Onboard Functional Requirements for Specific Category UAS and Safe Operation Monitoring

Christoph Torens
German Aerospace Center (DLR), Institute of Flight Systems
Research Scientist
38108 Braunschweig, Germany
christoph.torens@dlr.de

Florian Nikodem
German Aerospace Center (DLR), Institute of Flight Systems
Research Scientist

Johann C. Dauer
German Aerospace Center (DLR), Institute of Flight Systems
Research Scientist

Joerg S. Dittrich
German Aerospace Center (DLR), Institute of Flight Systems
Head of Department Unmanned Aircraft

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 software components without reducing the overall safety of the unmanned aircraft system (UAS). Based on a safety assessment, the so called *specific category* enables new aircraft system architectures and mission designs. In this context, this paper proposes runtime monitoring as a mitigation strategy for the operation getting out of control to formally assure predefined properties in flight and thus assure the safety of the operation in progress. One particular aspect of this safe operation monitoring is geofencing, the capability to assure containment of the UAS in a previously restricted area. In the regulatory framework of a *specific operation* risk assessment, such a geofence can be interpreted as a harm barrier. The functional requirements for this geofencing use case are discussed regarding their impact on the underlying *specific operation* risk assessment. To achieve this, we develop a taxonomy of geofencing characteristics. 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, exemplified in this paper with the use case of geofencing, 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 3 categories of UAS operation that can be regulated and certified based on the intrinsic risks involved [1][2][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 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 rigor 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. By this means, 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 rigor 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, rigor 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. By designing the aircraft and defining appropriate use cases the risks involved can be determined. In particular it is important to develop a suitable, high-quality set of functional and safety requirements to support the necessary risk assessment. Furthermore, DLR is researching the use of a runtime monitor onboard a UAS to further support the concept of specific operation, Fig. 2. We refer to this monitor as to *safe operation monitor*. In particular, it is planned to monitor the aircraft at runtime and supervise specific properties and requirements that are related to safety as well as the specific mission operation. In contrast to manned aviation, where the pilot on-board manages hazardous situations, there is no person on board. Instead, the suggested monitor takes over parts of the supervisional tasks of the pilot that, 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 harm barrier 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 has to be suitable for an integration into the SORA holistic risk model in combination with the aforementioned monitoring approach.

The remainder of the paper is structured as follows: After highlighting some of the important related work in Section 2, the SORA process is briefly explained in Section 3. This process is used in Section 4 to explain and motivate the concept of monitoring of specific properties in flight. Section 5 categorizes 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 Section 6. These requirements are assessed in Section 7 with respect to the necessary SORA process and the resulting robustness levels are discussed and exemplified. Finally, Section 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, 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 quality measure of the software product or as basis for requirement definition [6][7][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 safety risks involved in 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 on risk based approaches, as does this work. In fact, EASA plans to implement risk based approaches in the near future [1][2][3][11]. The integration of UAS in civil airspaces, its safety aspects and risks thus received particular research interest, e.g. [12][13][14]. Smaller scale UAS often operate in very low level flight, which has been considered for airspace integration as well [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 also specifically targeted the safety requirements for geo-fencing [18]. One challenging aspect of geofencing approaches is the need of an assured source of positioning information as GPS can suffer from reliability issues. In [19], an architecture for a geofencing system is presented including a hazard assessment. The work suggests additional position infrastructure independent of GPS. Furthermore, an example of a geofencing system capable of handling automatic and remotely piloted

Christoph Torens, Florian Nikodem, Johann C. Dauer, Joerg S. Dittrich
Institute of Flight Systems, DLR - German Aerospace Center

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 a 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 by using mathematical rigor. Nonetheless, there is still 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 research is 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 SAFETY ASSESSMENT

As briefly discussed above, the open category addresses UAS operations that, regarding the risks to people and environment do not require an authorization by the national aviation authorities prior to the operation. For example, very small UAS and toy drones that do not pose any risk 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 phase of definition. The necessary efforts for certification of a specific category UAS are based on the SORA [4], which scales to the overall risk with an increasing level of rigor for aircraft development. 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.

