Toward Cybersecurity of UAS operations under "Specific" category

Trung Duc Tran[1,2], Jean-Marc Thiriet[1], Nicolas Marchand[1], Amin El Mrabti[2]

***Abstract*— Nowadays, the increasing number of UAS operations raises the public concerns on cybersecurity issues. Therefore, it requires a methodology to address these issues during the UAS development. The Specific Operation Risk Assessment (SORA) is a risk assessment methodology developed by Joint Authorities for Rulemaking on Unmanned Aircraft System (JARUS). This methodology is endorsed by European Union Aviation Safety Agency (EASA) as an acceptable means to fulfill the requirements of EU regulation related to UAS operations under Specific category. The original SORA methodology focus on Safety risk scenarios only, which relate to unintentional threats and the harms to people's life. In this paper, we introduce our solution to extend the methodology toward cybersecurity aspects. The extended methodology concerns risk scenarios relating to intentional digital threats and some other harms (e.g privacy violation, damage to critical infrastructure). A part of this solution is developed and is presented in this paper.**

I. INTRODUCTION

A. Context

For several years, the civil Unmanned Aircraft Systems (UAS) have become more and more popular with many applications such as aerial photography, goods transportation, surveillance, etc [1]. However, the lack of human observation, communication capacities, and protection makes UAS a good target for cyber attacks. Therefore, the risk related to the cybersecurity of UAS should be assessed and taken into account in the early phase of UAS development.

Fig. 1: Three categories of UAS operations A refaire - Nico

To deal with the progressive increase in the number of UAS operations, the European Aviation Safety Agency (EASA) classified UAS operations into three categories from Low to High risk level: Open, Specific and Certified [2]. It is forecast that most of commercial UASs will operate under Specific Category [3]. In this category, we could expect the operation of large drones flying above populated areas, out of the visual line of sight of the pilot and sharing airspace with manned aircraft. These operations could pose significant harms to the people overflown and the manned aircraft, specially in case of a cyber attack. For these reasons, our works presented in this paper focus on the cybersecurity issue of operations under the Specific Category.

B. Related works and contribution

Regarding UAS applications, there are a lot of researches on cybersecurity breaches from the two sides: attack and defense. Vattapparamban et al. experimented with several hijack attacks against small UASs by exploiting the vulnerabilities of their WiFi communication [1]. A framework to defend against these kinds of attacks is proposed by Hooper et al. [4]. Heiges et al. [5] experimented with an injection attack on an autopilot to reroute an Unmanned Aircraft (UA). To defend against this attack, the authors developed a solution that compares the change on the autopilot with the pilot inputs. Javaid et al. simulated GPS Jamming and GPS Spoofing attacks by using UAVSim [6]. Against these attacks, several countermeasures were proposed such as the Bayesian network-based method [7], the machine learning-based method [8], [9], the vision-based method [10]. Davidson et al. argued that the optical flow sensors used for navigation represent a vector for adversarial control and demonstrated this argument with a real UAV [11]. The researches in individual security breaches are important because they help us anticipate the potential attacks against UAS operations and possible countermeasures. However, it is still a lack of researches on the decision-making process which helps to analyze globally the cybersecurity environment and balancing the operation performance vs. the economic cost of implementing countermeasures.

In the other industrial domains, there are standards and methodologies which provide different guidances for risk assessment related to cybersecurity. In the information system domain, **ISO 27005** standard was first considered as guidance to information security but it does not provide a specific risk assessment method [12]. One of the ISO27005-based methodologies is **Method for Harmonized Analysis of Risk (MEHARI)** [13], which provides different tools to audit the information security of an organization and a database of possible countermeasure. For Industrial Automation and Control Systems (IACS), **IEC62443** standard guides on assessing risks and provides a list of requirements that need to meet during designing and implementing a secured system [14]. In the automobile domain, **E-safety Vehicle Intrusion proTected Applications (EVITA)** [15] [16] is a methodology dedicated to the cybersecurity of an on-board

*This work was supported by SOGILIS Company, Corresponding author: Trung-Duc.Tran@gipsa-lab.fr

[1] Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-lab, 38000 Grenoble, France

[2] SOGILIS Company, 38000 Grenoble, France

network, which has many common points with UAS (sensors, gps, actuators, control system etc.). This methodology aims to analyze cybersecurity breaches, define requirements and verify cyber-security solutions. In the aeronautic domain, **DO326/ED203** is the first guidance for the airworthiness security process. This standard adds a new cybersecurity brick on the current manned aircraft development process, which traditionally focuses on the safety [17]. DO326/ED203 and manned aircraft development process are considered too costly for most of UAS operations, especially under the Specific category [2].

