A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category

Trung Duc Tran, Jean-Marc Thiriet, Nicolas Marchand, Amin El Mrabti

Noname manuscript No.
(will be inserted by the editor)

A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category

Trung Duc Tran · Jean-Marc Thiriet · Nicolas Marchand · Amin El Mrabti ·

Received: date / Accepted: date

Abstract Nowadays, safety and cybersecurity are some of the most important issues involving the development of Unmanned Aircraft System (UAS) operations. For safety, the lawmakers and aviation authorities have a lot of efforts to establish an adequate safety level for UAS operations within the current airspace system. One of them is the Specific Operation Risk Assessment (SORA) methodology developed by Joint Authorities for Rulemaking on Unmanned Aircraft System (JARUS). This methodology provides a guide to conduct risk assessments for UAS operations under the Specific Category. However, the methodology supports only some problems related to safety. In this paper, we introduce our approach to extend the SORA methodology toward cybersecurity. We illustrate this approach by extending the methodology to cover the privacy problem - an aspect related to cybersecurity. Besides that, we also introduce our supporting tool in the form of a web application that helps users conduct automatic risk assessments.

Keywords UAS · Specific Operation · Cybersecurity · SORA · Risk assessment · Privacy

This is an extended version of the paper published in the Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS'20), Athens, Greece [1]

Trung Duc Tran
Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-lab, 38000 Grenoble, France
SOGILIS Company, 38000 Grenoble, France
E-mail: tran.trung.duc1503@gmail.com

Jean-Marc Thiriet
Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-lab, 38000 Grenoble, France
E-mail: Jean-marc.thiriet@gipsa-lab.grenoble-inp.fr

Nicolas Marchand
Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-lab, 38000 Grenoble, France
E-mail: Nicolas.Marchand@gipsa-lab.grenoble-inp.fr

Amin El Mrabti
SOGILIS Company, 38000 Grenoble, France
E-mail: amin@sogilis.com

1 INTRODUCTION

1.1 Context

The history of UASs started in the late 1900s when they were first used as targets for military practices [2]. From that moment, the UAS market has been shaped. In the last century, the market focused on only military applications, such as recognition/combat missions, while civil applications of UAS were not recognized. Since the 2000s, the UAS market for civil applications has started to grow up. In the beginning, unmanned aircraft were used as toys for individual entertainment purposes in the civilian context. Then, the development of technology (such as miniaturizing components, increasing computing power, improving sensor and battery capacity) makes UASs smaller and more attractive for professional and commercial uses in many sectors of the economy, such as photography/media, agriculture, transportation, energy, etc. [3]. For the last decade, we have recognized an explosion of the civil UAS market. From 2012 to 2019, over $3 billion were invested in this domain, and the market size grows from $2 billion in 2016 [4] to $14.1 billion in 2018 [5].

Looking forward to the future of the civil UAS, many organizations and market research companies present market forecasts. SESAR Joint Undertaking predicts that there will be around 400,000 commercial drones flying over the sky of Europe (excluding seven million leisure drones) in 2050 [6]. According to Market Research Future, the civil drone market's size will be $70 billion of valuation in 2027 [7]. The Drone Industry Insights predicts that the civil drone market will reach $ 43.1 billion in 2024 [4]. Interact Analysis company forecasts $15 billion as the market's value in 2022 [8]. Although these numbers are only predictions that could be more or less accurate, they are all optimistic. In other words, these numbers reflect the confidence in the growth of the civilian drone market in the near future. However, there are still barriers to the advantage of this market. One of the most important issues involves the current regulations, limiting the application of UASs for some reasons: safety, security, and privacy [9].

To deal with the progression of UAS operations and develop a regulatory framework for UASs, the European lawmakers considered firstly the UASs with more than 150 kg takeoff weight in the Regulation (EC) No 216/2008, then all kinds of UASs in the new Regulation (EU) 2018/1139. These regulations define the common rules in the field of civil aviation. For the UAS operations, the 2018/1139 regulation sets down the risk-based approach to develop a regulatory framework. It means that the rules and procedures applied to a UAS operation should be proportional to the risk involved. In 2019, following the common rules, the European Commission issued the Delegated Regulation 2019/945 and the Implementing Regulation 2019/947. They consist of detailed rules on many aspects: certification, EU operators, third countries operators, UAS design, and communication systems [10]. According to the operation classification proposed by the European Aviation Safety Agency (EASA), these rules are defined. There are three risk-based operation categories: Open, Specific, and Certified [11]. For all "Specific" and "Certified" operations, the Implementing Regulation 2019/947 requires to conduct operation risk assessments to obtain operational authorizations. In this work, we are interested in the risk assessment under the "Specific" category, covering most commercial UAS operations. Moreover, the risk assessment should not be limited to aviation safety.

It should consider the safety of other domains depending on the operation context (e.g., telecommunication, infrastructures, transportation, and so on.); it should also cover the interdependence between safety and cybersecurity/privacy [10, 12].

1.2 Related works and contribution

Generally, the risk assessment consists of several tasks such as risk identification, risk analysis, risk evaluation. For these tasks, a lot of techniques have been developed. In the field of safety, risk assessment techniques have been considered since the 1940s. Up to now, there are more than a hundred different techniques [13]. Some typical and widely used ones could be named HAZOP, Fault Tree Analysis (FTA), Fault Mode and Effect Analysis (FMEA), Bow-tie analysis, Markov Analysis, Petri-nets Analysis. Meanwhile, in cybersecurity, the risk assessment started to be considered later in the 1980s when the digital systems became more and more popular with the increase of connectivity. Safety and cybersecurity (and security in general) have many common points. The biggest difference between them is that security refers to the risk originating from malicious actions/attacks while safety addresses the risk originating from accidents [14], [15], [16], [17]. Therefore, many risk assessment techniques in cybersecurity are inspired by the existing ones in the field of safety. For example, the Attack Tree Analysis (FTA) is based on the Fault Tree Analysis (FTA) [18]; the Intrusion Modes and Effects Analysis (IMEA) comes from from the Failure Mode and Effects Analysis (FMEA) [19]. Markov analysis [20], and Petri-net analysis [21] are brought from safety to security. Moreover, there also seems to be a trend towards developing integrated techniques to conduct the safety risk assessment and the cybersecurity risk assessment. For example, Kornecki et al. proposed an integrated technique based on FTA for air traffic management system [22]; Schmittner [23] proposed another one based on FMEV and illustrated it in the context of an Industrial Control and Automation System (ICAS); Abdo [24] proposed a technique to deal with uncertainties in a risk assessment combining safety and security.

Besides individual techniques, industrial standards and methodologies related to safety or security have been developed and introduced to provide completed guidelines in different industries. For example, we have the IEC 61508 standard for the safety of electrical/electronic/programmable electronic (E/E/PE) systems [25]; the ARP4761 standards for the safety of avionic systems [26]; the ISO 27000 standard series for the security of information systems [27]; the IEC 62443 standard for cybersecurity of ICAS [28], the EVITAD project for networked automobile systems [29], the DO-326 standard for the cybersecurity of avionic systems [30]... The safety and security integrated approaches also attract the consideration of the industries. For example, the DO-326 standard was developed to extend the safety-based process defined in the ARP4761 standard toward cybersecurity. Another example is the evolution of the IEC 61508 - the IEC 63187 standard, which is being developed to adapt better the current technology development and take into account the cybersecurity aspect [31].