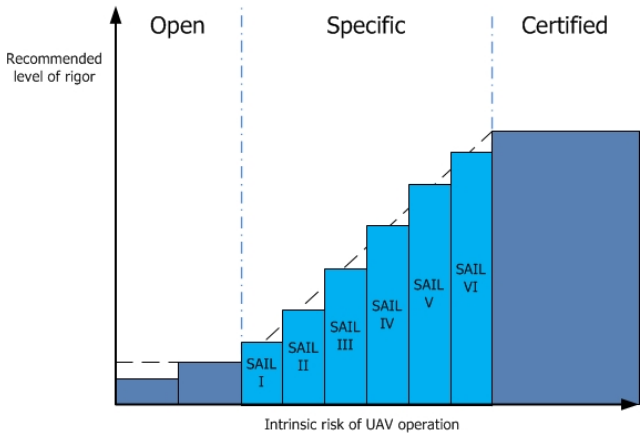

Figure 1: Specific assurance and integrety level, following [4]

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. 3. 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 scoring for ground and air risk can be done. 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 overflown area and a distinction between flight in visual line of sight (VLOS) and beyond visual line of sight (BVLOS). The air risk class, on the other hand, depends on the expected air traffic density near the flight path. Again, a distinction between VLOS and BVLOS is made. The higher of both classes determines the overall SAIL.

Each SAIL contains a number of requirements for the UAS and its operation, the so called threat barriers. These barriers 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 threat barrier has four level of robustness: optional, low, medium and high. As the SAIL increases, the same is required for the robustness of the threat barriers. Additionally, so called harm barriers are proposed. Harm barriers are measures to mitigate 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 harm barrier (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 a reduction of required robustness level of the threat barriers. A schematic of the underlying risk model with harms and threats as well as their barriers in interaction with the UAS operation out of control event is shown in Fig. 2.

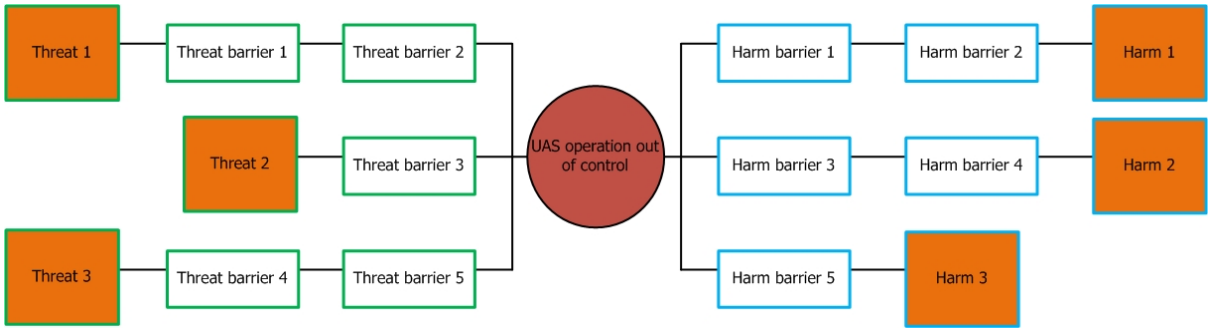

Figure 2: SORA risk model schematic, following [4]

Since the costs for certification by assuring threat barriers with high robustness can increase to levels almost equivalent to those of the certified category, it is expected to be cost effective to add harm barriers and increase their robustness to achieve an overall reduction of UAS development and operation costs. The interaction of the implementation and operation costs of harm and threat barriers, 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.

The harm barriers have so far been divided in four different categories for the ground risk class and six different categories for the air risk class. One of the harm barriers that can be found in ground and air risk class that is specifically important for this paper is “Technical containment to reduce the number of people at risk is in place and effective”. A possibility to reduce the number of people at risk is to restrict the UAS area of operation. Our approach uses runtime monitoring to supervise properties of the aircraft as well as the operation. A specific use case of restricting operational behaviour is geofencing. Geofencing and its functional as well as quality requirements will be discussed as an exemplary use case for our monitoring approach.

