Received: 25 April 2019 | Revised: 6 August 2019 | Accepted: 3 October 2019
DOI: 10.1002/we.2433

WILEY

RESEARCH ARTICLE

Improving reliability and safety of airborne wind energy systems

Volkan Salma[1,2] | Felix Friedl[3] | Roland Schmehl[1]

[1]Faculty of Aerospace Engineering, Delft University of Technology, Delft, The Netherlands
[2]ESA-ESTEC, Noordwijk, The Netherlands
[3]Kitepower B.V., Delft, The Netherlands

Correspondence
Roland Schmehl, Faculty of Aerospace Engineering, Delft University of Technology, Kluyverweg 1, 2629 HS Delft, The Netherlands.
Email: r.schmehl@tudelft.nl

Present Address
Roland Schmehl, Faculty of Aerospace Engineering, Kluyverweg 1, 2629 HS Delft, The Netherlands

Funding information
EU H2020 ITN - Airborne Wind Energy System Modelling, Control and Optimisation (AWESCO), Grant/Award Number: 642682; EU H2020 FTIPilot - Resource Efficient Automatic Conversion of High-Altitude Wind (REACH), Grant/Award Number: 691173

Abstract

Airborne wind energy systems use tethered flying devices to harvest wind energy beyond the height range accessible to tower-based wind turbines. Current commercial prototypes have reached power ratings of up to several hundred kilowatts, and companies are aiming at long-term operation in relevant environments. As consequence, system reliability, operational robustness, and safety have become crucially important aspects of system development. In this study, we analyze the reliability and safety of a 100-kW technology development platform with the objective of achieving continuous automatic operation. We first outline the different components of the kite power system and its operational modes. In the next step, we identify failure modes, their causes, and effects by means of failure mode and effects analysis (FMEA) and fault tree analysis (FTA). Potentially hazardous situations and mechanisms which can render the system nonoperational are identified, and mitigation measures are proposed. We find that the majority of these measures can be performed by a failure detection, isolation, and recovery (FDIR) system for which we present a hierarchical architecture adapted from space industry.

KEYWORDS

airborne wind energy, fault detection, fault isolation, fault recovery, FDIR, FMEA, FTA, health monitoring, kite power, reliability, safety

1 | INTRODUCTION

The increasing need for renewable energy has led to a 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 because the wind power density generally increases with the distance from the ground, as a result of the wind shear.[2] On the other hand, the cost of larger 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, on the other hand, use tethered flying devices to harvest wind energy beyond the height range accessible to tower-based turbines.[4,5] The use of a tether allows the harvesting height to be adjusted continuously to optimize the availability of the wind resource. Compared with 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.[6] Of particular interest are deep-sea applications because a tower is in principle not needed for the operation of the system. The tether attaches to the ground station at sea level, which substantially reduces the structural loads and thus also the required material.[7,8] The lower material effort, 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.

However, the technology is operationally more complex than conventional wind turbines. Most implemented concepts rely on 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 as well as other users of the airspace is another important point. Yet, despite the differences between the various AWE concepts, the industry

The peer review history for this article is available at https://publons.com/publon/10.1002/we.2433

consensus is that safe and robust operation with a sufficient degree of autonomy is a prerequisite for successful market introduction and public acceptance.[9] The importance of demonstrating reliable long-term operation of airborne wind energy systems in a relevant wind environment has also been confirmed by a recently commissioned study for the European Commission.[10] To our knowledge, none of the commercial prototypes has been operated continuously more than a few days.

Reliability engineering provides several methods to systematically improve the availability and safety of complex technical systems.[11-13] Failure mode and effects analysis (FMEA) is a "bottom-up" analytical method that is used in the design phase to map and examine failures of individual components and to trace forward the potential effects on the performance of the entire system. FMEA is widely used in automotive and aerospace engineering as well as in many other domains. The method has also been adopted for wind turbines.[14] Fault tree analysis (FTA) is the reverse of FMEA, a "top-down" deductive analysis, aiming at the identification and analysis of conditions that lead to a particular system failure, commonly the catastrophic event. Failure detection, isolation, and recovery (FDIR) is a technique to monitor the system during operation, identify faults that occur, and pinpoint the type of fault and its location to isolate it and to take appropriate recovery actions.

Only few studies have addressed the reliability and safety of AWE systems. Kruiff and Ruiterkamp[15] 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[16] describe the aviation-related risks introduced by AWE systems and give an overview of existing and expected regulations for AWE systems. Stoeckle[17] proposes an FDIR approach for autonomous parafoils that resemble kites with suspended control unit. Friedl[18] and Friedl et al[19] 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[20] 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.[21] No study to date has offered a complete methodology on improving the safety and reliability level of AWE systems.

The present study proposes a systematic approach for AWE system development in order to reach the required reliability and safety levels. For this purpose, a set of requirements for an FDIR system is defined. These requirements are gathered by a reliability analysis using FMEA and FTA methods. The obtained requirements in fact mitigate the failure cases of the system. Although we present the methodology for a specific AWE system, the flexible-wing kite power system of Delft University of Technology and Kitepower B.V., it is generic and can be applied to different types of AWE systems. The paper is organized as follows. Section 2 outlines the functional components and modes of operation of the system. Section 3 describes the systematic safety assessment and improvement using FMEA and FTA, complementing this by an FDIR system as an integral part of the fault management strategy. In Section 4, the achieved results are presented, and Section 5 finalizes the study with conclusions.

2 | SYSTEM DESCRIPTION

In this section, we describe the technology demonstrator developed by Delft University of Technology and operated on a regular basis from 2010 to 2015.[22,23] This platform has been designed for pumping cycle operation of a lightweight flexible-membrane wing with an average traction power of 18 kW during reel-out of the tether. Depending on the kite used, this platform achieved a mechanical net power of up to 7 kW.[23] From 2016 onwards, the technology base has also been used as a starting point for the commercial development of a scaled-up version by the spin-off company Kitepower B.V.[24] The description mainly captures the development status at the time the technology was transferred to the commercial team. Since then, the development has progressed to second and even third component generations to accommodate the stepwise scaling of the system to an electrical net power of 100 kW. Important adaptations of the commercial development are included in the description.