Besides the methodologies and standards widely accepted in the industry, there are a lot of researches proposing the new risk assessment methodologies related to cybersecurity. Some of such methodologies are extended versions of existing risk assessment methodologies for safety [18]–[22]. Schmittner developed the FMVEA (Failure Mode, Vulnerabilities and Effects Analysis) method based on the traditional FMEA (Failure Mode and Effect Analysis) [18]. The authors extended the original risk model to cover new incidents original from attacks and introduced new parameters to evaluate the attack likelihoods. Abdo et al. [19] treated the cybersecurity and safety issues for critical infrastructures in the same risk assessment process. The authors developed an approach to represent exhaustively risk scenarios and evaluate the likelihoods based on the Bow-tie model, which is commonly used in safety methodology (for example in the SORA methodology [23]). Xu et al. [21] proposed a methodology to identify and analyze systematically cybersecurity risks based on Fault tree analysis and Hazard analysis methods commonly used for safety in the aerospace industry.

To the best of our knowledge, the most common risk assessment methodology in the UAS domain is **Specific Operation Risk Assessment (SORA)**, which is endorsed by European Aviation Safety Agency (EASA) as an acceptable means to fulfill the requirements of the EU regulations related to UAS. However, at this moment, the methodology focuses on only the safety aspect and ignores the cybersecurity aspect [24]. Therefore, we introduce a solution to extend the SORA methodology to take into account the cybersecurity aspect of UAS operation under the Specific category. The expected result of the application of the extended method is a list of cybersecurity and safety objectives which need to be addressed at the beginning UAS development process.

The remaining of this document is organized as follows. The concept of the SORA methodology is then given in Section II. A solution to extend the methodology to cybersecurity issues is given in Section III. An extension of SORA methodology with a new harm category is given in Section IV. We conclude our works and present our perspective on the future works in Section V

II. General concept of the SORA methodology

Under the Specific category, to gain flight permission, operators (who deploy and control the drone) have to demonstrate the safety of operation to aviation authorities by carrying out a risk assessment. One acceptable means to carry out this risk assessment is the Specific Operations Risk Assessment (SORA) methodology proposed by a group of experts from the National Aviation Authorities - Joint Authorities for Rulemaking on Unmanned Systems (JARUS) [25], [26]. SORA is a holistic and operation-centric methodology [23]. It focuses on analyzing qualitatively consequences of safety issues related to an intended operation and then to determine the safety objectives (in training, system performance, organization, development), which need to be met to gain an approval. From the point of view of manufacturers (who design and develop UAS), the SORA methodology could be used to determine safety feature that their designs need to reach to targeted operations under Specific category. In this section, we explain the general concept of the methodology including two parts: (1) risk model risk scenarios under consideration, (2) assessment process.

A. Risk model

At this moment, the SORA methodology basically considers only risks of harms to a person's life: "fatal injuries to third parties on ground", "fatal injuries to third parties in air". To illustrate the risk scenarios related to these harms (or how these harms could happen), the methodology provides a risk model as shown in Figure 2. This risk model includes three major segments: Harms, Hazard, Threats. The harms are in the right part of the model. The direct causes of these harms is a generic hazard "UAS operation out of control" shown in the center of the model. This hazard is defined as an operation being conducted outside of the operators intention (e.g the aircraft flies outside of visual observation of the pilot in a Visual Line Of Sight operation). The hazard could be caused by several threats which are grouped into categories in the left part of the model. Because SORA methodology considers only the safety aspect but not the security aspect, only unintentional threats are represented in the model. However, according to the authors, this model could be extended to cover more risk scenarios [24].

To mitigate the above risks, several means of mitigation should be applied. There are two types of means of mitigation:

- Harm barrier, which mitigates the likelihood of harms after an occurrence of hazard (e.g. parachute, plan to save the victim on the ground). The harm barriers are pre-defined by operators/manufactures and are analyzed during risk assessment.
- Threat barrier, which mitigates the likelihood of hazard "UAS operation out of control" caused by considered threats. For each category of threat, different threat barriers will be determined at the end of risk assessment under the form of Operation Safety Objective (OSO). Each OSO is detailed in three levels of robustness (Low, Medium, High). An example of OSO is that "the UAS is developed to authority recognized design standards" [28]. At low robustness level of this OSO, the applicant should only declare the required standards are achieved. Meanwhile at the high robustness level, the applicant has to provide supporting evidence (such as analysis,

simulation), which will be valided by a competent third party.

