PhD Position

Modeling framework for design specification and safety assessment of Unmanned Aerial Systems

---

Keywords: MBSE, MBSA, Systems Engineering

PhD Supervisor: Prof. Pierre de Saqui-Sannes (ISAE-SUPAERO)
PhD Co-Supervisors: Prof. Jean-Charles Chaudemar (ISAE-SUPAERO)
Dr. Kevin Delmas (ONERA)

Apply to: pdss@isae-supaero.fr
jean-charles.chaudemar@isae-supaero.fr
kevin.delmas@onera.fr

Funding: Fédération de recherche ONERA – ISAE-SUPAERO – ENAC
3 years

Starting in: as soon as possible

Location: ONERA, Toulouse, France

Context and problematic

The acronym MBSE was coined to denote model-based systems engineering approaches that enable to rely on model to design and implement a system in order to meet stakeholders' expectations and confidence. These expectations involve manifold viewpoints that need to be tackled throughout the early design phase.

Inspired from aeronautics standards, new methodologies (such as Specific Operations Risk Assessment) account for acceptability matters for Unmanned Aerial Systems (UAS). These methodologies take into account social acceptability through an expected resilience with respect to the selected operational context: type of environment (population density, threats …) and type of foreseen operation (delivery, surveillance …).

In this context, this PhD aims to define a modeling framework for a UAS, specifying operational concepts, and taking social and technological concerns into account. Thus, the realization a tooled methodology is suitable for assuring the consistency and the relevance of models based on the system lifecycle and its environment evolution.

Regarding risks acceptability for UAS, classification methods are specific and differ from conventional methods in commercial aviation due to the diversity of operational contexts. To cope with this diversity, we need to come up with a trade-off between operational context, drone resilience, communication system resilience and resilience of air traffic control procedures. Fixing such a trade-off turns out to refine and allocate requirements to each system's component. In addition, the trade-off shall avoid useless iterations and reduce the certification cost by providing the relevant artifacts to the certification authority.

Objectives

This PhD work aims at defining an overall modeling framework that enables to account for social and technological aspects for the design of UAS. Social aspects include human-machine interaction, risk acceptability and assessment, and sustainability. More precisely risk acceptability consists in:

1. Defining acceptable thresholds on failure occurrence probability with regards to the gravity of the effects. Probabilities become quantitative safety objectives.
2. Performing safety analysis and assessment.

The proposed modeling method will take into account multi-agent behaviours (integrate the remotely pilot's behaviour as well) to provide the argumentation basis for exchanges with stakeholders (French Defense Ministry, safety authority).

Expected outcome

- Define a modeling framework for operational concepts and systems engineering processes accounting for sustainable and social stakes, along with standards (SORA).
- Provide a tooled method for analysis (consistency) and allocation of requirements to system components (drone, ground station, ATM...) to ease both design and certification activities.
- Consolidate and apply the methodology to a UAS whose mission is to be defined.

References

- Bieber, Pierre, Bougnol, Christian, Castel, Charles, Heckmann, Jean-Pierre , Kehren, Christophe, Metge, Sylvain and Seguin, Christel. *Safety assessment with Altarica*. In Building the Information Society, pp 505-510. Springer, 2004.
- FAA. *Concept of operations*, 2018.
- JARUS. *Jarus guidelines on specific operations risk assessment*, 2017.
- Leveson N., M. S. Herring, B. D. Owens, M. Ingham, and K. A.Weiss. *Safety-driven model-based systems engineering methodology*. Technical report, MIT, 2007.
- SAE. Aerospace Recommended Practices 4761 - *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*, 1996.
- SAE. Aerospace Recommended Practices 4754a - *Development of Civil Aircraft and Systems*, 2010.
- Villemeur, Alain. *Reliability, availability, maintainability and safety assessment*. John Wiley & Sons, 1992.
- Delmas, Kevin, Seguin, Christel and Bieber, Pierre. *Tiered Model-Based Safety Assessment*. In International Symposium on Model-Based Safety and Assessment. pp. 141-156 Springer 2019.

Cadre méthodologique global d'analyse et de spécification

Directeur : Pierre de Saqui- Sannes (ISAE-SUPAERO)
Co-directeurs : Jean-Charles Chaudemar (ISAE-SUPAERO)
Kevin Delmas (ONERA)

Laboratoire d'accueil

ONERA

Financement

Fédération de recherche ONERA–ISAE-SUPAERO–ENAC

Contexte et problématique scientifique

L'ingénierie des exigences dirigée par les modèles vise à guider le concepteur tout en garantissant un bon niveau de confiance des parties prenantes. Ainsi un des enjeux importants est d'assurer une cohérence entre les différents points de vue adressés lors de la phase amont d'un projet.

En s'inspirant des standards aéronautiques existants ARP4754 et ARP4761, de nouveaux standards et méthodologies comme la SORA (Specific Operations Risk Assessment) issue du groupe de réflexion JARUS (Joint Authorities for Rulemaking on Unmanned Systems) considèrent d'ores et déjà les questions d'acceptabilité pour les systèmes drone. L'approche retenue dans ces standards consiste à traduire l'acceptabilité sociale par une résilience attendue du système drone en fonction du cadre opérationnel choisi c'est-à-dire le type d'environnement dans lequel le drone évolue (densité de population, agressivité,...) et le type d'opération prévu (transport de colis, surveillance,...).