2.1 | Functional components

The functional system components are illustrated in Figure 1. The traction force is generated by a flexible-membrane wing that is steered by a kite control unit (KCU). This remote-controlled cable robot is suspended in the rear bridle line system and also modulates the force level by

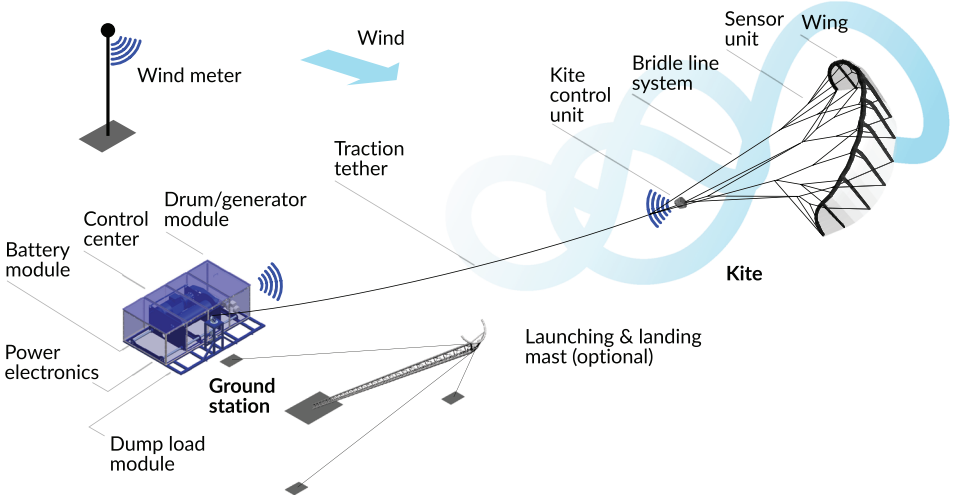

FIGURE 1 Components of the kite power system, equipped with a 18-kW ground station and 25 m^2 LEI V3 tube kite

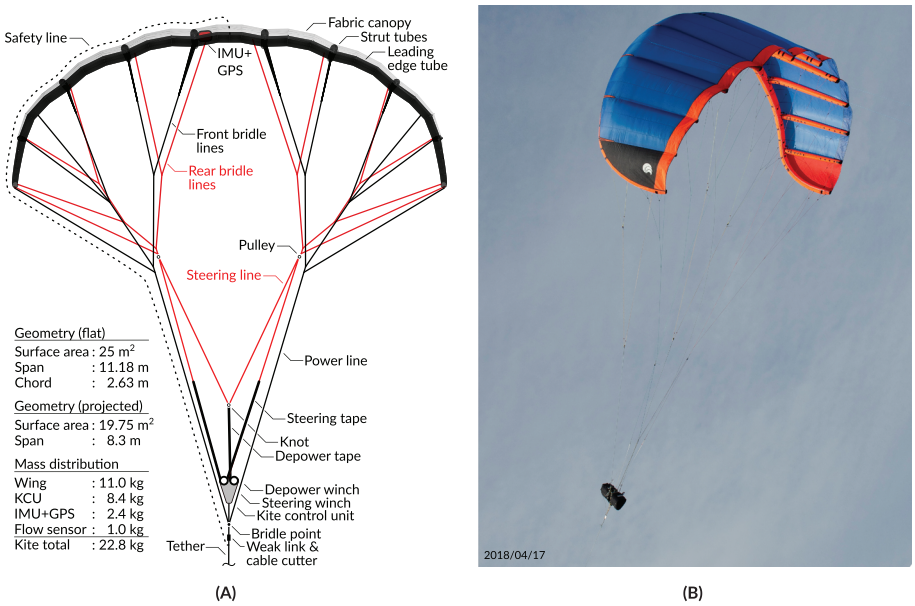

FIGURE 2 A, Front view of the LEI V3 kite[25]; B, Photo of the V5.40 with 40 m^2 wing surface area (courtesy of Kitepower B.V.)

adjusting the pitch angle of the wing. The airborne subsystem of wing, bridle line system, and KCU is denoted as kite and has been described in detail by Oehler and Schmehl.[25] The tether is deployed from the drum/generator module of the ground station. A continuous positive net power output of the system 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.[26] These figure-of-eight flight patterns are hinted in Figure 1. To reel in, the maneuvers are discontinued and the kite is depowered by pitching the wing to lower its angle of attack, which substantially reduces the traction force and the required energy to retract the kite. The part of the generated electrical energy that is used to retract the kite is buffered with a rechargeable battery. The described working principle crucially relies on active control of tether reeling and kite flight path. The individual components of the system are detailed in the following.

2.1.1 | Wing

As illustrated in Figures 1 and 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 tubes. The distributed aerodynamic load acting on the flying wing is 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 kite boarding. 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 has a substantial influence on the aerodynamic characteristics of the wing,[27] and on the other hand, the tubular frame defines the shape of the unloaded wing. During flight, the wing deforms substantially and its shape is mainly controlled by the geometry of the bridle line system. Next to its main 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 enable the kite to fly a turning maneuver.[28,29] A symmetric actuation, on the other hand, modulates the traction force by adjusting the pitch angle of the wing and by that its angle of attack. The degree of symmetric actuation is quantified by the depower setting. Because this also shifts the aerodynamic load in chordwise direction, the entire kite pitches around the bridle point.[25] The depicted LEI V3 kite with a 25-m^2 wing surface area can structurally support an aerodynamic load of up to 8 kN. The commercial development includes scaled wing prototypes of 25, 40, 60, and 100 m^2 surface area, with the aim to converge on a size below 80 m^2 for the 100-kW system. These kites use fabric materials with higher durability and ultraviolet (UV) coating for extended lifetime. Alternative designs without inflatable leading edge tube are also investigated.

2.1.2 | Bridle line system

The leading edge tube and the front sections of the strut tubes are supported by the front bridle lines. The left and right line branches transfer the major part of the aerodynamic load and connect to the left and right power lines, respectively. These bypass the KCU and attach directly to the tether at the bridle point. The trailing edge of the wing and its tips are supported by the rear bridle lines. The two line branches connect via pulleys to the two steering lines. Together with the steering and depower tapes that are deployed from the KCU, the two steering lines form two connected line loops that are used for asymmetric or symmetric actuation of the wing. The KCU is connected to the bridle point by a short line segment. Depending on the kite, the bridle line system may include additional pulleys at bridle split points to allow the line geometry to passively adjust to a varying load distribution and shape of the wing. Just below the bridle point, the tether incorporates a weak link and a separate cable cutter. While the weak link breaks at a predefined tether force to avoid overload and possible damage of the system, the cable cutter severs the tether in an emergency situation on command. In case of such a 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 normal operation, connecting the center of the leading edge tube directly with the tether below the weak link. With the bridle point separated from the tether, the kite is instantly depowered. The relatively heavy KCU swings below the wing, which can be retracted to the ground station in a stable payload flight configuration at fairly low flight speed.[17]

2.1.3 | Kite control unit

Central components of the KCU are the actuation drive trains comprising steering and depower motors, gearboxes, tape drums, and 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. Additionally, a direct manual remote control of the KCU can be established via a 2.4-GHz link. The on-board voltage of 11.6 V is provided by a rechargeable battery module. The KCU uses two onboard computers. A Micromint Electrum motherboard is used for tasks that are not too time-critical, like communications, while motor control is performed by a faster motherboard, developed at Delft University of Technology. All components are mounted in an aluminum chassis, enclosed by two watertight 5-mm high-density polyethylene (HDPE) covers, an additional foam padding, and a fabric outer hull. The commercial development includes second and third generation control units to meet the increased force levels of the 100-kW system.[30,31] These units are equipped with an airborne wind turbine to power all onboard systems.

2.1.4 | 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.[32] The tether is a major safety-critical system component. Because it is not redundant, it is designed according to a safe-life philosophy and has to be replaced when reaching a certain number of load cycles or a certain age. The tether of the commercial 100-kW system has a diameter of 14 mm and transfers a nominal traction force of 50 kN.

