A Comprehensive Probabilistic Assessment Method of UAS Ground Collision Risk

Théo Serru, Kevin Delmas

A Comprehensive Probabilistic Assessment Method of UAS Ground Collision Risk

Théo Serru

Laboratory ETIS, France. E-mail: theo.serru@ensea.fr
APSYS, France

Kevin Delmas

DTIS, ONERA, France. E-mail: kevin.delmas@onera.fr

Unmanned Aircraft Systems are widely experienced but using these systems for missions near to populated areas raises new safety challenges. To address these challenges, the European Aviation Safety Agency requires assessing, for a given operational profile, the likelihood of on-ground collision with critical infrastructure or people. Various works use Model Based Safety Assessment to identify the failure contributing to the crash, while some works provide probabilistic estimation methods of an on-ground collision. In these methods the assessment is performed thanks to Monte Carlo simulation known to be time-consuming to estimate the probability of rare events.
This paper will thus provide a comprehensive tooled method to estimate the on-ground collision probability and uses Importance Sampling method to tackle Monte Carlo limitations. Through a comparative study based on a drone use-case, this paper provides a demonstration of the benefits of Importance Sampling over Monte Carlo method. Indeed, this method allows a reduction in the number of simulations and thus the time needed to compute probabilities, with a high confidence in the results. The experiments are based on a safety model formalized with the Open AltaRica platform on an ad-hoc simulator to perform both Monte Carlo and important sampling simulations.

Keywords: Dependability, Safety, Importance Sampling, UAV, MBSA.

1. Introduction

Context

Unmanned Aircraft Systems (UAS) are widely experienced in domains such as transportation, delivery or infrastructure surveillance. However, using these systems for missions near to populated areas raises safety issues. To address these issues, the European Aviation Safety Agency has published safety assessment guidelines for unmanned operations (EASA, 2020). Some safety objectives, mostly the Operational Safety Objective #5, request to assess the likelihood of on-ground collision with critical infrastructure or people.

Problem statement

Despite these regulatory requirements, the probabilistic assessment of on-ground collision is only partially addressed by existing works. On one hand, various works (Delmas et al., 2019) promote the Model Based Safety Assessment to identify the failures contributing to the crash. On the other hand, some works (Bertrand et al., 2017) provide probabilistic estimation methods of an on-ground collision knowing that the drone is unable to ensure flight continuation. The assessment provided by these methods is performed thanks to Monte Carlo (Morio and Balesdent, 2015) simulation. However the computational effort to estimate the probability of rare events with a high confidence using standard Monte Carlo (MC) method becomes intractable.

Contributions

The main contribution of this paper is a comprehensive tooled method to estimate the on-ground collision probability by considering the contribution of on-board failures, reconfiguration mechanisms and operational specificity. To tackle Monte Carlo limitations, variance reduction methods (Morio and Balesdent, 2015) and more specifically Importance Sampling (IS) is used to obtain quicker and tighter estimation of the probability than standard Monte Carlo method. The paper provides a detailed presentation of the method and a demonstration of Importance Sampling benefits over Monte Carlo through a comparative study on a UAS case study. The experiments are based on a safety model formalized with the Open AltaRica platform (SystemX, 2017) and on an ad-hoc simulator to perform both Monte Carlo and important sampling simulations.

Paper organization

The sequel of this article is organized as follows. The section 2 provides a reminder of the available safety assessment methods dedicated to drones.

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_027-cd

Then, the section 3 introduces the drone used to illustrate the work. Section 4 focuses on Importance Sampling estimation of UAS failure and, on computation of the final casualty probability. This part details the major contribution of this work and illustrates the method on the case study. The section 5 discusses the results of the safety assessment on the drone Jerry with respect to the regulation requirements. Finally, section 6 outlines related works that allow to compute probabilities of complex dynamic systems.

2. Reminder on safety assessment for UAS

The UAS safety assessment process and tools used to illustrate the case study are introduced in this section. Starting with the safety modeling of failure propagation within the drone.

2.1. *Failure propagation modeling of complex reconfigurable systems*

Ensuring safety is essential in complex and critical systems such as Unmanned Aircraft Vehicles, as it deals with human lives. Classical safety formalism like fault-trees, Markov chains or Petri nets are widely used but give little information about the architecture of the system under study. Furthermore, changes in the architecture might lead to laborious changes in the safety model. To overcome these limitations, Model Based Safety Assessment (MBSA) methods (Lisagor et al., 2011) have been developed. Such methods are architecture-oriented as they define the dysfunctional behavior of *components*, *linked* one to another to build a *system*. The primary interests of MBSA are to easily consider changes in the system architecture, to generate the combination of faults leading to undesired events and to compute the likelihood of such events.