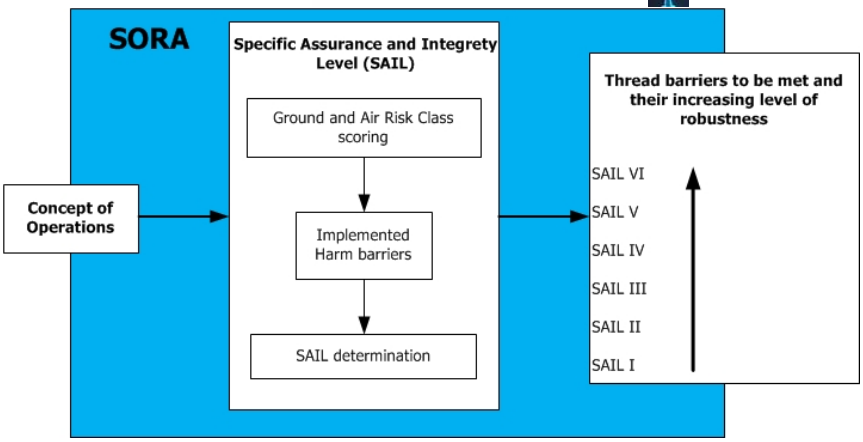

Figure 3: Simplified SORA process, following [4]

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 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 a lot of 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 methodology for the monitoring 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 monitoring of specific properties that is capable of describing complex time-dependent properties, additional, also higher level tasks, can be safely automated. In this paper we discuss the functional requirements of geofencing and how geofencing can be implemented using a runtime monitoring methodology.

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

In the case of geofencing the monitoring module must be able to assess various data of the UAS in real time. The current geo-localization of the UAS needs to be assessed in context of a given geofence. It is the responsibility of the monitoring to determine if the aircraft poses a risk in the given situation, see Section 3.

The monitoring alone, however, cannot render the aircraft operation safe. It rather enables to take an action that will resolve the situation. The action that is triggered by a monitor 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 out of the economic perspective, this approach can guarantee a permanent safe state, as long as the aircraft stays within the geofence. It is, however, possible, in addition to the safe termination, to define additional contingency procedures that try to prevent a termination, see Fig 4.

