercialization, a similar approach is necessary to realize FDIR.

5. What is a suitable roadmap for AWES certification? Which tactical and operational mitigations would facilitate the certification process?

   AWES are expected to operate in Class G airspace where interaction with other users is possible. Therefore, it is expected that commercial AWE systems will have to comply with international airspace regulations. Currently, for the European case, Unmanned Arial Systems (UAS) operation approval conditions for non-regular ('specific') UAS by The European Union Aviation Safety Agency (EASA) provide the most mature and systematic way forward for airworthiness certification. The SORA framework guides the applicant for the 'specific' UAS operation permit. This study executed the SORA guideline on a hypothetical commercial system to define the "Specific assurance and integrity level" (SAIL) of commercial AWES. A similar approach should be followed to get a 'specific' UAS operation permit from EASA. The initial ground risk is reduced by two factors in SORA classifications with an FDIR system that detects the airborne component's control loss case and immediately reduces the kite's kinetic energy.

   By proposing a detect and avoid (DAA) system and a separation maneuver designed for emergency separation, the air risk is reduced to "ARC-B." in SORA terminology. The consolidated level of confidence that the AWES operation will stay under control is increased by two levels and determined as "SAIL: II."

   The proposed mitigations in this study significantly increase the safety levels of commercial AWES according to the SORA framework. If facilitating AWES's airworthiness certification process is aimed, proposed tactical mitigations should be applied.

This thesis contributes to the scientific understanding of the commercial deployment of Airborne Wind Energy (AWE) on the following points:

Chapters 1 and 2 examine the current state of Airborne Wind Energy (AWE) technology, with a particular emphasis on reliability and safety. This novel analysis incorporates independent studies from various sources, as well as survey responses from major AWES companies, to provide a comprehensive understanding. The review identifies the need for a systematic assessment of reliability and safety as a crucial first step in addressing potential reliability weaknesses and safety risks.

Chapter 4 applies two safety analysis methods, widely used in the aircraft industry, to a specific Airborne Wind Energy System (AWES) described in Chapter 3. The analysis steps are thoroughly detailed, providing a clear example of how to perform a safety analysis for complex, safety-critical systems. The outcome of this analysis is the design of an active Fault Detection, Isolation, and Recovery (FDIR) system.

Based on the safety analysis in Chapter 4, Chapter 5 presents a detailed FDIR architecture that meets the specific requirements for automation, robustness, and safety in commercial Airborne Wind Energy (AWE) systems. To the author's knowledge, this is the first FDIR subsystem proposed in the AWES literature that is both widely applicable and flexible enough to accommodate different AWES designs.

Chapter 6 provides an in-depth discussion of the airworthiness certification aspects for commercial Airborne Wind Energy Systems (AWES). It outlines, for the first time, the key stakeholders involved in the regulatory process and reviews potentially applicable regulations. Additionally, recent developments in UAV airworthiness certification are examined. Chapter 6 establishes the foundation for certification considerations and concludes that classifying commercial AWES as a ’specific’ type of unmanned aerial system is the most feasible approach moving forward.

Building on the content of Chapter 6, Chapter 7 outlines the path forward for obtaining airworthiness certification for commercial Airborne Wind Energy Systems (AWES) as a ’specific’ type of unmanned aerial system. The discussions within each SORA (Specific Operations Risk Assessment) guideline step provides key insights into the critical areas developers must address. The risk analyses and mitigation strategies proposed throughout the chapter highlight the necessity of implementing safety systems to reduce ground risk and mitigate mid-air collision risk in the event of a tether rupture, as well as the need for a detect-and-avoid system. To the best of the author’s knowledge, this chapter represents the first systematic study of the operational requirements for commercial AWES.

8.2. RECOMMENDATIONS

This work investigates the applicability of existing rules and standards whose objective is to manage aviation-related risks. In essence, these standards define the acceptable risks to other airspace users, people, and property on the ground. Although existing standards can be partially applied to ground components, such as the low-voltage directive (LVD) 2006/95/EC for electrical installation and machine directives 2006/42/EC or IEC 61400 for wind turbines, systematic work is required for ensuring the ground equipment’s safety and reliability.

To maximize reliability, the most likely sources of failures must be quantified through uncertainty quantification. The source of failure may start with an extreme weather event, a sudden component failure, or a logic failure in the control system. Current AWE simulation frameworks focus on optimizing energy generation and control schemes. These frameworks need to be extended to simulate the challenging reliability cases.

Once established, systematic maintenance is required to maintain the systems’ reliability and safety level. Both for rigid-wing and flexible kites, modeling of wearing characteristics is required as the first step. Preventive maintenance methods using machine learning and continuous monitoring of the systems would further decrease the operation cost, speeding up the commercialization of the systems.

This work considered only a single AWE system for the reliability and safety assessment. Nevertheless, if multiple systems operate in an AWE farm, the interaction among the systems would affect the total reliability and safety. The SORA process needs to be reworked to be able to consider the interaction of multiple systems. More modeling-based research is needed to analyze and improve the safety and reliability of AWE farms.

REFERENCES

1. International Renewable Energy Agency (IRENA): Innovation Outlook: Offshore Wind. Accessed Dec 7, 2023, International Renewable Energy Agency, Abu Dhabi, June 2016. https://irena.org/-/media/Files/IRENA/Agency/Publication/2016/IRENA_Innovation_Outlook_Offshore_Wind_2016.pdf Accessed Nov 21, 2023
2. De Castro, C., Mediavilla, M., Miguel, L., Frechoso, F.: Global wind power potential: Physical and technological limits. Energy Policy **39**(10), 6677–6682 (2011). doi: 10.1016/j.enpol.2011.06.027
3. Burton, T., Jenkins, N., Sharpe, D., Bossanyi, E.: Wind Energy Handbook. 2nd ed. John Wiley & Sons (2011). doi: 10.1002/9781119992714. Section 3.2.3: "The Betz Limit" and Section 6.2: "Rotor Diameter"
4. Ahrens, U., Diehl, M., Schmehl, R. (eds.): Airborne Wind Energy. Green Energy and Technology. Springer, Berlin Heidelberg (2013). 611 pp. doi: 10.1007/978-3-642-39965-7
5. Cherubini, A., Papini, A., Vertechy, R., Fontana, M.: Airborne Wind Energy Systems: A review of the technologies. Renewable and Sustainable Energy Reviews **51**, 1461–1476 (2015). doi: 10.1016/j.rser.2015.07.053
6. Cherubini, A., Moretti, G., Fontana, M.: Dynamic Modeling of Floating Offshore Airborne Wind Energy Converters. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 15, pp. 137–163. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_7
7. Nelson, V.: Innovative Wind Turbines: An Illustrated Guidebook. CRC Press, Boca Raton, FL (2019). 156 pp. doi: 10.1201/9781003010883
8. Schmehl, R.: Airborne Wind Energy: An Introduction to an Emerging Technology. https://awesco.eu/awe-explained/. Accessed Nov 2, 2023
9. Bechtle, P., Schelbergen, M., Schmehl, R., Zillmann, U., Watson, S.: Airborne Wind Energy Resource Analysis. Renewable Energy **141**, 1103–1116 (2019). doi: 10.1016/j.renene.2019.03.118
10. Durakovic, A.: Shell and Google Owner Enter Offshore Energy Kite Venture. Accessed Dec 7, 2023. https://www.offshorewind.biz/2019/02/12/shell-and-google-owner-enter-offshore-energy-kite-venture/.
11. T. Stehly D. Heimiller, G. S.: Cost of Wind Energy Review. Accessed Dec 7, 2023, NREL Report. https://www.nrel.gov/docs/fy18osti/70363.pdf Accessed Dec 9, 2018
12. Weber, J., Marquis, M., Cooperman, A., Draxl, C., Hammond, R., Jonkman, J., Lemke, A., Lopez, A., Mudafort, R., Optis, M., Roberts, O., Shields, M.: Airborne Wind Energy. NREL/TP-5000-79992, National Renewable Energy Laboratory (NREL), Golden, CO, Aug 2021. doi: 10.2172/1813974
13. European, C.: Study on challenges in the commercialisation of airborne wind energy systems. ECORYS Report PP-05081-2016, Brussels, Sept 2018. doi: 10.2777/87591

14. International Renewable Energy Agency (IRENA): Future of wind: Deployment, investment, technology, grid integration and socio-economic aspects (A Global Energy Transformation paper, International Renewable Energy Agency, Abu Dhabi, June 2019. https://www.irena.org/publications/2019/Oct/Future-of-wind Accessed Nov 21, 2023
15. Airborne Wind Europe. Accessed April 7, 2024. https://edu.nl/r4vrm.
16. Fagiano, L., Quack, M., Bauer, F., Carnel, L., Oland, E.: Autonomous Airborne Wind Energy Systems: Accomplishments and Challenges. Annual Review of Control, Robotics, and Autonomous Systems **5**(1), 603–631 (2022). doi: 10.1146/annurev-control-042820-124658
17. United States Department of Energy (DOE): Challenges and Opportunities for Airborne Wind Energy in the United States. Report to Congress. Accessed Dec 7, 2023, Washington, DC 20585, Nov 2021. https://www.energy.gov/eere/wind/articles/new-report-discusses-opportunities-and-challenges-airborne-wind-energy
18. Watson, S., Moro, A., Reis, V., Baniotopoulos, C., Barth, S., Bartoli, G., Bauer, F., Boelman, E., Bosse, D., Cherubini, A., Croce, A., Fagiano, L., Fontana, M., Gambier, A., Gkoumas, K., Golightly, C., Latour, M. I., Jamieson, P., Kaldellis, J., Macdonald, A., Murphy, J., Muskulus, M., Petrini, F., Pigolotti, L., Rasmussen, F., Schild, P., Schmehl, R., Stavridou, N., Tande, J., Taylor, N., Telsnig, T., Wiser, R.: Future emerging technologies in the wind power sector: A European perspective. Renewable and Sustainable Energy Reviews **113**, 109270 (2019). doi: 10.1016/j.rser.2019.109270
19. Geraci, A., Katki, F., McMonegal, L., Meyer, B., Lane, J., Wilson, P., Radatz, J., Yee, M., Porteous, H., Springsteel, F.: IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries, pp. 1–217. IEEE Press (1991). doi: 10.1109/IEEESTD.1991.106963
20. Verma, A. K., Srividya, A., Karanki, D. R.: Reliability and Safety Engineering, vol. 43. Springer Series in Reliability Engineering. Springer, London (2010). doi: 10.1007/978-1-4471-6269-8
21. Wilkins, D. J.: The Bathtub Curve and Product Failure Behavior. https://edu.nl/xb698. Accessed Feb 2, 2021
22. Kaplan, S., Garrick, B. J.: On the quantitative definition of risk. Risk analysis **1**(1), 11–27 (1981). doi: 10.1111/j.1539-6924.1981.tb01350.x
23. Peirce, C. S.: On the Algebra of Logic: A Contribution to the Philosophy of Notation [Continued in Vol. 7, no. 3]. American Journal of Mathematics **7**(2), 180–196 (1885). doi: 10.2307/2369451
24. Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment, Volume 1, Methods and Techniques. Wiley (1992)
25. Arabian-Hoseynabadi, H., Oraee, H., Tavner, P.: Failure Modes and Effects Analysis (FMEA) for wind turbines. International Journal of Electrical Power & Energy Systems **32**(7), 817–824 (2010). doi: https://doi.org/10.1016/j.ijepes.2010.01.019
26. Wikipedia, The Free Encyclopedia: Probabilistic risk assessment. https://en.wikipedia.org/wiki/Probabilistic_risk_assessment. Accessed Sept 11, 2021
27. Pouliezos, A. D., Stavrakakis, G. S.: Real Time Fault Monitoring of Industrial Processes. Springer (2013). 542 pp. doi: 10.1007/978-94-015-8300-8
28. Hyers, R., McGowan, J., Sullivan, K., Manwell, J., Syrett, B.: Condition monitoring and prognosis of utility scale wind turbines. Energy materials **1**(3), 187–203 (2006). doi: 10.1179/174892406X163397

