CEAS Aeronautical Journal (2020) 11:767–779
https://doi.org/10.1007/s13272-020-00451-0

ORIGINAL PAPER

Geofencing requirements for onboard safe operation monitoring

Christoph Torens[1] · Florian Nikodem[1] · Johann C. Dauer[1] · Sebastian Schirmer[1] · Jörg S. Dittrich[1]

Received: 12 August 2019 / Revised: 10 March 2020 / Accepted: 3 April 2020 / Published online: 16 May 2020

Abstract
The new concept for operation of drones, published by EASA in 2015, enables new ways to influence and possibly reduce the necessary safety targets of certain system components without reducing the overall safety of the unmanned aircraft system (UAS). Based on the safety assessment, the specific category enables new aircraft system architectures and mission designs. In this context, this paper analyzes runtime monitoring as a strategy to contain the UAS in its operational volume. To assure predefined properties in flight and thus assure the safety of the operation in progress with a high robustness, a formal methodology for safe operation monitoring is utilized. With this approach, this work targets to link the concept of safe operation monitoring with the upcoming regulations regarding the specific category and the specific operation risk assessment (SORA). One particular aspect of this safe operation monitoring is geofencing, the capability to contain a UAS in a previously restricted area. In the regulatory framework of a specific operation, risk assessment is required and so is the containment of the UAS in its operational volume. The functional and safety requirements for geofencing regarding their impact on the underlying specific operation risk assessment are discussed. To facilitate this discussion, a taxonomy of geofencing characteristics is derived based on a literature survey. Consequently, the geofencing requirements are assessed regarding their robustness and applicability for certification purposes. As a result, by monitoring the integrity of the system at runtime using geofencing as an example, it is investigated if the requirements and thus costs of development and certification process for the remaining components can be reduced.

Keywords UAS · Safety requirements · Specific operation risk assessment (SORA) · Runtime monitoring · Geofencing

1 Introduction

In late 2015, EASA introduced three categories of UAS operation that can be regulated and certified based on the intrinsic risks involved [1–3]. The three categories are referred to as open, specific and certified. The open category is reserved for low risk operation under strict restrictions of unmanned aircraft below 25 kg used in the visual line of sight (VLOS), requiring no or minimal regulation. The certified category is used for operations that are of an equivalent level of risk comparable to manned aviation, using the same level of rigour and requiring an aircraft type certification. The core of the new concept, however, is the specific category that allows a stepwise adaptation of regulation and certification requirements between the two other categories (Fig. 1). According to it, the necessary certification effort scales with the actual risks of the operation of interest. The specific category uses a so-called specific operation risk assessment (SORA) for analysis and categorizes the required level of rigour for UAS development and operation [4]. This approach is not targeted solely on the UAS, but towards the operation of a specific UAS in its entirety, including: the mission, the environment, operation conditions, rigour during development as well as operator and pilot qualification.

The DLR (German Aerospace Center) is currently applying the SORA to a cargo application with the project ALAADy (automated low altitude air delivery) [5] and investigates different means to exploit the advantages of the new specific category concept. In this project, different drone configurations are compared, all of which carry approximately one metric ton of payload. The mission is cargo delivery on a range of around 600 km flying over sparsely populated areas. The drones are intended to fly at low altitude to circumvent most of the air traffic. Technologically and economically, different concepts are analyzed and

✉ Christoph Torens
christoph.torens@dlr.de

[1] German Aerospace Center (DLR), Institute of Flight Systems, 38108 Braunschweig, Germany

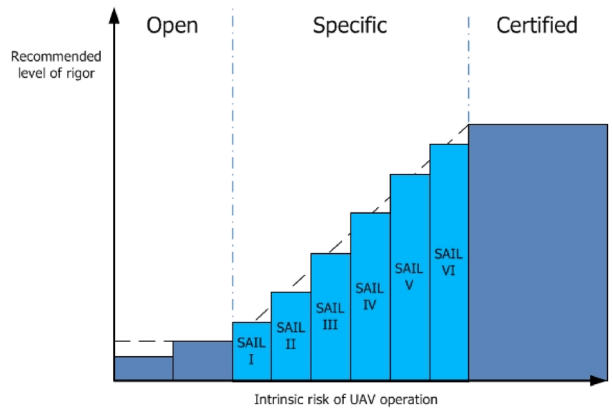

Fig. 1 Specific assurance and integrety level, following [4]

discussed. This includes aspects of the required levels of autonomy, concepts of infrastructure, and the system components required to achieve the goal of cargo transportation. By designing the aircraft configurations and defining appropriate use cases, the risks involved are determined. In particular, it is important to develop a suitable, high-quality set of functional and safety requirements to support the necessary risk assessment that is required to evaluate applicability within the specific category. The discussion of this paper is based on this mission specification with the bigger picture of general drone operation in mind.

DLR is researching the use of a runtime monitor onboard an UAS to further support the concept of specific operation. We refer to this monitor as safe operation monitor. In particular, it is planned to monitor the aircraft at runtime and supervise specific properties and requirements that are related to both safety and the specific mission operation. In contrast to manned aviation, where the pilot on-board manages hazardous situations, there is no person on-board in the drone context. Instead, the suggested monitor takes over parts of the supervisional tasks of the pilot who, if present at all, is located at a remote pilot station. This paper exemplifies geofencing, which is the capability of the UAS to safely avoid certain predefined areas, as a containment strategy of the specific category approach on one hand; and as a use case of runtime monitoring using our proposed safe operation monitor on the other hand. The resulting set of functional and safety requirements under investigation, along with the aforementioned monitoring approach, must be suitable for integration into the SORA holistic risk model.

The remainder of the paper is structured as follows: after highlighting some of the important related work in Sect. 2, the SORA process is briefly explained in Sect. 3. Section 4 introduces the concept of runtime monitoring as a way of implementing the containment requirement of SORA. Section 5 assesses the applicability of the safe operation monitoring in the context of the SORA process. In this paper, we focus on the aspect of geofencing but the concept presented can be applied to other means of operation as well. The necessary requirements for this geofence monitoring are derived by developing a generic taxonomy for geofencing in Sect. 6. These requirements are assessed in Sect. 7 with respect to the necessary SORA process and the resulting robustness levels are discussed and exemplified. Finally, Sect. 8 summarizes the proposed approach and results.

2 Related work

Developing software for safety critical systems has provided topics for research for years. In general, to consider safety within the development, some sort of safety assessment is performed. The well-known functional hazard assessment (FHA) can be used as a structured approach, and the two alternatives are: a use case or scenario-based analysis [6] or fault trees [7]. The results of this analysis can then be considered as a quality measure of the software product or as a basis for the requirement definition [6–8].