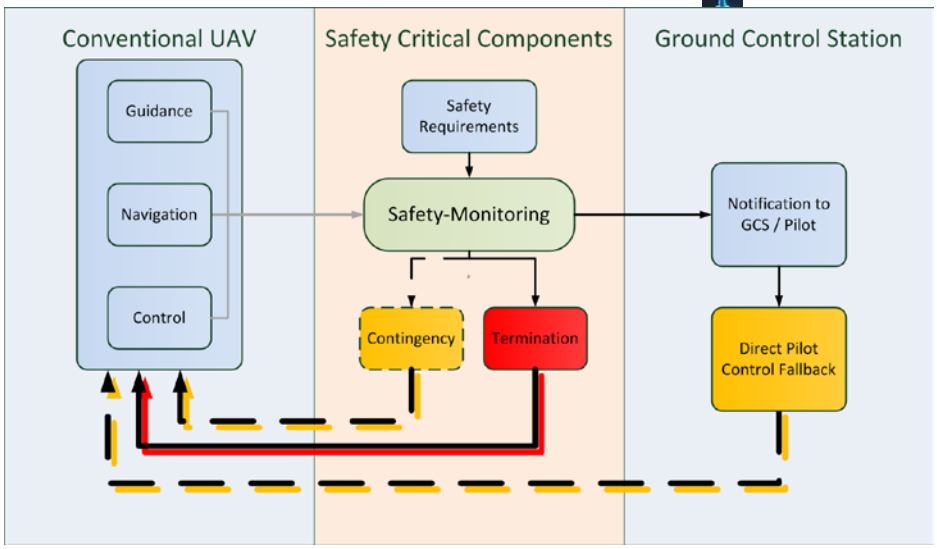

Figure 4: UAS Safe Operation Monitor Concept

5 ASSESSMENT OF MONITORING AS PART OF SORA

It was mentioned before that our monitoring approach, for the use case of geofencing, can be interpreted as a harm barrier. In addition to that, an important question is, if in general the concept of runtime monitoring may also be used as a threat barrier. As stated above, threat barriers are active before an event occurs that may lead to UAS operation out of control. Harm barriers are active after such an event occurred. Regarding this definition, a monitoring concept that implements geofencing can act as both, harm and a threat barrier. In the case that the UAS leaves the geofence, the operation is out of control. As a result, the monitoring would immediately trigger the termination of the UAS. In this scenario, the monitoring acts as a harm barrier according to SORA, since the intervention takes place after the event occurs.
On the other hand, it is possible to let the monitor assess the general risk of the UAS violating the geofence with respect to the actual flight state and ensure necessary safety buffers. In that case, a contingency procedure could be triggered even before the UAS leaves the geofence. As a result, the monitor would act as a threat barrier. Furthermore, the proposed safe operation monitor may also be used as an unrelated threat barrier. For example, the system can monitor the GPS signal performance and, in case of deterioration, can initiate contingency procedures to improve GPS signal strength. These contingency procedures would be defined in the concept of operations and could ultimately prevent the need to terminate the UAS. In particular, a GPS signal source can be regarded as an “external system that supports the UAS operation” and the management of its deterioration is a threat barrier according to SORA. Aspects of contingency management using the runtime monitoring approach are discussed in [24]. As a result, threat barriers play an important role, regarding the economic efficiency, the general acceptance of UAS and the public view on their reliability.
In conclusion, it can be stated that the harm barrier aspect of the safe operation monitor has to be carried out as robust as possible to achieve a lower SAIL. In addition to that, a complete runtime monitoring concept should of course include threat barriers to further support system reliability. When used as threat barrier the minimum robustness requirement determined by the SAIL has to be met.

6 MONITORING FUNCTIONAL REQUIREMENTS

Requirements management is a crucial part of each development process. The general approach to develop functional requirements is to derive them from higher level aircraft requirements. In this case, our functional requirements result from UAS high level functions and high level system 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 behavioral 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 fulfill 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.

6.1 Characteristics of geofencing

Geofencing simply means that the area where an unmanned aircraft is allowed to fly in is restricted, and that restriction 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. The 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 fly as near 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, see Fig. 5.

Buffer type 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 safety buffer*. 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 producing a serious risk. 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 an 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 *predictive* control, by using complex models for flight envelope calculation.

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 by using a *separate hardware system* for the geofencing system. A *complete independence* of the geofencing could be achieved by utilization of dedicated sensors.

The *mitigation type* is sub categorized in *mitigation action* and *level of autonomy*. The ultimate mitigation action to contain a UAS inside a geofence, even for severe malfunctions, is the safe *termination* 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 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