Regarding UAS operations, in 2019, the European Union Aviation Safety Agency endorsed the methodology Specific Operation Risk Assessment (SORA) as an acceptable means for the rules about the risk assessment in the Implementing Regulation 2019/947. The methodology provides users with a guide to conduct a

risk assessment. Using this guide, users need only to consult the provided tables to identify safety measures that are required for their UAS operations. However, the concept of this tool is not clearly introduced in its documentation. This methodology concerns only the safety aspect of Specific UAS operations but not the cybersecurity [32]. Therefore, we want to extend the SORA methodology toward cybersecurity aspects.

The present paper completes our previous paper presented in the 2020 International Conference on Unmanned Aircraft Systems (ICUAS) [1]. In the conference paper, we explained the SORA methodology's principles and introduced our general scheme to extend this methodology toward cybersecurity. In the present paper, we first refine the explanation of the SORA methodology and our scheme. Then we introduce our web-based tool to automatically perform a risk assessment based on the extended SORA methodology. In the end, we perform a risk assessment with our tool for a real case study.

The remaining of this document is organized as follows. The concept of the SORA methodology is explained in Section 2. An approach to extend the methodology is given in Section 3. An extension of SORA methodology with the privacy harm is given in Section 4. Our web-based risk assessment tool is introduced in Section 5. A case study is presented in Section 6. We conclude our works and present our perspective on the future works in Section 7.

2 Explanation of the SORA methodology

The Specific Operations Risk Assessment (SORA) is a holistic and operation-centric methodology [33] proposed by a group of experts from the National Aviation Authorities - Joint Authorities for Rulemaking on Unmanned Systems (JARUS) [34, 35]. The methodology helps analyze a given UAS operation to determine the safety objectives (in training, system performance, organization, development), which need to be achieved. This methodology could be useful for different kinds of stakeholders. Operators (who operate the UAS) and the aviation authorities could use this methodology to conform to the EU regulations and used for the communication purpose in administrative processes. Manufacturers (who design and develop UAS) could use the SORA methodology to determine safety features that their designs need to reach for targeted operations under Specific category. In this section, we explain the methodology's general concept, including two parts: risk model, assessment process.

2.1 Risk model

The SORA methodology uses a bow-tie model (Figure 1) to illustrate the risk scenarios under consideration. It is necessary to understand the model to understand the basics of the methodology. The main elements of this model include (1) a Hazard, (2) Threats, (3) Harms, and (4) Barriers.

1. The Hazard is the central point of the bow-tie graph. It refers to the situation that an operation is conducted outside of the operator's intention (e.g the aircraft flies outside of visual observation of the pilot in a Visual Line Of Sight operation).

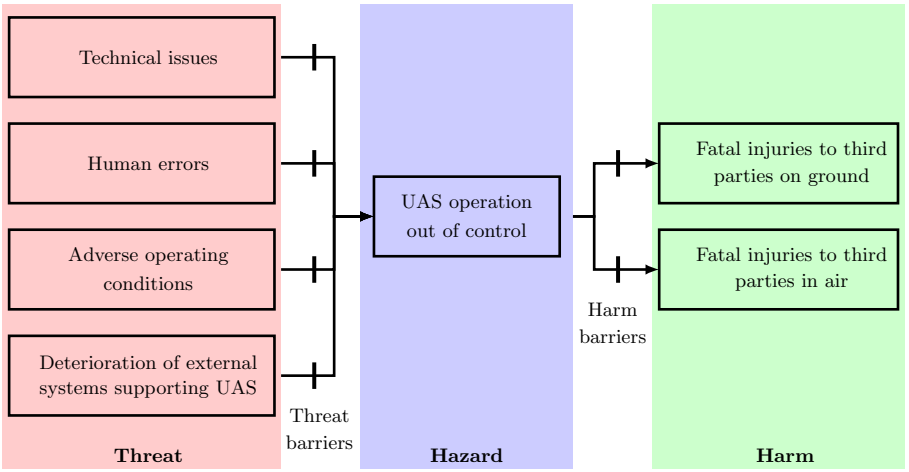

Fig. 1: Risk model of the SORA methodology represented as a bow-tie graph

2. The Threats locate on the left of the Hazard. They are the possible causes of the Hazard. Because the SORA methodology considers only the safety aspect, the bow-tie graph illustrates only some unintentional threat categories as shown in Figure 1.
3. The Harms locate on the Hazard's right side and represent the possible consequences of Hazard or the final outcome of the scenarios. At this moment, the SORA methodology considers only two kinds of harms related to person's life: "fatal injuries to third parties on ground", "fatal injuries to third parties in air" (see Figure 1). The likelihood of each Harms could be decomposed into three elements as shown in Figure 2.

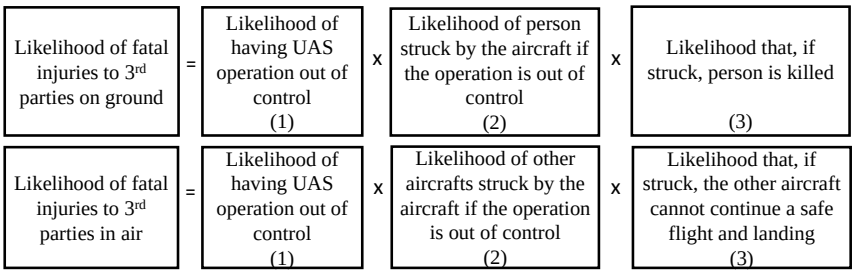

Fig. 2: Likelihood of fatal injuries on ground and in air [32]

4. There are two kinds of barriers: Threat barrier and Harm barrier. Harm barriers prevent the occurrence of Harms after a Hazard occurrence. In other words, the Harm barriers allow us to decrease the value of the elements (2) and the elements (3) shown in Figure 2. Threat barriers prevent Hazard occurrences. In other words, the Threat barriers allow us to decrease the likelihood of having a UAS operation out of control (element (1) in Figure 2). For each category of threat, different Threat barriers will be determined at the end of the risk

assessment under the form of Operation Safety Objectives (OSO). Each OSO is detailed in three levels of robustness (Low, Medium, High). An example of OSO is that "the UAS is developed according to design standards recognized by authorities" [36]. At different robustness levels of this OSO, the applicant should satisfy different requirements. At the low robustness level, the applicant should only declare the required standards are achieved. At the medium robustness, the applicant has to provide supporting evidence (such as analysis, simulation result) to prove the compliance with the declared standards. At the high robustness level, the supporting evidence shall be validated by competent third parties.

In the next part, we explain the assessment process of the SORA methodology based on the above risk model.

2.2 Assessment process

The SORA methodology proposes a qualitative approach for the assessment as shown in Figure 3. This approach could be explained as follows:

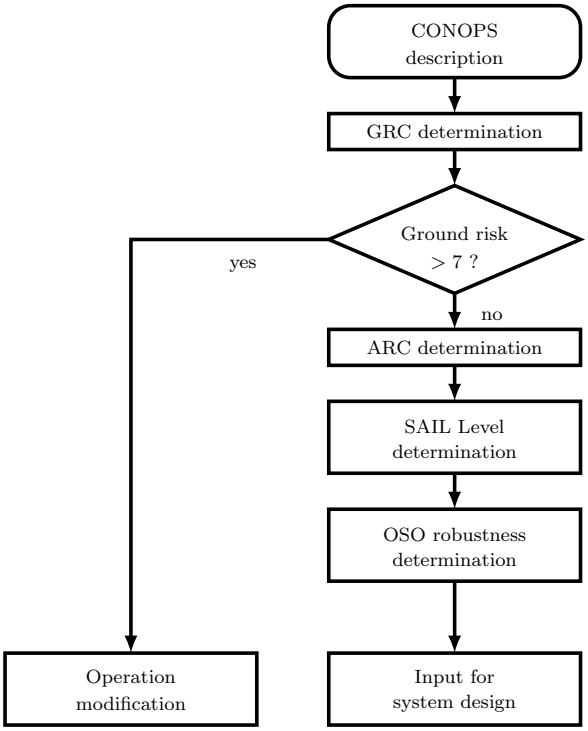

Fig. 3: Simplified risk assessment process

– **Objective:** Given a UAS operation, we need to maintain the likelihood of each harm at an acceptable level.