2.1.5 | 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 fixed transmission ratio. As shown in Figure 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 ground 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.

2.1.6 | Distributed sensor network

A network of distributed sensors is used to measure environmental conditions and operational parameters of the system.[23] However, only some of this information is required for automatic operation, some is for research and development purposes. We concisely describe here the sensor data that is useful for fault detection. The wind speed and direction 6 m above ground is 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 is equipped with potentiometers and temperature sensors for both the steering and depower motors; also, the battery voltage is measured and recorded. As illustrated in Figure 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 data that is misleading although the sensors actually work fine.

2.1.7 | Winch controller

The winch controller modulates the reeling speed of the tether to maximize the energy output and at the same time ensure 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[26] 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 an overloading of the system due to natural fluctuations of the wind speed, we use set values 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.[33,34]

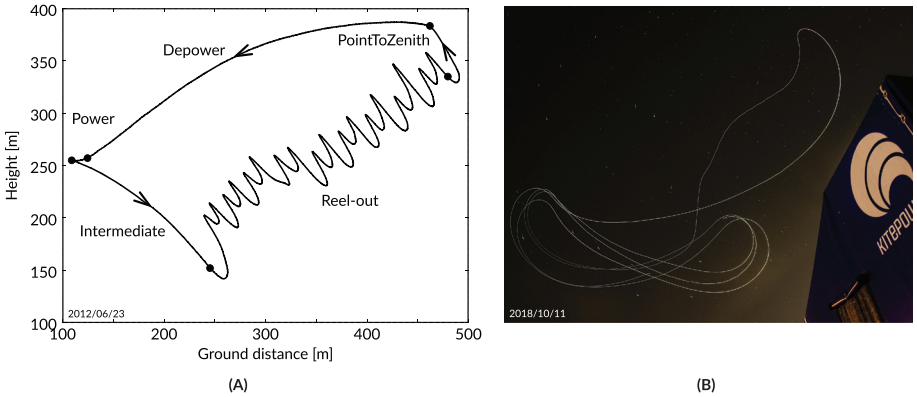

FIGURE 3 A, Side view of the measured flight path of a representative pumping cycle with indicated flight phases between switch points[18]; B, Photographic visualization of a pumping cycle during night operation by tracing a marker light on the kite from the ground station (right) using long-term exposure (courtesy of Kitepower B.V.)

2.1.8 | 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 the guidance or navigation controller of an aircraft. It is not involved in the actual steering of the kite but maps out the future system states, making use of the path and course controllers to reach those states. Thus, the flight path planner exercises control on pumping cycle level. The five individual flight phases of a pumping cycle are illustrated in Figure 3A. The flight phases correspond to specific system states: 'Rreel 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 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, and switching conditions are clearly defined. When reaching the switch criteria for a certain flight phase, the path planner updates the desired system state and by that 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 depower 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. In order to achieve the optimal pulling force in varying wind conditions, a measurement of the prevailing wind speed is used to calculate the desired elevation angle. The flight path controller has the authority to add a certain offset elevation to the fixed target points for optimizing 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[18] and the heading required to fly this course. The actual heading, estimated or measured, is then compared with the desired heading, and an anti-windup PID controller is used to minimize the error.

2.1.9 | 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 with the three computers in the ground station via wireless links. For this reason, an accurate timing of the communication between the distributed hardware components is of crucial importance. During early flight tests, we observed unstable control behavior when the latency between a measurement and the corresponding reaction of an actor exceeded 100 ms.[35] To address this, we chose a Linux tuned for low latency as main operating system. 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 which is transferred to the Micromint Electrum motherboard 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 the transport layer ZeroMQ.[36] This message library is easy to apply, supports the use of various programming languages, and its publish-subscribe pattern is well-suited for distributed designs. In combination with the flexible and straightforward serialization library Google Protocol Buffers,[37] the required time budget is met.

2.2 | 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 certain minimum wind speed, the cut-in speed, is exceeded. To maximize the net energy output and to ensure a safe operation of the system, the pumping operation is adjusted for 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

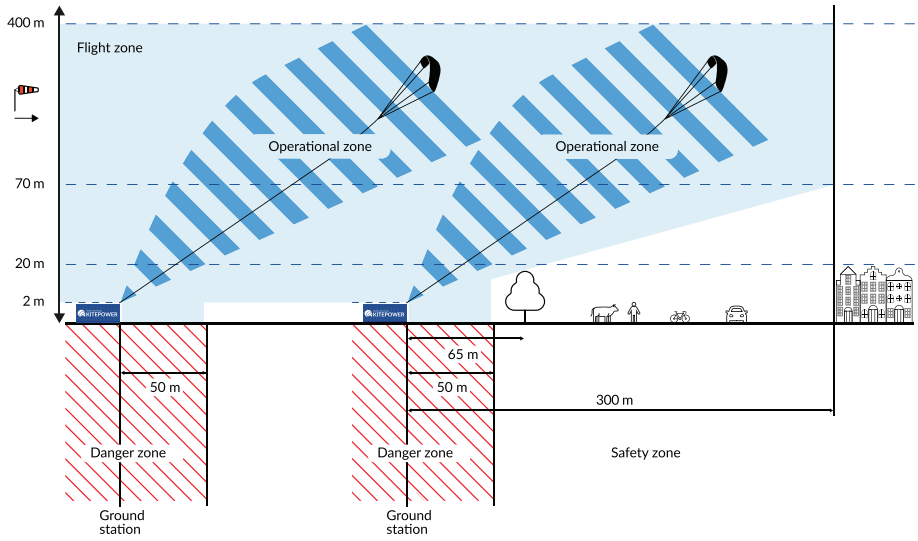

FIGURE 4 General spacial layout of pumping kite power systems (courtesy of Kitepower B.V.)

position. This parking mode can also be initiated in reaction 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 literature, we will adhere to the following terminology[38]: 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 the state of functioning different than aimed, and a mitigation measure is the action for reducing the severity or probability of an undesired event. The wind window is the 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; we first propose a zoning concept for pumping kite power systems and then detail the different modes of operation.

2.2.1 | Zoning concept

How the specific operation of two or more pumping kite power systems affects the use of airspace and land has been analyzed theoretically by Faggiani and Schmehl[39] for flexible wing systems and by Licitra[40] for rigid wing systems. The zoning concept for the commercial 100-kW system of Kitepower B.V. is depicted in Figure 4. The operational zone covers the volume swept by the kite and the tether during normal pumping cycle operation. The flight zone, on the other hand, covers the larger volume in which the kite and tether may fly during launching, landing, and parking. The zone also includes an additional safety margin to cover deviations from normal flight path. On the ground, the danger zone is accessible only to experienced personnel. In the surrounding safety zone, people, animals, or light transportation are allowed but there has to be an awareness of the flight operations above. Accordingly, the safety zone excludes busy roads, railways, or open water. It is important to consider that this zoning concept is only a first proposal that is based on a decade of operational experience with a single system. Especially the joint operation of multiple systems in a park configuration is 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.[16]

2.2.2 | Launching

The standard procedure to start-up 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. For the commercial system, the wing is retained by a ground anchoring system. 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.[22,41]

2.2.3 | 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 3A. As described in Section 2.1.8, the planned path is adjusted for each cycle depending on the expected wind resource.