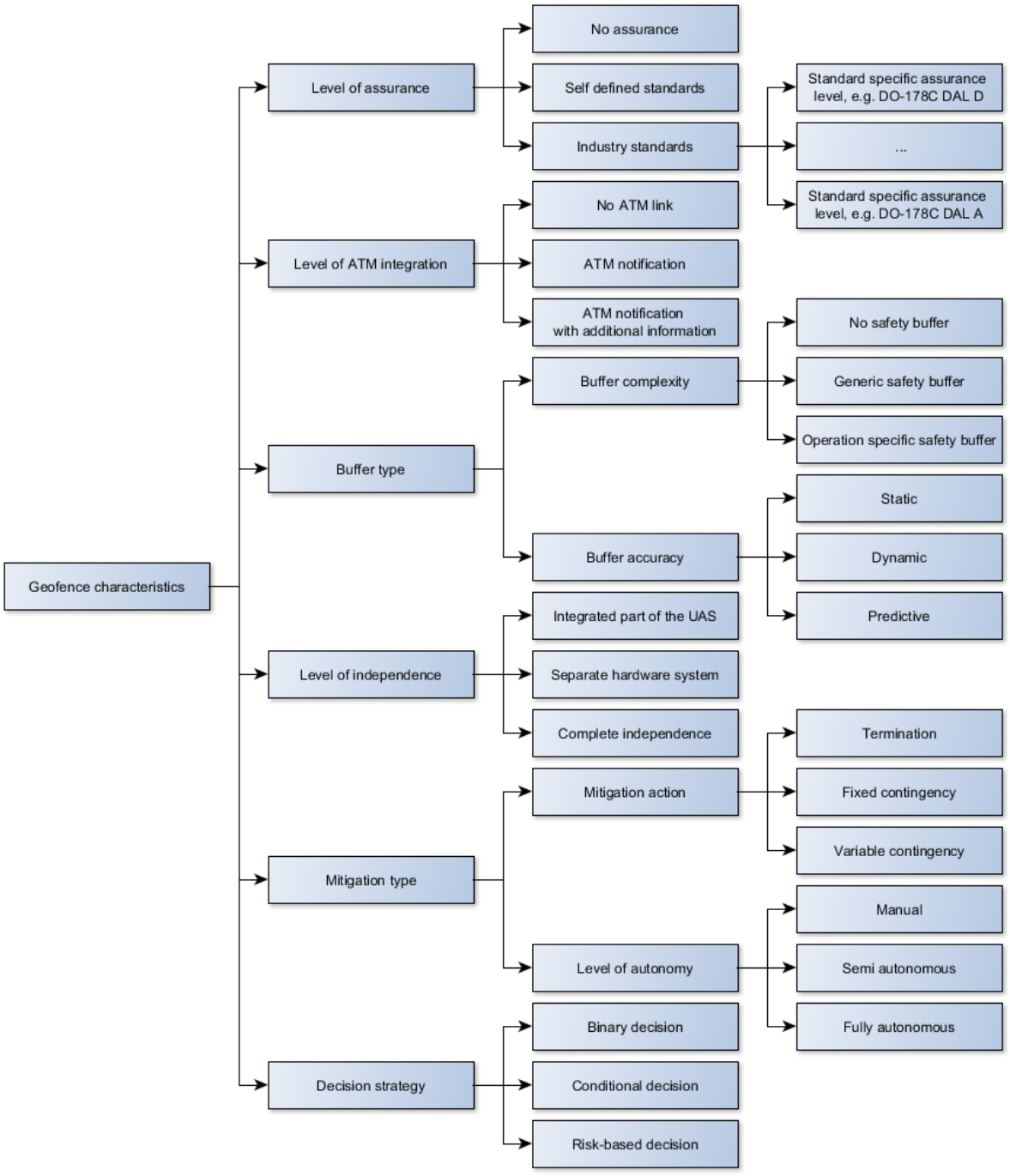

Figure 5: Taxonomy of geofencing characteristics

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 a mitigation action cannot be overruled by a pilot.

The *level of assurance* describes the verification and validation aspects of the geofencing implementation. This aspect is considered a quality requirement. There could simply be *no assurance*. Additionally, the assurance could be implemented by *self-defined standards* for verification and validation by the operator or manufacturer. The next step would be to use *industry standards* for verification and validation. Additionally, it should be noted that industry standards, such as DO-178C, define different design assurance levels with increasing requirements for higher assurance levels,

Christoph Torens, Florian Nikodem, Johann C. Dauer, Joerg S. Dittrich
Institute of Flight Systems, DLR - German Aerospace Center

according to the results of a safety assessment. Finally, the utilization of formal methods can improve assurance, since specific properties can be verified with mathematical rigor.