Among the MBSA methods, the ALTARICA formal language is one of the most popular formalism, used both in industry and academic research. The third version of the language introduced in (Prosvirnova, 2014) is based on Guarded Transition Systems (GTS) (Rauzy, 2008) and has been used to model the case study. This formalism encompasses reliability block diagrams, Markov chains and stochastic Petri nets to structure models and perform safety analyses. A system modeled with ALTARICA 3.0 is made of components described by the following elements: *state variables* describing the component state, *flow variables* describing its inputs and outputs, *events* susceptible to occur, *transitions* describing how the component's state changes when an event occurs and finally the *assertions* enforcing the value of the flow and state variables.

This version of the language comes with an open source modeling platform (SystemX, 2017). This platform allows the user to model systems using the ALTARICA 3.0 language and provides tools to perform safety assessment. These tools are: a fault tree compiler, a step-wise simulator and a stochastic simulator. The Open ALTARICA platform was used to model the use case and to perform stochastic simulation. This allowed to understand the behavior of the UAV in case of failures and to compute the probability of a feared event (as described in section 2.3).

2.2. *Estimation of ground risk maps for UAS*

Besides MBSA tools, several works such as (Bertrand et al., 2017), (Bertrand et al., 2021) and (Primatesta et al., 2020) focuses on UAV ground risk assessment and more precisely on **risk of casualties** (fatal injuries) **for people of inhabited areas and road network users**. They proposed tools to compute the risk on the ground by considering high level UAV failures (such as propulsion loss) and various aspects of the mission, mostly the planned trajectories and the location of inhabited areas along these trajectories.

The tool DROSERA used in this work is introduced in (Bertrand et al., 2017). It is used to simulate long range operation of UAVs. DROSERA gives a risk evaluation on the operation, a 3D visualization of the trajectory and the risks associated with the mission. One of the main interests of this tool is to provide indicators for a given drone on a given mission and generate them using standard formats, so that they can be visualized with COTS software such as Google Earth. The tool allows the user to generate:

- Mission statistics
- Risk exposition indicators on geographical representations
- Probabilistic maps and indicators
- Identification of risks relative to flight segments

These indicators are computed using Monte Carlo simulations (2.3) with inputs such as the UAV weight, span, flight speed and the mission GPS coordinates. Finally, the outputs of a simulation are printed in different files (.csv, .kml, .html) to deal with the needs of the stakeholders.

2.3. *Statistical-based assessment of feared events probabilities*

As introduced in 2.1, the calculation of a feared event probability depends on the architecture of the system and the probability of failure of each component. Since these safety-critical systems are dynamic, finding the analytical expression of the safety indicators may be overly complex. Thus, several methods have been developed, taking the growing computational power of computers as an

advantage, to approximate this probability with simulation-based methods.

The most common method is Monte Carlo simulations (see Landau and Binder (2005)). It relies on random sampling generation to obtain numerical results. For instance, one may want to estimate the mathematical expectation of $g(X)$ with *g* a deterministic scalar function and X a random variable of density f_X that is:

$$G = \mathbb{E}_{f_X}(g(X)) = \int_{\mathbb{R}^d} g(x)\, f_X(x)\, dx, \quad (1)$$

Using the law of large numbers, MC approximates G by the empirical mean of a large number of independents and identically distributed (iid) samples $x_1, x_2, ..., x_N$ following the failure distribution f_X:

$$G \simeq \widehat{E_{f_X}^{MC}} = \frac{1}{N} \times \sum\nolimits_{i=1}^{N} g(x_i) \quad (2)$$

When performing Monte Carlo simulations, two major limitations may be encountered. The first one relates to the computational effort requested when dealing with highly complex systems and low probabilities. The second limitation comes in the same specific case where truncation and round-off might lead to numerical errors.

To deal with the limitations of MC, several methods have been developed and are described in work such as (Landau and Binder, 2005) and (Morio and Balesdent, 2015). These works introduce statistical methods, reliability based approaches, quantum MC methods or variance reduction methods. This last category has been further explored in this work and among the variance reductions methods (e.g. crude Monte Carlo, importance sampling and more), Importance Sampling has been elected because of its proximity to MC that eases its integration in the safety assessment process.