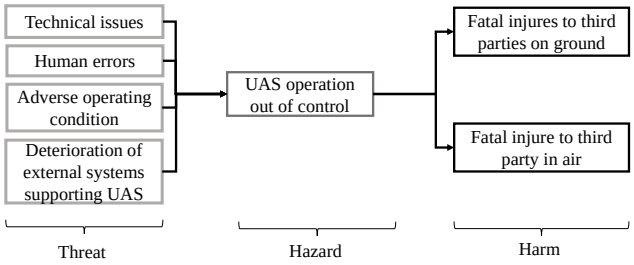

Fig. 2: Risk model de the SORA methodology A refaire - Nico

In the next part, we explain the assessment process of the SORA methodology based on the above risk model in both quantitative and qualitative approaches.

B. Assessment process

1) Quantitative approach: Traditionally, the risk assessment process requires to analyze two parameters of risk: likelihood and severity. However, the risks in the SORA methodology is tied to only likelihood parameters [24] because the methodology basically focuses on only risks of harms to person's life. The severity of these harms could be considered as extremely high. In other words, the safety objectives will be determined to maintain the likelihood of each harm under the acceptable value (10^{-6} fatal injuries per flight hour, equivalent to a manned aircraft operation [24]). The likelihood of these harms is decomposed into individual components as shown in Figure 3.

Likelihood of fatal injuries to 3^e parties on ground	=	Likelihood of having UAS operation out of control (1)	x	Likelihood of person struck by the UA if the operation is out of control (2)	x	Likelihood that, if struck, person is killed (3)	
Likelihood of fatal injuries to 3^e parties in air	=	Likelihood of having UAS operation out of control (1)	x	Likelihood of other A/C struck by the UA if the operation is out of control (2)	x	Likelihood that, if struck, the other A/C cannot continue a safe flight and landing (3)	

Fig. 3: Likelihood of fatal injuries on ground and in air [24] A refaire - Nico

The component 1 of each equation, "likelihood of having UAS operation out of control" is mainly affected by the threats and threat barriers [24]. The combination of component 2 and component 3 in each equation presents the likelihood of harms in case of having UAS operation out of control, which could be evaluated by analyzing the nature of operation under consideration (e.g location, altitude, kind of operation, harm barriers in place). Under the above assumption, the general concept of this methodology in the quantitative approach could be explained as follows:

- **Objective:** Given a UAS operation, we need to maintain the likelihood of each harm under acceptable value: 10^{-6} fatal injuries per flight hour
- **Firstly**, we collect the information on the intended operation of the UAS such as operation area, operation mode, pilot, weight of UA. This activity is called Concept Of Operations (CONOPS) description. The form of a CONCOPS description is provided in Annex A of SORA
- **Secondly**, we estimate the likelihood that the harms occur in case of "UAS operation out of control" based on collected information (e.g. 10^{-4} fatal injuries on ground per hazard and 10^{-3} fatal injuries in air per hazard).
- **Thirdly**, from the estimated values above, we calculate an **acceptable** value for the likelihood of having UAS operation out of control (10^{-2} hazard per flight hour from the first equation and 10^{-3} hazard per flight hour from the second one). The more critical value will be chosen as an objective needs to be reached (e.g 10^{-3} hazard per flight hour).
- **Lastly**, based on the objective value of "likelihood of having UAS operation out of control", the safety objectives with corresponding robustness will be defined.

2) Qualitative approach: The qualitative approach presented above is generally not realistic because of the lack of real data. Therefore, the SORA methodology proposes a qualitative approach based on the main ideas of the quantitative approach as shown in Figure 4. The qualitative approach could be explained as follows:

- **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 (CONOPS description)
- **Secondly**, we determine two qualitative factors: Ground Risk Class (GRC) and Air Risk Class (ARC). These factors present qualitatively the likelihoods that the harms occur in case of UAS operation out of control. The GRC and ARC are determined based on the intrinsic characteristics of the operation such as operational area, attitude, weight of UV and the availability of harm barriers.
- **Thirdly**, we determine two Specific Assurance and Integrity Levels (SAIL) values, which represent the level of confidence that the UAS operation will stay under control. One SAIL value corresponds to GRC and the other corresponds to ARC [24]. Then, the higher SAIL value will be 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 I.

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 I: SAIL determination [27] A refaire - Nico

- **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 [28].