Level of ATM integration details if there is a link between the geofencing system and air traffic management. There can be *no link* between geofence and ATM, but it would be 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.

As a final characteristic, we want to discuss 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. DLR currently researches these aspects in ongoing projects. As a result, the decision strategy could incorporate *conditional decisions* for crossing one geofence to enter another adjacent geofence 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.

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. As a use case of specific operation, DLR currently researches automated low altitude air delivery with its project ALAADy. The following requirements are motivated from this specific use case.

After developing such a set of functional safety requirements, these requirements need to be further analysed and transformed to properties suitable for runtime monitoring. The difficulty in the above requirements is a 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 Section 3.

7 MONITORING ROBUSTNESS REQUIREMENTS AND ASSESSMENT

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 low medium and high, but it is not defined yet what is necessary to gain a certain robustness classification. However the robustness of harm and threat barriers is used to express a determined Specific Assurance and Integrity Level (SAIL) to categorize the UAS operation. Following this wording it is intended that the robustness should be the interaction of a level of *integrity* and a level of *assurance*. The integrity represents the extent and quantity of the technical implementation of the harm or threat barrier itself. The assurance addresses the aspect of how the barrier is developed. The assurance level is a combination of the used standards in development, e.g. a self-defined standard or an industry standard, and the kind of certification of this standard.

The approach to determine the robustness level under the consideration of integrity and assurance is shown in the table below. The table shows a matrix of the integrity of technical implementation versus the standard of assurance in low, medium and high. Together they result in an overall robustness level of the evaluated harm or threat barrier. The matrix can be used to determine the robustness of any kind of harm or threat barrier.

Based on the geofence characteristic shown in Section 6 and Fig. 5, it is now discussed which robustness level is reasonable to achieve. The geofence characteristics, level of ATM integration, buffer type, level of independence, mitigation type and decision strategy correspond to the classification as integrity level of technical implementation. The level of assurance in the diagram

directly represents the standard of assurance in Table 2. No assurance will lead to a low overall robustness, even for complex concepts of harm barrier implementations. Self-defined standards

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 utilize 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 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 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.

Table 2: Matrix for harm and threat barrier robustness determination

Robustness aspects	Low standard of assurance	Medium standard of assurance	High standard of assurance
Low integrity of technical implementation	Low robustness	Low robustness	Low robustness
Medium integrity of technical implementation	Low robustness	Medium robustness	Medium robustness
High integrity of technical implementation	Low robustness	Medium robustness	High robustness

without a third party certification may correspond to a medium standard of assurance. The use of industry standards in addition to a third party certification of the organization or the convincing use of formal methods may comply with a high standard of assurance. However, for the development of a geofencing and safety operation monitoring concept there might be more than one adequate industry standard available. Different standards may address different levels of rigor. The requirements for an industry standard and the kind of certification still need to be discussed, but are beyond the scope of this paper.
For our specific use case, the ALAADy Project, the goal is to achieve a high robustness of geofencing to achieve a maximum reduction of harm risk and thus a lower classification in respect to the SAIL level. From the assurance level point of view, the use of formal methods enables strong evidence for verification and validation. An independent assessment by an authority is not in the scope of our current project, but is reasonable with growing acceptance of formal methods also for certification credit [28]. With the remaining aspect of robustness, the integrity of the technical implementation, we aimed for at least medium or high complexity for each of the geofence characteristics. Hence, the monitoring and geofence concept would be developed with the use of industrial known standards to achieve product level maturity. Additionally, an air traffic management notification is included if possible.
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. 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, by 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 impracticality 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, also economic aspects play in 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 special 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 if 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 high robustness in harm barriers and thus ultimately a lower SAIL classification. Finally, the differentiation between the different robustness levels will need further research and standardization, to determine what the requirements are for each category for a low, medium or high robustness.

8 CONCLUSION

This paper details on 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 in analogy to the shown approach. In particular, 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.