The key idea of Importance Sampling is to use an auxiliary distribution *h* to generate more samples $X_1, X_2, ..., X_N$, that will trigger the desired event (i.e. feared event) than the initial distribution *f*. To consider the change in the probability density function generating the samples, a weight is introduced in the probability estimate. Let w be the likelihood factor defined as:

$$w(X) = \frac{f_X(X)}{h(X)}$$

The equation 1 can be rewritten using the auxiliary distribution h and the likelihood factor w as follows:

$$\begin{aligned} G &= \mathbb{E}_h(g(X)w(X)) \\ &\simeq \widehat{E_h^{IS}} = \frac{1}{N} \times \sum\nolimits_{i=1}^{N} g(X_i)w(X_i) \end{aligned} \quad (3)$$

The variance of G estimated by IS is thus:

$$\begin{aligned} \mathbb{V}(\widehat{E_h^{IS}}) = \frac{1}{N}(&\mathbb{E}_h(g(X)^2 w(X)^2) \\ &- \mathbb{E}_h(g(X)w(X))^2) \end{aligned} \quad (4)$$

The main difficulty of IS is to find the best distribution for *h*, called h_{opt}. The reason why this method is called "variance reduction method" is that with the optimal auxiliary distribution, h_{opt}, the variance is null, that is:

$$\mathbb{E}_h(g(X)^2 w(X)^2) = \mathbb{E}_h(g(X)w(X))^2 \quad (5)$$

and thus:

$$h_{opt}(X) = \frac{h(x) f_X(x)}{\mathbb{E}_h(g(X)w(X))} \quad (6)$$

As $\mathbb{E}_h(g(X)w(X))$ is the value to be computed with IS, *h* needs to be found by an adaptive method to get close to h_{opt}. Therefore, in this work, the method relies on a preliminary MC simulation, to find a distribution *h* close to h_{opt} and thus lowering the variance. This method will be explained in the section 4.

3. Case study

This paper is illustrated by the case study of a UAV, named Jerry, thus this section provides some characteristics of the intended mission and the dysfunctional model.

Jerry is a fixed-wing aircraft used for the monitoring of linear infrastructures such as railways. The drone can be controlled by a pilot or an operator to perform the mission using nominal modes. In a case of adversary conditions or critical onboard failures, degraded modes can be activated either by the pilot or the drone itself to ensure safety.

The major risks associated with the UAV's mission are ground, air or infrastructure collisions that can occur either when the UAV is in nominal or degraded mode. In addition, if a critical failure preventing a safe flight continuation occurs then the drone will automatically crash according to one of the three termination modes which are: straight-lined (controlled) descent, spiral descent and uncontrolled fall. Thus the selected termination mode will affect the risk of a collision.

The first safety assessment of Jerry considered three feared events, taken from (OGE, 2018), which are:

- CAT-SOL: Incapacity to maintain the UAS in a continuous flight without a flight termination activation.
- HAZ-SOL1: Incapacity to maintain the UAS in a safe continuous flight with a flight termination activation.
- HAZ-SOL3: Unintentional flight termination.

In the above cited work, the two HAZ-SOL feared events (HAZ-SOL1 and HAZ-SOL3) were grouped into a single feared event. Therefore, in the sequel of this paper, the two feared events considered will be CAT-SOL and HAZ-SOL events.

Finally, Jerry was modeled using the AltaRica 3.0 language and the Open AltaRica platform (cf 2.1) and resulted in a model with 500 components and 88 failure modes. The probabilistic assessment was possible by considering that the failures of the drone's components follow an exponential law. No data were accessible to compute the failure rates of Jerry's components. Therefore, relevant generic values taken from the literature ((OGE, 2018) and (Belkheiri et al., 2013)) were used. We remind that the goal of this use-case is to compare the methods of probabilistic assessment with a coherent UAV model. Thus, even if other laws and data might give results closer to the reality, the primary concern here is the soundness and performance of the assessment method, introduced in the next section.

4. Importance sampling-based estimation of UAS critical failure and casualty computation

4.1. *Overview*

In the safety assessment process of the drone Jerry, MBSA, stochastic simulation and DROSERA are used. Indeed, these methods allow to: have a great understanding of the drone and its behavior, compute the probability of feared events and estimate the ground risk. This process is illustrated in the Figure 1.