Applying the same approach for UAS safety risk mitigation that is used for manned aviation is considered to hinder many of the UAS business cases. Traditional certification for manned aircraft imposes significant development costs. For this reason, aviation authorities as well as the UAS community are trying to identify the safety risks involved in the operation (cf [9].) and search for alternative approaches of certification, like the already mentioned SORA [4] or specific safety cases [10] in particular, for operation over populated areas. The overall trend currently emphasizes risk-based approaches, as does this work. In fact, EASA plans to implement risk-based approaches in the near future [1–3, 11]. The integration of UAS in civil airspaces, and its safety aspects and risks thus received particular research interest [12–14]. Smaller scale UAS often operate in very low level flight, which has also been considered for airspace integration [15]. An extension of the very low level airspace towards larger scale unmanned aircraft utilizing a risk-based approach is presented in [16].

To facilitate low level airspace integration, geofencing has recently been under investigation [17]; NASA specifically targeted the safety requirements for geofencing [18]. EUROCAE also investigates UTM geofencing and dynamic geofencing in working group 105, SG 33 [33]. In this group there are 2 specific documents being developed, Minimum Operational Performance Specification for UAS geo-caging as well as Minimum Operational Performance Standard for UAS geofencing. It is interesting to note that the working group is establishing separate definitions for the terms geocaging (authorized volume, not to exit) and geofencing (unauthorized volume, not to enter). In the scope of this work, there will be no differentiation between these two terms,

and geofencing will be used to describe both. One challenging aspect of geofencing approach is the need of an assured source of positioning information as GPS can suffer from reliability issues. In [19], an architecture for the geofencing system is presented including a hazard assessment. The work suggests additional infrastructure to determine position independent of GPS. Furthermore, an example of a geofencing system capable of handling automatic and remotely piloted flight is given in [20]. In [21], special requirements for a variable geofence are assessed, considering performance capabilities of the UAS and wind conditions.

In this context of geofencing, runtime monitoring especially utilizing formal methods can play an important role. For example, [22] presents a runtime monitor to check a non-assured control system by comparing its outputs against an assured implementation during operation. In [23], an approach is presented to assess the overall system health using runtime monitoring. In accordance, in [24] a contingency management architecture is presented that relies on such health information.

Certification for safety critical software sets high verification requirements that impose huge efforts on development and verification, especially using traditional verification approaches [25]. The aforementioned approaches utilize formal methods to systematically achieve provable system properties using mathematical rigour. Nonetheless, there is still a relatively little use of these methods in commercial projects. A 2013 study identifies nine barriers to the introduction of formal methods [26]. One of the reasons for the low spread of formal methods, even in safety–critical domains, is the uncertainty about the certification credit resulting from the use of these techniques. The software development standard for safety critical software DO-178B [27] did not include any guidelines for the use of formal methods. However, since late 2011, the successor standard DO-178C [28] directly supports the use of formal methods with a designated supplement DO-333 [29]. As a result, a lot of researches are looking at the effectiveness of formal methods in regard to certification for safety critical domains, for example, using Simulink and SCADE [30] as tools, as well as general guidance to use these methods for certification credit [31, 32]. It is therefore also of interest to assess the impact of the use of formal methods in the context of the SORA process.

3 Specific operation risk assessment

As briefly discussed above, the open category addresses UAS operations that do not require an authorization by the national aviation authorities prior to the operation due to minimal risks to people and environment. For example, very small UAS and toy drones that pose only small risks

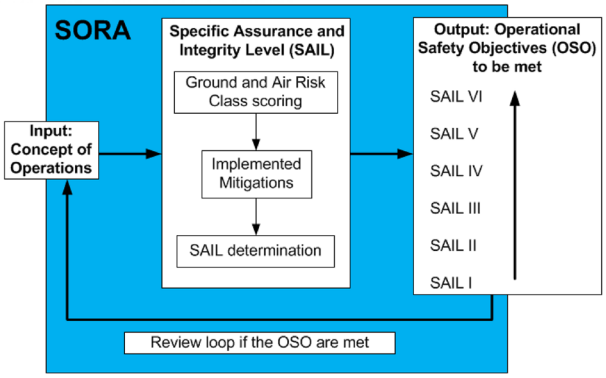

Fig. 2 Simplified SORA process, modified from [34] (SORA ED 1.0)

are categorized as open. In contrast to this, the certified category has very high safety requirements. UAS that operate in this category need to be certified by an official aviation authority, and handling needs to be done by a licensed pilot and an approved operator. While the open category has already been addressed in some detail by EASA, a lot of the details of the specific category are still in the definition phase. The necessary efforts for certification of a specific category UAS are based on the SORA [4], and these efforts scale to the overall risk with an increasing level of rigour for aircraft development and operation planning. This assessment is a risk-based approach considering not only the UAS but the whole intended operation. The SORA process proposes a holistic risk model that combines ground and air collision risk. As a result, SORA divides the specific category in six specific assurance and integrity levels (SAIL), Fig. 1.

The SORA process is meant to be used iteratively to determine the SAIL and consecutively perform a risk assessment. A simplified schematic of the SORA process is shown in Fig. 2. The input for SORA is a so-called concept of operations (CONOPS) document, which contains information on the operator, the planned operation, technical data of the UAS, mitigation strategies in case of a loss of control and information of the remote crew. With this information, a score for ground and air risk can be found. The SORA implements ground and air risk classes as a measurement for potential danger of the UAS and its operation to other people and infrastructure. The determined ground risk class depends on the characteristic dimension of the UAS, the population density of the area of operation and a distinction between flights in the visual line of sight (VLOS) and beyond the visual line of sight (BVLOS). The air risk class, on the other hand, depends on the airspace density and the operational flight altitude. A distinction is also made between flight altitude below 500 ft and flight altitude above 500 ft. The overall SAIL is determined by analysing both the ground risk and the air risk classes.