- **Firstly**, we collect the information on the intended operation by writing a Concept of Operation (CONOPS) description.
- **Secondly**, we determine the operation's GRC value (Ground Risk Class). This value represents the likelihood of injured on the ground due to a UAS operation out of control. In other words, this value corresponds to the combination of the elements (2) and (3) of the first equation in Figure 2. To determine the GRC, we assess the operation's intrinsic features and the Threat barriers in place. The intrinsic features, including aircraft characteristics and operation environment, allows us to determine the intrinsic value of GRC (see Table 1). Then, we consider the Threat barriers to adjust the final value of GRC. For example, a parachute is a Threat barrier which decreases the likelihood of Harms to the people on the ground. Therefore, we could reduce the GRC value by equipping the aircraft with a certified parachute. We could find the detail of Threat barriers within the official SORA document [37].

Intrinsic Ground Risk Class				
Max vehicle dimension	1 m	3 m	8 m	>8 m
Operation scenario				
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS in sparsely populated environment	2	3	4	5
BVLOS in sparsely populated environment	3	4	5	6
VLOS in populated environment	4	5	6	8
BVLOS in populated environment	5	6	8	10
VLOS over gathering of people	7	No available		
BVLOS over gathering of people	9			

Table 1: Intrinsic GRC table from the SORA methodology

- **Thirdly**, we determine qualitatively the likelihood of fatal accidents on the sky (collision) due to the operation out of control, or the ARC value. This value corresponds to the combination of the elements (2) and (3) of the second equation in Figure 2. To determine the ARC value, the SORA methodology categorizes UAS operation into 13 risk collision categories. These categories are characterized by altitude, airspace characteristics (controlled / uncontrolled airspace, airport/ non-airport airspace, rural/urban zone). Each category has a specific ARC value ranging from a to d. For example, because of a high traffic density, the airspace around an airport has an ARC of d. Similar to the GRC, the ARC could be reduced by considering Threat barriers such as operational restrictions (time, location) and following specific rules.
- **After that**, we determine two Specific Assurance and Integrity Levels (SAIL) values, which represent the level of confidence that the UAS operation will stay under control (inverse of the element (1) in Figure 2). One SAIL value is determined for GRC and another value for ARC [32]. Then, the higher SAIL value is chosen as an objective to drive the required safety objectives. In the most recent version of the SORA methodology, these activities are simplified by using Table 2.
- **Lastly**, we chose Operation Safety Objective (OSO) and their robustness level corresponding to the SAIL level of the operation. A list of all possible OSOs is provided in the annex E of SORA [36].

SAIL Determination				
	ARC			
GRC	a	b	c	d
≤ 2	I	II	IV	V
3	II	II	IV	V
4	III	III	IV	V
5	IV	IV	IV	V
6	V	V	V	V
7	VI	VI	VI	VI

Table 2: SAIL determination [37]

In this section, we explain the concept of the SORA methodology. It could be resumed as (1) firstly, evaluate the critical level of a UAS operation based on the likelihood of Harms in the case of "UAS operation out of control", (2) then determine Threat barriers corresponding to the critical level of the operation. In the next section, we propose a solution to extend this methodology to cover cybersecurity aspects.

3 Extension of the SORA methodology toward cybersecurity

Our proposed solution consists of two parts which are called Harm Extension and Threat Extension. Harm Extension extends the risk scenarios under consideration with new harms; and completes the evaluation of the critical level of a given UAS operation. Threat Extension extends the scenarios under consideration with new cybersecurity threats; and determines the corresponding Threat barriers for a given UAS operation. The development of the Harm Extension is presented in this paper while the Threat Extension, presently in development, will be published later.

In the Harm Extension, we concern the harm-side of the risk model (see Figure 4). The standard SORA methodology concerns only the harms to the person's life. However, besides the harms to the person's life the public concerns also the other harms [11, 32, 35, 38] such as:

- **Privacy violation**: A UAS could have a small size, a long operational range and high-performance on-board sensors; so it could intrude itself into private locations and collect information [39]. That violates the privacy of the owner. The privacy violation could be caused by a cyber attack or an error of the system. For example, police-operated UASs may frequently cross private properties on their way to an operational area. Under a cyber attack, the recorded video on the properties could be disclosed and then the privacy of owners overflown could be violated.
- **Physical damages to infrastructure**: It is supposed that the unmanned aircraft could fall down on critical infrastructures such as a highway, an electricity power line, a nuclear plant due to a cyberattack or an accident. This harm relates to some specific operations only in which aircrafts fly near or over critical infrastructures.
- **Digital damages to infrastructure**: It is supposed that a UAS could become a security breach to a critical infrastructure. For example, an attacker takes over control of the UAS and uses it to digitally attack an infrastructure via the connection between the UAS and the infrastructure.

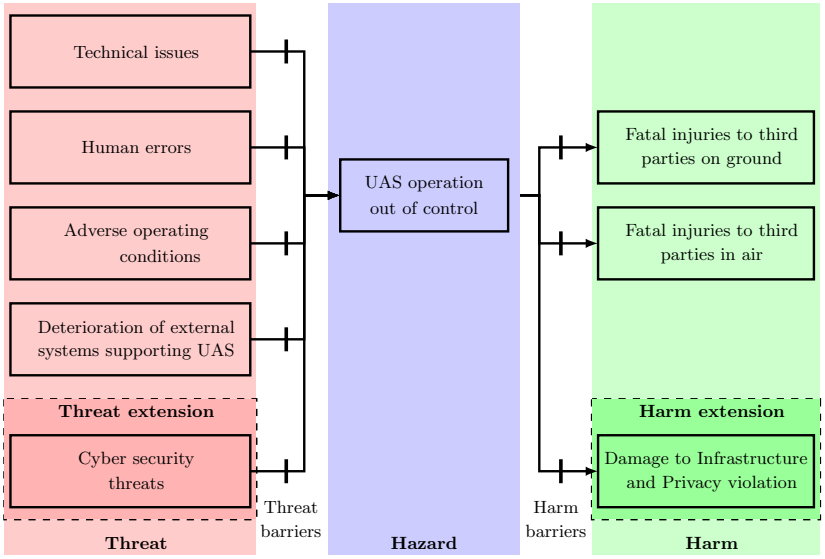

Fig. 4: Extended risk model

Therefore, these new harms come to mind as important issues that should be taken into account in the extended methodology. In the Harm Extension, our strategy to address the new harms includes four steps as follows:

1. Choose a new harm that needs to be addressed.
2. Determine factors/characteristics of the UAS operation, which have an impact on the likelihood of the chosen harm.
3. Establish formulas or tables to evaluate qualitatively the likelihood based on the determined factors.
4. Extend the "SAIL determination" step to cover the likelihood of the new harm.