One of the added values of this work was to link the three methods in a unified safety assessment process, as illustrated by the Figure 1. This chain of tools allows to **compute the probability of lethal impact** for a given drone and mission. This is thus a significant step to match with the requirements from regulations such as (JARUS, 2019).

The estimation of the probability of the occurrence of a feared event can be formalized as a mean value estimation problem stated by the equation 1. Indeed, the UAV can be modeled as a deterministic function ϕ

- taking a random input $\mathbf{X}$ of dimension d, corresponding to the date of failure for each component ($d = 88$ for Jerry), following an exponential distribution $f_{\mathbf{X}}$ in our case,
- and producing a binary output denoted $\phi(\mathbf{X})$ indicating whether the considered feared event occurred during the mission.

Thus, the probability of the occurrence of a feared event f over a mission is the unknown parameter P_f of the Bernoulli variable $\phi(\mathbf{X})$ we want to estimate. Let

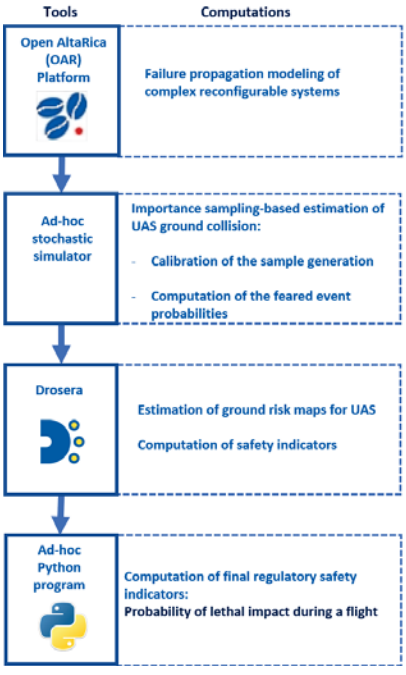

Fig. 1. Overview of the tooled UAV safety assessment process

$$g(X) = \mathbb{1}_{(\phi(\mathbf{X})=1)}$$

Then the parameter estimation can be formalized as follows:

$$P_f = \int_{\mathbb{R}^d} g(x) f_{\mathbf{X}}(\mathbf{x}) \mathbf{dx} = \mathbb{E}_{f_X}(g(X)) \quad (7)$$

Let the dimensions of the input vector be denoted $\mathbf{X} = \left(X^{(1)}, \ldots, X^{(d)}\right)$ and the random variables be independently and identically distributed with an exponential distribution of parameter $\lambda^{(i)}$. Hence the density $f(\mathbf{X})$ is the product of d exponential densities, that is:

$$\begin{aligned} f_{\mathbf{X}}(\mathbf{x}) &= f(x^{(1)}, \ldots, x^{(d)}) \\ &= \prod_{i=1}^{d} \lambda^{(i)} e^{-\lambda^{(i)} x^{(i)}} \end{aligned} \quad (8)$$

The probability P_f can be estimated by the empirical mean obtained with the Monte Carlo simulator from the Open AltaRica platform. However, MC limitations quickly appeared, as the simulations were too long or without enough confidence in the results. Thus, an ad-hoc Importance Sampling generator has been developed to be incorporated in the overall safety assessment process. This ad-hoc simulator is the principal contribution of this work and is introduced in the following

sections, starting with the choice of the auxiliary distribution.

4.2. *Calibration of the sample generation*

Section 2.3 introduced Importance Sampling and the notion of auxiliary distribution. To build the ad-hoc simulator, the first step is thus to compute this distribution *h*. As explained in the section 2.3, the main difficulty here is to find a good auxiliary density function that is close to the optimal value h_{opt}. To do so, the simulator uses a method based on a preliminary Monte Carlo simulation. The intuition is that the samples leading to a feared event in MC are distributed according to the optimal auxiliary function h_{opt}. Indeed, the distribution *h* is supposed to generate more failures than *f*. Thus, the optimum would be to generate a significant proportion of scenarios leading to a feared event. Then, using samples leading to failure from the preliminary MC simulation, a density function h_δ can be computed as follows:

