Contribution for AT-RASC 2015 (session: S-F2)

Autonomous Drones for Disasters Management: Safety and Security Verifications

Ludovic Apvrille[1], Yves Roudier[2] and Tullio Joseph Tanzi[1]
1Institut Mines-Telecom, Telecom ParisTech, LTCI CNRS, France,
ludovic.apvrille@telecom-paristech.fr , tullio.tanzi@telecom-paristech.fr ,
[2] EURECOM. Sophia Antipolis, France
Yves.Roudier@eurecom.fr

Information plays a key role in natural disaster crisis management and relief. We discussed in previous contributions how lightweight Unmanned Aerial Vehicles (UAVs) or (micro-)drones can effectively assist rescuers in order to improve the situational awareness and assessment [1] [2].

Drones can provide a vastly superior implementation to three types of humanitarian assistance scenarios: (1) communication and coordination of operations, (2) terrain coverage, and (3) search operations. In the last scenario, the fast deployment of drones supports the identification of scattered groups of disabled persons, and notably aims to determine whether victims are adults or children and their movements. Drones will also help locate the electromagnetic emissions of personal belongings of victims buried under ruined buildings or hiding in dense forests at a faster pace and with better precision.

The autonomy of drones is central to the acceptability of such a solution by search and rescue teams. The drone4u project [3] has developed functional building blocks supporting such an autonomous operation, on top of which the abovementioned scenarios can be implemented: (1) autonomous navigation based on the 3D reconstruction of the drone environment in order to detect obstacles; and (2) victim detection and tracking. Videos of the drones implementing these functionalities in action can be found at the project website [3] .

Autonomy however introduces stringent requirements as to the safety and security of the underlying architecture and mechanisms. Safety assurances aim to prevent further casualties due to failures of the drone system. Security assurances aim to prevent that, beyond humanitarian organizations in charge of relief operations, attackers would be able to abuse drones, notably in conflict areas, for e.g., espionage, unwanted disclosure and publication of pictures of victims in the newspapers, or deliberate obstruction to relief operations. This paper discusses the use of modeling and verification techniques in order to assess such properties for the missions described above.

We have defined the SysML-Sec [4] environment for handling both safety and security issues during the development of an embedded system. SysML-Sec has been successfully applied in the scope of the definition of a connected automotive architecture featuring safety critical subsystems and able to withstand network attacks. SysML-Sec supports the following methodological phases with UML/SysML diagrams: requirements elicitation, attack capture, hardware/software partitioning and software design. SysML-Sec is supported by the free and open-source toolkit named TTool [5]. Apart from diagram modeling, TTool enables the formal verification of safety and performance-

related properties from partitioning diagrams, and the formal verification of safety and security properties from design diagrams.

The paper discusses how SysML-Sec/TTool can be efficiently used for formally verifying the safety and security of an autonomous drone mission and flight. More specifically, we consider the architecture of the system that we have used in the scope of the drone4u project. A Parrot platform is used to capture videos of its surroundings. Those videos are transmitted by the UAV to a remote computer, which autonomously controls the drone according to its mission. We have modeled the UAV embedded system (properly speaking the drone capturing the videos, connecting to a WIFI network, and applying remote orders), as well as the communication itself, and the processing performed by the remote control computer.

Thanks to the SysML-Sec models, we can evaluate different architectures, notably the one that we have just described, but also an architecture in which all the processing is performed aboard the drone. For both architectures, we can study the performance of the system, for instance the number of images that can be processed per second. Also, we can express security properties in terms of confidentiality and authenticity, and prove their satisfiability with respect to the considered architectures.

The final paper will include diagrams of the different methodological phases (e.g., requirements, attack modeling, partitioning, design), and the results of the formal proofs for different architectural configurations. Finally, we will also explain how the same SysML-Sec environment may be used to assess the mission risk.

References

[1] L. Apvrille, T. Tanzi, and J.-L. Dugelay, "Autonomous drones for assisting rescue services within the context of natural disasters," in General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI, Aug 2014, pp. 1–4.

[2] T. Tanzi, L. Apvrille, J.-L. Dugelay, and Y. Roudier, "UAVs for humanitarian missions: Autonomy and reliability," in Global Humanitarian Technology Conference (GHTC), 2014 IEEE, Oct 2014, pp. 271–278.

[3] T. Tanzi, L. Apvrille, J.-L. Dugelay, "Drone4u project," http://drone4u.telecom-paristech.fr.

[4] L. Apvrille and Y. Roudier, "SysML-Sec: A SysML environment for the design and development of secure embedded systems," in APCOSEC 2013, Yokohama, Japan, Aug. 2013.

[5] L. Apvrille, "TTool website," in http://ttool.telecom-paristech.fr/, 2013.