In the Threat Extension, we focus on the threat-side of the risk model. The potential cybersecurity threats need to be identified and grouped in new threat categories. In other words, this calls for a taxonomy of cybersecurity threats related to a UAS operation. To illustrate the new scenarios, the new threat categories will be added into the threat-side of the risk model as shown in Figure 4. Corresponding to each new threat category, a list of possible Threat barriers will be also established. When the Threat Extension will be fully developed, the Threat barriers for a given UAS operation will be chosen from the proposed list in correspondence with the value of the SAIL factor. At this stage, the Threat Extension has not been developed yet. However our strategy to develop this extension could be described as follows:

1. Make a review of the cybersecurity threat against the UAS which are pointed out either from real scenarios or in the research context (e.g simulations, hypotheses).
2. Based on the review, create a taxonomy of cybersecurity threats.
3. Establish a list of generic Threat barriers for each threat category in the defined taxonomy. Each barrier will be defined with three level of robustness (Low,

Medium and High) according to the SORA method. This work is also based on the state of the art of cybersecurity countermeasures in related application fields such as automobile, robotics...
4. Determine the mechanism to choose the robustness of cybersecurity barriers for a given UAS operation.

Harm Extension and Threat Extension could be developed separately and then could be integrated into one completed methodology. In the remainder of this paper, we focus on developing a part of the Harm Extension related to the privacy issue.

4 Privacy issue as a harm extension

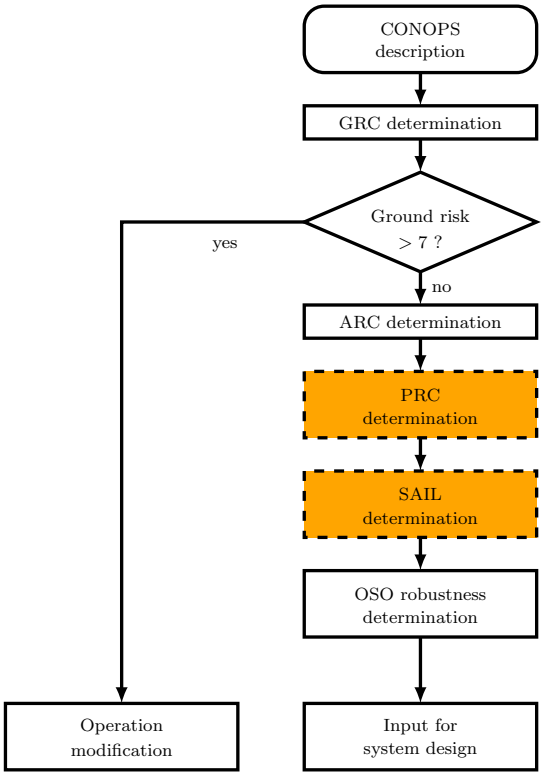

Fig. 5: The new risk assessment process

The privacy violation is one of the most concerned issues for public acceptance of UAS applications [32,38,40]. Therefore, we address it firstly in our works. It is difficult to define and address the concept of privacy precisely [41], we decided to focus on only three aspects: (1) disclosure of personal information; (2) illegal personal surveillance; and (3) intrusion into a private location. The first aspect is illustrated in the works of Li et al. [42]. The authors experimented a

password-stealing attack based on videos captured by a drone. The second aspect is mentioned in [43–45]. In these papers, the authors examined how the surveillance UAS application could impact on the privacy of people on the ground. Moreover, Park et al. [44] and Babiceanu et al. [46] proposed criteria for judging privacy violations of an UAS operation based on the quality of captured images/videos. The last aspect was addressed by Blank et al. [47]. The authors proposed a mechanism to recognize private spaces during creating flight-paths and to make sure that unmanned aircrafts would not fly over these private properties.

Our previous paper [1] proposes an extended SORA methodology considering the privacy violation as a new kind of harm. The risk assessment process of our extended methodology is shown in Figure 5. In this new process, we add a new step - Privacy Risk Class (PRC) determination and modify the SAIL determination step.

Type of operation	Rural zone, VLOS	Rural zone, BLOS	Urban zone, VLOS	Urban zone, BLOS
Image detail level				
Monitor	A	B	C	C
Detect	B	B	C	C
Observe	B	C	D	D
Recognize	C	C	D	D
Identify	C	D	E	E
Inspect	C	D	E	F

Table 3: Intrinsic PRC determination

In the PRC determination step, we qualitatively evaluate the likelihood of the privacy harms in the case of "UAS operation out of control". This likelihood is evaluated based on firstly three characteristics of the operation:

- **Operation area**: the likelihood of having a person or a private location exposed to the aircraft in an urban zone could be higher than in a rural zone, because of a higher population density
- **Operation type**: the likelihood of having a person exposed to the aircraft could be higher in a Beyond Visual Light Of Sight operation (BVLOS) than in a Visual Light Of Sight (VLOS) operation (VLOS). Because of a greater flight range, the number of persons overflown in a BVLOS operation could be higher than in a VLOS operation (with the same population density). Moreover, in a BVLOS operation, it isn't easy to prevent the aircraft from flying over people because the pilot does not have a visual reference.
- **Detail level of image** captured by UAS: For a person overflown by an unmanned aircraft, the likelihood of privacy violation depends on the detail level of images captured by the onboard camera. For example, let us suppose the images are at a too low resolution: in that case, the images are not detailed enough to recognize the person's face, so the likelihood of privacy violation could be small.

Based on the three characteristics above, we could determine the intrinsic PRC of the operation (see Table 3). Similar to the GRC and the ARC, we determine

the final PRC by considering Harm barriers in place. For the privacy harm, we proposed three kinds of Harm barriers: Privacy protection filter, Restriction on private area, Operation-aware announcement to the public. Each barrier could reduce one level of PRC.

In the new process, we determine the SAIL of the operation based on three factors: GRC, ARC, and PRC, instead of only two: GRC and ARC as in the standard process. We call the SAIL value obtained from three factors 3D-SAIL and the SAIL obtained from 2 factors 2D-SAIL. 3D-SAIL is a combination of PRC and 2D-SAIL (see Table 4).

	2D-SAIL					
PRC	I	II	III	IV	V	VI
A	I	II	III	IV	V	VI
B	II	II	III	IV	V	VI
C	III	III	III	IV	V	VI
D	IV	IV	IV	IV	V	VI
E	V	V	V	V	V	VI
F	VI	VI	VI	VI	VI	VI

Table 4: 3D-SAIL determination

The more detailed explanations of these steps are presented in our previous paper [1].

5 Risk assessment tool

5.1 Description and purpose

Our tool helps users conduct automatically risk assessments based on the SORA methodology and its extension. The users are first prompted to provide input information on the extended operations. Based on this information, our tool then determines automatically the SAIL level corresponding to such operations and the associate safety objectives. This tool is developed for different kinds of users with different purposes: (1) an operator could determine rapidly the objectives related to the intended operation; (2) an operator could configure the intended operation and balance the operational performance with the cost for satisfying the objectives; (3) UAS manufacturers/constructors could anticipate rapidly the objectives related to specific operations of their clients; (4) an authority could use also this tool to verify rapidly operations for which an authorization is requested. Moreover, this tool is developed in the way that it is easy to extend the tool for the new extensions of the SORA methodology in the future such as taking into consideration new harms, new threats. The beta version of the application is available at https://trantrungduc15032.wixsite.com/soraplus

5.2 Design and implementation

The tool is in the form of a web application built based on the Wix platform. This platform provides the necessary tools/services to create a website easily and