(1) The ad-hoc simulator uses the Open AltaRica MC simulator to generate N samples $X_1, \ldots, X_N$ following $f_{\mathbf{X}}$ with the considered laws and parameters.
(2) Among them, let us consider that $X'_1, \ldots, X'_k$ samples are such that the considered feared event has been triggered during the simulation, that is when $\mathbb{1}_{(g(\mathbf{X}_i)=1)} = 1$.
(3) Then the ad-hoc simulator computes the mean failure time value of each input (failure mode) over all the runs leading to the feared event. Since the failures follow an exponential distribution one may estimate the failure rate as follows:

$$\delta = \frac{1}{\mathbb{E}(X)} \tag{9}$$

Let ${X'}_i^{(j)}$ correspond to the value of the input j of the run i, then the new parameter $\delta^{(j)}$ for each input $j \in [1, d]$ is:

$$\frac{1}{\delta^{(j)}} = \frac{1}{k} \sum_{i=1}^{k} g(X'_i) {X'}_i^{(j)} \tag{10}$$

Now, the auxiliary density $h_{\boldsymbol{\delta}}$ is defined, one can estimate the probability of failure by Importance Sampling. The next step is to simulate N' additional runs with the new density $h_{\boldsymbol{\delta}}$. To assess the confidence in the estimation we will use the coefficient of variation denoted c_X defined as follows:

$$c_X = \frac{\sqrt{\mathbb{V}(X)}}{\mathbb{E}(X)} \tag{11}$$

The lower its value is, the more confident we are in the results of the simulation. To illustrate this method, we use the model of Jerry and generate a preliminary Monte Carlo simulation. The number of samples generated is $1e^8$ and the mission duration is 200 seconds. During the auxiliary distribution computation, the failure having the most impact on the feared event had its rate changed from $\lambda_{MC} = 10^{-6}/h$ to $\delta_{IS} = 1.9/h$, leading to an auxiliary distribution $h_{\boldsymbol{\delta}}$ speeding up failures.

4.3. *Estimation of the feared event probabilities*

Following the auxiliary distribution, the simulator generates N' additional runs using MC. At the end of the simulation, it collects the state of the inputs X_i for each $i = 1, \ldots, N'$. Then it can estimate the probability using Importance Sampling with the density h_δ and the initial density f_X:

$$P_f \simeq \widehat{E_h^{IS}} = \frac{1}{N'} \sum_{i=1}^{N'} g(X_i) \frac{f_{\mathbf{X}}(X_i)}{h_{\boldsymbol{\delta}}(X_i)} \tag{12}$$

As the inputs are independent *f(X)* and *h(X)* are the product of the densities. Thus, the expectation can be written as:

$$\widehat{E_h^{IS}} = \frac{1}{N'} \sum_{i=1}^{N'} g(X) \prod_{j=1}^{d} \frac{f_{\lambda^{(j)}}(X_i^{(j)})}{h_{\delta^{(j)}}(X_i^{(j)})} \tag{13}$$

where samples X_i are iid following the density h_δ, and N' expected to be lower than N. To validate the results, the coefficient of variation on the estimator is computed. With this method, the coefficient is expected to be lower with the IS. A greater error can indicate a *low confidence* Monte Carlo or IS estimation of P_f.

The first MC simulation for the CAT-SOL event gave a coefficient of variation $c_{CAT} = 1.96e^{-1}$. Then, the IS simulation allowed to compute a new probability with a new coefficient of variation $c_{CAT} = 1.65e^{-2}$ with a similar estimation, $\widehat{E_h^{IS}} = 2.96e^{-7}$, and $N' = 1e^5$ simulations. Thus, by adding a simulation of only $1e^5$ samples, the coefficient of variation was divided by 10.

With a higher confidence in the simulation results and a lower simulation time, the computed probability can be used in the overall safety process. The next section focuses on computing the final probability of lethal impact.

4.4. *Computation of final regulatory safety indicators*

As written in the two documents (OGE, 2018) and (JARUS, 2019), the primary goal of a safety assessment is to ensure a minimum risk for the population while performing UAVs operations. Therefore, the indicator of risk for the population is the probability of a lethal impact during a mission. As depicted in the Figure 1, this indicator is computed by the last step of the process. More

precisely, the indicator is computed thanks to the equation 14, proposed by (Bertrand et al., 2017):

$$\begin{array}{l} p(cslty) = p(loss) \times p(imp|loss) \\ \times p(coll|imp \cap loss) \\ \times p(cslty|coll \cap imp \cap loss) \end{array} \quad (14)$$

Where:

- *loss* stands for *Loss of control of the UAV* that is the vehicle starts a non-controlled descent to the ground.
- *imp* stands for *Non-controlled ground impact* that is the vehicle crashes with a non-controlled speed or on a non-prepared landing area.
- *coll* stands for *Collision with someone* that is the crash results in a collision between the UAV and someone on the ground.
- *cslty* stands for *Fatal injury to someone* that is the collision with someone results in fatal injuries to that person.