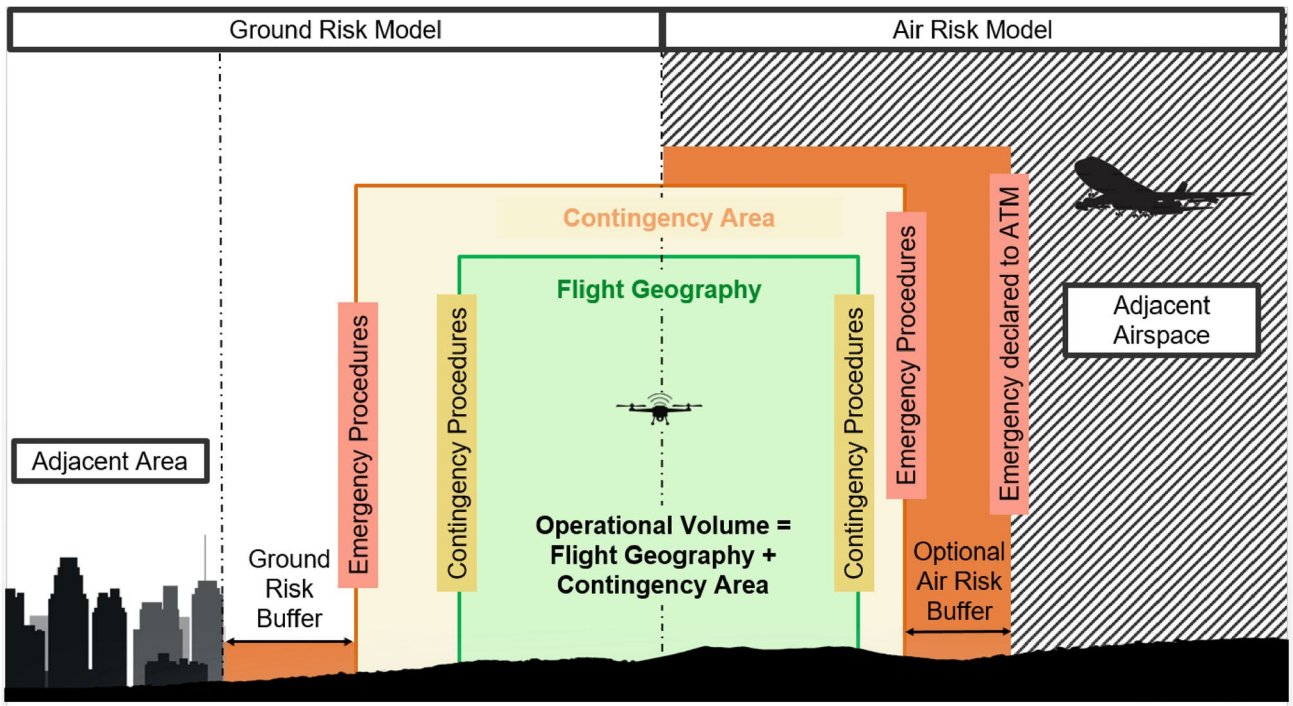

Fig. 3 Graphical representation of operational volume and risk buffer interaction, modified from [4]

Each SAIL entails different levels of robustness required for a set of operational safety objectives (OSO) established to ensure safe UAS operations. These objectives are meant to reduce the risk of an operation getting out of control. An UAS operation is out of control when the operation is conducted outside of the approved concept of operations. An operation being out of control does not necessarily mean that the UAS itself is technically out of control, e.g., a change in weather conditions can lead to an operation being outside of the defined concept of operations. Each OSO has four level of robustness: optional, low, medium and high. The level of robustness of each OSO can be understood as the necessary rigour and is expressed with a level of integrity and a level of assurance. The assurance is a requirement on how the effectivity of the OSO must be verified. Generally speaking, a low level assurance is achieved by self-declaration; a medium level assurance by supporting evidence such as analyses and simulations, and a high level assurance can only be achieved by a third party verification. In contrast, the integrity is a requirement on how the OSO has to be applied. As the SAIL increases, the same is required for the robustness of the OSO.

Additionally, the so-called mitigations are proposed. Mitigations are measures to reduce the consequences and the likelihood of harm to other people or infrastructure, in case the UAS operation is in fact out of control. Depending on the robustness of the mitigation (not implemented, low, medium or high), it is possible to reduce the ground and air risk classes. This reduction can lead to a lower SAIL classification, which also results in the reduction of required robustness level of the OSO.

In SORA, there are pre-described mitigations that can be applied to reduce the ground risk and air risk classes. Mitigations for ground risk are meant to reduce the number of people at risk or the severity of an impact on ground. In contrast, the mitigations for air risk shall prevent mid-air collision. Some of them are required depending on the air risk class, such as detect and avoid systems. Within SORA, the required mitigations for air risk are called tactical mitigations. Those are more comparable to the OSO. Others such as airspace restriction or reduction of time of exposure are optional and have an impact on the air risk class. Those optional mitigations are called strategic mitigations within SORA.

"Strategic mitigations for ground risk" is a very important concept to minimize ground risks, by including a risk buffer around the area of operation. This concept is also applicable to the air risk class as a strategic mitigation. The buffer is meant to reduce risks to people and other aircraft by increasing the distance between the UAS operational volume and adjacent areas where more victims could potentially exist. A schematic of the interaction of the risk buffer with the operational volume is shown in Fig. 3.

The robustness of the risk buffer depends on the strategy to determine the buffer size. A buffer following a simple one-to-one rule, meaning at a flight altitude of 150 m

the buffer must be at least 150 m in size, is regarded with a low robustness. For medium and high robustness levels, the buffer size has to consider weather conditions as well as aircraft behaviour in case of normal, abnormal and emergency situations. Additionally, the reduction of people at risk has to be proven by local population density data.

The risk buffer mitigation is strongly linked to an additional containment requirement. Regardless of the use of a risk buffer, it is still required to contain the UAS against volumes with higher risk ratings than the claimed operational volume. SORA has two levels of rigour regarding the containment requirement. The general requirement regarding safety is [4]:

> "No probable failure of the UAS or any external system supporting the operation shall lead to operation outside of the operational volume."

If the operational volume must be contained to avoid gatherings of people, high density airspace, or if the ground risk buffer has been used in populated environment to reduce the initial ground risk, following safety requirements apply [4]:

> "The probability of leaving the operational volume shall be less than 10^{-4} per flight hour. No single failure of the UAS or any external system supporting the operation shall lead to operation outside of the ground risk buffer. 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."

Since the costs for certification by assuring OSO with high robustness can increase to levels almost equivalent to those of the certified category, it is expected to be cost effective to add mitigations and increase their robustness to achieve an overall reduction of UAS development and operation costs. New results within the aforementioned DLR ALAADy project show that it is beneficial to add mitigations to reduce the risk class, at least for moderate and higher risk operations [35].

However, the interaction of the implementation and operation costs of mitigations and OSO, especially if these involve limitations in operation, has not yet been completely answered. Handling this interplay and deriving sweet spots of safeness and operation costs will be a great challenge for the near future. Especially, transferring this holistic view of the SORA on safety to a holistic view on system design including the operators, pilots and operation itself might enable new realizations of UAS that, to this day, have not yet been possible.

To target the benefit of applying mitigations, our approach uses runtime monitoring to supervise properties of the aircraft as well as the operation. One specific use case of restricting operational behaviour is geofencing as an option to assure the mitigation "risk buffer". Geofencing and its functional as well as quality requirements will be discussed as an exemplary use case for our monitoring approach.

4 Runtime monitoring concept

In general, monitoring is the concept of supervising specific values and properties of a system. Runtime monitoring does this in parallel to the running system, in this case for an aircraft in flight. For specific purposes, this is already done in several layers throughout the aircraft system as well as aircraft operations. For example, some low level tasks exist with automated forms of monitoring, but many monitoring tasks are manual. In particular, the final as well as high-level task of supervision of the flight itself is still performed by a pilot. Flight supervision is performed manually for manned aviation, but also for UAS, utilizing a multitude of displays in a ground control station.

We propose the use of a formal method for the monitoring on the aircraft level as well as on the mission level. This approach enables to achieve a high degree of assurance and the possibility to achieve certification, even for complex monitoring properties. By relying on a trustworthy module for the monitoring of specific properties that is also capable of describing complex time-dependent properties, higher level tasks can additionally be automated. In this paper, we discuss the functional requirements of geofencing and how geofencing can be implemented using a runtime monitoring methodology. The idea of using a formal methodology is that, based on the formal specification, a provable correct implementation of the monitoring can be generated. There are also on-going researches on generating FPGA hardware implementations of such a monitoring solution.

