Master thesis @ ISAE-SUPAERO, 4-6 months

Safety-security methodology for UAV/UAS case study

Possibility to continue with a PhD

Contact: Jean-Charles Chaudemar, jean-charles.chaudemar@isae-supaero.fr
Co-tutor: Marina Dehez-Clementi, marina.dehez-clementi@isae-supaero.fr
Start: April, 2025 (asap)
Scientific domain: Safety-security methods, systems engineering, computer science

Context and Objectives
Unmanned Aerial Vehicles (UAV) are widely used for various missions (surveillance, transport, maintenance/overhaul) in the civil and military domains. Therefore, an UAV is prone, in operation, to undesired events such as attacks and flaws. According to the nature of these events, a specific methodology is applied to mitigate their effects on the UAV itself and its environment. An attack-threat implies a security approach, whereas a fault relies on a safety analysis. Is it possible to merge safety and security approaches? How could we efficiently design a more robust and reliable, and safer UAV?

The certification process enables to tackle these issues. Also, the U-space regulatory framework (EU 2021/664) provides a set of guidelines for the management of drones, which impacts the UAV's embedded systems. The implementation of these guidelines in terms of Acceptable Means of Compliance and Guidance Material (AMC/GM) is of the upmost importance for the certification of drones designed to share the airspace with other aircraft. The guidelines address all aspects of the development and the operation for the drones and the stakeholders. Thus, the Specific Operations Risk Assessment (SORA) methodology defines about twenty-one Operational Safety Objectives (OSOs) for various risks such as the Air Risk Class (ARC). OSOs require high-level properties of the Unmanned Aerial Systems (UAS), which encompass not only the UAV but also the ground control station, communication links, and any supporting infrastructure needed for operation. For instance, OSO #11 states that "procedures are in-place to handle the deterioration of external systems supporting UAS operations" [1][2][3]. As for the security, the MITTRE ATT&CK[1] data base provides us with a set of tactics et techniques used by attackers. The standard NIST Cybersecurity Framework [4] defines the five main properties for data and services in the field of information processing systems (namely systems that embed computers): confidentiality, integrity, availability, authenticity, accountability [5][6]. To ensure the security of an information system, we aim to guarantee the triad of properties. Regarding UAV/UAS, this triad is as follows:

[1] https://attack.mitre.org/

- Confidentiality: Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- Integrity: Guards against improper information modification or destruction, including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- Availability: Ensures timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

In the context of the internship, our main objectives are to define a merged methodology for the security and safety of an UAV/UAS, to propose a methodological framework based on models, and to validate it on an UAV's architecture integrating Paparazzi[2] system. Several attack scenarios will be investigated within a given demonstrator methodology.

Description

The axiomatic category theory paves the way for the model transformation throughout the graph transformation [7][8]. In a model-driven engineering approach, the model transformation defines a process of linking two models/domains at least in terms of consistent semantics between them. For instance, when it comes to software engineering, the implementation of this transformation link is depicted by a compiler from a high-level language (specification) into a code source. As for a system viewpoint, models rely on productions or artefacts of engineering methods, thus only high-level languages are considered over early design phases [9].

The certification process imposes an early verification and validation for the development of models at each stage, but also the consistency of their transformation. Thanks to formal methods, a few model transformations leverage theorem provers. To do so, a formal semantics of the source domain together with a formal semantics of the target domain have to be defined. To avoid reinventing the wheel, a thorough literature survey is compulsory. The languages, the scope of each domain, the formal methods are all concepts to delve more deeply for the sake of the model transformation.

Work agenda

The roadmap of the intern will be organized around three main tasks:

1) To do a state-of-the-art or survey about safety and security modelling methods in general, and for UAV case study, specifically: there exist tools for each approach, but a few questions can be raised about the semantics and about the interoperability.
2) To identify key properties for a merged safety-security methodology: e.g., how to state its correctness?
3) To propose a strategy for a domain specific modelling language that supports this methodological framework: e.g., could we model any UAVs?

[2] https://paparazziuav.org

Expected skills

The applicants are Master students (1st or 2nd year) in computer science or systems engineering with a tough background on safety and/or security methods. In addition to the tasks about the setting out of a domain specific modelling language and method, the applicant will develop own method or high-level language. Fluency in English and soft skills are required abilities.

IT skills are as follows:

- languages: C, Java, Python, QVT, ATL
- modelling: MBSE, MBSA, cybersecurity, formal methods

The applications should be sent by e-mail to the supervisor, enclosing CV, cover letter mandatorily, and master transcript optionally.

References

[1] Mathou, C., Delmas, K., de Saqui Sannes, P., and Chaudemar, J.-C.: “UAS procedures model with system architecture for safety analysis”. In : 2024 International Conference on Unmanned Aircraft Systems (ICUAS). 2024, p. 873-880. doi: 10.1109/ICUAS60882.2024.10557098.

[2] Mathou, C., Delmas, K., de Saqui Sannes, P., and Chaudemar, J.-C.: “Safety-oriented dynamic procedure modeling”. In: IEEE International Systems Conference, SysCon 2024, Montreal, QC, Canada, April 15-18, 2024. IEEE, 2024, p. 1-8. doi : 10.1109/SYSCON61195.2024.10553507.

[3] He, X., Chaudemar, J.-C., Huang, J., Defaÿ, F.: “Fault tolerant control of a quadrotor based on parameter estimation techniques and use of a reconfigurable PID controller”. In: 2016 24th Mediterranean Conference on Control and Automation (MED), pp. 188–193 (2016). IEEE.

[4] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 2.0. U.S. Department of Commerce, February 2024.

[5] Dehez-Clementi, Marina, et al. "When air traffic management meets blockchain technology: a blockchain-based concept for securing the sharing of flight data." 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC). IEEE, 2019.

[6] Baptista, Frederico, Marina Dehez-Clementi, and Jonathan Detchart: "DFly: A Publicly Auditable and Privacy-Preserving UAS Traffic Management System on Blockchain." (2024).

[7] Schubert H. Categories. Springer Berlin Heidelberg; 1972.

[8] Schürr, A., Nagl, M. and Zündorf, A. eds., 2008. Applications of Graph Transformations with Industrial Relevance: Third International Symposium, AGTIVE 2007, Kassel, Germany, October 10-12, 2007, Revised Selected and Invited Papers (Vol. 5088). Springer Science & Business Media.

[9] Broy, M.: “A logical approach to systems engineering artifacts: semantic relationships and dependencies beyond traceability—from requirements to functional and architectural views”. Software & Systems Modeling, pp. 365-393, 2018.