$p(loss)$ is generated by the ad-hoc simulator and the three other terms are generated by DROSERA . Furthermore, the probability of a casualty is also computed by DROSERA , but for each second of the flight and not for the entire mission duration. Thus, a conversion is performed to provide indicators consistent with the final safety objective. Let $p(cslty^f)$ be the probability of a casualty for a given feared event f among $\mathcal{F}$ disjoint feared events, then the probability of casualty can be expressed as:

$$p(cslty) = \sum\nolimits_{f \in \mathcal{F}} p(cslty^f) \quad (15)$$

Let A_i stand for a casualty at $t = i$ after the triggering of the feared event f, then the terms $p(cslty^f)$ can be estimated as follows:

$$p(cslty^f) = \sum\nolimits_{i=0}^{t} p(A_i) \times \prod\nolimits_{j=0}^{i-1} p(\overline{A_j}) \quad (16)$$

For Jerry, two feared events are considered, CAT and HAZ, so the probability will be:

$$p(cslty) = p(cslty^{CAT}) + p(cslty^{HAZ}) \quad (17)$$

Hence, the proposed process allows to assess the acceptability of lethal impact of the drone with respect to the final safety objective. This process benefits from the use of Importance Sampling to speed up the estimation of the crash probability. Nevertheless, the efficiency of Importance Sampling is tied to the estimation of h_δ that is empirical and do not come with strong guarantees of variance reduction. That is why this method is experimented on Jerry and its efficiency discussed by comparison to classical Monte Carlo.

5. Results

The results of the experiments performed on Jerry are gathered in the table 2. Concerning CAT_SOL, the results demonstrate a one order of magnitude reduction of the coefficient of variation with few additional simulations ($1e^5$) compared to the $1e^8$ samples used to obtain an initial estimation of the mean value. We see that the coefficient of variation obtained on the $1.001e^8$ samples is still better than the one obtained with $2e^8$ samples and thus reduces the computational costs.

Nevertheless, this reduction is significant if the number of Monte Carlo samples are quite close to the minimum number of samples needed to estimate the probability *i.e.* $1e^N$ samples to estimate a $1e^{-N}$ mean value. If the number of samples is large enough, which is the case for HAZ_SOL ($1e^{-5}$ mean value estimated with $1e^8$ samples), then the advantages of the importance sampling are less significant as showed by the table 2. On the other hand, a *poor* initial guess of the mean value used to compute the auxiliary distribution also lead to poor IS results as shown in the table for $N = 1e^7$.

The next step is the computation of the probability of lethal impact for each second of the flight by DROSERA . Thus, two simulations have been launched for a mission of $t = 200\ seconds$ in the french city of Tournay with $p(loss) = 2.96e^{-7}$ for the first CAT_SOL simulation and $p(loss) = 8.16e^{-5}$ for the HAZ_SOL simulation.

The result obtained by processing the Drosera results with the equation 16 are $p(cslty^{CAT}) = 4.02e^{-10}$ and $p(cslty^{HAZ}) = 1.01e^{-7}$ resulting in a total casualty probability of $p(cslty) = 1.01e^{-7}$.

By comparing these results to the safety objective from the OGE-I (OGE, 2018):

$$\begin{array}{c} p(cslty^{CAT}) = 4.02e^{-10} < 10^{-7} \\ p(cslty^{HAZ}) = 1.01e^{-7} < 10^{-5} \end{array}$$

it gives an excellent overview on the level of safety of the UAV. Here, the drone could be validated regarding the OGE-I on the evaluation of the probability of failure. Thus, even if the failure rates are not the real one, it is clear that the safety assessment process is in line with the regulations and their expectations.

6. Related works

The safety assessment method introduced in this work relies upon other methods, enabling the computation of indicators such as the probability of the crash of the drone. The choice of using Monte Carlo and then Importance Sampling was made after analyzing the state of the art.