2.2.4 | Restricted operation

Restricted operation is the only health state that allows pumping operation even after detecting a fault. The issued 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 in such a way that the load on the motors is reduced. This can be done, for example, by flying larger figure-of-eight maneuvers with larger turning radius.

2.2.5 | Parking

The kite is maneuvered into a parking position by terminating the crosswind maneuvers and steering the wing to point towards zenith. With the flight speed dropping to zero, also 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 system state PointToZenith that follows the reel-out phase of a pumping cycle, as described in Section 2.1.8. Temporarily parking the kite can be useful, for example, to avoid landing and relaunching in case of a passing thunderstorm. Parking can also be triggered by the FDIR system as a reaction to an anomaly. This obviously makes sense only for faults that can potentially cause a malfunction of the system, but not a failure. Because other than a failure, a malfunction disappears with time such that 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 of 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 level by covering a worst case of loosing the wireless connection to the control center.

2.2.6 | Immediate landing

Extensive loss of operational safety or other situations requiring repair or maintenance on the ground cause 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 make sure that tether forces stay well 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 certain other requirements are met, the kite adapts its depower setting and dives into the wind window, passing three waypoints. Figure 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 decent, the kite decelerates and eventually drops to the ground.

2.2.7 | Emergency landing

An emergency landing is initiated when the FDIR system diagnoses that the flight control system has lost steering authority. This 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.[42] To start the emergency landing, the cable cutter separates the KCU from the main tether. As consequence, the relatively heavy KCU, which is still attached to all bridle lines,

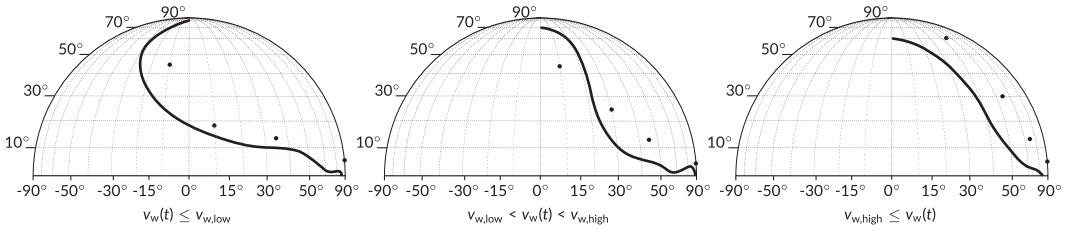

FIGURE 5 Landing paths of the kite on the flattened spherical coordinate plane for different wind speed ranges[18]

FIGURE 6 A and B, Experimental mast-based launch of the LEI V3 kite; C, breaking weak link due to a sudden overload; and D and E, descent of the damaged wing while being secured by the safety line

swings below the wing, such that the kite can now 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 2.1.2. An emergency landing can also be initiated passively by a breaking weak link, as illustrated in Figure 6, showing an early test of a mast-based launching system. At this stage of development, the response time of the winch controller was still insufficient and operation in a gusty wind environment could lead to temporary overload of the weak link.[35] The debris visible in the large photo is the remainder of a shock damper construction that is integrated with the KCU to avoid an overload of the safety line itself. 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.

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, we use FMEA together with FTA to assess and systematically improve the reliability and safety of the technology development platform described in Section 2. Because FMEA and FTA depend strongly on the mix of people who contribute to them, we have involved team members with different professional backgrounds, such as system design, operations, safety, legal, and finances, to ensure a high quality. As an integral part of the fault management strategy, we propose a FDIR system. The operation target for this reliability analysis is 1 week of flight without human intervention, except for launching and landing.

3.1 | Failure mode and effect analysis

The 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, as, for example, automotive engineering, for quality management to identify and overcome weak points already during the early design phases of a product. The highly structured approach assesses, one by one, all possible failure modes and their consequences for all system components. For each failure mode, the worst consequence is taken into account. For these failures with high severity or high probability, mitigation measures are proposed. However, the process considers only one failure at a time and 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.[43]

For the FMEA, the system is first divided into subsystems which are then broken down into components, as shown in Table 1. In the present study, we distinguish mechanical components, electronic hardware (HW) components, and software (SW) components. Software malfunctions (ie, wrong calculations, data corruption, and processing delays) and failures (ie, crash and not function at all) are investigated separately, while for other types of components, only failures are considered. Depending on the operation mode a failure mode can have different effects. Whenever this is the case, the failure mode is duplicated to investigate its effect for 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 investigated properties such as (a) the potential fault mode (software malfunction, software fault, hardware fault, wrong configuration, data corruption, or data delay), (b) causes and mechanisms, (c) the foreseeable sequence of post-failure events, (d) the hazardous situation, (e) the worst case harm (physical injury or damage to the health of people, or damage to property or the environment), (f) the corresponding severity and (g) probability, (h) the proposed mitigation measure, (9) the residual, post-mitigation worst case harm, (i) severity, and (j) probability. The probability definitions used in the analysis are listed in Table 2, while Table 3 lists the severity definitions and the associated global harm.

TABLE 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, and message forwarder software
Sensing system	Inertial measurement unit (IMU) communication software, IMU hardware, global positioning system (GPS) communication software, and GPS hardware
Actuation system	Steering motor hardware, depower motor hardware, motor driver microcontroller hardware, and 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, and microcontroller unit hardware
Onboard power system	Airborne wind turbine (AWT) hardware, maximum power point tracking hardware, batteries hardware, and power board hardware
Ground control system	System state controller software, ground state estimator software, winch control software, clock software, message forwarder software, and 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, and grid connection (optional)

TABLE 2 Probability definitions for the failure modes

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 3 Severity definitions and harm of the failure modes

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[a]	Maintenance
III	3	Minor, low damage, no injuries[b]	Harm to environment
IV	4	Moderate, moderate damage, injuries possible[c]	Financial loss Injury from fire, smoke, explosion (operator harm) Injury by tether (operator harm) Injury by tether (3rd person harm)
V	5	Critical[d]	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[e]	Injury by kite collision or crash (many people)[f]

[a]Only results in a maintenance action, noticed by alert customers.

[b]Affects very little of the system, noticed by average customers.

[c]Most customers are annoyed, mostly financial damage.

[d]Causes a loss of primary function; loss of all safety margins, severe damage, severe injuries, maximum one possible death.

[e]Product becomes inoperative; failure may result in complete unsafe operation and possible multiple deaths.

[f]Only possible if kite leaves the operation zone, which is also the top event for the FTA discussed in Section 3.2.

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

$$R = S \cdot P \tag{1}$$

and a proper assignment of these values is crucial for the risk evaluation of the specific failure mode. For this reason, the values for S and R are evaluated in close collaboration with the engineering team of Kitepower B.V. working on the 100-kW system.