The formal methodology for the description of monitored properties is LTL, linear temporal logic. This mathematical formalism allows describing properties that not only use the current state, but also the previous values of states and variables. It is possible through LTL to reference future states of a property; however, this requires a so-called late evaluation which delays the evaluation until all relevant inputs values are available. Technical details of this approach are in active research, but first results can be found in [23, 36].

In the case of geofencing, the monitoring module supervises the position and acts as an independent geofencing mechanism. For this, the monitoring must be able to assess various data of the UAS in real time (Fig. 4). Foremost, the current geo-localization of the UAS needs to be assessed in the context of a given geofence as the safety requirement to

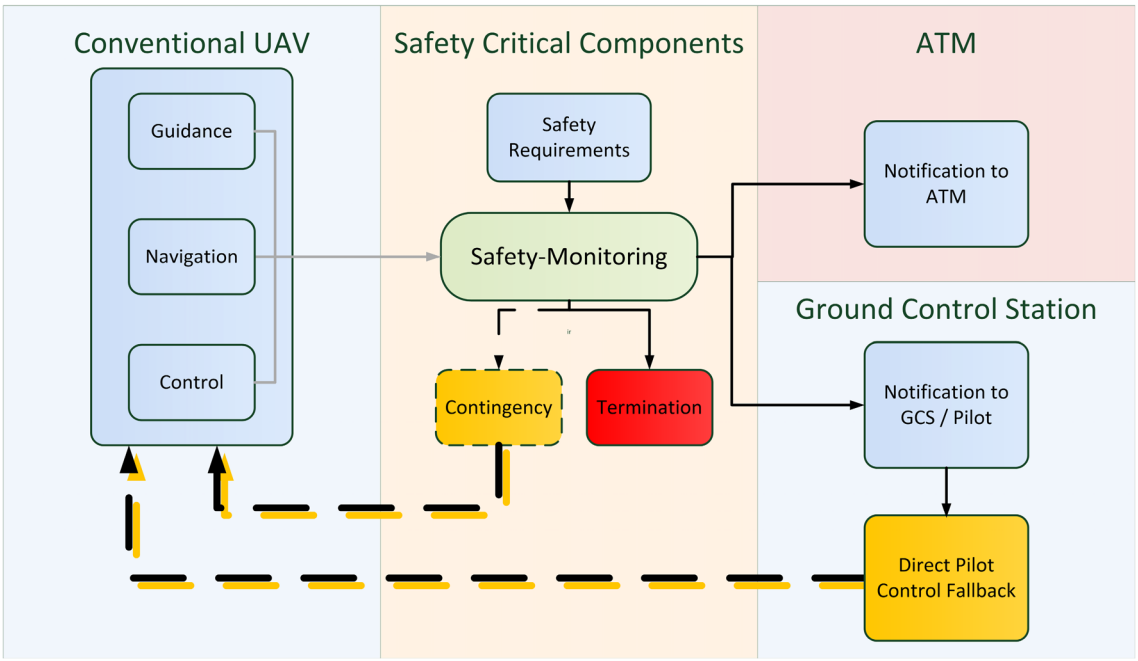

Fig. 4 UAS safe operation monitor concept

check if the aircraft is violating its borders. It is the responsibility of the monitoring to determine if the aircraft poses a risk in the given situation (see Sect. 3). For complete independence, it is also possible that the safe operation monitoring utilizes its own sensors for geo-localization.

The monitoring alone, however, cannot render the aircraft operation safe. It rather enables a subsequent action that will resolve the situation. The action that is triggered by the safe operation monitoring has to be able to transition the system to a safe state without posing additional risks. For the operation over sparsely populated areas, in the context of the geofence, a last resort of such an action would be the safe termination of the aircraft before violating the given geofence border. Although this might seem a harsh solution from the economic perspective, this approach can autonomously guarantee a permanent safe state, even if the aircraft attempts to violate the geofence. It is however possible, in addition to the safe termination, to define additional contingency procedures [24] that try to prevent a termination (Fig. 4). This will further benefit the economical perspective, but not the safety perspective; however, in scope of this work we are concentrating on the safety perspective. Additionally, it is possible that the monitoring only triggers a warning to the ground control station to enable the pilot to resolve the situation manually, depending on the level of autonomy that is performed by the UAS.

To summarize, the geofencing functionality that assures the safety of the specific operation will be implemented by the formal runtime monitoring approach, as discussed in this section. The formality of the approach assures correctness of the behaviour and allows generating modules or FPGA implementations with independence of the flight system of the aircraft. This enables high levels of robustness and assurance. A cost reduction is expected for this approach, compared to manual implementations of geofencing functionality, because the monitoring modules can be generated and the certification efforts will be reduced, due to the formality of the approach. As a result, the approach transfers the efforts of certification from the manually implemented safe operation monitor to the formal specification language approach. However, it is expected that the formality of the approach is beneficial for a certification approach.

5 Assessment of monitoring as part of SORA

The question if runtime monitoring can be beneficial in the context of SORA cannot be generally answered. The SORA tries to cover a broad range of different UAS types and operational scenarios. Therefore, the benefit of a monitoring system strongly depends on the use case. We plan to contribute to an in-depth discussion on system architectures, including monitoring systems, on the basis of SORA and the qualitative estimation on implementation efforts in the near future. However, we will give an abstract of this discussion regarding monitoring as part of SORA in this section.

SORA basically has two layers to enforce safety to third parties on ground or in air; one layer being the

requirements on containment and the other layer being the OSOs on UAS design and operator behaviour. From SAIL I to SAIL III, the containment requirements are the main driver for safety, whereas in SAIL V and VI, the level of rigour of the OSOs is superior than the containment requirements. SAIL IV can be seen as a transition phase where safety constraints are equally distributed between containment requirements and OSOs. Throughout this section it will be shown that a runtime monitoring concept is most beneficial in SAILs I to IV.

The containment requirements the UAS has to fulfil are mentioned in Step#9 of the SORA process. Depending on the operation there are two level of rigour for the containment. Within this section the more strict containment requirements are discusses, assuming the reasoning will also apply for the less strict requirements. According to SORA, more strict containment requirements apply when adjacent areas to the area of operation are:

- High frequented airspaces such as airport environment or European class C airspace; or
- Areas where gathering of people are expected; or
- M1 mitigation (ground risk buffer) has been applied to lower the GRC

Especially mitigation M1 and its link to geofence will often force to apply the following containment requirements:

- The probability of leaving the operational volume shall be less than 10E-4 per flight hour
- No single failure of the UAS or any external system supporting the operation shall lead to operation outside toe ground risk buffer
- 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

A monitoring system as discussed throughout this paper can help to fulfil these requirements. However, it needs to be mentioned that the monitoring system needs to be linked to a system that can manipulate the UAS in a way that, at least, ends the flight within the ground risk buffer, or can apply contingency measures. For the context of this section, it is implied that a monitory system has excess to one of those abilities. Such a monitoring system complies with the "no single failure" requirement by its existence as backup system. This kind of redundancy also implies that there are no development errors which directly lead to operations outside the ground risk buffer. Of course, the redundancy because of the monitoring system also contributes to leaving the operational volume requirement.