29. Hameed, Z., Hong, Y., Cho, Y., Ahn, S., Song, C.: Condition monitoring and fault detection of wind turbines and related algorithms: A review. Renewable and Sustainable energy reviews **13**(1), 1–39 (2009). doi: 10.1016/j.rser.2007.05.008

30. Amirat, Y., Benbouzid, M. E., Bensaker, B., Wamkeue, R.: Condition monitoring and ault diagnosis in wind energy conversion systems: a review. In: 2007 IEEE International Electric Machines & Drives Conference, vol. 2, pp. 1434–1439, IEEE, (2007). doi: 10.1109/IEMDC.2007.383639

31. Lu, B., Li, Y., Wu, X., Yang, Z.: A review of recent advances in wind turbine condition monitoring and fault diagnosis. In: 2009 IEEE Power Electronics and Machines in Wind Applications, pp. 1–7, Lincoln, NE, USA, June 24–26, 2009. doi: 10.1109/PEMWA.2009.5208325

32. Dennehy, C. J., Fesq, L. M.: The Development of NASA's Fault Management Handbook. IFAC Proceedings Volumes **45**(20), 295–300 (2012). doi: https://doi.org/10.3182/20120829-3-MX-2028.00250

33. National Aeronautics and Space Administration (NASA): Fault Management Handbook. NASA Technical Handbook NASA-HDBK-1002, Washington, DC, Mar 12, 2012. https://snebulos.mit.edu/projects/reference/NASA-Generic/NASA-HDBK-1002.pdf

34. Glass, B.: A Review of Wind Standards as they Apply to Airborne Wind Turbines. In: Schmehl, R. (ed.). Book of Abstracts of the International Airborne Wind Energy Conference, p. 81, Presentation video recording available from: https://collegerama.tudelft.nl/Mediasite/Play/90b60bc1e2bf44759ddc1b18185383791d, Delft, The Netherlands, June 15–16, 2015. doi: 10.4233/uuid:7df59b79-2c6b-4e30-bd58-8454f493bb09

35. Ruiterkamp, R., Salma, V., Kruijff, M.: Update on Certification and Regulations of Airborne Wind Energy Systems – The European Case for Rigid Wings. In: Schmehl, R. (ed.). Book of Abstracts of the International Airborne Wind Energy Conference 2015, pp. 78–79, Delft, The Netherlands, June 15–16, 2015. doi: 10.4233/uuid:7df59b79-2c6b-4e30-bd58-8454f493bb09. Presentation video recording available from: https://collegerama.tudelft.nl/Mediasite/Play/c8a9806aea024394a36cc35f9d6e98a81d

36. Langley, W. R.: Go, Fly a Kite: The Promises (and Perils) of Airborne Wind-Energy Systems. Texas Law Review **94**, 425–450 (2015). https://texaslawreview.org/wp-content/uploads/2016/03/Langley.Final_.pdf Accessed Nov 20, 2023

37. Hardham, C.: Response to the Federal Aviation Authority. Docket No.: FAA-2011-1279; Notice No. 11-07; Notification for Airborne Wind Energy Systems (AWES), Makani Power, Feb 7, 2012. https://www.regulations.gov/comment/FAA-2011-1279-0015 Accessed Nov 20, 2023

38. Federal Aviation Administration: Notification for Airborne Wind Energy Systems (AWES), FAA-2011-1279, Dec 2011. https://www.federalregister.gov/d/2011-31430 Accessed Nov 20, 2023

39. Kruijff, M., Ruiterkamp, R.: A Roadmap Towards Airborne Wind Energy in the Utility Sector. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 26, pp. 643–662. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_26

40. Salma, V., Ruiterkamp, R., Kruijff, M., Paassen, M. van, Schmehl, R.: Current and Expected Airspace Regulations for Airborne Wind Energy Systems. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 29, pp. 703–725. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_29

41. Friedl, F.: Fault-Tolerant Design of a Pumping Kite Power Flight Control System. M.Sc.Thesis, Graz University of Applied Sciences & Delft University of Technology, 2015. http://resolver.tudelft.nl/uuid:e704e8aa-2371-437b-8de9-80b3b7067241 Accessed Oct 20, 2023
42. Friedl, F., Braun, L., Schmehl, R., Stripf, M.: Fault-Tolerant and Reliable Design of a Pumping Kite Power System. In: Book of Abstracts, EST, Energy Science Technology, International Conference & Exhibition, p. 101, Karlsruhe, Germany, May 20–22, 2015. doi: 10.5445/IR/1000044290
43. Perez Damas, C., Gozluklu, B.: Safety Analysis of Airborne Wind Energy Systems. In: Diehl, M., Leuthold, R., Schmehl, R. (eds.). Book of Abstracts of the International Airborne Wind Energy Conference, p. 104, Poster available from http://awec2017.com/images/posters/Poster_Reyes.pdf, Freiburg, Germany, Oct 5–6, 2017. doi: 10.6094/UNIFR/12994
44. Stoeckle, M. R.: Fault detection, isolation, and recovery for autonomous parafoils. M.Sc.Thesis, Massachusetts Institute of Technology, 2014. http://hdl.handle.net/1721.1/90612 Accessed Nov 3, 2023
45. Rapp, S., Schmehl, R., Oland, E., Haas, T.: Cascaded Pumping Cycle Control for Rigid Wing Airborne Wind Energy Systems. Journal of Guidance, Control, and Dynamics **42**(11), 2456–2473 (2019). doi: 10.2514/1.G004246
46. Rapp, S., Schmehl, R.: Vertical Takeoff and Landing of Flexible Wing Kite Power Systems. Journal of Guidance, Control, and Dynamics **41**(11), 2386–2400 (2018). doi: 10.2514/1.G003535
47. Thedens, P., Oliveira, G., Schmehl, R.: Ram-air kite airfoil and reinforcements optimization for airborne wind energy applications. Wind Energy **22**(5), 653–665 (2019). doi: 10.1002/we.2313
48. Eldeeb, H., Abdel-Khalik, A. S., Hackl, C. M.: Highly efficient fault-tolerant elelctrical drives for airborne wind energy systems. In: Diehl, M., Leuthold, R., Schmehl, R. (eds.). Book of Abstracts of the International Airborne Wind Energy Conference (AWEC 2017), pp. 75–77, Freiburg, Germany, Oct 5–6, 2017. http://resolver.tudelft.nl/uuid:d091e755-be2e-4056-81b1-ac29552908b2
49. Rapp, S., Schmehl, R.: Enhancing Resilience of Airborne Wind Energy Systems Through Upset Condition Avoidance. Journal of Guidance, Control, and Dynamics **44**(2), 251–265 (2021). doi: 10.2514/1.G005189
50. Airborne Wind Europe: Key Safety Principles for Operation of Experimental and Developmental Airborne Wind Energy Systems. Guideline, Apr 22, 2020. doi: 10.5281/zenodo.8427694
51. Houle, C., Petrick, K.: An introduction to the Specific Operations Risk Assessment (SORA) for Airborne Wind Energy, Airborne Wind Europe, Jan 25, 2021. doi: 10.5281/zenodo.7801830
52. Blom, H. A., Jiang, C., Grimme, W. B., Mitici, M., Cheung, Y. S.: Third party risk modelling of Unmanned Aircraft System operations, with application to parcel delivery service. Reliability Engineering & System Safety **214**, 107788 (2021)
53. Minderhoud, C.: Safety Evaluation of Kitepower Operations. (2021)
54. Petrick, K., Houle, C.: Safe Operation and Airspace Integration of Airborne Wind Energy Systems. White Paper, Airborne Wind Europe, Sept 23, 2023. doi: 10.5281/zenodo.7797227
55. Schmidt, H., Vries, G. de, Renes, R. J., Schmehl, R.: The Social Acceptance of Airborne Wind Energy: A Literature Review. Energies **15**(4), 1384 (2022). doi: 10.3390/en15041384
56. Salma, V., Friedl, F., Schmehl, R.: Improving Reliability and Safety of Airborne Wind Energy Systems. Wind Energy **23**(2), 340–356 (2019). doi: 10.1002/we.2433

57. Van der Vlugt, R., Peschel, J., Schmehl, R.: Design and Experimental Characterization of a Pumping Kite Power System. In: Ahrens, U., Diehl, M., Schmehl, R. (eds.) Airborne Wind Energy, Green Energy and Technology, Chap. 23, pp. 403–425. Springer, Berlin Heidelberg (2013). doi: 10.1007/978-3-642-39965-7_23
58. Van der Vlugt, R., Bley, A., Noom, M., Schmehl, R.: Quasi-Steady Model of a Pumping Kite Power System. Renewable Energy **131**, 83–99 (2019). doi: 10.1016/j.renene.2018.07.023
59. Kitepower, B.: https://kitepower.nl/tech/. Accessed Feb 5, 2019
60. Oehler, J., Schmehl, R.: Aerodynamic characterization of a soft kite by in situ flow measurement. Wind Energy Science **4**(1), 1–21 (2019). doi: 10.5194/wes-4-1-2019
61. Loyd, M.: Crosswind kite power. Journal of Energy **4**(3), 106–111 (1980). doi: 10.2514/3.48021
62. Folkersma, M., Schmehl, R., Viré, A.: Boundary layer transition modeling on leading edge inflatable kite airfoils. Wind Energy **22**(7), 908–921 (2019). doi: 10.1002/we.2329
63. Oehler, J., van Reijen, M., Schmehl, R.: Experimental investigation of soft kite performance during turning maneuvers. Journal of Physics: Conference Series **1037**(5), 052004 (2018). doi: 10.1088/1742-6596/1037/5/052004
64. Fechner, U., Schmehl, R.: Flight Path Planning in a Turbulent Wind Environment. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 15, pp. 361–390. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_15
65. Peschel, J., Breuer, J., Schmehl, R.: Kitepower - Commercializing a 100 kW Mobile Wind Energy System. In: Diehl, M., Leuthold, R., Schmehl, R. (eds.). Book of Abstracts of the International Airborne Wind Energy Conference, pp. 47–51, Presentation video recording available from: http://www.awec2017.com/presentations/johannes-peschel, Freiburg, Germany, Oct 5–6, 2017. doi: 10.6094/UNIFR/12994
66. Roschi, S.: Clean energy from high above. https://drive.tech/en/stream-content/high-altitude-wind-ernergy-from-kites. Accessed Dec 9, 2018
67. Bosman, R., Reid, V., Vlasblom, M., Smeets, P.: Airborne Wind Energy Tethers with High-Modulus Polyethylene Fibers. In: Ahrens, U., Diehl, M., Schmehl, R. (eds.) Airborne Wind Energy, Green Energy and Technology, Chap. 33, pp. 563–585. Springer, Berlin Heidelberg (2013). doi: 10.1007/978-3-642-39965-7_33
68. Fechner, U., Schmehl, R.: Model-Based Efficiency Analysis of Wind Power Conversion by a Pumping Kite Power System. In: Ahrens, U., Diehl, M., Schmehl, R. (eds.) Airborne Wind Energy, Green Energy and Technology, Chap. 14, pp. 249–269. Springer, Berlin Heidelberg (2013). doi: 10.1007/978-3-642-39965-7_14
69. Fechner, U., van der Vlugt, R., Schreuder, E., Schmehl, R.: Dynamic Model of a Pumping Kite Power System. Renewable Energy **83**, 705–716 (2015). doi: 10.1016/j.renene.2015.04.028
70. Fechner, U., Schmehl, R.: Design of a Distributed Kite Power Control System. In: Proceedings of the 2012 IEEE International Conference on Control Applications, pp. 800–805, Dubrovnik, Croatia, Oct 3–5, 2012. doi: 10.1109/CCA.2012.6402695
71. National Aeronautics and Space Administration (NASA): Software Safety Guidebook. NASA Technical Standard NASA-GB-8719.13. Appendix B, Washington, DC, Mar 31, 2004. https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/nasa-gb-8719.13.pdf Accessed Nov 3, 2023