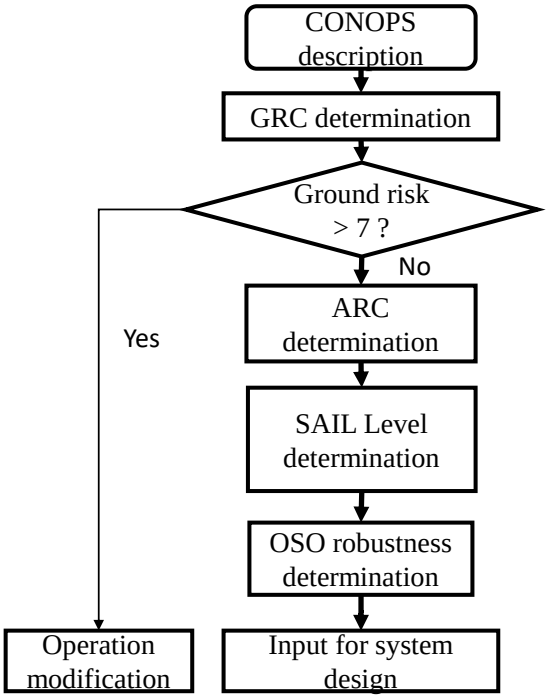

Fig. 4: Simplified risk assessment process A refaire - Nico

In this section, we explained the original 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 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 explain a solution to extend this methodology to cover cybersecurity aspect based on this concept.

III. Solution to extend 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 critical level of a given UAS operation. Threat Extension extends the scenarios under consideration with new cyber security threats; and determines the corresponding threat barriers for a given UAS operation. The development of Harm Extension is now in process while Threat Extension has not been developed yet.

In Harm Extension, we concern the harm-side of the risk model (see 5). At this moment, the classical SORA methodology concerns only the harms to person 's life. However, besides the harms to person's life the public concerns also the other harms [2], [24], [26], [29] 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 [30]. 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 people overflown could be violated.
- **Physical damages to infrastructure**: It is supposed that a UA could fall down on critical infrastructures such as highway, electricity power line, nuclear plant. This harm relates to only some specific operations in which UAs fly near or over critical infrastructures.
- **Digital damage to infrastructure**: It is supposed that a UAS could become a security breach to critical infrastructure. For example, an attacker takes over control the UAS and uses it to attack an infrastructure via the connection between the UAS and the infrastructure.

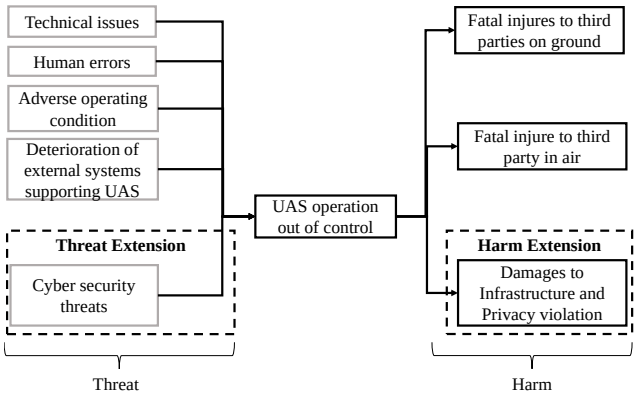

Fig. 5: Extended risk model A refaire - Nico

Therefore, they come to mind as important issues that should be taken into account in the extended methodology. In Harm Extension, our strategy to address the new harms includes 5 steps as follows:

1) Chose a new harm that needs to be addressed
2) Determine factors/characteristics of a UAS operation which have impact on the likelihood of the chosen harm.
3) Establish formals or tables to evaluate qualitatively the likelihoods based on the determined factors
4) Extend "SAIL determination" step to cover the new harm.
5) OSO (?)

In Threat Extension, we will concern 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 "completed" taxonomy of cybersecurity threat related to a UAS operation. To illustrate the new scenarios, the new threat categories will be added into the harm-side of the risk model as shown in Figure 5. Corresponding to each new threat category, a list of possible threat barriers will be also established. For a given UAS operation,

the new threat barriers are chosen in correspondence with the SAIL value.

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

IV. SORA METHODOLOGY WITH PRIVACY ISSUE

Nowadays, the privacy violation is one of the most concerned issues for public acceptance of UAS applications [24], [29], [31]. Therefore, we consider it as important and address it firstly in our works. However, the general privacy is a very large term. It is difficult to define precisely [32] and address this term at large, so we focus on only three aspects of this harm: disclosure of personal information; illegal personal surveillance; and intrusion into a private location. The first aspect is illustrated in the works of Li et al. [33]. The authors experimented a password-stealing attack by analysing the video captured by the drone. The second aspect is mentioned in [34]–[36]. 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. [35] and Babiceanu et al. [37] proposed criteria for judging privacy violation of an UAS operation based on the quality of captured images/videos. The last aspect was addressed by Blank et al. [38]. The authors proposed a mechanism to recognize the private spaces during creating flight-paths and make sure that UAs would not fly over these private properties.

For the next, (A) we first analyse the likelihood of the privacy violation to determine the possible factors related to this harm, which could be used for the assessment. Then we propose extensions for the assessment process: (B) a new step named “Privacy risk class (PRC) determination” to evaluate the likelihood of this harm in case of “UAS operation out of control” and (C) an extension of the ”SAIL determination” step (see Figure 6). At the end, (D) a case-study is shown.