Ainsi, dans le cadre de cette thèse, le cadre de modélisation du système drone doit non seulement formaliser les concepts/aspects opérationnels mais aussi intégrer des concepts/aspects sociétaux et technologiques au plus haut niveau de modélisation. Pour cela, la réalisation d'un meta-modèle élaboré à partir d'une méthodologie outillée et adaptée au cycle de vie du système et à son environnement, permet d'assurer la cohérence et la pertinence des modèles générés.

Concernant l'acceptabilité des risques, les méthodes de classification des risques inhérents à un système drone différent de celles rencontrées dans le domaine aéronautique notamment par la diversité des cadres opérationnels considérés bien supérieure à celle rencontrée dans l'aviation traditionnelle. Un compromis entre cadre opérationnel (logistique urbaine, surveillance d'infrastructure isolée, ...), résilience du drone, résilience des systèmes de communication et résilience des procédures de contrôle (liens de communication avec le sol, système de gestion du trafic aérien,...) est demandé au concepteur. La résolution d'un tel compromis revient à raffiner et allouer des exigences sur chacun des éléments constituants du système pour soutenir les exigences de haut niveau. Le choix d'un compromis a donc un fort impact sur les phases avales de conception et doit donc être minutieusement justifiés pour éviter des itérations chronophages et onéreuses de conception. Par ailleurs, tracer au plus tôt les justifications de ces choix de conception permet de construire, tout au long du cycle de développement, les éléments nécessaires à la démonstration aux autorités compétentes de la pertinence de la réponse aux enjeux sociétaux apportée par le système drone.

Objectifs

Dans le cadre du projet Concorde de la fédération de recherche ONERA-ISAE-ENAC, on vise à définir un cadre méthodologique global permettant de répondre aux enjeux sociétaux (développement durable, économie,…) et technologiques (performances, missions,…) pour la conception et l'usage de drones. Ainsi le cadre à étudier doit intégrer des concepts/aspects sociétaux tels que les impacts des systèmes drones-humains sur des populations, à savoir des menaces ou opportunités affectant leur milieu de vie ou bien des ressources. L'une des menaces majeures qui doit être considérée par la méthodologie envisagée est d'assurer l'acceptabilité des risques inhérents au déploiement d'un système drone. Plus précisément, assurer l'acceptabilité des risques consiste :

1. à définir des seuils acceptables sur la probabilité d'occurrence d'une défaillance en fonction de la gravité de ses conséquences sur l'environnement du système, ces probabilités deviennent alors des objectifs de sécurité ;
2. à mener des analyses de sûreté de fonctionnement pour assurer que le système remplit les objectifs fixés.

La modélisation proposée prendra en compte des comportements multi-agent (au-delà du vecteur seul) qui devront permettre d'analyser les modèles et servir de base argumentaire pour les échanges avec les différentes parties prenantes, notamment au sein du projet Concorde.

Au vu de la problématique établie, les éléments d'investigation proposés pour cette thèse sont :

1. Définir une modélisation générique des concepts opérationnels et des processus d'ingénierie traduisant les enjeux environnementaux et sociétaux en tenant compte des standards et méthodologies existants (SORA).
2. Fournir une méthode outillée d'analyse (cohérence) et d'allocation des exigences de haut niveau du système drone vers les éléments du système (drone, station sol, ATM,...) afin de prendre en compte au plus tôt les problématiques de conception et de certification. Au vu de la dimension critique du système, un intérêt particulier sera porté sur l'aspect sûreté de fonctionnement tant du point de vue analyse qu'allocation.
3. Consolider la méthodologie proposée en accord avec les autres projets et thèses du projet Concorde.

Informations utiles

Candidatures (CV et lettre de motivation) à envoyer à : pdss@isae-supaero.fr, jean-charles.chaudemar@isae-supaero.fr, kevin.delmas@onera.fr

Démarrage souhaité au plus tôt.

Références

- Bieber, Pierre, Bougnol, Christian, Castel, Charles, Heckmann, Jean-Pierre , Kehren, Christophe, Metge, Sylvain and Seguin, Christel. *Safety assessment with Altarica*. In Building the Information Society, pp 505-510. Springer, 2004.
- FAA. *Concept of operations*, 2018.
- JARUS. *Jarus guidelines on specific operations risk assessment*, 2017.

- Leveson N., M. S. Herring, B. D. Owens, M. Ingham, and K. A.Weiss. *Safety-driven model-based systems engineering methodology*. Technical report, MIT, 2007.
- SAE. Aerospace Recommended Practices 4761 - *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*, 1996.
- SAE. Aerospace Recommended Practices 4754a - *Development of Civil Aircraft and Systems*, 2010.
- Villemeur, Alain. *Reliability, availability, maintainability and safety assessment*. John Wiley & Sons, 1992.
- Delmas, Kevin, Seguin, Christel and Bieber, Pierre. *Tiered Model-Based Safety Assessment*. In International Symposium on Model-Based Safety and Assessment. pp. 141-156 Springer 2019.