Regarding the assurance of such a monitoring system, there is no explicit requirement given. Though, assurance might be derived from the M1 mitigation when applied and done with the same system or the operator can take OSO #10/#12 into account. The OSO level of integrity sounds fairly similar to the containment requirements and tries to accomplish the same goal. SAIL I and II would need a low robustness assurance, whereas SAIL III and IV need a medium level of assurance.

Regarding the high SAILs V and VI, a monitoring system seems not as relevant regarding safety requirements. The containment requirement is still relevant, however OSO#5 now states:

- Major failure conditions are not more frequent than remote
- Hazardous failure conditions are not more frequent than extremely remote
- Catastrophic failure conditions are not more frequent than extremely improbable
- Software (SW) and airborne electronic hardware (AEH) whose development error(s) may cause or contribute to hazardous or catastrophic failure conditions are developed to an industry standard or methodology recognized as adequate by the competent authority and/or in accordance with thr means of compliance acceptable to that authority

Those requirements have a huge impact on the UAS design and architecture and now failure conditions have to be considered that require a very robust and safe overall UAS design. Depending on the use case a monitoring system may still positively contribute to such a system. However it is expected that the focus and effort will be mostly on highly reliable and robust flight control systems.

6 Monitoring safety and functional requirements

Depending on the robustness required for mitigations and OSO, the SAIL results in a large number of safety and functional requirements. The management of these requirements is a crucial part of each development process. The general approach to develop functional requirements is to derive them from aircraft requirements. However, in addition to the standard processes of requirements management, this work focuses on the aspect relevant to the specific operation concept. The functional requirements in the context of this work mainly describe the behavioural properties and capabilities of the UAS. The main purpose of these requirements is to derive the properties that are used for the safe operation monitoring of the aircraft. Given a complete set of

safety requirements, each safety incident would be the result of a failure of the UAS to fulfil a specific requirement. As a result, supervising these critical properties during flight in real time would give the possibility to enact upon a failure at the earliest possible moment. As an example functional requirement, geofencing is used. For a more detailed analysis of this functionality, the characteristics of geofencing will be discussed in the following section.

6.1 Characteristics of geofencing

Geofencing simply means that the area where an unmanned aircraft is allowed to fly in is limited, and that limitation is enforced by a technical implementation of the UAS. For example, for the use case of a field that is inspected or fertilized by a drone, it would be possible to define a geofence for exactly that field. Geofencing would allow the UAS to move freely inside the geofence, but would assure that the UAS would not break out of the intended area where the mission takes place. This seemingly easy problem solution is already a research topic for itself [18, 19]. The problem is that on one hand the goal is to maximize the flyable area and thus to be able to fly as close to the border of the geofence as possible, on the other hand the goal is to assure that the UAS does not leave the geofence, even in case of a malfunction.

To systematically define functional requirements for geofencing, this paper defines a taxonomy of geofencing characteristics and uses this to analyse the necessary requirements. The identified characteristics are: level of assurance, level of ATM integration, level of independence, buffer type, mitigation type, and decision strategy (Fig. 5).

Buffer type, which is a reference to SORA mitigation M1, is further sub categorized in buffer accuracy and buffer complexity. Buffer complexity describes the safety buffer of a geofence. The simplest solution would be to have no additional safety buffer to the SORA required minimum one-to-one rule regarding flight altitude and buffer size. This approach would simply check if the UAS is inside or outside the defined area, and as soon as a breach of the geofence is detected, a mitigation action would be executed. In that case, however, the UAS would already be outside of the intended area restriction in the event of mitigation, therefore to have no safety buffer may only be applicable for the lowest SAIL category, if any. A generic safety buffer would improve on this by defining a second border. By triggering the mitigation action as soon as this safety border is breached, the geofence would still be in effect. The safety buffer could be defined in terms of distance or time to contact at a maximum flight speed. An operation specific safety buffer would also define a second border, but use the holistic approach from the SORA to define the specific buffer that is necessary for the operation. The necessary aspects to consider for a holistic point of view would include: system dynamics, weather conditions, pilot skills, mitigation actions, and mission characteristics, such as flight attitude, manoeuvre complexity and speed.

Buffer accuracy describes the variability of the geofence. It could be statically defined, e.g., for each area or for each operation, but could also be dynamically accessed to the situation in flight. A statically defined safety border could mean that a change of weather conditions would result in the operation to be aborted, because strong winds would increase the risk of breaching the defined geofence. A dynamically assessed safety border could incorporate a change of weather conditions and allow for the operation to continue (in a degraded way), with an increased safety border and leading to a smaller allowable area of flight. Similar scenarios are possible with each of the necessary aspects of the operation specific safety buffer. Finally, such a dynamic border could include elements of prediction, where expected behaviour of the aircraft is determined based on a system model and environment conditions are considered using forecasts.

Level of independence is an important aspect of safety. Geofencing could be an integrated part of the UAS itself. For example, the flight control computer could include this feature. On the other hand, a single failure in the flight control system would result in a failure of the geofencing functionality as well as of the flight control at the same time. This can be solved using a *separate hardware system* for the geofencing system. A complete independence of the geofencing could be achieved by utilization of dedicated sensors. A hint that independence is beneficial within the SORA can be found in step #9 of adjacent area and airspace considerations where the UAS is required to meet failure conditions and single failure requirements regarding the operational volume and the safety buffer. Generally similar requirements can also be found in OSOs #10 and #12 addressing the risk of a fatality while operating over populated environments by technical containment requirements.

The mitigation type is sub categorized in mitigation action and level of autonomy and addresses SORA-required contingency and emergency strategies. A mitigation action is triggered if the UAS tends to enter the safety buffer. The ultimate mitigation action to contain a UAS inside a geofence, even for severe malfunctions, is the safe termination[1] of the UAS. In fact, for safety reasons, this mitigation should always get implemented. However, it should also be possible to define an additional fixed contingency procedure, e.g., a turn manoeuvre, which could be triggered as a failsafe to prevent the termination. It would even be possible to define

[1] Safe termination considers the environment in which the drone is terminated and refers to a fast way of ending the flight without causing harm.

multiple variable contingency procedures, specific to the situation at hand. But even in this case, it should be noted that a termination would still need to get triggered if these contingencies fail.

The level of autonomy can be manual in case only a warning is issued to a pilot and the pilot has to initiate the mitigation action. A semi-autonomous level is achieved if a warning is issued to a pilot, but mitigation is triggered automatically if there is no pilot interaction. Finally, the system is fully autonomous if it is designed to act completely without human interaction and the mitigation action cannot be overruled by a pilot.