Furthermore, it discusses that the safe operation monitoring is suitable for implementing harm barriers in regard to the SORA process, by triggering failsafe mechanisms and ensuring 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 a threat barrier 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 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 overall SAIL level that is determined by the SORA process can be reduced to lower the overall development and certification efforts and costs. However, this imposes that the safe operation monitoring itself is developed assuring a high level of robustness. It is therefore recommended to use formal methods for the implementation or verification of the safe operation monitoring, to assure specific properties with mathematical rigor.

REFERENCES

1. EASA; 2015; “Introduction of a regulatory framework for the operation of unmanned aircraft”; Technical Opinion; European Aviation Safety Agency.
2. EASA; 2015; “Introduction of a regulatory framework for the operation of drones” Advance Notice of Proposed Amendment 2015-10; European Aviation Safety Agency.
3. EASA; 2017; “Introduction of a regulatory framework for the operation of drones”; Advance Notice of Proposed Amendment 2017-05; European Aviation Safety Agency.
4. JARUS; 2016; “JARUS guidelines on Specific Operations Risk Assessment (SORA)”; JAR-DEL_WG6-D.03; Draft for public consultation; V0.2 Joint Authorities for Rulemaking of Unmanned Systems
5. J. C. Dauer, S. Lorenz, J. S. Dittrich; 2016; “Automated Low Altitude Air Delivery“; *Deutscher Luft- und Raumfahrtkongress DGLR*; Braunschweig, Germany; 13.-15. Sep. 2016; http://publikationen.dglr.de/?tx_dglrpublications_pi1[document_id]=420129
6. K. Allenby, T. Kelly; 2001; “Deriving Safety Requirements Using Scenarios”;; *Fifth IEEE International Symposium on Requirements Engineering*; Toronto; Canada; Aug. 27-31; pp. 228-235.
7. K. M. Hansen, A. P. Ravn, V. Stavridou; 1998; "From safety analysis to software requirements;" *IEEE Transactions on Software Engineering*; **24**(7); pp. 573-584.
8. D. Firesmith; 2005; “Engineering Safety Requirements, Safety Constraints, and Safety-Critical Requirements”, *Journal of Object Technology*, **3**(3); March-April; pp. 27-42.
9. EASA; 2016; “UAS Safety Risk Portfolio and Analysis”; Report of Safety Intelligence and Performance SM1.1; European Aviation Safety Agency; October.
10. R.A. Clothier, B.P. Williams, A. Washington; 2015; “Development of a Template Safety Case for Unmanned Aircraft Operations Over Populous Areas”; SAE AeroTech 2015 Congress and Exhibit; Seattle; September.
11. A. Ilker; 2016; “Regulating Commercial Drones: Bridging the Gap Between American and European Drone Regulations”; *Journal of International Business and Law*; **15** (2); Article 11.
12. K. Dalamagkidis, K.P. Valavanis, L.A. Piegl; 2012; “On integrating unmanned aircraft systems into the national airspace system - Issues, Challenges, Operational Restrictions. Certification, and recommendations”; Second Edition; Springer; Berlin; New York.
13. R.E. Weibel, R.J. Hansman Jr; 2005; „An Integrated Approach to Evaluating Risk Mitigation Measures for UAV Operational Concepts in the NAS”; Infotech@Aerosspace; Arlington; Virginia 26-29; AIAA 2005-6957
14. R.A. Clothier, B.P. Williams, N.L. Fulton; 2015; “Structuring the safety case for unmanned aircraft system operations in non-segregated airspace”; *Safety Science*; 79; pp. 213-228.
15. P. Kopardekar, J. Rios, T. Prevot, M. Johnson, J. Jung, J. Robinson; 2016 “Unmanned Aircraft System Traffic Management (UTM) Concept of Operations” *16th AIAA Aviation Technology, Integration, and Operations Conference*; Washington DC; June 13.-17.; AIAA 2016-3292.
16. Peinecke, Niklas; Volkert, Andreas; Korn, Bernd; 2017; “Minimum Risk Low Altitude Airspace Integration for Larger Cargo UAS”; *Proceedings of the IEEE Integrated Communications Navigation and Surveillance Conference (ICNS 2017)*; Washington DC; April 18.-20.
17. E.M. Atkins; 2014; “Autonomy as an Enabler of Economically-Viable; Beyond-Line-of-Sight; Low-Altitude UAS Applications With Acceptable Risk” *AUVSI Unmanned Systems*; Orlando, FL; May; pp. 200-2011.