Feared Event	Method	Sample size	Estimated probability	Coefficient of variation	Computation time
CAT_SOL	Monte Carlo	$1e^7$	$6.00e^{-7}$	$4.08e^{-1}$	47s
	Importance Sampling	$1.01e^7$	$3.45e^{-7}$	$4.17e^{-1}$	71s
	Monte Carlo	$1e^8$	$2.60e^{-7}$	$1.96e^{-1}$	449s
	Importance Sampling	$1.001e^8$	$2.96e^{-7}$	$1.65e^{-2}$	474s
	Monte Carlo	$2e^8$	$2.85e^{-7}$	$1.3e^{-1}$	920s
HAZ_SOL	Monte Carlo	$1e^7$	$7.6e^{-5}$	$3.6e^{-2}$	47s
	Importance Sampling	$1.01e^7$	$1.74e^{-4}$	$2.81e^{-1}$	51s
	Monte Carlo	$1e^8$	$7.45e^{-5}$	$1.15e^{-2}$	449s
	Importance Sampling	$1.001e^8$	$8.16e^{-5}$	$7.30e^{-3}$	451s

Fig. 2. Estimated probability of feared event occurrence during Jerry mission

Dynamic system assessment

The computation of probabilistic indicators for dynamic systems has been extensively studied in the literature. **Markov Chains** based approaches have been used to compute probabilities in (Hastings, 1970) as a Monte Carlo sampling method, or in (Baier et al., 2000) as a base for a model checking tool. The typical Fault Trees (FT) have also been adapted in **Dynamic Fault Trees** (DFTs) to consider the dynamic aspect of complex systems. Various works propose dedicated formalisms to analyse DFTs such as (Merle, 2010) based on an algebraic method. **Dynamic Event Trees** (DETs) have also been used in the nuclear industry to perform safety analyses. Finally, **Petri Nets** have been extensively used for decades to model complex systems, and works such as (Wang, 2007), illustrates their use on dynamic systems. As stated in the section 2, ALTARICA is based on guarded transition systems encompassing the presented formalisms, hence could be translated into one of them and benefits from the developed assessment methods. Nevertheless, such translations are not available on the platform provided for ALTARICA 3.0, that is why the Monte-Carlo method requesting only the access to a simulator has been elected.

Variance reduction

The use of Importance Sampling has been introduced in section 4 and has been motivated by other works using variance reduction methods. The first of these works is (Morio and Balesdent, 2015) and focuses on the estimation of rare event probabilities in complex aerospace systems. It introduces the main rare event estimation techniques such as **crude Monte Carlo**, **Importance Sampling**, **extreme value theory** or **directional sampling**. However, other methods have been developed in works such as (Echard et al., 2013). In this paper, the authors are introducing a method mixing **Importance Sampling** and **Kringing metamodel** to assess small probabilities. The paper (Gomes and Awruch, 2004) introduces other methods and compares them to MC and adaptive IS. These methods, **response surface and neural networks**, are supposed to reduce the computational cost of structural evaluations. The choice of Importance Sampling has been motivated once again by the possibility to use the MC simulator provided by the AltaRica platform.

Calibration of samples generation

Among works on Importance Sampling, there are many ways to compute the auxiliary distribution. Indeed, the choice of this distribution h is crucial to lower the variance effectively. A first method is introduced in (Tomasson and Soder, 2017) which defines the **cross entropy method** to estimate the auxiliary distribution for composite power systems. The work (Morio and Balesdent, 2015) also define several methods such as **non adaptive IS** (scaling, mean translation, exponential twisting), **adaptive IS** (cross entropy, non parametric adaptive IS). The first method gives good results for rather simple systems and is easy to implement, where the second is better for complex and high dimensional systems but are harder to use in practice. Thus, a version of the cross entropy method (using only 1 iteration) has been used in this work as it was quicker to implement into the safety assessment while giving satisfying results on a complex case study as shown in section 5.

7. Conclusion

Summary

In this paper, we presented a tooled process to assess the compliance of a UAS to some of the probabilistic requirements requested by the applicable regulations. More precisely, the assessment of the collision probability between a drone and a third person on the ground is estimated.

This process relies upon three main steps with dedicated tools. First, the drone is modeled using the ALTARICA 3.0 language with its failure parameters. Then an ad-hoc Importance Sampling simulator computes the probability of a flight termination activation due to internal failures. This simulator allows to overcome some limitations of

the classical Monte Carlo simulations to compute, with fewer samples, a sound probability. The tool DROSERA is then used to compute the probability of lethal impact between the drone and a third person on the ground. Eventually a final computation derives the collision probability for the mission from the DROSERA computation. This tooled process is mostly automatized and benefits from well-known academic tools. The process has been applied on the case study Jerry to illustrate the benefits and limitations of the proposed approach.