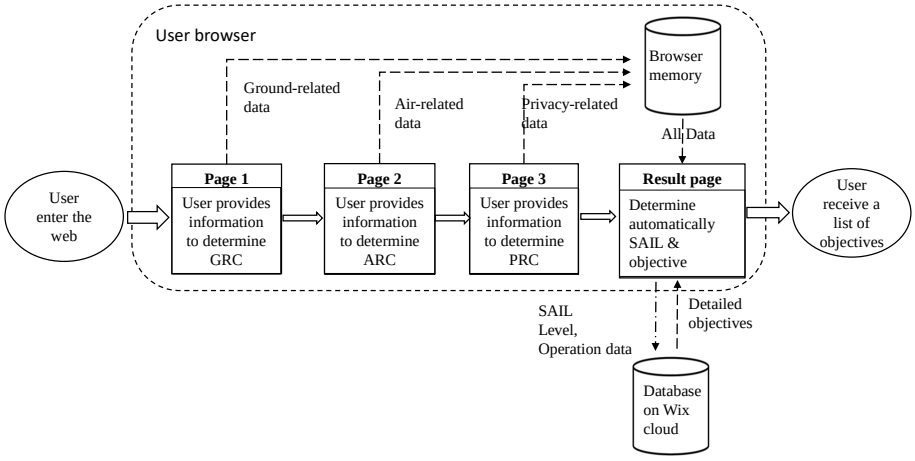

Fig. 6: Overview of the application

supports the Java-script language to create customized functions. The structure of the application is shown in Figure 6. The methodology's fundamental is represented by four pages. The user will go through one to other pages during the risk assessment. The first page represents the *GRC determination* step. This page requires the user to provide information related to the ground risk such as the size of the aircraft, operation area, mitigation measures (a part of the page is shown in Figure 7). For some "yes/no" options, the user could explain how such options are chosen. Such explanations will be used to create a final report at the end of the risk assessment. Based on the provided information, the tool shall automatically determine the GRC factor of the operation. The operation information and the determined GRC shall be stored on the browser's memory for the following steps. Similarly, the second and third pages represent the ARC and PRC determination steps. Based on the values of GRC, ARC, and PRC provided by the three first pages, the last page first determines the SAIL level corresponding to the operation automatically. This page lets the user choose which kinds of risks are considered to determine the SAIL value. For example, a user could choose only ground risk and air risk as in the standard methodology; or all three risks as in the extended one. Then the page sends a request to the database on the Wix cloud to get the detailed objectives associated with the determined SAIL value. Finally, all required objectives corresponding to the intended operation are displayed to the user. With the current design, our tool could be easily extended to adopt other SORA methodology extensions. For a new harm extension, we need to add a new page to prompt the user to provide information related to this kind of harm and modify a little bit the result page. Meanwhile, we need to add a new page to prompt the user to provide information related to this kind of threat and add new objectives into the database for a new threat extension.

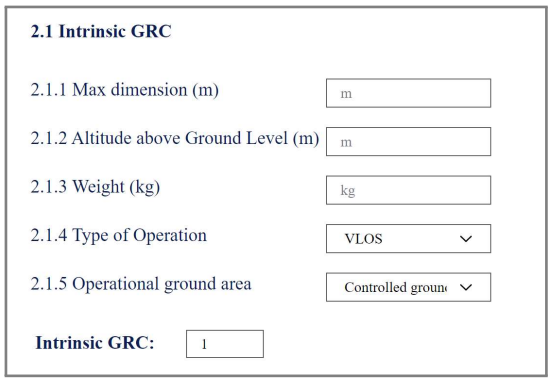

Fig. 7: Some required information

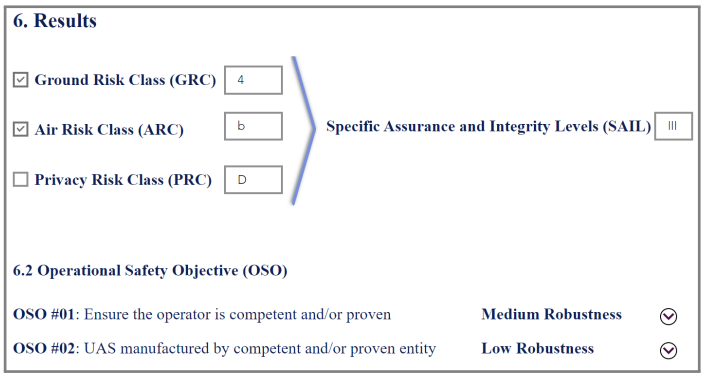

Fig. 8: SAIL determination with the standard methodology

6 Case study

To illustrate our extended methodology and tool, we conduct risk assessments for the UAS operation mentioned in the EU-funding MULTIDRONE project (https://multidrone.eu). This project does not relate to our work. However, the mentioned operation is chosen to analyze because its description is public and detailed enough to apply the extended methodology. Before our works, Capitán et al. [48] analyzed this operation with the first version of the SORA methodology (published in 2017). This version was replaced by the version 2 in 2019. This version is based on the same fundamental concept as version 1 but with different evaluation tables. In this work, we extend version 2. In the following, we refer to "standard methodology" for the version 2 and to "extended methodology" for our methodology taking account of privacy issues. For this paper's remain, we re-analyze the same MULTIDRONE operation with both the standard methodology and our extended methodology presented earlier in the paper. As aforementioned, the two methodologies are similar in the *GRC determination* and *ARC determination* steps. The differences between them appear in the *PRC determination*, *SAIL determination* and *OSO robustness determination* steps.

Main UAS and operation specification	
Frame	DJI S1000+
Autopilot	Pixhawk 2.1
Communication	Thales LTE/Wi-Fi Communication Module
Parachute	Galaxy GRS 10/350
Camera	BMMC + Panasonic Lumix G X Vario Lens
Size	1,45 m
Weight	11 kg
Altitude	10 m
Flight mode	Autonomous
Operation Type	BVLOS

Table 5: UAS and operation specifications, from the Multidrone project [48, 49]

6.1 CONOPS description

A full description (as mentioned in Annex A of the SORA methodology) of the operation is very long because it contains information not only for the risk assessment but also the administrative purposes. Therefore, we give only a summarized description containing the necessary information to conduct risk assessments in this step. More detailed information could be found in [48, 49]. In this operation, the drone flies following the boats to take photo-shots. Because the operation is conducted in a large area (with a race path of 15 km), the drone flies Beyond Visual Light of Sight (BVLOS) of pilots and at the auto mode. The operation takes place in a rural area with a low population density. It is supposed that there could be audiences on both sides of the river, and the drones do not fly over them. Table 5 summaries the essential information on the intended operation.

6.2 GRC determination

This step is similar for both methodologies. We first determine the intrinsic GRC of the operation, which refers to the intrinsic risk to the people on the ground without considering Harm barriers. Because the drone flies in a rural area and does not fly over audiences, we classify the operation area as a *Sparsely populated environment*. With the information on the operation area and the size of the vehicle, we assigned 4 for the intrinsic GRC according to the GRC table from the SORA methodology (see Table 1).

Then, we study the Harm barriers of the operation, which could reduce the intrinsic GRC. The intended operation does not implement any Emergency Response Plan and does not mention any Strategic Mitigations for ground risk. That lead to an increase in GRC. To reduce the risk the operator applies only one Harm barrier: Parachute (Reducing the effect of ground impact). However, the operator doesn't mention how they ensure that the parachute aligns with the intended operation. Therefore this mitigation is not robust enough to reduce GRC. The final GRC of the operation is 4. The result from our application is shown in Figure 9.