72. Faggiani, P., Schmehl, R.: Design and Economics of a Pumping Kite Wind Park. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 16, pp. 391–411. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_16
73. Licitra, G., Koenemann, J., Bürger, A., Williams, P., Ruiterkamp, R., Diehl, M.: Performance assessment of a rigid wing airborne wind energy pumping system. Energy **173**, 569–585 (2019). doi: 10.1016/j.energy.2019.02.064
74. Jehle, C., Schmehl, R.: Applied Tracking Control for Kite Power Systems. Journal of Guidance, Control, and Dynamics **37**(4), 1211–1222 (2014). doi: 10.2514/1.62380
75. Crowe, D., Feinberg, A. (eds.): Design for Reliability. 1st ed. CRC Press (2001). doi: 10.1201/9781420040845
76. Birolini, A.: Reliability Engineering – Theory and Practice. 8th ed. Springer, Berlin Heidelberg (2017). doi: 10.1007/978-3-662-54209-5
77. Peeters, J., Basten, R., Tinga, T.: Improving failure analysis efficiency by combining FTA andFMEA in a recursive manner. Reliability Engineering and System Safety **172**, 36–44 (2018). doi: 10.1016/j.ress.2017.11.024
78. Wikipedia contributors: Failure mode and effects analysis — Wikipedia, The Free Encyclopedia. [Online; accessed 15-August-2024], 2024. https://en.wikipedia.org/w/index.php?title=Failure_mode_and_effects_analysis&oldid=1237595238
79. Ruijters, E., Stoelinga, M.: Fault Tree Analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review **15–16**, 29–62 (2015). doi: 10.1016/j.cosrev.2015.03.001
80. Daniels, D.: Are we there yet? A Practitioner's View of DO-178C/ED-12C. In: Dale, C., Anderson, T. (eds.) Advances in Systems Safety, pp. 293–313. Springer, London (2011). doi: 10.1007/978-0-85729-133-2_17
81. Barringer & Associates, Inc: Reliability Learning Forever. https://edu.nl/ud96w. Accessed Apr 7, 2024
82. Rauzy, A.: New algorithms for fault trees analysis. Reliability Engineering & System Safety **40**(3), 203–211 (1993). doi: 10.1016/0951-8320(93)90060-C
83. Salma, V., Schmehl, R.: Flight Anomaly Detection for Airborne Wind Energy Systems. Journal of Physics: Conference Series **1618**(3), 032021 (2020). doi: 10.1088/1742-6596/1618/3/032021
84. Olive, X.: FDI (R) for satellites: How to deal with high availability and robustness in the space domain. International Journal of Applied Mathematics and Computer Science **22**(1), 99–107 (2012). doi: 10.2478/v10006-012-0007-8
85. Isermann, R.: Supervision, fault-detection and fault-diagnosis methods-an introduction. Control engineering practice **5**(5), 639–652 (1997). doi: 10.1016/S0967-0661(97)00046-4
86. Frank, P. M.: Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results. Automatica **26**(3), 459–474 (1990). doi: 10.1016/0005-1098(90)90018-D
87. Mamdani, E. H., Assilian, S.: An experiment in linguistic synthesis with a fuzzy logic controller. In: Dubois, D., Prade, H., Yager, R. R. (eds.) Readings in Fuzzy Sets for Intelligent Systems, pp. 283–289. Morgan Kaufmann (1993). doi: 10.1016/B978-1-4832-1450-4.50032-8
88. Mamdani, E., Assilian, S.: An experiment in linguistic synthesis with a fuzzy logic controller. International Journal of Man-Machine Studies **7**(1), 1–13 (1975). doi: https://doi.org/10.1016/S0020-7373(75)80002-2

89. Clothier, R. A., Palmer, J. L., Walker, R. A., Fulton, N. L.: Definition of airworthiness categories for civil unmanned aircraft systems (UAS). In: Proceedings of the 27th International Congress of the Aeronautical Sciences, (2010). http://www.icas.org/ICAS_ARCHIVE/ICAS2010/PAPERS/177.PDF Accessed Nov 20, 2023

90. European Parliament and Council of the European Union: Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 Feb 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, Feb 20, 2008. http://eur-lex.europa.eu/eli/reg/2008/216/2013-01-29 Accessed Nov 20, 2023

91. European Commission: Commission Regulation (EU) No 748/2012 of 3 Aug 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations, Aug 3, 2012. http://eur-lex.europa.eu/eli/reg/2012/748/oj

92. Federal Aviation Administration (FAA): Aeronautical Information Manual. Official Guide to Basic Flight Information and ATC Procedures. (2015). http://www.faa.gov/air_traffic/publications/media/AIM.pdf Accessed Nov 20, 2023

93. Joint Authorities for Rulemaking on Unmanned Systems (JARUS). http://jarus-rpas.org/ (2017). Accessed Oct 1, 2017

94. Joint Authorities for Rulemaking of Unmanned Systems (JARUS): JARUS guidelines on Specific Operations Risk Assessment (SORA). Edition 2.0, 30-01-2019. http://jarus-rpas.org/wp-content/uploads/2023/07/jar_doc_06_jarus_sora_v2.0.pdf (2019). Accessed Dec 6, 2023

95. Croon, G. C. H. E. de, Groen, M. A., De Wagter, C., Remes, B., Ruijsink, R., Oudheusden, B. W. van: Design, aerodynamics and autonomy of the DelFly. Bioinspiration & Biomimetics **7**(2), 025003 (2012). doi: 10.1088/1748-3182/7/2/025003

96. Northrop Grumman: RQ-4 Block 40 Global Hawk. https://en.wikipedia.org/wiki/Northrop_Grumman_RQ-4_Global_Hawk. Accessed Apr 7, 2024

97. North Atlantic Treaty Organization (NATO): UAV Systems Airworthiness Requirements (USAR) for North Atlantic Treaty Organization (NATO) Military UAV Systems, NATO STANAG 4671 draft, 1st ed., Mar 2007

98. European Aviation Safety Agency (EASA): Certification Specifications for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes, EASA CS-23, Nov 14, 2003. https://www.easa.europa.eu/system/files/dfu/decision_ED_2003_14_RM.pdf Accessed Sept 24, 2015

99. North Atlantic Treaty Organization (NATO): Light Unmanned Aircraft Systems Airworthiness Requirements, NATO STANAG 4703 draft, 1st ed., Sept 2014

100. International Civil Aviation Organization (ICAO): Adoption of Amendment 6 to Annex 7, ICAO State Letter AN 3/1-12/9, Apr 4, 2012. https://www.icao.int/Meetings/UAS/Documents/Adoption%20of%20Amendment%206%20to%20Annex%207.pdf

101. International Civil Aviation Organization (ICAO): International Standards and Recommended Practices. Annex 2 – Rules of the Air, 10th ed., July 2005. https://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf

102. International Civil Aviation Organization (ICAO): Unmanned Aircraft Systems (UAS), ICAO Circular 328-AN/190, Apr 2012. https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

103. International Civil Aviation Organization (ICAO): Manual on Remotely Piloted Aircraft Systems (RPAS), ICAO 10019, Mar 2015

104. European Aviation Safety Agency (EASA): Airworthiness Certification of Unmanned Aircraft Systems (UAS), Policy Statement EASA E.Y013-01, Aug 25, 2009. https://www.easa.europa.eu/system/files/dfu/E.Y013-01_%20UAS_%20Policy.pdf

105. European Aviation Safety Agency: Equipment, Systems and Installations in Small Remotely Piloted Unmanned Systems (RPAS), EASA SC-RPAS.1309-01, July 2015. https://www.easa.europa.eu/system/files/dfu/SC-RPAS.1309-01_Iss01-public%20consultation.pdf Accessed July 24, 2015

106. European Aviation Safety Agency (EASA): Transposition of Amendment 43 to Annex 2 to the Chicago Convention on remotely piloted aircraft systems (RPAS) into common rules of the air, EASA NPA 2014-09, Apr 3, 2014. https://www.easa.europa.eu/system/files/dfu/NPA%202014-09.pdf

107. United States Government: Title 14 Code of Federal Regulations – Aeronautics and Space, http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title14/14tab_02.tpl Accessed May 29, 2016

108. Hayhurst, K. J., Maddalon, J. M., Morris, A. T., Neogi, N., Verstynen, H. A.: A Review of Current and Prospective Factors for Classification of Civil Unmanned Aircraft Systems. NASA TM-2014-218511, NASA Langley Research Center, Aug 2014. https://shemesh.larc.nasa.gov/people/jmm/NASA-TM-2014-218511.pdf

109. Federal Aviation Administration: Model Aircraft Operating Standards, FAA Advisory Circular 91-57, June 1, 1981. https://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf

110. University of Washington Technology Law and Public Policy Clinic: Domestic Drones – Technical and Policy Issues. Clinic Policy Report, University of Washington, School of Law, 2013, pp. 1–20. https://www.law.washington.edu/clinics/technology/reports/droneslawandpolicy.pdf

111. United States Congress: FAA Modernization and Reform Act of 2012. 112th Congress (2011–2012), House Resolution 658, Became Public Law No 112-95, Feb 2012. https://www.congress.gov/bill/112th-congress/house-bill/658

112. United States Next Generation Air Transportation System Joint Planning & Development Office: Unmanned Aircraft Systems (UAS) Comprehensive Plan, Washington, DC, USA, Sept 2013. https://www.faa.gov/about/plansreports/unmanned-aircraft-systems-uas-comprehensive-plan Accessed Sept 24, 2015

113. Federal Aviation Administration (FAA): Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, 1st ed., Nov 7, 2013. https://irp.fas.org/program/collect/uas_roadmap_2013.pdf

114. Federal Aviation Administration (FAA): Unmanned Aircraft Systems (UAS) Operational Approval, FAA N 8900.227, July 30, 2013. https://www.faa.gov/documentLibrary/media/Notice/N_8900.227.pdf Accessed Nov 20, 2023

115. Federal Aviation Administration (FAA), DOT.: Airborne Wind Energy Systems (AWES) Policy Statement. https://www.federalregister.gov/documents/2022/12/23/2022-27993/airborne-wind-energy-systems-awes-policy-statement. Accessed Aug 27, 2023

116. International Civil Aviation Organization (ICAO): International Standards and Recommended Practices. Annex 4 – Aeronautical Charts, 11th ed., July 2009

117. International Civil Aviation Organization (ICAO): International Standards and Recommended Practices. Annex 14, Vol. 1 – Aerodrome Design and Operations, 6th ed., July 2013

118. Vermillion, C., Glass, B., Rein, A.: Lighter-Than-Air Wind Energy Systems. In: Ahrens, U., Diehl, M., Schmehl, R. (eds.) Airborne Wind Energy, Green Energy and Technology, Chap. 30, pp. 501–514. Springer, Berlin Heidelberg (2013). doi: 10.1007/978-3-642-39965-7_30

119. European Aviation Safety Agency (EASA): Certification Specifications and Acceptable Means of Compliance for Tethered Gas Balloons, EASA CS-31TGB, July 1, 2013. https://www.easa.europa.eu/system/files/dfu/Annex%20to%20ED%20Decision%202013-011-R.pdf