In the next step, the investigated failure modes are prioritized based on the calculated risk numbers and corresponding mitigation measures proposed. Most of the failure modes can be mitigated by the FDIR system presented in Section 3.3. 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, we present the result of the FMEA and detail two specific failure modes as examples.

3.2 | Fault tree analysis

As mentioned in the previous section, an FMEA does not consider combined occurrences of failures and their effects. However, also faults with low individual risk factors can cause hazardous situations when occurring simultaneously. To take this into account, we complement the FMEA by an FTA.[43] The method has been developed in the 1960s for the analysis of a ballistic missile system and subsequently been applied in a broader context to analyze the risks related to safety and economically critical assets.[11,44] 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 level 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 state of the entire system. The top event corresponds to the particular system failure that is investigated. Commonly used are AND, OR, and conditional logic gates, while events are top, intermediate, and basic events as well as undeveloped and conditional events.[45] For quantitative failure analysis, the logic diagram is extended 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 operation phase or physical characteristics of the failure. Thus, the number of possible combinations of these failure modes is very large when considering the entire AWE system. 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 the 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 is 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, we define the catastrophic event as completely unsafe operation with possibly multiple deaths. 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,[16]
- crashing into a critical infrastructure on the ground,
- crashing on a highway and causing accidents, and
- crashing directly on many people in a crowded area.

Because of the severity of these consequences, we define the case of the kite leaving the operation zone as the top event (see also Table 3). We analyze only these events which bring the system to this specific top event. Crashes or other undesired events *within* the operation zone are not included in the FTA because their consequences are not considered as catastrophic. We create the fault tree and model component failures for the same operational target as for the FMEA, namely 1 week flight without any pilot intervention. The complete fault tree is depicted in Figure 7, with 31 different 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, we decided to not do this and instead assign integral probability models to both events. The parts of the fault tree highlighted in different colors are further detailed in Figures 8 to 11. The top event with one abstracted branch represented by a triangle symbol is shown in Figure 8. The intermediate event "malfunction in tether length control" is caused by any of the four events at lower level, ie, "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" cause the intermediate event "tether does not keep the kite in operation zone." If this occurs together with the condition "kite steering wrong or not existing," the top event "kite outside operation zone" is caused. Figures 9 to 11 show branches that are fully detailed, 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. 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

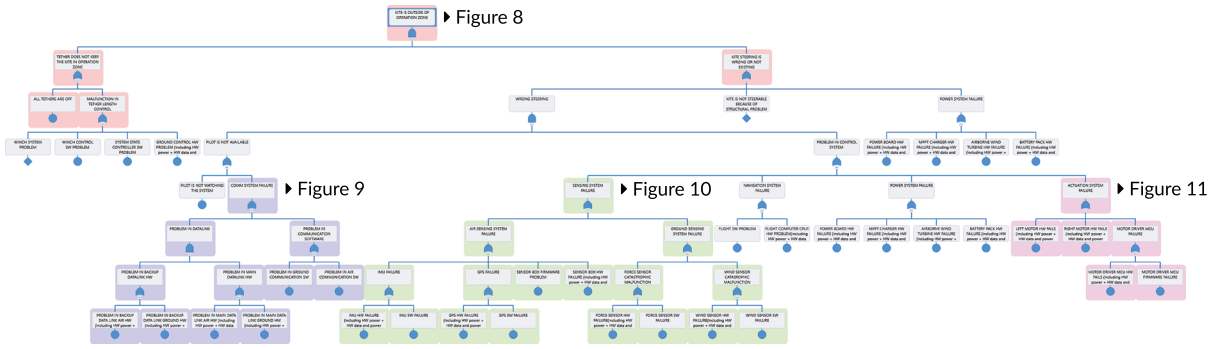

FIGURE 7 Complete fault tree (see Figure 8 for symbol legend)

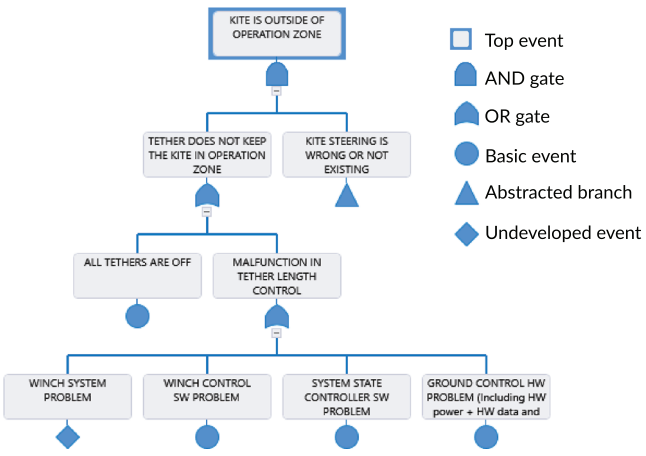

FIGURE 8 Fault tree for the top event "Kite is outside of operation zone"

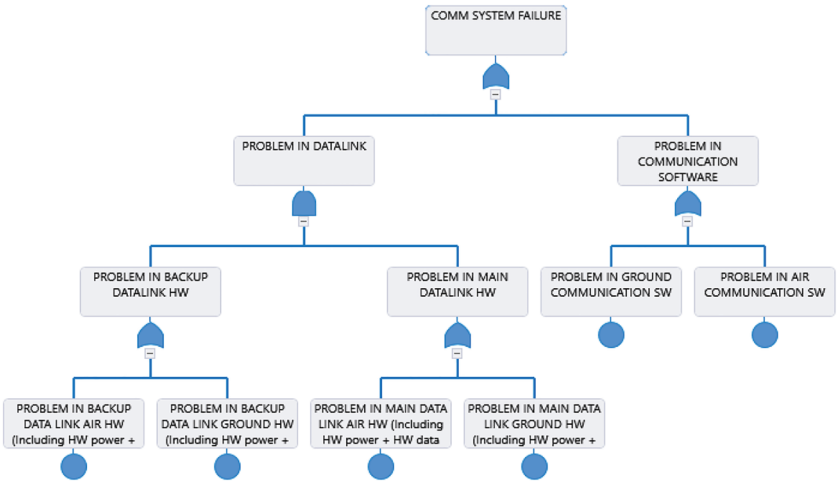

FIGURE 9 Fault tree for the intermediate event "Communication system failure"

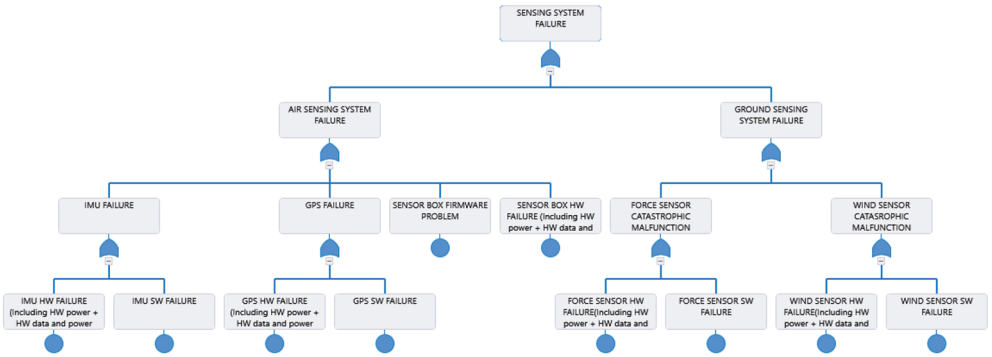

FIGURE 10 Fault tree for the intermediate event "Sensing system failure"