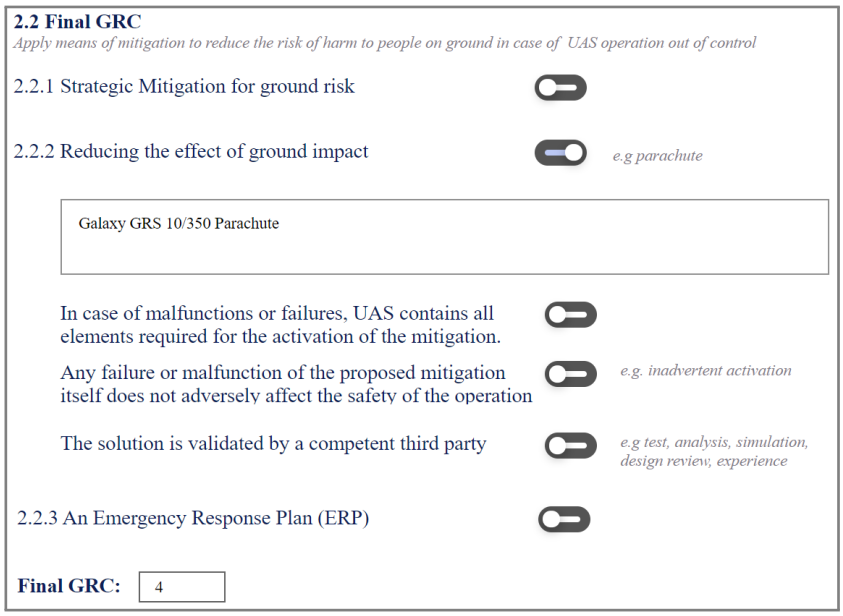

Fig. 9: Final GRC determination

6.3 ARC determination

This step is similar for both methodologies. We first determine the operation's initial ARC, which refers to the risk of collision with other planes without considering Harm barriers. Because the aircraft flies at an altitude of 10 m above the ground level, in the rural area and uncontrolled airspace, the risk of collision with another aircraft is low. Therefore, the intended operation has an initial ARC of b with a generalized flight density of 1 (on a scale of 5 levels [37]). Figure 10 presents the result from our application for this step. To reduce the operation's air risk, the operator implements *mitigation by boundary* as a Harm barrier to restrict operational volume. However, in this case, according to the SORA methodology, the Harm barrier is not useful because the initial probability of collision is too low to reduce (low flight density area). For this reason, the final ARC remains at the level of b.

6.4 PRC determination

This step is available within the extended methodology only. We first determine the initial Privacy Risk Class (PRC), which refers to privacy violation risk without considering Harm barriers. Most of the input data for this step have been provided in the operation description (see Table 5). However, the operation description does not provide the minimum Angle Of View of the camera (AOV). We could calculate it manually based on the camera specifications, which is shown in Table 6.

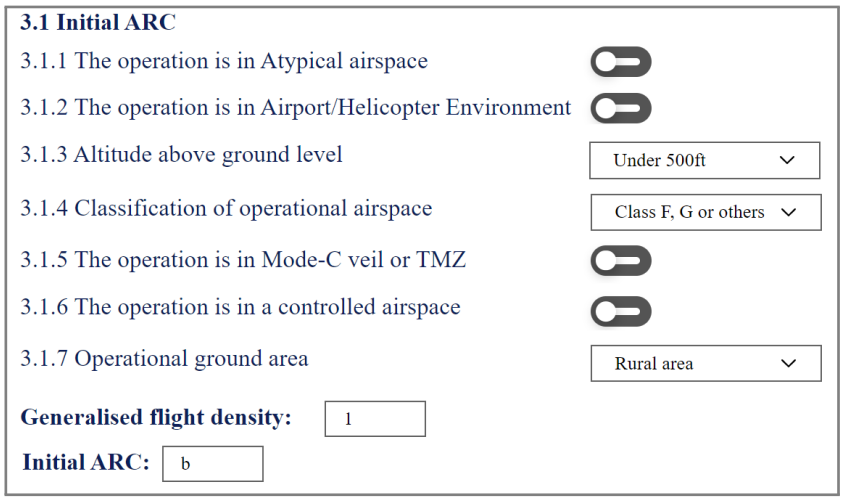

Fig. 10: Initial ARC determination

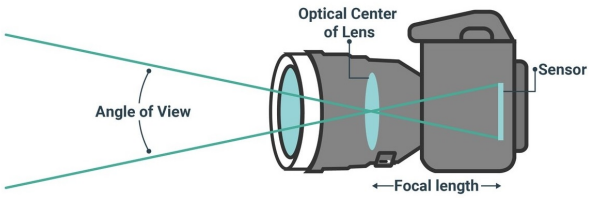

Fig. 11: Camera specification [50]

BMMC camera with Panasonic Lumix G X Vario Lens	
Resolution	2432 x 1366
Sensor size	16.64 mm x 14.04 mm
Focal length	from 14 to 42 mm

Table 6: Camera specifications

The minimum AOV of the camera is calculated as follows:

$$minAOV = 2 * \arctan \frac{\text{sensor width}}{2 * \text{max focal length}} = 11.2^{\circ}$$

As a result, the image detail is at the "Inspect" level (see Table II of our previous paper [1]). Additionally, the aircraft flies in the BVLOS mode and over a rural zone. Therefore, we assign the intrinsic PRC of D for this operation (see Table 3). The final PRC of the operation is the initial PRC subtracting the risk reduction provided by Harm barriers. However, the operation description does not mention any mitigation for the loss of privacy of people on the ground. Therefore, we suppose that the operator does not apply any Harm barriers, and the final PRC is still D. The result from our application for this step is shown in Figure 12.

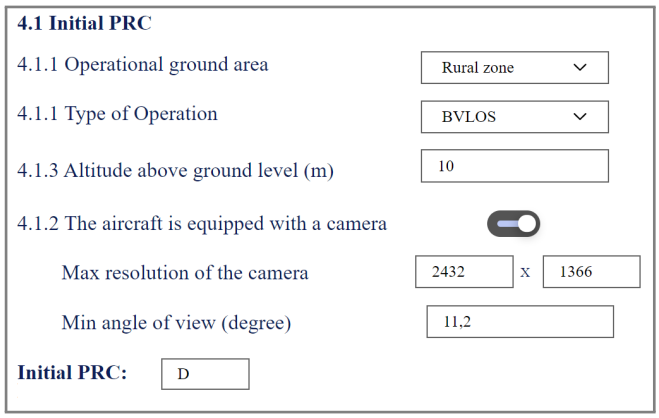

Fig. 12: PRC value from the application

6.5 SAIL determination

This step is different between the two methodologies. In the standard methodology, the SAIL is a combination of two factors: GRC and ARC (2D-SAIL). The operation is assigned to an ARC of b and a GRC of 4. Therefore the value of the SAIL (2D-SAIL) is III (see Table 2). In the extended methodology, the SAIL is a combination of three factors ARC, GRC, and PRC (3D-SAIL). In other words, it is a combination of 2D-SAIL and PRC. With the 2D-SAIL of III and the PRC of D, the value of SAIL (3D-SAIL) is IV (see Table 4). For this step, based on the user's selection, our assessment tool could calculate and display both the 2D-SAIL (Figure 8) and the 3D-SAIL (Figure 13) of the intended operation.