120. European Parliament and Council of the European Union: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, May 17, 2006. http://eur-lex.europa.eu/eli/dir/2006/42/oj Accessed Nov 20, 2023

121. National Transportation Safety Board: In-Flight Breakup During Test Flight Scaled Composites SpaceShipTwo, N339SS, Near Koehn Dry Lake, California October 31, 2014. NTSB/AAR-15/02, Washington, DC, USA, July 28, 2015. https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1502.pdf Accessed Nov 20, 2023

122. Salma, V., Schmehl, R.: Operation Approval for Commercial Airborne Wind Energy Systems. Energies **16**(7) (2023). doi: 10.3390/en16073264

123. Zillmann, U., Bechtle, P.: Emergence and Economic Dimension of Airborne Wind Energy. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 1, pp. 1–25. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_1

124. International Renewable Energy Agency (IRENA): Offshore Renewables: An Action Agenda for Deployment, Abu Dhabi, 2021. https://www.irena.org/Publications/2021/Jul/Offshore-Renewables-An-Action-Agenda-for-Deployment Accessed Nov 3, 2023

125. Rapp, S., Schmehl, R.: Enhancing Resilience of Airborne Wind Energy Systems Through Upset Condition Avoidance. Journal of Guidance, Control, and Dynamics **44**(2), 251–265 (2020). doi: 10.2514/1.G005189

126. Koopman, P., Ferrell, U., Fratrik, F., Wagner, M.: A Safety Standard Approach for Fully Autonomous Vehicles. In: Romanovsky, A., Troubitsyna, E., Gashi, I., Schoitsch, E., Bitsch, F. (eds.). Computer Safety, Reliability, and Security, Chap. 26, pp. 326–332, Cham (2019). doi: 10.1007/978-3-030-26250-1_26

127. Eickhoff, J., Chintalapati, B., Stoecker, P., Kader, W. von, Traussnig, R., Sayer, C., Peel, R., Keynes, M.: The Flexible LEO Platform for Small Satellite Missions. In: Deutscher Luft- und Raumfahrtkongress 2018, Friedrichshafen, Germany (2018). doi: 10.25967/480157

128. National Aeronautics and Space Administration (NASA): The core Flight System (cFS). https://cfs.gsfc.nasa.gov. Accessed Aug 12, 2021

129. European Space Agency (ESA): SAVOIR-FDIR Working Group. https://savoir.estec.esa.int/SAVOIRFDIR.htm. Accessed Feb 1, 2023

130. Underwriters Laboratories partners: ANSI/UL 4600 Standard for Safety for the Evaluation of Autonomous Products, Aug 12, 2021. https://ul.org/UL4600

131. European Union Aviation Safety Agency (EASA): Specific Operations Risk Assessment (SORA). https://www.easa.europa.eu/en/domains/civil-drones-rpas/specific-category-civil-drones/specific-operations-risk-assessment-sora. Accessed Jan 29, 2023

132. Janik, P., Zawistowski, M., Fellner, R., Zawistowski, G.: Unmanned Aircraft Systems Risk Assessment Based on SORA for First Responders and Disaster Management. Applied Sciences **11**(12) (2021). doi: 10.3390/app11125364

133. Joint Authorities for Rulemaking of Unmanned Systems (JARUS): JARUS guidelines on SORA. Annex F Theoretical Basis for Ground Risk Classification and Mitigation. http://jarus-rpas.org/wp-content/uploads/2024/06/SORA-v2.5-Annex-F-Release.JAR_doc_29pdf.pdf (2024). Accessed Aug 15, 2024

134. Ancel, E., Capristan, F. M., Foster, J. V., Condotta, R. C.: Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM). In: 17th aiaa aviation technology, integration, and operations conference, p. 3273, (2017)

135. Bertrand, S., Raballand, N., Viguier, F., Muller, F.: Ground risk assessment for long-range inspection missions of railways by UAVs. In: 2017 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1343–1351, IEEE, (2017)

136. Cour-Harbo, A. la: Quantifying risk of ground impact fatalities for small unmanned aircraft. Journal of Intelligent & Robotic Systems **93**(1), 367–384 (2019)

137. Melnyk, R., Schrage, D., Volovoi, V., Jimenez, H.: A third-party casualty risk model for unmanned aircraft system operations. Reliability Engineering & System Safety **124**, 105–116 (2014)

138. Houle, C., Petrick, K.: Safe AWE Testing CONOPS Guidelines. Reference Document, Airborne Wind Europe, Jan 25, 2021. doi: 10.5281/zenodo.7799777

139. Airborne Wind Europe: Glossary. https://airbornewindeurope.org/glossary-2/. Accessed Mar 11, 2023

140. Joint Authorities for Rulemaking of Unmanned Systems (JARUS): JARUS guidelines on SORA - Annex A, Guidelines on collecting and presenting system and operation information for a specific UAS operation. http://jarus-rpas.org/wp-content/uploads/2023/10/jar_09_doc_JARUS_SORA_Annex_A_V1.0.pdf. Accessed Aug 16, 2021

141. Peschel, J.: Kitepower and the Journey Towards 24/7 Operation. In: Schmehl, R., Tulloch, O. (eds.) 8th international Airborne Wind Energy Conference (AWEC 2019): Book of Abstracts. http://resolver.tudelft.nl/uuid:5bea59d6-be63-46c6-aba5-d60967d7783b, Accessed Mar 1, 2023. University of Strathclyde, Glasgow, United Kingdom; Delft University of Technology, Delft, The Netherlands (2019)

142. Joint Authorities for Rulemaking of Unmanned Systems (JARUS): JARUS guidelines on SORA - Annex I, Glossary of Terms. http://jarus-rpas.org/wp-content/uploads/2023/10/jar_09_doc_JARUS_SORA_Annex_I_V1.0.pdf. Accessed Aug 16, 2021

143. Wikipedia, The Free Encyclopedia: Flight level. https://en.wikipedia.org/wiki/Flight_level (2021).

144. Wikipedia, The Free Encyclopedia: Mode C Veil. https://en.wikipedia.org/wiki/Mode_C_veil (2021).

145. Joint Authorities for Rulemaking of Unmanned Systems (JARUS): JARUS guidelines on SORA - Annex C, Strategic Mitigation Collision Risk Assessment. http://jarus-rpas.org/wp-content/uploads/2023/07/jar_doc_06_jarus_sora_annex_c_v1.0.pdf. Accessed Aug 16, 2021

146. Iris Automation: Detect-and-Avoid Drone Collision Avoidance System. https://www.irisonboard.com/casia/. Accessed Dec 6, 2023

147. Echeverri, P., Fricke, T., Homsy, G., Tucker, N., on behalf of the Makani team: The Energy Kite Selected Results from the Design, Development and Testing of Makani's Airborne Wind Turbines Part III, Technical Artifacts. https://storage.googleapis.com/x-prod.appspot.com/files/Makani_TheEnergyKiteReport_Part3.pdf (2020). Accessed Feb 10, 2021

148. Makani Technologies LLC: 20171116 RPX-07 - Testing Faired Bridles on Makani M600 in Crosswind Flight [Full Flight]. https://archive.org/details/20171116-rpx-07-camera-7-bridle-point. Accessed Feb 10, 2021

149. Echeverri, P., Fricke, T., Homsy, G., Tucker, N., on behalf of the Makani team: The Energy Kite Selected Results From the Design, Development and Testing of Makani's Airborne Wind Turbines Part I. https://storage.googleapis.com/x-prod.appspot.com/files/Makani_TheEnergyKiteReport_Part1.pdf (2020). Accessed Feb 10, 2021

150. Makani Technologies LLC: 20180410 RPX-09 - Mid-Air Break Up of Makani M600 During Crosswind Flight [Excerpt]. https://archive.org/details/20180410-go-pro-11-bridle-knot-for-audacious-all-hands. Accessed Feb 10, 2021

151. Makani Technologies LLC: 20190808 FCW-01 - Offshore - End of Flight Zoom View Makani M600 [Excerpt]. https://archive.org/details/20190808-zoom-end-of-flight-trim-with-bleeps. Accessed Oct 31, 2023

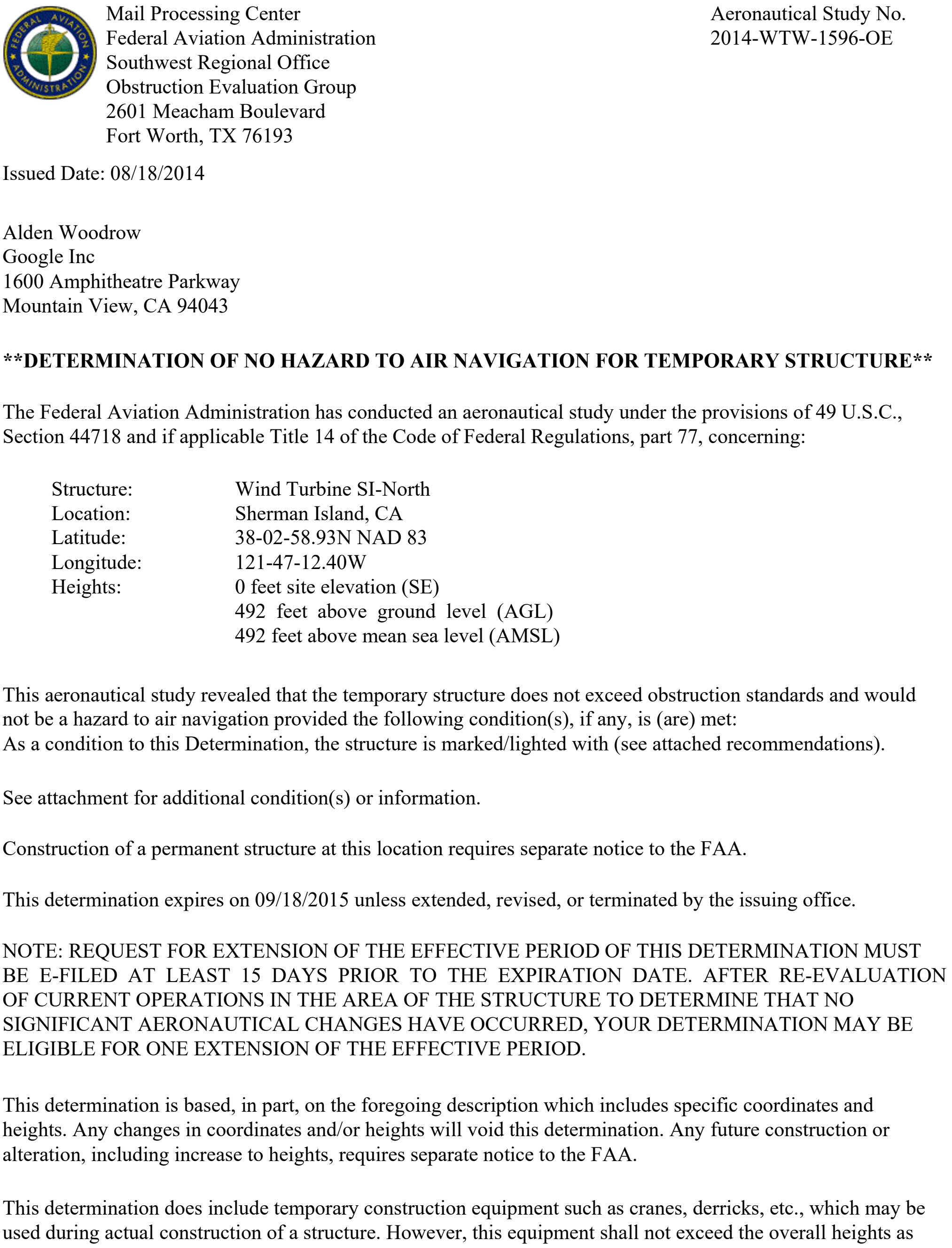
152. Bruinzeel, L., Klop, E., Brenninkmeijer, A., Bosch, J.: Ecological Impact of Airborne Wind Energy Technology: Current State of Knowledge and Future Research Agenda. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 28, pp. 679–701. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_28

A

APPENDIX A

Correspondence between The Federal Aviation Authority (FAA) and Makani Power regarding the conditional flying permit [147].