UAS designed to standards is directly coupled to SORA OSO #4 and refers to applied design standards to the UAS and all its sub-systems. This OSO as well as our taxonomy distinguishes between three levels of integrity. However, SORA is not that clear about which standards should be applied; in all three cases, SORA only mentions standards that the competent authority considers adequate for the desired level of integrity. We suggest to consider the usage of at least parts of well-known aircraft design and development standards such SAE ARP 4754A and DO-178C design assurance level (DAL) C at medium level of integrity. For high level of integrity, we recommend the full use of SAE ARP 4754A and DO-178C standards in combination with the JARUS AMC RPAS.1309 document. The AMC RPAS.1309 document is an acceptable means of compliance for unmanned aircraft that defines required failure rates and design assurance level of unmanned aircraft.

Level of ATM integration details if there is a link between the geofencing system and air traffic management. This general characteristic is meant to address possible strategic and tactical mitigations of the air risk class section within SORA with our geofence-monitoring approach. There can be no link between geofence and ATM, but it is also possible to trigger an ATM notification in case of a breach of the geofence. For full transparency, to enrich the simple notification, additional information regarding UAS position, speed, and type of malfunction could be transmitted. Furthermore, a communication link between pilot and ATM could be initiated to provide this additional information.

The next characteristic that will be discussed is the decision strategy of a geofence. In the traditional sense a geofence is a binary decision. The UAS is either safely contained inside the geofence, or there is a breach of it, or at least a risk of breaching the geofence, that is requiring a mitigation action. However, future missions might require more sophisticated approaches towards containment to enable missions that span over large areas or make use of extended flight paths. As a result, the decision strategy could incorporate conditional decisions for crossing adjacent geofences with possibly different requirements and characteristics. For example, one geofence could require constant pilot supervision, while an adjacent geofence could be supervised automatically. A crossover between two geofence zones would only be possible in case of a stable communication link and authorization from a pilot. This approach could be extended to a risk-based decision strategy, incorporating detailed environmental information.

The level of assurance describes the verification and validation aspects of the geofencing implementation and depends on the SORA assurance requirements of the mentioned SORA references of the other characteristics. This aspect is considered a quality requirement and therefore coloured different. The three levels of assurance are derived from SORA assurance level definition. A low level of assurance is a self-declaration of the operator that the required integrity is achieved, whereas the operator has to have supporting evidence such as simulations or analyses for a medium level of assurance. In case of a high level of assurance, the supporting evidence has to be checked by an independent and competent authority-accepted third party. Additionally, it should be noted that standards, such as DO-178C, define different design assurance levels with increasing requirements for higher assurance levels, according to the results of a safety assessment. The utilization of formal methods can further improve assurance, since specific properties can be verified with mathematical rigour.

6.2 Derived requirements of geofencing

The characteristics of geofencing that have been discussed in the previous section result in a set of geofencing functional and quality requirements. In the context of the DLR project ALAADy, concerning the very low level cargo delivery over sparsely populated areas, the requirements shown in Table 1 can be derived.

After developing such a set of functional and safety requirements, these requirements need to be further analysed and transformed to properties suitable for runtime monitoring. The difficulty of implementing these requirements lies in the real-time supervision of specific properties of the UAS, in particular, flight speed, altitude, weather conditions and incorporating this data into calculations to determine dynamic safety buffers for the geofence. The proposed concept of runtime monitoring is suitable for exactly that purpose. However, the variable degree of complexity that will be used to implement geofencing functionality is a trade-off between effort and benefit resulting from the SORA process, as was discussed in Sect. 3.