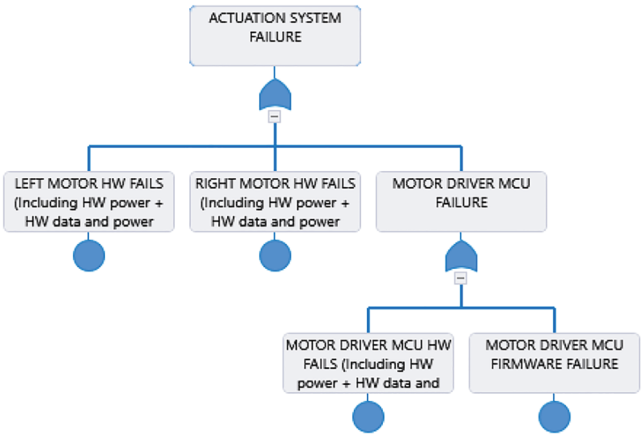

FIGURE 11 Fault tree for the intermediate event "Actuation system failure"

(Software Considerations in Airborne Systems and Equipment Certification) with Development Assurance Level (DAL) D.[46] Even though no formal standard was followed during the development of the current software, we consider using DAL-D level failure rate reasonable on the basis of the generated artifacts, test intensity, and use history of the software components. Failure databases provide generic failure data collected from a variety of sources. For some of the hardware components, Weibull failure coefficients from Barringer & Associates, Inc[47] are used as a starting point. For some of the basic events in the fault tree, data was not available in the failure databases. For such events, expert opinion and engineering judgment was used to estimate the failure probability. The expected mean time to failure for a nonrepairable 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.

3.3 | Fault detection, isolation, and recovery

FDIR is an integral part of the fault management strategy because it implements the mitigation measures proposed by the reliability analyses. A generic high-level FDIR functionality for AWE systems is outlined in Table 5. We aim at a minimal implementation complexity for several reasons. First, because this generally reduces the effort to validate the implemented FDIR system. Physical models that can be part of such a system are in most cases validated only for nominal operation with often insufficient prediction quality for off-design scenarios resulting from

TABLE 4 Failure events and probability density functions used for the FTA

Subsystem	Failure Event	Probability Density Function
	Pilot offline[a]	MTTF(MTTF=5)
Traction power system	All tethers off,[b] 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($q = 0.001$)

Note. Hardware (HW) includes HW power, HW data, and power cabling.

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

[b]Includes safety line.

TABLE 5 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		

Abbreviations: AWE, airborne wind energy; HW, hardware; SW, software.

anomalies. An example is a damaged bridle line system, which can substantially alter the flight dynamic behavior of the wing. An extreme case is shown in Figure 6D,E. Second, the overall complexity of the system has to be manageable. Therefore, detection mechanisms are designed only for those failure modes that have been identified by the FMEA and FTA. For the same reason, the mitigation measures are grouped as much as possible, using a common FDIR implementation per group.

We adapt an hierarchical FDIR architecture that is used in space industry[48] because it fits well to the investigated AWE system. Satellites, for example, have also high reliability requirements, incorporate a safe mode, and use holistic anomaly detection. The layered structure supports a

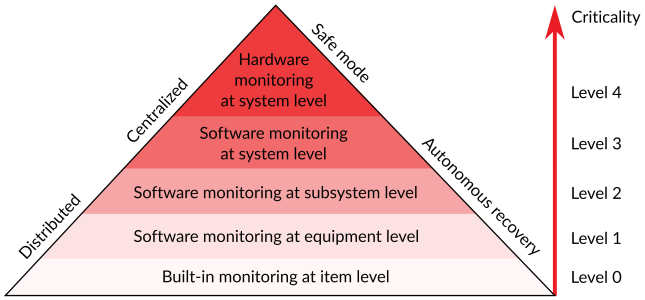

FIGURE 12 Hierarchical failure detection, isolation, and recovery (failure detection, isolation, and recovery [FDIR]) architecture

clear organization of tasks and makes it difficult to overlook aspects. 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 12. 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, also the criticality of the inspected faults increases. Fault monitoring and detection starts at the lowest level. Successively higher levels are triggered only after activating the lower level several times without catching the fault. The five levels are introduced in the following.

- Level 0 performs built-in monitoring at item level. Some functional units have to be capable of recovering autonomously from faults without affecting the performance of the system. This is necessary especially if the recovery time for a specific fault is critical. Software and hardware watchdogs in microcontroller boards are typical examples for Level 0 FDIR.
- Level 1 monitors software at equipment level for units that can not detect and recover autonomously from faults. At this level, detection, recovery, and isolation (if required) are performed by the subsystem. Switching from the faulty sensor to a redundant one or deriving the data from different sensor(s) are examples of Level 1 FDIR. For the subsystems, inputs and outputs are checked by the Level 1 FDIR with regards to data consistency (continuity and frequency checks), measurement consistency (range check, rate check, comparison with a redundant sensor), and command consistency(command timing and feedbacks).
- Level 2 monitors software performance at subsystem level. At this level, faults are caught that could not be localized at lower levels. 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 software performance at system level. One or more faults which could not be recovered at the lower levels are caught by the Level 3 FDIR if it affects the system performance. Heuristic methods[49] or model-based methods[50] are in use for detecting such a system-wide anomaly. In general, the flight dynamic response of the kite to steering commands is a good indicator for the overall health status of the airborne subsystem. In our study, an empirical correlation[42] 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, taking also into account the dependency on the depower setting.
- Level 4 performs hardware-only monitoring at system level to protect the system from catastrophic events. There are no recovery or isolation actions at this level. An example for such a hardwired system-level alarm is the cutting of the tether for a controlled landing in the event of a loss of control.

Levels 3 and 4 are centralized and monitor the entire system 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 to this, Levels 0, 1, and 2 are decentralized. Each subsystem has its own FDIR component which may consists of Levels 1 and 2. Similarly, items may have their own 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 is determined by the FMEA. Thus, for noncritical faults, detection mechanisms only at higher levels, eg, Levels 3 and 4, may be sufficient.

4 | RESULTS

Within the scope of the FMEA, we investigated 80 different failure modes of electronic hardware and software components. Based on the risk number calculated from Equation (1), we compiled a prioritized list of failure modes that could lead to potentially hazardous situations. To increase the system-wide reliability and safety, we distinguish modes that can be mitigated by an FDIR system and modes that require a redesign of the involved components to meet stricter reliability standards. As an example, Table 6 details a malfunction of the flight path controller software that can be mitigated by FDIR. The rows listing the residual severity, probability, and risk number indicate the improvement that can be achieved by the proposed mitigation measure. The specific operational target has an impact on the foreseeable sequence of events and the suitable mitigation measures. For example, for short flights, certain sensor failures may be tolerable when the pilot is in the loop. However, but for 1 week of flight, intervention of a pilot can not be proposed as a mitigation measure.