AA Temporary Determination of No Hazard



Mail Processing Center
Federal Aviation Administration
Southwest Regional Office
Obstruction Evaluation Group
2601 Meacham Boulevard
Fort Worth, TX 76193

Aeronautical Study No.
2014-WTW-1596-OE

Issued Date: 08/18/2014

Alden Woodrow
Google Inc
1600 Amphitheatre Parkway
Mountain View, CA 94043

****DETERMINATION OF NO HAZARD TO AIR NAVIGATION FOR TEMPORARY STRUCTURE****

The Federal Aviation Administration has conducted an aeronautical study under the provisions of 49 U.S.C., Section 44718 and if applicable Title 14 of the Code of Federal Regulations, part 77, concerning:

Structure:	Wind Turbine SI-North
Location:	Sherman Island, CA
Latitude:	38-02-58.93N NAD 83
Longitude:	121-47-12.40W
Heights:	0 feet site elevation (SE) 492 feet above ground level (AGL) 492 feet above mean sea level (AMSL)

This aeronautical study revealed that the temporary structure does not exceed obstruction standards and would not be a hazard to air navigation provided the following condition(s), if any, is (are) met:
As a condition to this Determination, the structure is marked/lighted with (see attached recommendations).

See attachment for additional condition(s) or information.

Construction of a permanent structure at this location requires separate notice to the FAA.

This determination expires on 09/18/2015 unless extended, revised, or terminated by the issuing office.

NOTE: REQUEST FOR EXTENSION OF THE EFFECTIVE PERIOD OF THIS DETERMINATION MUST BE E-FILED AT LEAST 15 DAYS PRIOR TO THE EXPIRATION DATE. AFTER RE-EVALUATION OF CURRENT OPERATIONS IN THE AREA OF THE STRUCTURE TO DETERMINE THAT NO SIGNIFICANT AERONAUTICAL CHANGES HAVE OCCURRED, YOUR DETERMINATION MAY BE ELIGIBLE FOR ONE EXTENSION OF THE EFFECTIVE PERIOD.

This determination is based, in part, on the foregoing description which includes specific coordinates and heights. Any changes in coordinates and/or heights will void this determination. Any future construction or alteration, including increase to heights, requires separate notice to the FAA.

This determination does include temporary construction equipment such as cranes, derricks, etc., which may be used during actual construction of a structure. However, this equipment shall not exceed the overall heights as indicated above. Equipment which has a height greater than the studied structure requires separate notice to the FAA.

This determination concerns the effect of this temporary structure on the safe and efficient use of navigable airspace by aircraft and does not relieve the sponsor of compliance responsibilities relating to any law, ordinance, or regulation of any Federal, State, or local government body.

Any failure or malfunction that lasts more than thirty (30) minutes and affects a top light or flashing obstruction light, regardless of its position, should be reported immediately to (877) 487-6867 so a Notice to Airmen (NOTAM) can be issued. As soon as the normal operation is restored, notify the same number.

A copy of this determination will be forwarded to the Federal Aviation Administration Flight Procedures Office if the structure is subject to the issuance of a Notice To Airman (NOTAM).

If you have any questions, please contact our office at (816) 329-2525. On any future correspondence concerning this matter, please refer to Aeronautical Study Number 2014-WTW-1596-OE

Signature Control No: 210250986-227234966 (TMP -WT)
Donna O'Neill
Specialist

Attachment(s)
Additional Information
Map(s)

AA Temporary Determination of No Hazard

Additional information for ASN 2014-WTW-1596-OE

The project consists of the four corners of an area that will be used to operate an Airborne Wind Energy System (AWES) that would be located approximately 9.47-9.62 nautical miles (NM) southwest of the Rio Vista Municipal Airport (O88), Rio Vista, CA, at a site known as Sherman Island. Sherman Island is located in the Sacramento River near Suisun Bay. This area is a VFR (Visual Flight Rules) flyway for fixed and rotary wing aircraft between the San Francisco Bay area and the San Joaquin Valley. The four corner of this area have been studied under Aeronautical Study No. 2014-WTW-1596 through 1599-OE. The AWES does not exceed any 14 CFR Part 77 obstruction standard. However, due to its operating height and special characteristics the following conditions apply during its operations.

1) The proponent shall ensure that a Notice to Airmen (NOTAM) is issued each time prior to the beginning of operations and shall be cancelled each time when operations end. The NOTAM should include the latitude/longitude, radial, and distance from Scaggs Island (SDG) VORTAC and Sacramento (SAC) VORTAC, and the operating area including radius distance from center point and maximum altitude (AMSL) of the vehicle. For NOTAM purposes the vehicle should be referred to as an Airborne Wind Energy System (AWES).

2) The lighting and marking plan for the proposed AWES at Sherman Island will be considered preliminary/temporary as part of a research and development effort with the FAA's Airport Technology R&D Branch, ANG-E26. As part of this effort, the FAA will be working with the developer to determine the optimal marking and lighting techniques for AWESs, and adopt these findings as a national standard. For this determination, the AWES should be marked and lighted (for daytime operation) as follows:

Marking: The AWES should be painted and/or marked with areas of contrasting colors that will provide sufficient contrast against terrain and the sky. High-visibility orange or high visibility green may be suitable colors. The ground station should be marked with white paint to provide contrast against terrain. The tether, at this time, does not require any marking.

Lighting: The AWES should be lighted with high-output white strobe lights, mounted on the wing tips, programmed to flash when the AWES reaches its highest and lowest points when in orbit. When the AWES is not in orbit and is in straight flight, the high-output white strobe lights should flash at 30 flashes per minute until it is either docked at the ground station or enters into orbit. The ground station should be equipped with a FAA Type L-865 white strobe light that will be programmed to flash in unison with the wing-tip lights of the AWES. The tether, at this time, does not require any lighting.

Daytime/Nighttime: At this time, details for nighttime lighting and marking have not been determined. Night time operations are prohibited. Further research will be needed to make that determination.

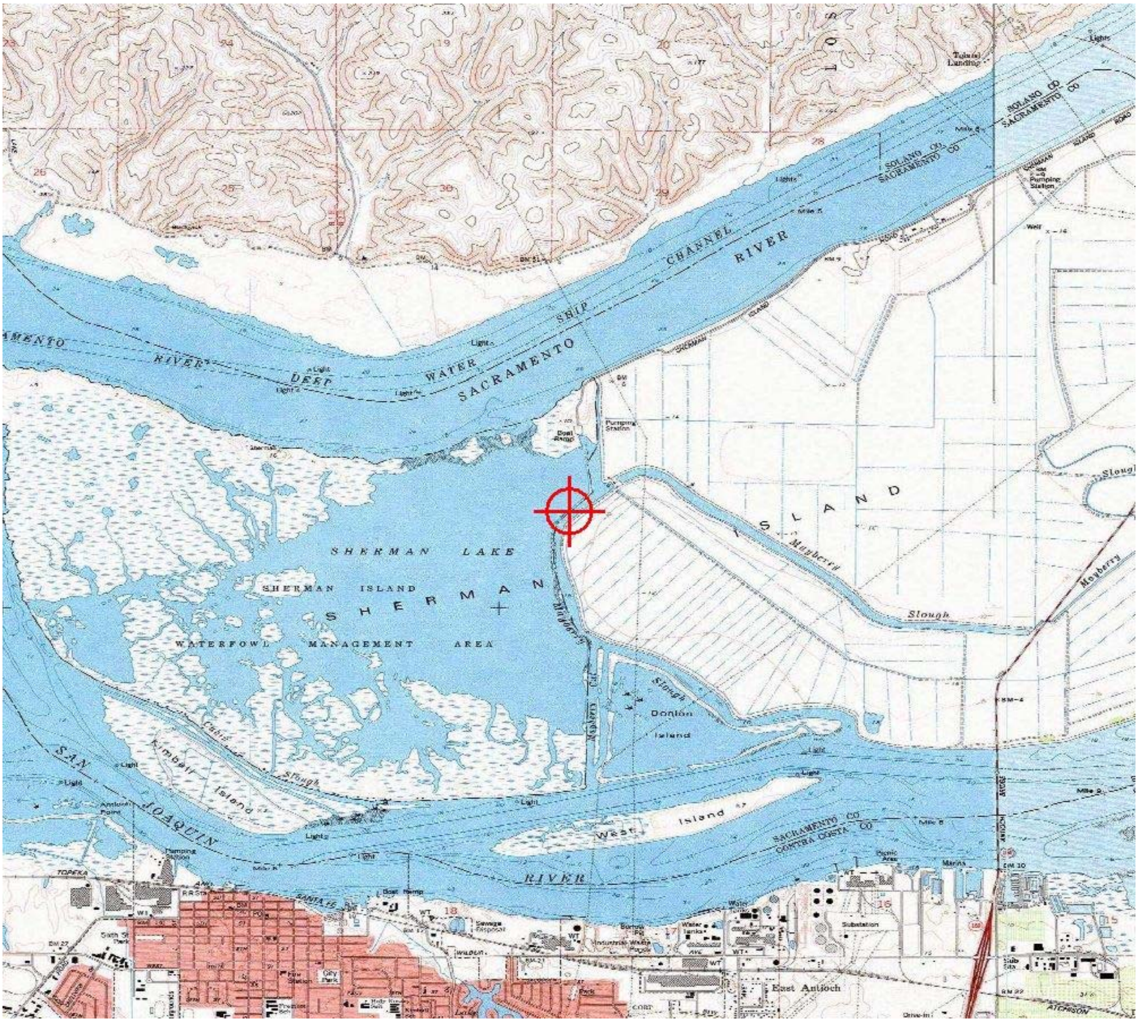
Duration of preliminary/temporary lighting and marking plan: This plan shall be valid for a period of one year. If at anytime during this period the FAA determines that the preliminary/temporary lighting and marking plan implemented under this determination is unsafe or that safety is being compromised due to insufficient lighting/marking, the operation of the AWES shall be suspended until a remedy is identified.

Light Outages: Due to the limited number of lights being utilized, operation of the AWES without all lights functioning is not permitted.