A. Likelihood of privacy violation

With the privacy harm taken into account, the objective of risk assessment is extended to maintain also that the likelihood of harms to privacy is under certain acceptable level. Similar to the likelihood of harm to person’s life, the one of the privacy harm could be decomposed as shown in Figure 7. The combination of the two components (2) and (3) of this equation represents the likelihood that the privacy of third parties is violated after ”UAS operation out of control”.

For a given operation, the likelihood of a person exposed to the UA (insides the sensing range or under the UA) depends on the nature of operation zone (urban zone vs. rural zone) and the type of operation (Beyond Light of Sight vs. Visual Light of Sight). In urban zones, the population density and the number of private locations is higher than in rural zones. Therefore, the likelihood of having a person or a private location exposed to a UA in an urban zone is higher than in a rural zone. In a Beyond Light Of Sight

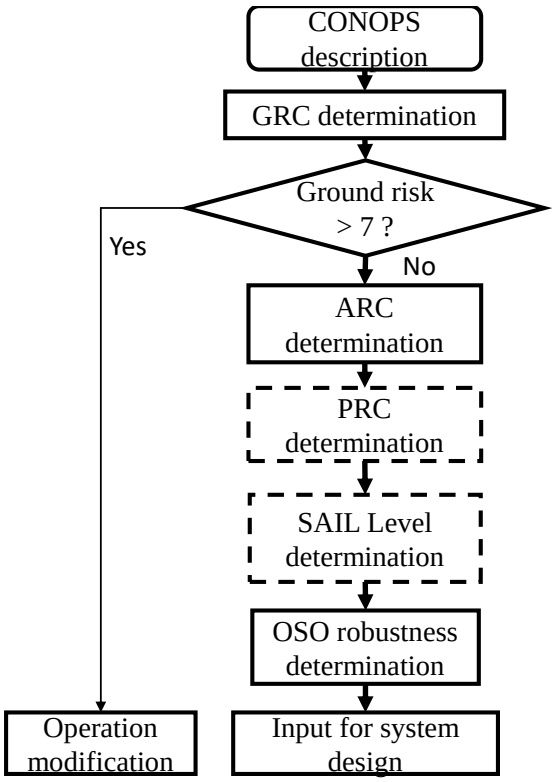

Fig. 6: New steps for Harm Extension A refaire - Nico

(BLOS) operation, the operation range of UA is greater than in a Visual Light Of Sight (VLOS) operation. Therefore, the number of persons under or near a UA in a BLOS operation is higher than in a VLOS operation. That’s why the likelihood of having a person or a private location exposed to UA is higher in a BLOS operation than in a VLOS operation.

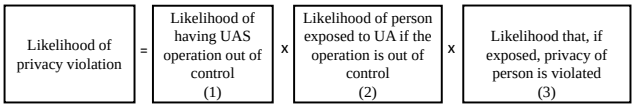

Fig. 7: Likelihood of privacy violation A refaire - Nico

For a person exposed to the UA, the likelihood of privacy violation depends on the detail level of image collected by on-board camera. For example, if the photo taken by the UAS is at a too low resolution, the image of the person is not detailed enough to recognize her/his face so the likelihood of privacy violation is low. The detail level of image could be evaluated by the pixel density - the number of pixels in a captured image representing a meter on ground. To simplify the calculation we assume that the ground is flat. Therefore, for a UAS operation, the highest value of pixel density is reached when the camera direction is perpendicular to the ground as shown in Figure 8. In this case, the pixel density is a function of the height above ground of UA (h), the resolution of the camera and the smallest angle of view of camera (α) as follows:

$$PD = \frac{\text{number of horizontal pixels}}{2 * h * \tan\frac{\alpha}{2}} (pixels/m)$$

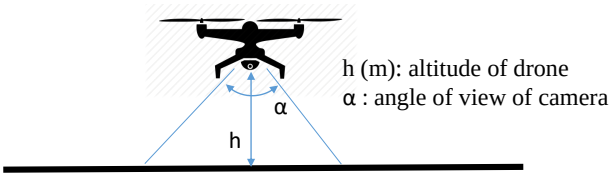

Fig. 8: Maximum pixel density position A refaire - Nico

Because there are common points related to privacy issue between UAS application and Closed-circuit television (CCTV) application [29], [35], [36], we adopt a classification of image detail levels introduced by the British Security Industry Association (BSIA) for CCTV application as shown in Table II.