TABLE 6 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
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, 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 2.2.5)
Residual harm (worst case)	Maintenance required
Residual severity	2
Residual probability	3
Residual risk number	6

Abbreviations: FDIR, failure detection, isolation, and recovery; FMEA, failure mode and effects analysis.

TABLE 7 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
Foreseeable sequence of events	Loss of steering authority, tether tension can be controlled by depower motor, controlled immediate landing within operational zone (see Section 2.2.6)
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

Abbreviations: FMEA, failure mode and effects analysis.

Table 7 shows an example for reducing the risk of a failing motor driver microcontroller software by defining a stricter software standard, for example, by changing the DAL level from D to C. The total risk number of the technology development platform calculated by the FMEA is 569. Applying the proposed mitigation measures this number can be decreased to 370. 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 failures causing the catastrophic event, which we define as the kite leaving the operation zone and potentially colliding with other users of the airspace or crashing on the ground with the possible consequence of multiple deaths.

With the FTA we focused on combinations of failures causing the catastrophic event. Based on the fault tree illustrated in Figure 7, we determined 33 different component failure events which in combination may trigger the catastrophic event. A probability model is assigned to each of these failure events, and then, the exact probability of the catastrophic event is determined using the binary decision diagram (BDD) method[51] and considering Boolean logical relationships of the failure events. During the probability calculation, minimal cut sets (MCS) are also extracted. In a fault tree, an MCS is the smallest combination of basic events causing the system failure. Unlike the classical MCS method, the BDD method provides exact values for the cut set unavailability and relative importance. We define unavailability as the probability that a specific cut set is in a failed state at time t and we use the Vesely-Fussell importance factor defined as the fraction of system unavailability contributed by a specific cut set.[44] Table 8 lists the MCSs, their unavailability, and relative importance for the technology development platform.

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

Abbreviations: GPS, global positioning system; HW, hardware; IMU, inertial measurement unit; MPPT, maximum power point tracker.

TABLE 8 First 10 minimal cut sets with unavailability and Vesely-Fussell (VF) importance factor calculated for one week of operation

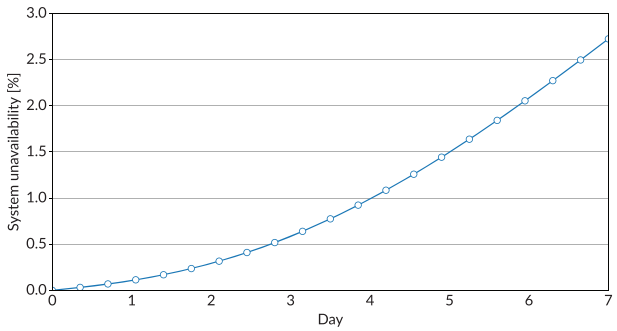

FIGURE 13 Unavailability of the kite power system

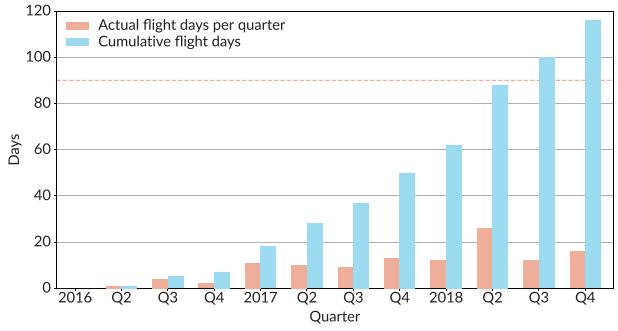

FIGURE 14 Number of flight days for Kitepower B.V. from 2016 until today

Figure 13 shows the computed unavailability of the investigated system as a function of the days in operation. The computed unavailability after 1 week of operation is 2.75%, which is equivalent to a system failure rate of 0.163×10^{-3}/h. The minimal cut sets listed in Table 8 amount to a joint unavailability after one week of 2.70%, which means that these first 10 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 reliability analysis step by step. As a result, the design of some of the critical components was improved and also some modules of the FDIR system were implemented. Even with the partial implementation of these measures, a reliability improvement can be recognized from the flight logs. Figure 14 illustrates the increasing number of flight days per quarter as well as the total accumulated number of flight days. The dashed line indicates the limit of continuous operation at around 90 days per quarter.

5 | CONCLUSIONS

System reliability, operational robustness, and safety are of crucial importance for the successful commercialization of AWE. Given the inherent complexity of the technology, these aspects have to be taken into account already early in the system design process. In this study, we combine a FMEA and a FTA 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 a 18-kW electrical machine. Potentially hazardous situations are mitigated by FDIR using an hierarchical architecture from space industry that fits well the design of AWE systems. To our knowledge, this is the first published study defining a safety and reliability engineering process for AWE systems.

In the FMEA, we consider only single failure modes, one by one, proposing mitigation measures for each mode to increase the system-wide reliability and safety. With the FTA, we focus on simultaneous failures and determine the resulting probability of the worst-case event, defined as the kite leaving the operation zone in an uncontrolled way. We reveal the underlying fault mechanisms that can cause this event and provide this information 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 certain 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 also 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.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to the team of Kitepower B.V. for sharing valuable details of the technology and for supporting this research. The authors would further like to thank Reliotech SAS for providing the software TopEvent FTA. Roland Schmehl has been supported financially by the project AWESCO, funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant 642682, and the project REACH, funded by the European Union's Horizon 2020 research and innovation program under the grant 691173.

ORCID

Volkan Salma https://orcid.org/0000-0001-6122-329X
Roland Schmehl https://orcid.org/0000-0002-4112-841X