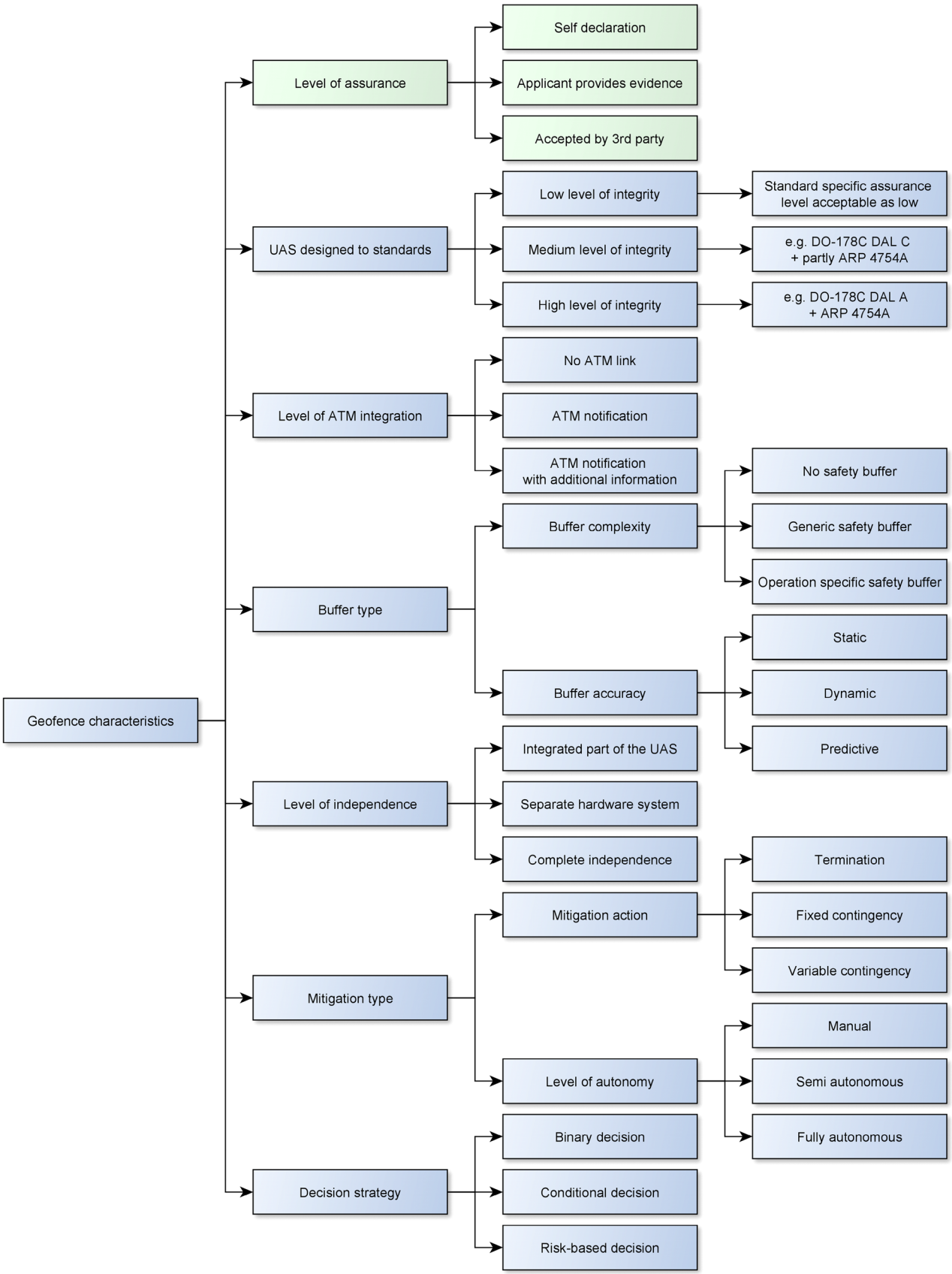

Fig. 5 Taxonomy of geofencing characteristics

Table 1 Example of geofencing requirements for specific category operation

ID	Characteristic	Requirement
1	Level of assurance	The geofencing system shall be developed using appropriate industry standards and utilizing a formal methodology (quality requirement)
2	Buffer type	The geofencing system shall supervise the UAS geo-localization and analyse the UAS position in regard to defined geofence borders to determine a geofence violation. In particular, this requires supervision and analysis of: Geofence coordinates UAS geo-localization
3	Buffer type, buffer complexity	The geofencing system shall incorporate an operation-specific safety buffer to maintain the geofence as a strict border even in case of a failure. In addition to already mentioned requirements, this includes supervision and analysis of worst-case assumptions: System dynamics, in particular, flight speed and altitude Termination scenario details Weather conditions
4	Buffer type, Buffer accuracy	The geofencing system shall calculate a dynamic safety buffer to maximize the flyable areas inside the geofence. In addition to already mentioned requirements, this includes supervision and analysis of real-time data: System dynamics, in particular, flight speed and altitude Weather conditions
5	Level of independence	The geofencing system shall be implemented by an independent hardware system to prevent single failures to cause a breach of the geofence
6	Mitigation type	The geofencing system shall trigger a mitigation action in case of a violation of the borders of the geofence
7	Mitigation type, Mitigation action	The mitigation shall ultimately result in a safe termination of the UAS to ensure containment of the geofence
8	Mitigation type, Mitigation action	The geofencing system may have additional contingency procedures for mitigation that try to prevent an impending safe termination
9	Mitigation type, Level of autonomy	The geofencing system shall have a semi-autonomous mode of operation, assuring containment of the geofence even without further pilot interaction
10	Level of ATM integration	The geofencing system shall trigger a notification to ATM in case of a violation of the geofence
11	Decision strategy	The geofencing system shall support conditional decisions to enable the crossing of borders between two adjacent geofencing areas of different types and properties

7 Monitoring robustness requirements

This section addresses the analysis of robustness of the proposed safe operation monitoring in respect to geofencing according to SORA. The current version of SORA offers a classification of robustness in two dimensions, integrity and assurance, with each three levels of graduation.

Based on the geofence characteristic shown in Sect. 6, it is now discussed which level of robustness is reasonable to achieve containment using geofence monitoring.

For our specific use case, the ALAADy project, the goal is to achieve the high robustness requirement level with our formal safe operation monitoring to be able to fly adjacent to populated environments.

To optimally use the concept of the specific category, the geofence safety buffer complexity should also be specific to the operation. It would result in a serious risk to allow the UAS to leave the geofence without any safety buffer before taking mitigation action. A simple generic safety buffer might define a time interval to react and trigger mitigation or as simple one-to-one rule. But without considering specific aspects, there might still remain the risk of the UAS violating the geofence during the mitigation action itself. As a result, this approach might result in extremely large safety buffers or may ultimately not be safe. However, the specific operation would allow tailoring the geofence to the exact operation using information defined in the concept of operations. This information could include system dynamics, mitigation actions, constraints for weather conditions and mission characteristics, such as flight attitude, manoeuvre complexity and speed. This approach allows for the exact tailoring of the geofence for the specific risk and thereby reducing safety buffers. Similarly, a dynamic safety buffer may not be needed to achieve a high robustness, but can be used to further reduce the safety buffer according to real-time flight attitude, speed as well as weather conditions, without increasing the risk. As a result, an operation-specific, and possibly dynamic safety buffer might enable operations that are not possible with a generic safety buffer, either due to remaining risk or impractically huge safety buffers. The implementation of the geofencing and monitoring hardware should be as independent as possible;

however, independent sensors may pose a challenge. To achieve safety and high automation, the level of autonomy should be high. However, economic aspects also play an important role in this. A conditional decision strategy is currently in research, as this approach could be necessary for some specific operations, such as air delivery. The mitigation action will be designed as a safe termination; a specially designed emergency parachute will be used to reduce the possible impact force significantly. Additional contingency procedures are planned, but would not be necessary from a safety perspective. Further research will need to elaborate whether the efforts to achieve the maximum level of robustness for each geofence characteristic are necessary, possible or commercially attractive. The overall goal is to lower the overall development costs by realizing a monitoring system that fulfils the containment requirements by itself.

8 Summary

This paper details the functional and quality requirements for UAS safe operation monitoring, specifically for the concept of specific operations that was introduced by EASA in late 2015. The proposed approach of safe operation monitoring is exemplified for the use case of geofencing; however, other use cases could be implemented analogously to the shown approach. Furthermore, a taxonomy of geofencing characteristics has been introduced and resulting requirements have been analysed in interdependence with the specific operation risk assessment and the concept of a safe operation monitor. This taxonomy was validated against the ALAADy use case. It can help to assess other geofencing implementations and might be reused and extended by other researchers.

Furthermore, the safe operation monitoring is suitable for implementation as a containment measure in regard to the SORA process because it triggers failsafe mechanisms and ensures a safe state. In the case of geofencing, this is done by a safe termination. Additionally, safe operation monitoring is also suitable to act as an operational safety objective (OSO) by triggering contingency procedures, e.g. by initiating a turn manoeuvre before violating the geofence. Finally, the robustness of geofencing implementations is discussed and assessed using the introduced taxonomy of geofencing characteristics in regard to the SORA process.

By always ensuring a safe termination and additionally utilizing the contingency procedures to prevent this termination, the safety hazard of an operation being out of control can be effectively managed by the proposed safe operation monitoring approach. As a result, the containment requirement level of rigour that is determined by the SORA process can be satisfied to lower the overall development and certification efforts and costs. However, this imposes that the safe operation monitoring itself is developed according to the higher level of rigour regarding the containment requirements. It is therefore recommended to use formal methods for the implementation or verification of the safe operation monitoring, to assure specific properties with mathematical rigour.

By doing this, this approach transfers efforts and costs from the overall aircraft specifically to the assurance of the monitoring methodology. The idea is that the formal language for specifying monitoring properties has to be developed once, and then properties and specifically geofences can be easily formulated and adapted. As long as the overall aircraft architecture respects the monitoring concept, the effort of implementing new monitors or a new geofence is limited to formulating it in the formal language. It is further important to notice that the monitoring approach is suitable to different kinds of properties. It is part of an ongoing research to determine what aircraft properties are necessary to supervise aircraft safety and enable a safe operation. One of these properties is the geofencing. As such, the safe operation monitoring can be reused for additional safety properties.

Acknowledgements Open Access funding provided by Projekt DEAL.