Future works

In this paper, we greatly discussed about the uncertainties brought by the estimation method. Nevertheless, other sources of uncertainties, on the failure rates for instance, may have a dramatic impact on the estimation. Therefore a sensitivity analysis could be used to identify the more impacting sources of uncertainties and help to drive the uncertainty reduction in the proposed process.

Since each flight termination mode leads to different crash trajectories, a way to improve our estimation would be to exploit the ability of DROSERA to consider alternative flight termination modes (e.g. parachute, descending glide/spiral). To do so, DROSERA must be complemented with additional dynamic models capturing the crash trajectories for such termination modes.

Moreover, the degraded modes introduced in 3, are not considered when computing the ground impact probability. For example, during a "Return to Base" mode, the UAV will go straight to a previously identified location. It will neither follow the route previously taken nor continue its flight. These modes may have a significant impact over the collision probability and thus must be taken into account.

Acknowledgment

This work has been achieved in the PHYDIAS project granted by DGAC.

References

Baier, C., B. Haverkort, H. Hermanns, and J. Katoen (2000). Model Checking Continuous-Time Markov Chains by Transient Analysis. In *CAV*.

Belkheiri, R. Ares, and K. Zurbuch (2013). Exploitation de données de retours d'expérience multi-industriels pour la consolidation des modèles FIDES. pp. 15.

Bertrand, S., N. Raballand, S. Lala, and B. Levasseur (2021). Drosera: a drone simulation environment for risk assessment. *31th European Safety and Reliability Conference (ESREL21)*.

Bertrand, S., N. Raballand, F. Viguier, and F. Muller (2017). Ground risk assessment for long-range inspection missions of railways by uavs. *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, 1343–1351.

Delmas, K., C. Seguin, and P. Bieber (2019). Tiered model-based safety assessment. In *International Symposium on Model-Based Safety and Assessment*, pp. 141–156. Springer.

EASA (2020). Easy Access Rules for Unmanned Aircraft Systems.

Echard, B., N. Gayton, M. Lemaire, and N. Relun (2013, March). A combined Importance Sampling and Kriging reliability method for small failure probabilities with time-demanding numerical models. *Reliability Engineering & System Safety 111*, 232–240.

Gomes, H. M. and A. M. Awruch (2004, January). Comparison of response surface and neural network with other methods for structural reliability analysis. *Structural Safety 26*(1), 49–67.

Hastings, W. K. (1970). Monte Carlo sampling methods using Markov chains and their applications. pp. 13.

JARUS (2019). Jarus guidelines on Specific Operations Risk Assessment (SORA). *2*.

Landau, D. P. and K. Binder (2005). *A Guide to Monte Carlo Simulations in Statistical Physics* (2 ed.). Cambridge: Cambridge University Press.

Lisagor, O., T. Kelly, and R. Niu (2011). Model-based safety assessment: Review of the discipline and its challenges. *The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety*, 625–632.

Merle, G. (2010). Algebraic modelling of Dynamic Fault Trees, contribution to qualitative and quantitative analysis. pp. 223.

Morio, J. and M. Balesdent (2015). *Estimation of rare event probabilities in complex aerospace (and other) systems - a practical approach*.

OGE (2018). Opération de Grande Elongation Intérimaire.

Primatesta, S., A. Rizzo, and A. la Cour-Harbo (2020). Ground risk map for unmanned aircraft in urban environments. *Journal of Intelligent & Robotic Systems 97*(3), 489–509.

Prosvirnova, T. (2014). *AltaRica 3.0: a Model-Based approach for Safety Analyses*. Ph. D. thesis, École Polytechnique.

Rauzy, A. (2008, December). Guarded Transition Systems: a new States/Events Formalism for Reliability Studies. *Proceedings of The Institution of Mechanical Engineers Part O-journal of Risk and Reliability 222*.

SystemX, I. (2017). The Open Altarica Platform.

Tomasson, E. and L. Soder (2017, June). Improved importance sampling for reliability evaluation of composite power systems. In *2017 IEEE Manchester PowerTech*.

Wang, J. (2007). Petri Nets for Dynamic Event-Driven System Modeling. pp. 17.