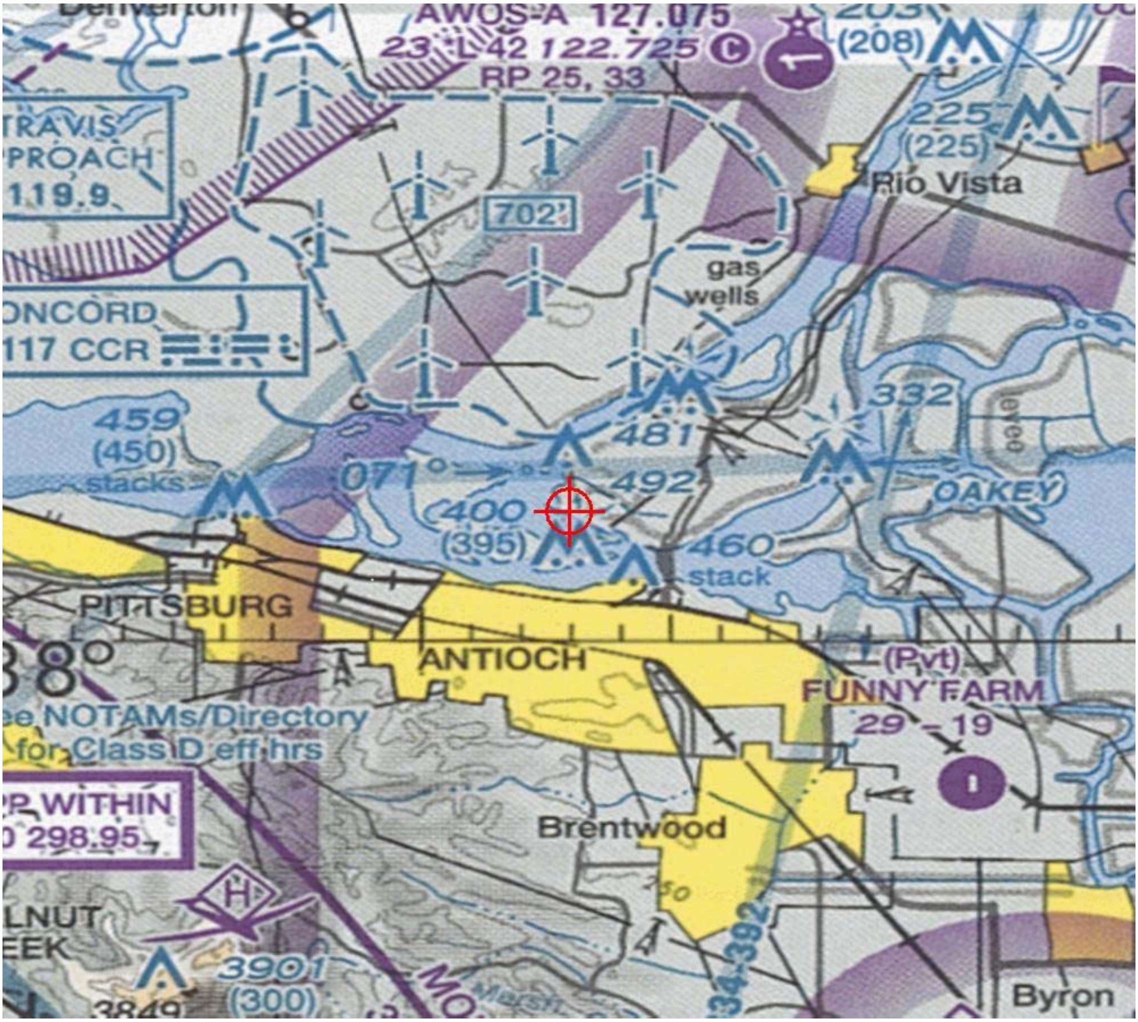
Research Provisions: The FAA Airport Technology R&D Branch may, at their discretion, request that the AWES, the ground station, or the tether be fitted with lighting and/or marking with different characteristics to assist with identifying the optimal technique for identifying AWESs. As part of this determination, the developer agrees to assist the FAA with this research and be as accommodating as possible, should such a request be received. It must be understood that the marking and lighting plan described in this determination is considered preliminary/temporary as part of a research and development effort. While the intent is to identify a final lighting and marking configuration during this research effort, the final configuration that will be described in FAA Advisory Circular 70/7460-1 (AC) may or may not be the same as described in this determination. Once a final marking and lighting configuration is made and identified in the AC, the developer understands that they may be required to change the existing, interim marking and lighting to be in accordance with the AC.

AA Temporary Determination of No Hazard

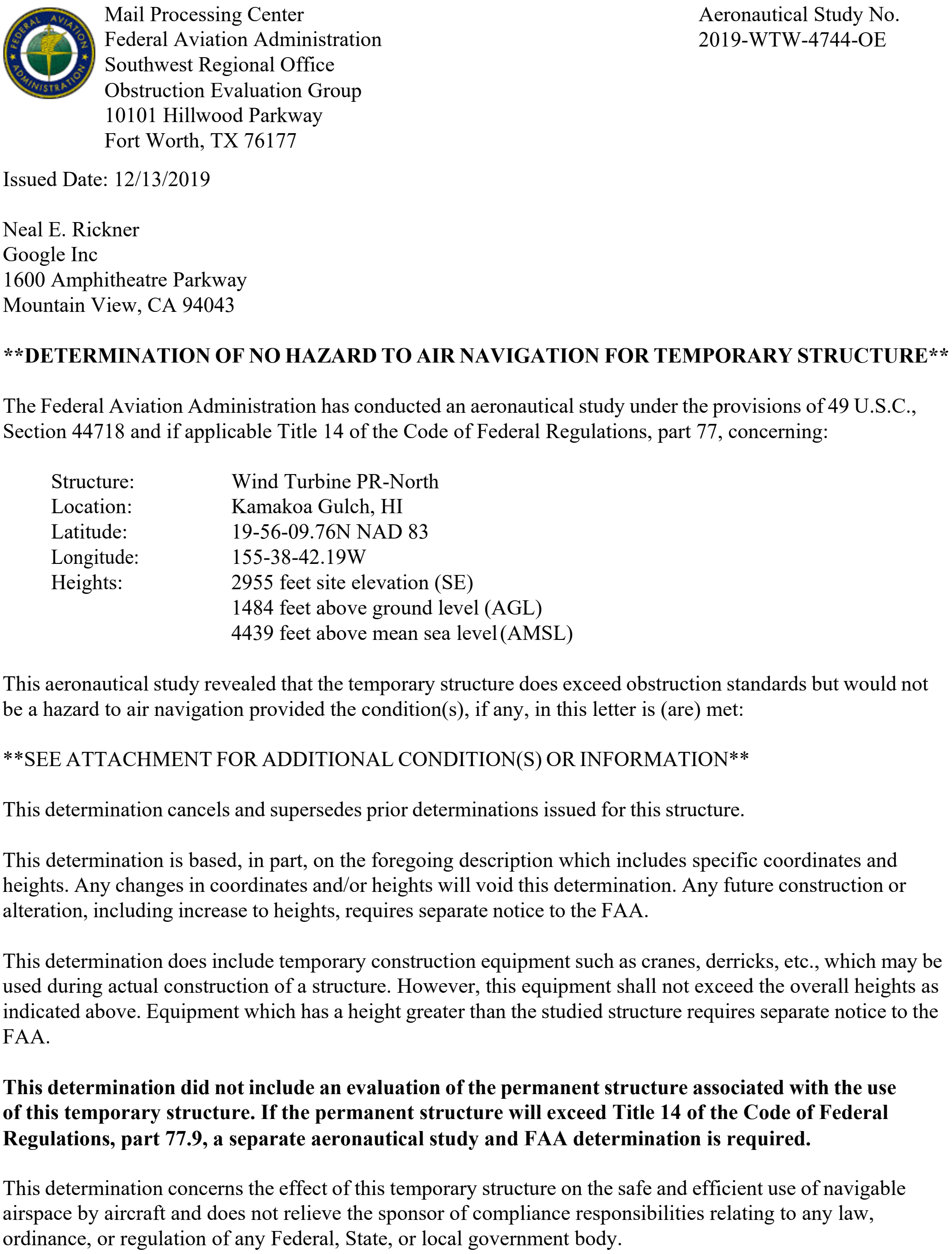
TOPO Map for ASN 2014-WTW-1596-OE



Sectional Map for ASN 2014-WTW-1596-OE



AA Temporary Determination of No Hazard



Mail Processing Center
Federal Aviation Administration
Southwest Regional Office
Obstruction Evaluation Group
10101 Hillwood Parkway
Fort Worth, TX 76177

Aeronautical Study No.
2019-WTW-4744-OE

Issued Date: 12/13/2019

Neal E. Rickner
Google Inc
1600 Amphitheatre Parkway
Mountain View, CA 94043

****DETERMINATION OF NO HAZARD TO AIR NAVIGATION FOR TEMPORARY STRUCTURE****

The Federal Aviation Administration has conducted an aeronautical study under the provisions of 49 U.S.C., Section 44718 and if applicable Title 14 of the Code of Federal Regulations, part 77, concerning:

Structure:	Wind Turbine PR-North
Location:	Kamakoa Gulch, HI
Latitude:	19-56-09.76N NAD 83
Longitude:	155-38-42.19W
Heights:	2955 feet site elevation (SE) 1484 feet above ground level (AGL) 4439 feet above mean sea level (AMSL)

This aeronautical study revealed that the temporary structure does exceed obstruction standards but would not be a hazard to air navigation provided the condition(s), if any, in this letter is (are) met:

SEE ATTACHMENT FOR ADDITIONAL CONDITION(S) OR INFORMATION

This determination cancels and supersedes prior determinations issued for this structure.

This determination is based, in part, on the foregoing description which includes specific coordinates and heights. Any changes in coordinates and/or heights will void this determination. Any future construction or alteration, including increase to heights, requires separate notice to the FAA.

This determination does include temporary construction equipment such as cranes, derricks, etc., which may be used during actual construction of a structure. However, this equipment shall not exceed the overall heights as indicated above. Equipment which has a height greater than the studied structure requires separate notice to the FAA.

This determination did not include an evaluation of the permanent structure associated with the use of this temporary structure. If the permanent structure will exceed Title 14 of the Code of Federal Regulations, part 77.9, a separate aeronautical study and FAA determination is required.

This determination concerns the effect of this temporary structure on the safe and efficient use of navigable airspace by aircraft and does not relieve the sponsor of compliance responsibilities relating to any law, ordinance, or regulation of any Federal, State, or local government body.

A copy of this determination will be forwarded to the Federal Aviation Administration Flight Procedures Office if the structure is subject to the issuance of a Notice To Airman (NOTAM).

If you have any questions, please contact our office at (816) 329-2526, or bill.kieffer@faa.gov. On any future correspondence concerning this matter, please refer to Aeronautical Study Number 2019-WTW-4744-OE

Signature Control No: 404837550-425249765 (TMP -WT)
Bill Kieffer
Specialist

Additional Condition(s) or Information for ASN 2019-WTW-4744-OE

Proposal: To construct and/or operate a(n) Wind Turbine to a height of 1484 feet above ground level, 4439 feet above mean sea level.

Location: The structure will be located 4.11 nautical miles south of MUE Airport reference point.

Part 77 Obstruction Standard(s) Exceeded and Aeronautical Impacts, if any:

Preliminary FAA study indicates that the above mentioned structure would:
have no effect on any existing or proposed arrival, departure, or en route instrument flight rules (IFR) operations or procedures.
have no physical or electromagnetic effect on the operation of air navigation and communications facilities.
have no effect on any airspace and routes used by the military.

Based on this aeronautical study, the structure would not constitute a substantial adverse effect on aeronautical operations or procedures because it will be temporary. The temporary structure would not be considered a hazard to air navigation provided all of the conditions specified in this determination are strictly met.

As a condition to this Determination, the structure is to be marked/lighted with See Additional Information.

Any failure or malfunction that lasts more than thirty (30) minutes and affects a top light or flashing obstruction light, regardless of its position, should be reported immediately to (877) 487-6867 so a Notice to Airmen (NOTAM) can be issued. As soon as the normal operation is restored, notify the same number.

This determination expires on 06/13/2020 unless extended, revised, or terminated by the issuing office.

NOTE: REQUEST FOR EXTENSION OF THE EFFECTIVE PERIOD OF THIS DETERMINATION MUST BE E-FILED AT LEAST 15 DAYS PRIOR TO THE EXPIRATION DATE. AFTER RE-EVALUATION OF CURRENT OPERATIONS IN THE AREA OF THE STRUCTURE TO DETERMINE THAT NO SIGNIFICANT AERONAUTICAL CHANGES HAVE OCCURRED, YOUR DETERMINATION MAY BE ELIGIBLE FOR ONE EXTENSION OF THE EFFECTIVE PERIOD.

Additional information for ASN 2019-WTW-4744-OE

THIS AMMENDED TEMPORARY DETERMINATION IS NOT ELIGIBLE FOR EXTENSION AND EXPIRES ON 06/13/2020.