Level of quality	Description
Monitor (12.5pixels/m)	Enable to view direction and speed of movement of people, if knowing their present.
Detect (25 pixels/m)	Enable to reliably if a person is present
Observe (62.5 pixels/m)	Enable to characterize some details of an individual
Recognize (125 pixels/m)	Enable to determine whether or not an individual shown is the same as someone they have seen before
Identity (250 pixels/m)	Enable identification of an individual beyond a reasonable doubt.
Inspect (1000 pixels/m)	Enable the identity of an individual

TABLE II: Image detail classification [39] A refaire - Nico

Based on this analysis, we define three intrinsic features of a UAS operation to evaluate the likelihood of privacy violation in case of "UAS operation out of control":

- Density of operational area: urban zone vs. rural zone
- Type of operation: BLOS vs. VLOS
- Level of detail of the captured image.

Similar to harms introduced in the classical SORA methodology, the likelihood of privacy harm could be reduced by applying some harm barriers. In this extension, we address three types of threat barriers to mitigate the privacy harm:

- Privacy protection filters: these algorithms reduce unnecessary information that could violate the privacy of person from the video/image such as Blurring, Pixelization, Masking, Warping [36]
- Restriction on private space: the operator avoids make a flight path across a private space [38]
- Operation-aware announcement to public: the public under observation of a UAS operation should be informed about it.

In the next parts of the paper, we provide the details of the PRC determination step and the SAIL determination step.

B. Privacy Risk Class determination step

In this step, the likelihood of privacy violation in case of "UAS operation out of control" is represented qualitatively by the Privacy Risk Class (PRC) value. The intrinsic PRC value is determined based on the intrinsic features of operation as shown in Table III. Then the final PRC is

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 III: Intrinsic PRC determination A refaire - Nico

determined based on the availability of three harm barriers:"Privacy protection filters", "Restriction on private space" and 'Operation-aware announcement to public'". Each means of mitigation helps decrease the intrinsic PRC factor one level.

For example, a UA is equipped with a camera of 1920 x 1080 resolution and 10 degree view angle (α); flies in BLOS mode and at 150m above ground. In this operation the maximum pixel density is 36 pixels/m and corresponds to Detect level (see Table II). According to Table III, the intrinsic PRC is at the C level. Upon analysis of the privacy issue, the operator decides to upgrade the on-board camera with a digital filter that makes image of a person blur and unable to be recognized. In this case, the final PRC is reduced to the B level.

C. New SAIL Determination

The last step consists in the new SAIL determination, the process is described as follows:

1) Determine a SAIL value corresponding to ARC and GRC values by using Table I (classical SORA methodology).
2) Determine a SAIL value corresponding to PRC value denoted by PRC-SAIL (see Table IV)
3) Choose the higher value SAIL (more critical) as the final value SAIL (3D-SAIL) corresponding to the operation (see Table IV).

	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 IV: 3D-SAIL determination A refaire - Nico

For example, a UAS operation is assigned level 6 of GRC, level b of ARC and level B of PRC. By using Table I, we

assign the operation to 2D-SAIL of V. Then using Table IV, we define the final SAIL value corresponding to the operation as V.

D. Case study

To illustrate the application of the SORA methodology with Harm Extension, a simple operation of using drone to make a film is analyzed.

1) CONOPS description: The completed CONOPS description is very long (as mentionned on Annex A of the SORA methodology). Therefore, in this step, we collect only some important information to illustrate the Harm Extension. It is supposed that a film maker company uses a drone Phantom 4 Pro to make film shots in the center of a city. During the operation, the drone is flied manually by a pilot at 10m above the ground and in VLOS mode. Some important specifications of this drone are as follows:

- Weight: 1.3 kg
- Parachute: yes
- Camera resolution: 4896x2592
- Angle of view: 84 degrees

2) GRC determination: The UA is deployed in the centre of a city, so the probability that people on the ground could be struck by the UA (in case of out of control) is quite high. This operation is classified as a VLOS operation over a populated environment. In the case of a crash, corresponding to the height and the weight of the UA, the kinetic energy is about 127 J. This value is estimated by using a simple approach, in which we assume the drone drops vertically without draft force. Based on the Ground Risk Class table provided in the SORA methodology, this operation is assigned to a GRC of 4. Because the drone is equipped with a parachute, the final GRC is decreased to 3.

3) ARC determination: Because the UAV fly under 500ft (152m) above the ground, in uncontrolled airspace (far from any airports) and over urban area, the operation is assigned to an ARC of c (The decision table is presented in the document of the SORA methodology [27])

4) PRC determination: Based on the information on the camera specifications and the attitude of drone, we could calculate the maximun density pixel of the image captured in this operation as follows:

$$PD = \frac{4896}{2 * 10 * \tan(42)} = 272(pixels/m)$$

So the image detail is at the Identity Level (see Table II). As the UA flies in VLOS mode and over an urban zone, the intrinsic PRC of this operation is assigned to E. Because there are not any means of mitigation in place to prevent privacy violation in case of "UAS operation out of control", the final PRC is maintained unchanged at E level.