REFERENCES

1. International Renewable Energy Agency. Innovation outlook: offshore wind, Abu Dhabi, International Renewable Energy Agency; 2016. https://irena.org/-/media/Files/IRENA/Agency/Publication/2016/IRENA_Innovation_Outlook_Offshore_Wind_2016.pdf
2. De Castro C, Mediavilla M, Miguel LJ, Frechoso F. Global wind power potential: physical and technological limits. *Energy Policy*. 2011;39(10):6677-6682.
3. Burton T, Jenkins N, Sharpe D, Bossanyi E. *Wind energy handbook*. 2nd ed. Chichester, West Sussex: John Wiley & Sons; 2011.
4. Ahrens U, Diehl M, Schmehl R, eds. *Airborne wind energy*, Green Energy and Technology. Berlin Heidelberg: Springer; 2013.
5. Cherubini A, Papini A, Vertechy R, Fontana M. Airborne wind energy systems: a review of the technologies. *Renew Sustain Energy Rev*. 2015;51:1461-1476.
6. Bechtle P, Schelbergen M, Schmehl R, Zillmann U, Watson S. Airborne wind energy resource analysis. *Renew Energy*. 201910;141:1103-1116.
7. 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. Singapore: Springer; 2018:137-163.
8. Durakovic A. Shell and google owner enter offshore energy kite venture. https://www.offshorewind.biz/2019/02/12/shell-and-google-owner-enter-offshore-energy-kite-venture/. Accessed: 13 February 2019.
9. Watson S, Moro A, Reis V, et al. Future emerging technologies in the wind power sector: a European perspective. *Renew Sustain Energy Rev*. 2019;113:109270.
10. European Commission. Study on challenges in the commercialisation of airborne wind energy systems. ECORYS Report PP-05081-2016, Brussels; 2018.
11. Birolini A. *Reliability engineering – theory and practice*. 8th ed. Berlin Heidelberg: Springer; 2017.
12. Crowe D, Feinberg A. *Design for reliability*. 1st ed. Boca Raton, FL: CRC Press; 2001.
13. National Aeronautics and Space Administration. Fault management handbook. NASA Technical Handbook NASA-HDBK-1002, Washington, DC, National Aeronautics and Space Administration; 2012. https://www.nasa.gov/pdf/636372main_NASA-HDBK-1002_Draft.pdf
14. Arabian-Hoseynabadi H, Oraee H, Tavner PJ. Failure modes and effects analysis (FMEA) for wind turbines. *Int J Electr Power Energy Syst*. 2010;32(7):817-824.
15. 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. Singapore: Springer; 2018:643-662.
16. Salma V, Ruiterkamp R, Kruijff M, van Paassen MM, 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. Singapore: Springer; 2018:703-725.

17. Stoeckle MR. Fault detection, isolation, and recovery for autonomous parafoils. *Master's Thesis*: Massachusetts Institute of Technology; 2014. http://hdl.handle.net/1721.1/90612
18. Friedl F. Fault-tolerant design of a pumping kite power flight control system. *Master's Thesis*: Graz University of Applied Sciences & Delft University of Technology; 2015. http://resolver.tudelft.nl/uuid:e704e8aa-2371-437b-8de9-80b3b7067241
19. 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; 2015; Karlsruhe, Germany:101.
20. 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*. Delft, The Netherlands: Delft University of Technology; 2015:81. Presentation video recording available from: https://collegerama.tudelft.nl/Mediasite/Play/90b60bc1e2bf44759ddc1b18185383791d
21. 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*. Freiburg, Germany: University of Freiburg | Delft University of Technology; 2017:104. Poster available from http://awec2017.com/images/posters/Poster_Reyes.pdf
22. van der Vlugt R, Bley A, Noom M, Schmehl R. Quasi-steady model of a pumping kite power system. *Renew Energy*. 2019;131:83-99.
23. 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. Berlin Heidelberg: Springer; 2013:403-425.
24. Kitepower B. V. https://kitepower.nl/tech/. Accessed: 5 February 2019.
25. Oehler J, Schmehl R. Aerodynamic characterization of a soft kite by in situ flow measurement. *Wind Energy Sci*. 2019;4(1):1-21.
26. Loyd ML. Crosswind kite power. *J Energy*. 1980;4(3):106-111.
27. Folkersma M, Schmehl R, Viré A. Boundary layer transition modeling on leading edge inflatable kite airfoils. *Wind Energy*. 2019;22(7):908-921.
28. 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. Singapore: Springer; 2018:361-390.
29. Oehler J, van Reijen M, Schmehl R. Experimental investigation of soft kite performance during turning maneuvers. *J Phys Conf Ser*. 2018;1037(5):52004.
30. 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*. Freiburg, Germany: University of Freiburg | Delft University of Technology; 2017:47-51. Presentation video recording available from: http://www.awec2017.com/presentations/johannes-peschel
31. Roschi S. Clean energy from high above. https://drive.tech/en/stream-content/high-altitude-wind-ernergy-from-kites. Accessed: 9 December 2018.
32. 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. Berlin Heidelberg: Springer; 2013:563-585.
33. 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. Berlin Heidelberg: Springer; 2013:249-269.
34. Fechner U, van der Vlugt R, Schreuder E, Schmehl R. Dynamic model of a pumping kite power system. *Renew Energy*. 2015;83:705-716.
35. Fechner U, Schmehl R. Design of a distributed kite power control system. In: Proceedings of the 2012 IEEE International Conference on Control Applications; 2012; Dubrovnik, Croatia:800-805.
36. ZeroMQ Distributed Messaging Library. http://zeromq.org/. Accessed: 9 December 2018.
37. Google Protocol Buffers. https://developers.google.com/protocol-buffers/. Accessed: 9 December 2018.
38. National Aeronautics and Space Administration. Software safety guidebook. NASA Technical Standard NASA-GB-8719.13, Washington, DC, National Aeronautics and Space Administration; 2004. https://www.system-safety.org/Documents/NASA-GB-8719.13.pdf. Appendix B.
39. 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. Singapore: Springer; 2018:391-411.
40. Licitra G, Koenemann J, Bürger A, Williams P, Ruiterkamp R, Diehl M. Performance assessment of a rigid wing airborne wind energy pumping system. *Energy*. 2019;173:569-585.
41. Rapp S, Schmehl R. Vertical takeoff and landing of flexible wing kite power systems. *J Guidance Control Dynam*. 20187;41(11):2386-2400.
42. Jehle C, Schmehl R. Applied tracking control for kite power systems. *J Guidance Control Dyn*. 2014;37(4):1211-1222.
43. Peeters JFW, Basten RJI, Tinga T. Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner. *Reliab Eng Syst Safety*. 2018;172:36-44.
44. Ruijters E, Stoelinga M. Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools. *Comput Sci Rev*. 2015;15–16:29-62.
45. Vesely W, Stamatelatos M. *Fault tree handbook with aerospace applications*. Washington, DC 20546: NASA Office of Safety and Mission Assurance; 2002. https://elibrary.gsfc.nasa.gov/_assets/doclibBidder/tech_docs/25.20NASA_Fault_Tree_Handbook_with_Aerospace_Applications20-20Copy.pdf
46. 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*. London: Springer; 2011:293-313.
47. Barringer & Associates Inc.. Reliability learning forever. http://www.barringer1.com/Contents.shtml. Accessed 30 July 2018.
48. Olive X. Fdi (r) for satellites: how to deal with high availability and robustness in the space domain. *Int J Appl Math Comput Sci*. 2012;22(1):99-107.
49. Isermann R. Supervision, fault-detection and fault-diagnosis methods-an introduction. *Control Eng Pract*. 1997;5(5):639-652.
50. Frank PM. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: a survey and some new results. *Automatica*. 1990;26(3):459-474.
51. Rauzy A. New algorithms for fault trees analysis. *Reliab Eng Syst Safety*. 1993;40(3):203-211.

How to cite this article: Salma V, Friedl F, Schmehl R. Improving reliability and safety of airborne wind energy systems. *Wind Energy*. 2019;1–17. https://doi.org/10.1002/we.2433