18. K.J. Hayhurst, J.M. Maddalon, N.A. Neogi, H.A. Versynen; 2015; "A Case Study for Assured Containment"; *International Conference on Unmanned Aircraft Systems (ICUAS*); Denver, CO; July.
19. E.T. Dill, S.D. Young, K.J. Hayhurst; 2016; "Safeguard – An Assured Safety Net Technology for UAS"; *35th Digital Avionics Systems conference (DASC)*; Sacramento, CA; September.
20. T. Gurriet, L. Ciarletta; "Towards a Generic and Modular Geofencing Strategy for Civilian UAVs"; *International Conference on Unmanend Aircraft Systems (ICUAS);* Arlington, VA; June.
21. S. D'Souza, A. Ishihara, B. Nikaido; 2016 "Feasibility of Varying Geo-Fence around an Unmanned Aircraft Operation based on Vehicle Performance and Wind"; *35th Digital Avionics Systems conference (DASC)*; Sacramento, CA; September.
22. K.H. Gross, M.A. Clark, J.A. Hoffmann, E.D. Swenson, A.W. Fifarek; 2017; "Run-Time Assurance and Formal Methods Analysis Nonlinear System Applied to Nonlinear System Control" *Journal of Aerospace Information Systems*; **14** (4); pp. 232-246
23. C. Torens, F.M. Adolf, P. Faymonville, S. Schirmer; "Towards Intelligent System Health Management using Runtime Monitoring"; *Infotech @ Aerospace*. Grapevine, Texas; January.
24. H. Usach, C. Torens, F.M. Adolf, J. Vila; 2017;" Architectural Considerations Towards Automated Contingency Management for Unmanned Aircraft";*Infotech @ Aerospace*. Grapevine, Texas; January.
25. C. Torens, F.M. Adolf, L. Goormann; 2014; "Certification and Software Verification Considerations for Autonomous Unmanned Aircraft" *Journal of Aerospace Information Systems*; **11** (10); pp. 649-664.
26. J. A. Davis, M. Clark, D. D. Cofer, A. Fifarek, J. Hinchman, J. Hoffman, B. Hulbert, S. P. Miller, L. Wagner; 2013; "Study on the Barriers to the Industrial Adoption of Formal Methods"; *FMICS 2013. Lecture Notes in Computer Science; vol 8187.* Springer; Berlin, Heidelberg; pp. 63–77.
27. RTCA; 1992; "DO-178B/ED-12B Software Considerations in Airborne Systems and Equipment Certification"; Published Standard Document.
28. RTCA; 2011; "DO-178C/ED-12C Software Considerations in Airborne Systems and Equipment Certification"; Published Standard Document.
29. RTCA; 2011; "DO-333 Formal Methods Supplement to DO-178C and DO-278A"; Published Standard Document.
30. M. Whalen, D. Cofer, S. Miller, B. H. Krogh, W. Storm; 2008; "Integration of formal analysis into a model-based software development process"; Formal Methods for Industrial Critical Systems; Springer; pp. 68–84.
31. I. Habli, T. Kelly; 2009; "A generic goal-based certification argument for the justification of formal analysis"; Electronic Notes in Theoretical Computer Science; Vol. 238; No. 4; pp. 27–39.
32. D. Brown, H. Delseny, K. Hayhurst, V. Wiels; 2010; "Guidance for using formal methods in a certification context"; Proc. Embedded Real-Time Systems and Software.