5) SAIL determination: The operation is assigned to an ARC of c and a GRC of 3, therefore the SAIL-2D value of the operation is IV (as shown in Table V).

With the level IV of SAIL-2D and level E of PRC, the operation is finally assigned a SAIL of level V (see Table VI).

	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 V: SAIL-2D determination A refaire - Nico

	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 VI: Final SAIL determination A refaire - Nico

Conclusion: In this case study, the final SAIL value determined the presented methodology is higher than the one determined in classical methodology (SAIL of V versus SAIL of IV). Therefore, threat barriers are required with higher robustness levels. For example, according to extended methodology, the applicant has to provides tests, simulations to prove that the UAS development conforms to authority recognized standards. Meanwhile, according to the classical methodology, the applicant has to only declare that the standards are conformed during UAS development.

V. Conclusio and perspectives

In this paper, first we explain the classical SORA methodology in both the quantitative and qualitative approaches. Based on the concept of the SORA methodology, we introduce our solution to extend it toward cybersecurity. Our solution includes two parts, which are maned Harm Extension and Threat Extension. Harm Extension aims to extend the risk scenarios under consideration with the new harms. Threat Extension aims to extend the risk scenarios under consideration with the new cybersecurity threats. At this moment, only Harm Extension is developed. In Harm Extension, we consider that the harm to privacy of third party is important and need to be addressed. For this purpose, we add a new step to evaluate the likelihood of this harm into risk assessment process of the SORA methodology and extend the "SAIL determination" step. These extensions are illustrated by a simple cas study.

For Harm Extension, further works need to be achieved to verify or improve the reasonableness of the decision table, especially Table IV. Then we start to develop Threat Extension to complete the extension solution.

References

[1] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, Sep. 2016, pp. 216–221. [Online]. Available: http://ieeexplore.ieee.org/document/7577060/

[2] *A-npa 2015-10: Introduction of a regulatory framework for the operation of drones*, European Union Aviation Safety Agency (EASA), Oct. 2015.

[3] *European Drones Outlook Study: Unlocking the value for Europe*, Single European Sky Atm Research Joint Undertaking (SESAR), Nov. 2016.

[4] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov 2016, pp. 1213–1218.

[5] M. Heiges, R. Bever, and K. Carnahan, "How to Safely Flight Test a UAV Subject to Cyber-Attacks," Georgia Tech Research Institute, Tech. Rep., 2015.

[6] A. Y. Javaid, F. Jahan, and W. Sun, "Analysis of Global Positioning System-Based Attacks and a Novel Global Positioning System Spoofing Detection/Mitigation Algorithm for Unmanned Aerial Vehicle Simulation," *Simulation*, vol. 93, no. 5, p. 427441, May 2017. [Online]. Available: https://doi.org/10.1177/0037549716685874

[7] D. Muniraj and M. Farhood, "A framework for detection of sensor attacks on small unmanned aircraft systems," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, June 2017, pp. 1189–1198.

[8] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescap, "A SVM-based detection approach for GPS spoofing attacks to UAV," in *2017 23rd International Conference on Automation and Computing (ICAC)*, Sep. 2017, pp. 1–11.

[9] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," in *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2019, pp. 1–6.

[10] Y. Qiao, Y. Zhang, and X. Du, "A Vision-Based GPS-Spoofing Detection Method for Small UAVs," in *2017 13th International Conference on Computational Intelligence and Security (CIS)*, Dec 2017, pp. 312–316.

[11] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with Sensor Input Spoofing Attacks," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. Austin, TX: USENIX Association, 2016. [Online]. Available: https://www.usenix.org/conference/woot16/workshop-program/presentation/davidson

[12] *ISO27005:2011 Information technology – Security techniques – Information security risk management*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Std.

[13] J. P. Jouas, J. L. Roule, D. Buc, O. Corbier, M. Gagn, M. Hazzan, G. Molines, C. Pineault, L. Poulin, P. Sasseville, C. Jolivet, and M. Touboul, *MEHARI Overview*, Club de la sécurité de l'information français (CLUSIF), Apr. 2010.

[14] P. Kobes, "Zoom sur la norme internationale IEC 62443 pour la cyberscurit des systmes numriques industriels," in *Cyberscurit des installations industrielles*. Cpadus, 2016.

[15] E. Kelling, M. Friedewald, T. Leimbach, M. Menzel, P. Säger, H. Seudié, and B. Weyl, "Specification and evaluation of e-security relevant use cases," E-safety vehicle intrusion protected applications project, Tech. Rep., 12 2009.