The proposed temporary construction is an Airborne Wind Energy System (AWES) that consists of an airborne wind energy kite connected to a ground station by a 1500 foot tether (cable). The cable would allow the energy kite to maneuver within 1500 feet of the ground station depending upon the prevailing winds. The AWES would be located approximately 4.11 - 4.57 nautical miles south of the Waimea-Kohala airport (MUE), Kamuela, HI. The four corners of this operating area were submitted for study under aeronautical study numbers 2019-WTW-4744 through 2019-WTW-4748-OE. The height of the terrain underlying the AWES varies and the tether would restrict the AWES to a maximum height of 4439 feet above mean sea level within the operating area.

The temporary structure is identified as an obstruction under the standards of 14 CFR, part 77, as follows:

Section 77.17(a)(1): A height more than 499 feet above ground level (AGL). The proposed structure would exceed by the following amounts for each corner of the operating area.

2019-WTW-4744-OE / 985 feet
2019-WTW-4746-OE / 909 feet
2019-WTW-4747-OE / 908 feet
2019-WTW-4748-OE / 1001 feet

Section 77.17(a)(2): A height that is 200 feet AGL, or above the established airport elevation, whichever is higher, within 3 nautical miles of the established reference point of an airport, excluding heliports, with its longest runway more than 3,200 feet in actual length, and that height increases in the proportion of 100 feet for each additional nautical mile from the airport up to a maximum of 499 feet. The proposed structure would exceed by the following amounts for each corner of the operating area.

2019-WTW-4744-OE / 1173 feet
2019-WTW-4746-OE / 1067 feet
2019-WTW-4747-OE / 1051 feet
2019-WTW-4748-OE / 1173 feet

The AWES would be located on the edge of traffic pattern airspace for category D aircraft that may utilize the Waimea-Kohala airport. Category D aircraft are those aircraft with an approach speed of between 141-165 knots. Aeronautical study disclosed no known or forecasted category D aircraft conducting operations at the Waimea-Kohala airport. The AWES would be located outside traffic pattern airspace for all aircraft that would normally utilize the Waimea-Kohala airport.

Aeronautical study disclosed that the temporary structure would have no effect on any existing or proposed arrival, departure, or en route Instrument Flight Rules (IFR) operations or procedures.

Study for possible Visual Flight Rules (VFR) effect disclosed that the temporary structure would not have a substantial adverse effect on any existing or proposed arrival or departure VFR operations or procedures. It would not conflict with airspace required to conduct normal traffic pattern operations at Waimea-Kohala airport or any other known public use or military airports. Aeronautical study for VFR en-route effect

AA Temporary Determination of No Hazard

disclosed that it would be necessary for the AWES to be satisfactorily marked/lighted to ensure conspicuity so that aircraft could safely navigate around the structure.

Due to this being an initial introduction of an emerging technology to the National Airspace System, additional conditions and notification procedures must be necessary prior to operation of the Makani M600 Airborne Wind Energy System (AWES).

Weather requirements:

The weather requirement for operation of the AWES must be a ceiling/visibility minimum of 1,500 feet above ground level and 3 statute miles at the base station.

NOTAM requirements:

Notify the Kona Operations Center, (808)-329-1083 at least one hour prior to the beginning of operation and again when operation has suspended for the day so that a local Notice to Airmen (NOTAM) can be issued. Provide to the operations center the latitude/longitude, direction, and distance in nautical miles from Waimea-Kohala airport (PHMU) and the operating area including radius distance in feet from center point (groundstation). For NOTAM purposes the vehicle should be referred to as an "Airborne Wind Energy System."

The lighting and marking plan for the proposed AWES at Kamakoa Gulch/Parker Ranch will be considered preliminary/temporary as part of a research and development effort with the FAA's Airport Technology R&D Branch, ANG-E26, Obstruction Evaluation Group, and Flight Standards Service - Flight Procedure Standards Branch. As part of this effort, the FAA will be working with the developer to determine the optimal marking and lighting techniques for AWESs, and possibly adopt these findings as a national standard. For this determination, the AWES should be marked and lighted as follows:

Marking requirements:

The tether for the energy kite must be painted and/or marked with areas of contrasting colors that will provide sufficient contrast against terrain and the sky. Alternating 150 foot bands of aviation orange and white are chosen to be tested; however this recommendation remains preliminary and is subject to change based on the results of the final airborne conspicuity testing. The ground station should be marked with white paint to provide contrast against terrain. The wing on the kite for this test is overall painted white with orange and yellow painted wing tips.

Lighting requirements:

The energy kite must be lighted with four flashing white strobe lights that meet or exceed the photometric specifications of FAA approved aircraft anti-collision lights (specified in Title 14 CFR Part 23.1397), mounted on the wing tips and tail, as necessary to provide 360 degree visual coverage. The ground station must be equipped with an FAA Type L-865 white strobe light that will be programmed to flash in unison with the wing-tip lights of the energy kite. It is desirable that the strobes be adjustable during the test to determine if different flash rates, number of flashes or positions to flash in the orbit of the vehicle add to the vehicles conspicuity. The tether, at this time, does not require any lighting.

Light Outages: Due to the limited number of lights being utilized, operation of the airborne wind energy system without all lights functioning is not permitted.

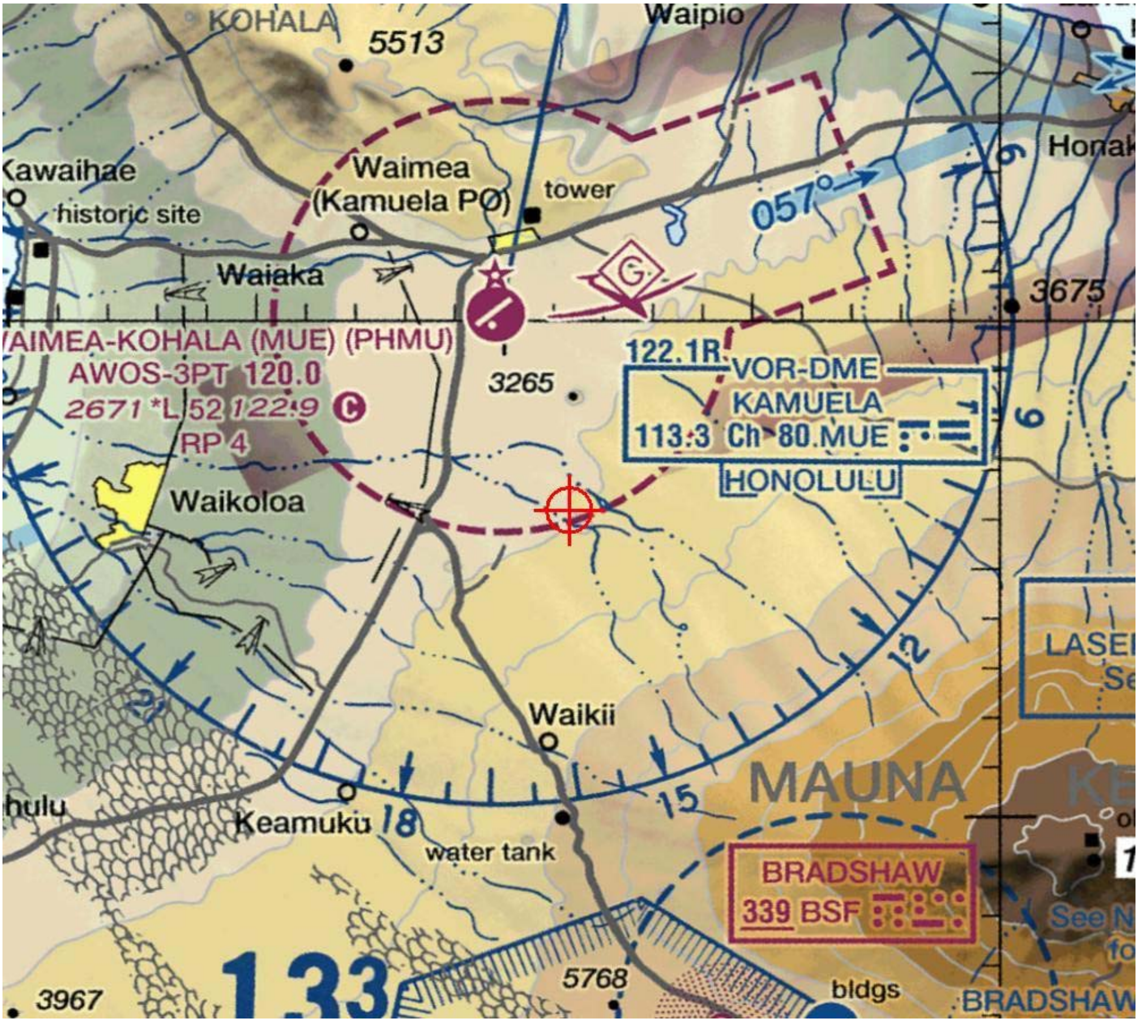
Research Provisions:

The FAA may, at their discretion, request that the AWES, the ground station, or the tether be fitted with lighting and/or marking with different characteristics to assist with identifying the optimal technique for identifying AWESs. As part of this determination, the developer agrees to assist the FAA with this research and be accommodating, should such a request be received. It must be understood that the marking and lighting plan described in this determination is considered preliminary/temporary as part of a research and development effort. While the intent is to identify a final lighting and marking configuration during this research effort, the final configuration that will be identified may or may not be the same as described in this determination. Once a final marking and lighting configuration is made the developer understands that they may be required to change the existing, interim marking and lighting.

The cumulative impact of the proposed temporary structure, when combined with other proposed and existing structures, is not considered to be significant. Study did not disclose any adverse effect on existing or proposed public-use or military airports or navigational facilities, nor would the proposal affect the capacity of any known existing or planned public-use or military airport.

Therefore, it is determined that the proposed temporary structure would not have a substantial adverse effect on the safe and efficient utilization of the navigable airspace by aircraft or on any air navigation facility and would not be a hazard to air navigation provided the conditions set forth in this determination are met.

Sectional Map for ASN 2019-WTW-4744-OE



B

APPENDIX B

B.1. AWES FLIGHT ANOMALY EXAMPLES

This appendix presents a few flight anomaly examples from two different AWE systems to show the observed reliability issues of current prototypes. Anomalies are categorized according to the source system component whose fault caused the anomaly. Kitepower's cases are refined from the test flights that took place between 2010 and 2015. Examples from Makani systems are taken from the resources that Makani has opened to the public after the company ended. Photo footage and video links are also provided as references when available.

B.1.1. FAILURES CAUSED BY TETHER FAULTS

FAILURE DUE TO WEAK LINK RUPTURE (KITEPOWER)

In one test, the weak link at the KCU broke, which is illustrated in Figure B.1. At the time of the test, the circular guide rail for the masthead was not yet available. Instead, the team used a straight tube mounted to the masthead to support the tether. The video footage shows that the tether entangles with this makeshift solution and suddenly snaps from the straight tube, leading to the overload. The debris visible in the large photo (C) originates from the progressive-tearing energy absorber that is integrated with the KCU to avoid an overload of the safety line. In this particular event, the bridle line system of the kite was damaged to such a degree that the wing curled up into a drag parachute-like structure [56]. The rupture of the weak link was an event that could be clearly identified in the data recording as well as in the photo and footage.

TETHER RUPTURE DURING THE FAIRING TEST (MAKANI: 16.11.2017)

Figure B.2 shows the incident during the tether and bridle fairings tests, high oscillation on the fairings, and then tether rupture, causing a crash. Video footage of the event is opened to the public [148]. The exact root cause of the failure is unclear in the available resources, but the team reports that they suspect shedding from stalled fairing that was misaligned.