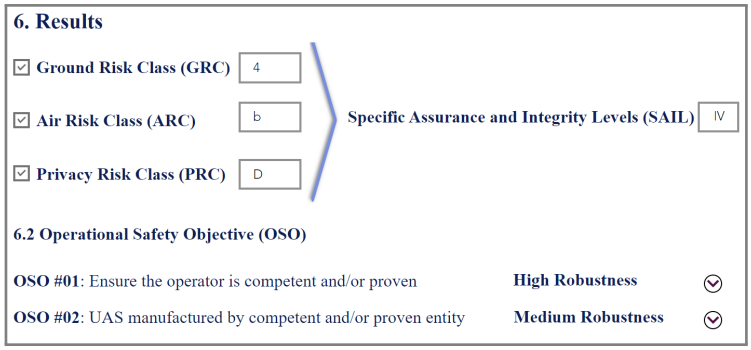

Fig. 13: Result page with 3D-SAIL

6.6 OSO robustness determination

With the determined SAIL values (III from the standard methodology and IV from the extended methodology), we could determine each OSO's robustness level and the detailed objectives that need to be achieved. Because the SORA methodology is designed to support an application for authorization to operate a UAS, some objectives relate to the operators rather than the manufacturer (such as evaluating weather conditions and operator competencies). Therefore, in this case study, from the manufacturer's point of view, we address some critical OSOs. They could be considered as inputs of a development process of a UAS for the intended operation. They are:

- **OSO#04 related to design standard**: With the SAIL of III from the **standard methodology**, the OSO#04 is only an optional objective. It means that the UAS does not have to be developed to any specific standard. With the SAIL of IV from the **extended methodology**, this objective should be satisfied at a low robustness level. It means that the UAS has to be developed to standards considered adequate by the competent authority. The standards should be applied with Low level of integrity (defined within these standards). The manufacturer does not have to provide supporting evidence and needs only to declare standard compliance. Nevertheless, nowadays, there are not any standards dedicated to UAS development. Alternatively, the manufacturer could apply some development standards widely accepted in the aeronautic domain, such as DO178C, DO256. The manufacture has also to take into account standards related to privacy and data protection.
- **OSO#06 related to the communication system**: With the SAIL of III from the **standard methodology**, this objective should be satisfied at a Low level of robustness. It requires that the characteristics of the communication link are appropriate for the operation. Because the unmanned aircraft flies in uncontrolled airspace and the pilot does not have to maintain the communication with the Air Control Traffic (ATC), the communication link is only to control the vehicle. The UAS could use an unlicensed band for communication for example 2.4 GhZ. However, the UAS needs to provide the pilot with means to monitor the communication link (such as signal strength, drop packet rate). With the SAIL of IV resulted from the **extended methodology**, we have to satisfy this OSO at a Medium level of robustness. At this level of robustness, the communication characteristics should conform with the specific standard accepted by the competent authority. For privacy, the communication link has to be capable of protecting the confidentiality of exchanged data.
- **OSO#18 related to Automatic protections of the flight envelope from Human Error**. With the SAIL of III, this objective should be satisfied at a Low level of robustness. In detail, the UAS should detect and prevent the incorrect pilot input that makes the aircraft excess its flight performance (e.g., the pilot let the aircraft go down too quickly). With the SAIL of IV, this objective should be satisfied at a Medium level of robustness. It requires an automatic protection system that could remain (or recover) the aircraft's state within the flight envelope after the pilot's errors. The system has to be developed to standards considered adequate by the competent authority.

6.7 Result

For this case study, we have conducted risk assessments for a UAS operation mentioned in the EU-funded MULTIDRONE project with both the standard SORA methodology (version 2) and our extended methodology. A summary of these assessments is presented in Table 7. According to this summary, our proposed methodology gives a more critical SAIL value than the one given by the standard methodology. (SAIL of IV vs. III). As a result, the objectives (OSO) should be satisfied with a higher robustness level (Medium or High level) when we consider the privacy harm in the risk assessment. This result is reasonable because the UAS is equipped with a high-performance camera, and the operation takes place in a crowded event. In other words, privacy is an essential aspect of this operation. However, to fulfill the objectives with one higher robustness level, it requires changing the operation and the UAS dramatically. These changes could make the operation more safe/secure but also impact the cost-effectiveness of the operation.

	Methodology	
	Standard SORA	Extended SORA
GRC	4	4
ARC	b	b
PRC	Not Applied	D
SAIL	III	IV
OSO	Low or Medium robustness level	Medium or High robustness level.

Table 7: Result summary

7 Conclusion and perspectives

This work extends the standard SORA methodology toward cybersecurity aspects and develops a web-based tool to conduct the risk assessment. The SORA methodology's current document explains only how to use it but does not explain how it works. Therefore, we first described the methodology's concept based on available papers and our knowledge about the risk assessment. Then based on this concept, we propose an approach to extend the methodology. The approach consists of two parts. The first one (Harm extension) is to consider new Harms that could result from cybersecurity/safety problems. To illustrate this part, we propose an extension for the "privacy violation" harm - an essential concern for the public acceptance of UAS operations. The second part (Threat extension) is to take into account the cybersecurity threats (or attacks) (versus the unintended threat covered by the standard methodology (version 2)) and also the relevant cybersecurity mitigation. This part is presently under development and has not been published yet. Besides the extension approach, we also propose a risk assessment tool in the form of a web-based application. This tool is designed to simplify the risk assessment tasks and quickly adapt to the new methodology extension. Finally, we conduct risk assessments for a real UAS operation with both the standard and extended SORA methodologies. The result comparison shows that the extended methodology requires the higher safety objectives to be met than the standard

methodology. On one hand, it means that by using the extended methodology, the UAS operation has to respect more safety requirements. On the other hand, to satisfy the higher safety level, it could require more resources and impact a UAS operation's cost-effectiveness. Therefore, to make the extended methodology more practical and widely-used, it requires tests and feed-backs from experts in the UAS industry. In the future, further works need to be done to integrate new cybersecurity threats and relevant cybersecurity objectives (Threat extension) into the methodology. Besides of that, the balance between the safety objectives and the cost-effectiveness should be also considered.

Acknowledgements We thank the authors of the MULTIDRONE project for publishing their works. Based on the information from this project we could test and discuss about the proposed methodology.

8 Declarations

8.1 Funding

This work is a part of a Ph.D. program funded by

- the SOGILIS company (France), 4 Avenue Doyen Louis Weil, 38000 Grenoble
- Association Nationale Recherche Technologique (ANRT), 33 rue Rennequin - 75017 Paris

8.2 Conflicts of interest/Competing interests

- Not applicable

8.3 Code availability

- Not applicable

8.4 Authors' Contributions

- Literature search: Tran Trung Duc
- Idea for the methodology: Tran Trung Duc, Amin El Mrabti, Jean-Marc Thiriet and Nicolas Marchand
- Case-study and result analysis: Tran Trung Duc and Jean-Marc Thiriet
- Writing - original draft preparation: Tran Trung Duc
- Writing - review and editing: Jean-Marc Thiriet and Tran Trung Duc