References

1. EASA: Introduction of a regulatory framework for the operation of unmanned aircraft; technical opinon. European Aviation Safety Agency, Cologne (2015)
2. EASA: Introduction of a regulatory framework for the operation of drones; advance notice of proposed amendment 2015–10. European Aviation Safety Agency, Cologne (2015)
3. EASA: Introduction of a regulatory framework for the operation of drones; advance notice of proposed amendment 2017–05. European Aviation Safety Agency, Cologne (2017)
4. JARUS Std. 2.0: JARUS guidelines on specific operations risk assessment (SORA) V2.0 (2019)
5. Dauer, J.C., Lorenz, S., Dittrich, J.S.: Automated low altitude air delivery. *Deutscher Luft- und Raumfahrtkongress DGLR*; Braunschweig, Germany; pp. 13–15 (2016). https://publikationen.dglr.de/?tx_dglrpublications_pi1[document_id]=420129. Accessed 8 May 2020
6. Allenby, K., Kelly, T.: Deriving safety requirements using scenarios. In: Fifth IEEE International Symposium on Requirements Engineering; Toronto; Canada; Aug. 27–31; pp. 228–235 (2001)

7. Hansen, K.M., Ravn, A.P., Stavridou, V.: From safety analysis to software requirements. IEEE Trans. Softw. Eng. **24**(7), 573–584 (1998)
8. Firesmith, D.: Engineering safety requirements, safety constraints, and safety-critical requirements. J. Object Technol. **3**(3), 27–42 (2005)
9. EASA.: UAS safety risk portfolio and analysis; report of safety intelligence and performance SM1.1, European Aviation Safety Agency (2016)
10. Clothier, R.A., Williams, B.P., Washington, A.: Development of a template safety case for unmanned aircraft operations over populous areas. In: SAE AeroTech 2015 Congress and Exhibit; Seattle; September (2015)
11. Ilker, A.: Regulating commercial drones: bridging the gap between american and european drone regulations. J. Int. Bus. Law **15**(2), (2016)
12. Dalamagkidis, K., Valavanis, K.P., Piegl, L.A.: On integrating unmanned aircraft systems into the national airspace system—issues, challenges, operational restrictions. Certification, and recommendations, 2nd edn. Springer, Berlin (2012)
13. Weibel, R.E., Hansman, R.J. Jr.: An integrated approach to evaluating risk mitigation measures for UAV operational concepts in the NAS. In: Infotech@Aerosspace; Arlington; Virginia 26–29; AIAA 2005–6957 (2005)
14. Clothier, R.A., Williams, B.P., Fulton, N.L.: Structuring the safety case for unmanned aircraft system operations in non-segregated airspace. Saf. Sci. **79**, 213–228 (2015)
15. Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., Robinson, J.: Unmanned aircraft system traffic management (UTM) concept of operations. In: 16th AIAA aviation technology, integration, and operations conference; Washington DC; June 13.-17.; AIAA 2016–3292 (2016)
16. Peinecke, N., Volkert, A., Korn, B.: Minimum risk low altitude airspace integration for larger cargo UAS. In: Proceedings of the IEEE Wnce (ICNS 2017); Washington DC; April 18–20 (2017)
17. Atkins, E.M.: Autonomy as an enabler of economically-viable; beyond-line-of-sight; low-altitude UAS applications with acceptable risk. In: AUVSI Unmanned Systems; Orlando, FL; May; pp. 200–2011 (2014)
18. Hayhurst, K.J., Maddalon, J.M., Neogi, N.A., Versynen, H.A.: A case study for assured containment. In: International Conference on Unmanned Aircraft Systems (ICUAS); Denver, CO; July (2015)
19. Dill, E.T., Young, S.D., Hayhurst, K.J.: Safeguard—an assured safety net technology for UAS. In: 35th Digital Avionics Systems conference (DASC); Sacramento, CA; September (2016)
20. Gurriet, T., Ciarletta, L.: Towards a generic and modular geofencing strategy for civilian UAVs. In: International conference on unmanend aircraft systems (ICUAS); Arlington, VA (2016)
21. D'Souza, S., Ishihara, A., Nikaido, B.: Feasibility of varying geofence around an unmanned aircraft operation based on vehicle performance and wind. In: 35th Digital Avionics Systems conference (DASC); Sacramento, CA; September (2016)
22. Gross, K.H., Clark, M.A., Hoffmann, J.A., Swenson, E.D., Fifarek, A.W.: Run-time assurance and formal methods analysis nonlinear system applied to nonlinear system control. J. Aerosp. Inf. Syst. **14**(4), 232–246 (2017)
23. Torens, C., Adolf, F.M., Faymonville, P., Schirmer, S.: Towards intelligent system health management using runtime monitoring. Infotech Aerospace, Grapevine (2017)
24. Usach, H., Torens, C., Adolf, F.M., Vila, J.: Architectural considerations towards automated contingency management for unmanned aircraft. Infotech Aerospace, Grapevine (2017)
25. Torens, C., Adolf, F.M., Goormann, L.: Certification and software verification considerations for autonomous unmanned aircraft. J. Aerosp. Inf. Syst. **11**(10), 649–664 (2014)
26. Davis, J.A., Clark, M., Cofer, D.D., Fifarek, A., Hinchman, J., Hoffman, J., Hulbert, B., Miller, S.P., Wagner, L.: Study on the barriers to the industrial adoption of formal methods. In: FMICS 2013. Lecture notes in computer science; vol 8187. Springer; Berlin, pp. 63–77 (2013)
27. RTCA.: DO-178B/ED-12B software considerations in airborne systems and equipment certification; Published Standard Document (1992)
28. RTCA.: DO-178C/ED-12C software considerations in airborne systems and equipment certification; Published Standard Document (2011)
29. RTCA.: DO-333 formal methods supplement to DO-178C and DO-278A; Published Standard Document (2011)
30. Whalen, M., Cofer, D., Miller, S., Krogh, B.H., Storm, W.: Integration of formal analysis into a model-based software development process: formal methods for industrial critical systems, pp. 68–84. Springer, Berlin (2008)
31. Habli, I., Kelly, T.: A generic goal-based certification argument for the justification of formal analysis. Electron. Notes Theor. Comput. Sci. **238**(4), 27–39 (2009)
32. Brown, D., Delseny, H., Hayhurst, K., Wiels, V.: Guidance for using formal methods in a certification context. In: Proceedigs of embedded real-time systems and software (2010)
33. https://www.eurocae.net/about-us/working-groups/. Accessed 8 Aug 2019
34. JARUS.: JARUS guidelines on specific operations risk assessment (SORA); JAR-DEL_WG6-D.04; Public Release; V1.0 Joint Authorities for Rulemaking of Unmanned Systems (2017)
35. Pape, M.: Potentialanalyse des Specific Operations Risk Assessments (SORA) für unbemannte Luftfahrzeuge, Studienarbeit TU Dresden, 30 April (2019)
36. Adolf, F.-M., Faymonville, P., Finkbeiner, B., Schirmer, S., Torens, C.: Stream runtime monitoring on UAS. In: lecture notes in computer science, 10548. Springer International Publishing AG 2017. International Conference on Runtime Verification, RV 2017, 13–16 Sep 2017, Seattle, WA, USA. https://doi.org/10.1007/978-3-319-67531-2_3 (2017) **(ISBN 978-3-319-67531-2)**