Figure B.1: Experimental mast-based launch of the LEI V3 kite (A-B), breaking weak link due to a sudden overload (C) and descent of the damaged wing while being secured by the safety line (D-E) [56].

Figure B.2: Rupture of tether (left) causing a controlled crash (right) [148].

B.1.2. Failures caused by wing structure(including the bridle line system) faults

Failure due to wing collapse (Kitepower: 09.09.2010)

The test was conducted in Friesland, Netherlands, the Mutiny V2 kite model, as well as the 50 m^2 ram-air wings, were flown. During one of the flights with the V1 kite, the wing collapsed 9 minutes and 34 s after the launch and then slowly descended to the ground, which took about 40 s. The event was video recorded simultaneously from the wingtip and the swivel head. A sequence of video stills of the collapse from the perspective of the wing tip is shown in Figure B.3. While the left photo shows the nominal wing shape under aerodynamic load, the center photo shows a significant indentation of the wing due to relative flow impinging on the suction side of the wing. This aerodynamic compression force eventually leads to the buckling of the entire C-shaped wing, which, in this particular case, could not be reversed.

To counteract such a buckling of the entire wing, an additional transverse line was added to the bridle line system, connecting the two halves of the C-shaped wing. This stabilizer line is visible in Figs. B.4 (center) and B.4 (left).

Figure B.3: Collapse of the entire wing during reel-in, from the perspective of the wing tip video camera.

Figure B.4: Wing and bridle line system during a down loop figure eight maneuver performing a right turn (left) and following straight flight diagonally upwards (center) and during retraction of the kite (right). Video stills taken from the KCU [64].

B.1.3. FAILURES CAUSED BY GROUND STATION (INCLUDING THE SOFTWARE) FAULTS

FAILURE DUE TO WINCH REELING SPEED CONTROL SOFTWARE INCOMPETENCE (KITEPOWER: 11.03.2010)

In this early test flight at the former naval airbase Valkenburg, near Leiden, Netherlands, the tether ruptured at the kite end while performing a crosswind flight maneuver. The kite power system was equipped with a Mutiny V1 kite and a radio-controlled improvised kite control unit. At the time, both kite and winch could only be controlled manually by two different operators, such that overload situations and flight anomalies occurred frequently. While data recording was not possible at this stage of development, the event was captured by the GoPro video camera mounted on the swivel head of the ground station. The tether ruptured 24 minutes and 10 seconds after launch while flying downwards during a figure-of-eight maneuver. Because the system was not yet equipped with a safety line and progressive-tearing energy absorber, the detached, highly-tensioned Dyneema® line lashed back towards the swivel head of the ground station into a wave-like shape before falling to the ground. This event, which is illustrated in Figure B.5, is characterized by a very short timescale, which is obvious from the fact that the fast-flying kite hardly moves during the backlash. The sudden drop of the tether force also jolted the ground station significantly, which can be seen in the video footage. The detached kite continued downward but was redirected into a gentle gliding descent.

Figure B.5: Backlash of the tether after rupture at the kite end. Video stills at 100 ms intervals.

To prevent future tether ruptures due to force peaks, the winch's control system is improved so that the reeling speed can be adjusted rapidly to keep the tether force within a specific range. To mitigate the effect of a tether rupture at the kite end, the safety system had been developed, consisting of a weak link, cable cutter, safety line, and energy absorber. The functioning of this safety system was demonstrated during a mast-based launch, illustrated in Figure B.1.

B.1.4. OTHER FAILURES

FAILURE DUE TO LOSS OF CONTROL (MAKANI: 10.04.2018)

For the Makani SN3 model, adding slats changed the center of gravity and the aerodynamic center of the main wing. These changes reduced the longitudinal and lateral static stability margins, in addition to open-loop stability. The control system was working to close the loop, but, especially in gusts, control surfaces were often saturated, leading to an open loop, marginally stable plant. Then, in test flight RPX-09, Makani Power lost their SN3 model. According to Makani's report [149], the main wing snapped in half in mid-air (Figure B.6), after a gust event which caused loss of control of the kite, leading to an uncontrolled and jerky return to the taut tether. Full video of the Mid-air break is available to the public [150].

LOSS OF KITE YM600-05 DUE TO LOSS OF ROLL ATTITUDE CONTROL (MAKANI: 08.08.2019)

In the course of Flight FCW-01, the autonomous flight controller encountered a sequence of critical events culminating in the loss of control over the kite's roll and yaw attitudes, ultimately resulting in the loss of the kite to the Atlantic Ocean. This occurrence transpired shortly after the kite's transition from a crosswind flight configuration to hover mode, specifically in preparation for the tether reel-in operation. During this phase known as "PrepTransformGsDown," the kite is in a specific mode to secure the tether while the Ground Station undertakes the transformation from the "crosswind tether anchoring" to the "reeling" configuration.

To attain this designated mode, the kite orchestrates a combination of altitude reduction and lateral translation. Approximately 22 s into this maneuver, the kite commenced experiencing challenges in countering the moment exerted by the bridle, leading to an inadvertent roll movement away from the tether. About 28 s into PrepTransformGsDown

Figure B.6: Mid-Air Break Up of Makani M600 During Crosswind Flight [150].

mode, the pilot took over control but could not successfully stabilize the kite B.7. A visual record of the flight's conclusion can be observed in the video titled "FCW-01 end of flight," [151].

According to Makani's detailed analysis [147] while some of the contributing factors leading to this incident were experienced in prior flights, their concurrent manifestation in FCW-01 resulted in a unique confluence that ultimately led to the loss of the kite. Furthermore, a distinctive factor contributing to the offshore operations in FCW-01 was the perturbation introduced by the motion of the buoy, which intermittently induced slackening of the tether during both the TransOut and PrepTransformGsDown phases.

BIRD STRIKE IMPACT (KITEPOWER: 23.06.2011)

Figure B.8 shows another anomaly which is caused by the rare situation of a bird, as part of a group of domestic pigeons (Columba livia domestica), impacting the tensioned tether, with the tether indenting and the bird recovering and continuing its flight. This anomaly does not cause a flight failure [152]. Important lessons learned from this event were that birds generally survive the impact with the tether, and that the impact is clearly visible and may be used for monitoring.

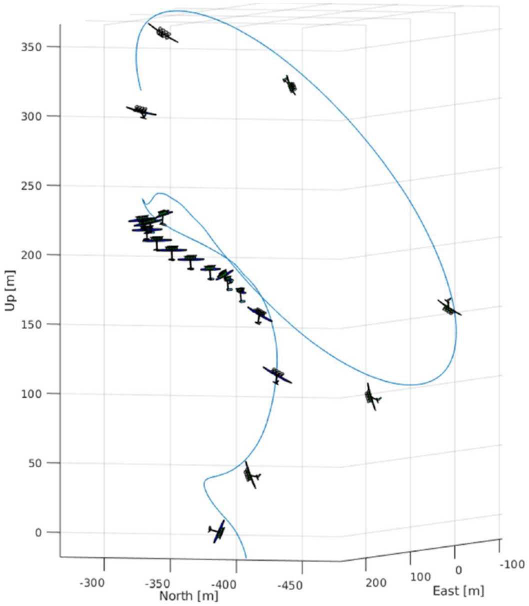


Figure B.7: The YM600-05's trajectory before the loss of the kite [147].

Figure B.8: Photo sequence capturing a bird impacting the tether: before the impact (left) and shortly after the impact (right). Photo: Max Dereta

ACKNOWLEDGEMENTS

It is a great honor for me to receive my Ph.D. degree from TU Delft. The excitement I felt upon being accepted into the faculty is still vivid in my memory.

Firstly, I would like to thank my promotor, Gerard van Bussel, for giving me the opportunity to conduct my research at his institute: Thank you very much for your always constructive feedback throughout my long Ph.D. journey.

Of course, the biggest thank goes to my supervisor, Roland Schmehl, a great mentor. Your support and encouragement were inspiring. Thank you very much for taking the time, despite your busy schedule, to solve all the challenges during the process. I hope our relationship continues after my graduation.

From the AWE industry side, I would like to thank Richard Ruiterkamp, Michael Kruijff, and Erik van Heide from Ampyx Power. They provided me a great working atmosphere at Ampyx. The AWE regulation chapter primarily focuses on Ampyx Power's experience. And for sure to Johannes Peschel, Joep Breuer and Bert Buchholz from Kitepower: They are always open to sharing their experience and data for the future of AWE technology. Many chapters in this work consist of data from the Kitepower system.

I want to dedicate this work to my family: My dear wife Yasemin, whose love and encouragement inspire me every day. My parents, Metin and Sevgi, for their wisdom, guidance, and unconditional love. My brother Serhat, who has been both a confidant and a friend. My sister Fatmanur, whose laughter brightens our lives. My brother-in-law Canberk, who brings joy and camaraderie. And our little Duru, whose innocence and curiosity remind us of life's simple pleasures. And soon, we eagerly await the arrival of our precious baby Luna, who will undoubtedly fill our hearts with even more love and joy.

Thank you all for being an integral part of my life.

Curriculum Vitæ

Volkan Salma

1985	Born in Kayseri, Turkey.

Education

2014–2024	Doctor of Philosophy (Ph.D.) degree in Aerospace Engineering Delft University of Technology
2009–2012	Master's degree in Computer Engineering Gazi University
2004–2008	Bachelor's degree in Electrical and Electronics Engineering Kırıkkale University

Experience

2017–Present	Flight Software Systems Engineer European Space Agency(ESA) - ESTEC, Noordwijk, The Netherlands
2016–2017	Software Engineer Dutch Ophthalmic Research Center, Zuidland, The Netherlands
2014–2016	Embedded Software Engineer Ampyx Power, The Hague, The Netherlands
2013–2015	Founder CVS System, Ankara, Turkey
2011–2014	Tactical UAV Program Flight Software Lead Vestel Defence, Ankara, Turkey
2008–2011	Research and Development Engineer KADE Vision, Ankara, Turkey

LIST OF PUBLICATIONS

1. Ruiterkamp, R., Salma, V., Kruijff, M.: Update on Certification and Regulations of Airborne Wind Energy Systems – The European Case for Rigid Wings. In: Schmehl, R. (ed.). Book of Abstracts of the International Airborne Wind Energy Conference 2015, pp. 78–79, Delft, The Netherlands, June 15–16, 2015. doi: 10.4233/uuid:7df59b79-2c6b-4e30-bd58-8454f493bb09

2. Salma, V., Friedl, F., Schmehl, R.: Systematic Reliability and Safety Analysis for Kite Power Systems. In: Diehl, M., Leuthold, R., Schmehl, R. (eds.). Book of Abstracts of the International Airborne Wind Energy Conference 2017, pp. 100–102, Freiburg, Germany, October 15–16, 2017. doi: 10.4233/uuid:4c361ef1-d2d2-4d14-9868-16541f60edc7

3. Salma, V., Ruiterkamp, R., Kruijff, M., Paassen, M. van, Schmehl, R.: Current and Expected Airspace Regulations for Airborne Wind Energy Systems. In: Schmehl, R. (ed.) Airborne Wind Energy – Advances in Technology Development and Research, Green Energy and Technology, Chap. 29, pp. 703–725. Springer, Singapore (2018). doi: 10.1007/978-981-10-1947-0_29

4. Salma, V., Friedl, F., Schmehl, R.: Improving Reliability and Safety of Airborne Wind Energy Systems. Wind Energy 23(2), 340–356 (2019). doi: 10.1002/we.2433

5. Salma, V., Schmehl, R.: Flight Anomaly Detection for Airborne Wind Energy Systems. Journal of Physics: Conference Series. (2020)

6. Salma V, Schmehl R. Operation Approval for Commercial Airborne Wind Energy Systems. Energies. 2023; 16(7):3264. doi:10.3390/en16073264