8.5 Ethics approval

- Not applicable

8.6 Consent to participate

– Not applicable

8.7 Consent for publication

– Not applicable

References

1. Tran, T.D., Thiriet, J.M., Marchand, N., El Mrabti, A.: Toward Cybersecurity of Unmanned Aircraft System operations under "Specific" category. In: 2020 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1433–1441 (2020)
2. Giones, F., Brem, A.: From toys to tools: The co-evolution of technological and entrepreneurial developments in the drone industry. Business Horizons **60**(6), 875–884 (2017)
3. Vattapparamban, E., Guvenc, I., Yurekli, A.I., Akkaya, K., Uluagac, S.: Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 216–221. IEEE (2016)
4. Moskwa, W.: World Drone Market Seen Nearing $127 Billion in 2020, PwC Says. Bloomberg (2016)
5. Drone market size and forecast 2019-2024. Drone Industry Insights. https://www.droneii.com/project/drone-market-size-and-forecast-2019-2024 (2019). Accessed 25 February 2021
6. European drones outlook study: Unlocking the value for europe. Single European Sky Atm Research Joint Undertaking (SESAR). https://www.sesarju.eu/node/2951 (2016). Accessed 10 September 2019
7. Drones market research report - forecast 2028. Market Research Future. https://www.marketresearchfuture.com/reports/drones-market-1124 (2018). Accessed 25 February 2021
8. Commercial drones in 2022. Interact Analysis. https://www.interactanalysis.com/drone-market-2022-predictions (2018). Accessed 25 February 2021
9. De Miguel Molina, B., Oña, M.S.: The drone sector in Europe. In: Ethics and civil drones, pp. 7–33. Springer, Cham (2018)
10. Bassi, E.: From here to 2023: Civil drones operations and the setting of new legal rules for the european single sky. Journal of Intelligent & Robotic Systems pp. 1–11 (2020)
11. A-NPA 2015-10: Introduction of a regulatory framework for the operation of drones. European Union Aviation Safety Agency (EASA). https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2015-10 (2015). Accessed 21 Feburary 2021
12. Commission implementing regulation (EU) 2019/947 of 24 may 2019 on the rules and procedures for the operation of unmanned aircraft. European Union Aviation Safety Agency (EASA). https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2019947 (2019). Accessed 26 February 2021
13. Ericson, C.A., et al.: Hazard analysis techniques for system safety. John Wiley & Sons (2015)
14. Piètre-Cambacédès, L., Bouissou, M.: Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety **110**, 110–126 (2013)
15. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety **139**, 156–178 (2015)
16. Raspotnig, C., Opdahl, A.: Comparing risk identification techniques for safety and security requirements. Journal of Systems and Software **86**(4), 1124–1151 (2013)
17. Steve Kremer Ludovic Mé, D.R., Roca, V.: Cybersecurity - current challenges and inria's research directions. Tech. rep., INRIA (2019)
18. Schneier, B.: Modeling security threats. Dr. Dobb's Journal (1999)
19. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A.: F(I)MEA-technique of web services analysis and dependability ensuring. In: Rigorous Development of Complex Fault-Tolerant Systems, pp. 153–167. Springer (2006)

20. Piètre-Cambacédès, L., Bouissou, M.: Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP). In: 2010 European Dependable Computing Conference, pp. 199–208. IEEE (2010)
21. McDermott, J.P.: Attack net penetration testing. In: Proceedings of the 2000 workshop on New security paradigms, pp. 15–21 (2001)
22. Kornecki, A.J., Liu, M.: Fault tree analysis for safety/security verification in aviation software. Electronics **2**(1), 41–56 (2013)
23. Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). In: A. Bondavalli, F. Di Giandomenico (eds.) Computer Safety, Reliability, and Security, vol. 8666, pp. 310–325. Springer International Publishing (2014)
24. Abdo, H.: Dealing with uncertainty in risk analysis : combining safety and security. PhD Thesis, Université Grenoble Alpes (2017)
25. Functional safety Essential to overall safety - An introduction to Functional safety and the IEC 61508 series. International Electrotechnical Commission (IEC), https://www.iec.ch/functionalsafety/explained/ (2015). Accessed 25 February 2021
26. Guidelines and Methods for Conducting the Safety Assessment Process on Airborne Systems and Equipments. SAE International. https://www.sae.org/standards/content/arp4761/ (1996). Accessed 24 February 2021
27. ISO/IEC 27000 glossary standard. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). http://www.iso27001security.com/html/27000.html. Accessed 26 February 2021
28. Kobes, P.: Zoom sur la norme internationale IEC 62443 pour la cybersécurité des systèmes numériques industriels. In: Cybersécurité des installations industrielles. Cépaduès (2016)
29. Idrees, S., Roudier, Y., Friedewald, M., Leimbach, T., Andreas, F., Sigrid, G., Olaf, H., Roland, R., Matthias, R., Henrik, B., Ludovic, A., Renaud, P., Gabriel, P., Alastair, R., David, W., Benjamin, W.: Security requirements for automotive on-board networks based on dark-side scenarios. Tech. rep., EVITA (2009)
30. EUROCAE: Airworthiness security process specification ED-202/ DO-326 (2014)
31. Favaro, J.: Report on the evolution of co-engineering standards. Tech. rep., Electronic Component Systems for European Leadership Joint Undertaking (2018)
32. Joint Authorities for Rulemaking on Unmanned Systems (JARUS): JARUS guidelines on Specific Operations Risk Assessment (SORA) (2017). Version 1
33. Nikodem, F., Bierig, A., Dittrich, J.S.: The New Specific Operations Risk Assessment Approach for UAS Regulation Compared to Common Civil Aviation Risk Assessment. In: DLRK 2018 (2018)
34. European Union Aviation Safety Agency (EASA): Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947 (2019)
35. European Union Aviation Safety Agency (EASA): Introduction of a regulatory framework for the operation of unmanned aircraft (2015)
36. Joint Authorities for Rulemaking on Unmanned Systems (JARUS): Annex E of SORA - Integrity and assurance levels for the Operation Safety Objectives (OSO) (2019)
37. Joint Authorities for Rulemaking on Unmanned Systems (JARUS): JARUS guidelines on Specific Operations Risk Assessment (SORA) (2019). Version 2
38. Pauner, C., Kamara, I., Viguri, J.: Drones. Current challenges and standardisation solutions in the field of privacy and data protection. In: 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), pp. 1–7 (2015)
39. Winkler, S., Zeadally, S., Evans, K.: Privacy and Civilian Drone Use: The Need for Further Regulation. IEEE Security & Privacy **16**(5), 72–80 (2018)
40. Zhi, Y., Fu, Z., Sun, X., Yu, J.: Security and Privacy Issues of UAV: A Survey. Mobile Networks and Applications pp. 95–101 (2019)
41. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European data protection: coming of age, pp. 3–32. Springer (2013)
42. Li, Z., Gao, C., Yue, Q., Fu, X.: Toward drone privacy via regulating altitude and payload. In: 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 562–566 (2019)
43. Villasenor, J.: Observations from above: Unmanned aircraft systems and privacy. Harvard Journal of Law Public Policy (2013)
44. Park, S., Lee, K.: Developing Criteria for Invasion of Privacy by Personal Drone. In: 2017 International Conference on Platform Technology and Service (PlatCon), pp. 1–7 (2017)

45. Bonetto, M., Korshunov, P., Ramponi, G., Ebrahimi, T.: Privacy in mini-drone based video surveillance. In: 2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), vol. 04, pp. 1–6 (2015)
46. Babiceanu, R.F., Bojda, P., Seker, R., Alghumgham, M.A.: An onboard UAS visual privacy guard system. In: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), pp. 1–8 (2015)
47. Blank, P., Kirrane, S., Spiekermann, S.: Privacy-Aware Restricted Areas for Unmanned Aerial Systems. IEEE Security Privacy **16**(2), 70–79 (2018)
48. Capitán, C., Capitán, J., Castano, A.R., Ollero, A.: Risk Assessment based on SORA Methodology for a UAS Media Production Application. In: 2019 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 451–459. IEEE (2019)
49. MULTIDRONE project - University of Bristol: Deliverable D2.1: Multidrone media production requirements (2017)
50. What is focal length and angle of view in photography. Capture the Atlas. https://capturetheatlas.com/what-is-focal-length/ Accessed 23 February 2021