[16] S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, F. Andreas, G. Sigrid, H. Olaf, R. Roland, R. Matthias, B. Henrik, A. Ludovic, P. Renaud, P. Gabriel, R. Alastair, W. David, and W. Benjamin, "Security requirements for automotive on-board networks based on dark-side scenarios," EVITA, Tech. Rep., 2009.

[17] *AIRWORTHINESS SECURITY PROCESS SPECIFICATION ED-202 / DO-326*, EUROCAE, 102 rue Etienne Dolet, 92240 MALAKOFF, France, Jun. 2014.

[18] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security Application of Failure Mode and Effect Analysis (FMEA)," in *Computer Safety, Reliability, and Security*, A. Bondavalli and F. Di Giandomenico, Eds. Springer International Publishing, 2014, vol. 8666, pp. 310–325.

[19] H. Abdo, "Dealing with uncertainty in risk analysis : combining safety and security," Theses, Université Grenoble Alpes, Dec. 2017. [Online]. Available: https://tel.archives-ouvertes.fr/tel-01829574

[20] E. Jonsson, "An integrated framework for security and dependability," in *NSPW '98 Proceedings of the 1998 workshop on New security paradigms*. ACM Press, 1998, pp. 22–29. [Online]. Available: http://portal.acm.org/citation.cfm?doid=310889.310903

[21] J. Xu, K. K. Venkatasubramanian, and V. Sfyrla, "A methodology for systematic attack trees generation for interoperable medical devices," in *2016 Annual IEEE Systems Conference (SysCon)*, April 2016, pp. 1–7.

[22] S. Kriaa, "Joint safety and security modeling for risk assessment in cyber physical systems," Theses, Université Paris-Saclay, Mar. 2016. [Online]. Available: https://tel.archives-ouvertes.fr/tel-01318118

[23] F. Nikodem, A. Bierig, and J. S. Dittrich, "The New Specific Operations Risk Assessment Approach for UAS Regulation Compared to Common Civil Aviation Risk Assessment," in *DLRK 2018*, August 2018. [Online]. Available: https://elib.dlr.de/121660/

[24] *JARUS guidelines on Specific Operations Risk Assessment (SORA)*, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Jun. 2017, version 1.

[25] *Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947*, European Union Aviation Safety Agency (EASA), Oct. 2019.

[26] *Introduction of a regulatory framework for the operation of unmanned aircraft*, European Union Aviation Safety Agency (EASA), Dec. 2015.

[27] *JARUS guidelines on Specific Operations Risk Assessment (SORA)*, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Oct. 2019, version 2.

[28] *Annex E of SORA - Integrity and assurance levels for the Operation Safety Objectives (OSO)*, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Jan. 2019.

[29] C. Pauner, I. Kamara, and J. Viguri, "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)*, Dec 2015, pp. 1–7.

[30] S. Winkler, S. Zeadally, and K. Evans, "Privacy and Civilian Drone Use: The Need for Further Regulation," *IEEE Security '—&' Privacy*, vol. 16, no. 05, pp. 72–80, sep 2018.

[31] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," *Mobile Networks and Applications*, pp. 95–101, Jan 2019. [Online]. Available: https://doi.org/10.1007/s11036-018-1193-x

[32] R. L. Finn, D. Wright, and M. Friedewald, *Seven Types of Privacy*. Dordrecht: Springer Netherlands, 2013, pp. 3–32. [Online]. Available: https://doi.org/10.1007/978-94-007-5170-5_1

[33] Z. Li, C. Gao, Q. Yue, and X. Fu, "Toward drone privacy via regulating altitude and payload," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, Feb 2019, pp. 562–566.

[34] J. Villasenor, "Observations from above: Unmanned aircraft systems and privacy," *Harvard Journal of Law Public Policy*, 2013.

[35] S. Park and K. Lee, "Developing Criteria for Invasion of Privacy by Personal Drone," in *2017 International Conference on Platform Technology and Service (PlatCon)*, Feb 2017, pp. 1–7.

[36] M. Bonetto, P. Korshunov, G. Ramponi, and T. Ebrahimi, "Privacy in mini-drone based video surveillance," in *2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, vol. 04, May 2015, pp. 1–6.

[37] R. F. Babiceanu, P. Bojda, R. Seker, and M. A. Alghumgham, "An onboard UAS visual privacy guard system," in *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, April 2015, pp. 1–8.

[38] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-Aware Restricted Areas for Unmanned Aerial Systems," *IEEE Security Privacy*, vol. 16, no. 2, pp. 70–79, March 2018.

[39] *Planning, design, installation and operation of CCTV surveillance systems. Code of practice and associated guidance*, British Security Industry Association (BSIA), Jul. 2014.