How can model driven development approaches improve the certification process for UAS?

Nicolas LARRIEU

ENAC / Telecom Laboratory

7 av Edouard Belin 31055 TOULOUSE CEDEX 4 France

Contact email: Nicolas.Larrieu@Enac.Fr

ABSTRACT

Unmanned Aerial Systems (UAS) are currently flying in specific and segregated airspaces, separated from regular aircraft. Nevertheless, to be widely used in the future, UAS will need to be deployed in the same airspace as regular aircraft. However, their unmanned and automated features make this goal very difficult to certify. Indeed, it is necessary to validate the different parts of the UAS (operating system, communication system or even payload depending on their application) in order to be compliant with the whole airspace certification process. This paper deals with new model driven development approaches that are inherited from existing aerospace and aeronautical systems and that could be useful for the certification of UAS design. In this paper we demonstrate how a model driven design can improve UAS system robustness. A case study is introduced and focuses on the main advantages for UAS design environment: modularity and reusability.

Categories and Subject Descriptors

Certification, integration, micro- and mini- UAS, networked swarms, security, UAS applications, UAS communications, UAS testbeds

1. Introduction

This paper deals with new Model Driven Development (MDD) approaches that are inherited from existing aerospace and aeronautical system developments and that could be useful for the certification of UAS (Unmanned Aerial System) design. The principle of MDD is to build the initial system with high level models and to take advantages of auto generation process to be able to produce software and byte codes of the final system directly from the high level modeling. This approach helps engineers not to be dependent of a specific development language (mainly C or ADA language in this field) and allows also verification, validation and certification of the final product at an early stage of the development life cycle.

This paper investigates how a model driven design can improve UAS system robustness. Indeed, UAS are currently flying in specific and segregated airspaces, separated from regular aircraft. Thus, to be widely used in the future, UAS will need to be deployed in the same airspace as regular aircraft. Nevertheless, their unmanned and automated features make this goal very difficult to certify. This is why it is necessary to verify, validate and certify the different parts of the UAS (operating system, communication system or even payload depending on their application) in order to be compliant with the whole airspace certification process.

Thus, this paper wants to demonstrate how MDD approaches which are extensively used in aerospace and aeronautical fields at this time can improve the development of complex systems in the UAS field. To do so, a specific MDD methodology is introduced and instantiated in the context of the French project SUANET (Secure Uav Ad hoc NETwork) which aims at developing a secure communication ad hoc network for UAV swarms.

The outline of this paper is the following. In the next section, we introduce the two main documents DO 178 C and DO 331 which were released by RTCA[1] in 2012. They provide guidance on model driven approaches for design and certification of aeronautical systems. In section 3, we focus on a specific UAS issue: how to integrate UAV swarms into the traditional airspace? By starting with this issue, we explain how UAS systems could take advantage to consider aeronautical model driven approaches in their own design cycle. We highlight a specific French research project (SUANET: Secure Uav Ad hoc NETwork) whose objectives are to integrate a UAV swarm into the French civilian airspace and we outline how we can benefit from model driven approaches for such a task. In the fourth section, we present a specific case study considered in the SUANET project where we have started to apply aeronautical model driven approaches. We introduce the main advantages for this practical use case on two aspects: modularity and reusability.

[1] RTCA: Radio Technical Commission for Aeronautics

PaperCept Inc

Finally, section 5 concludes this article and presents the different future contributions we are planning during the next months of the SUANET project.

2. Overview of model driven development approaches

Traditional software engineering has been using model driven development tools for a long time. Unified Modeling Language (UML) [1] is one of the most effective methodologies to conduct traditional software design. Nevertheless, when we consider more specific engineering fields such as aeronautical or aerospace system design this tool cannot be used “off the shelf”. The main problem with traditional UML-based software design is the lack of certification considerations in the tool chain used to generate the final system software. It may not be a problem for classical applications such as Web services [2], tools for engineering [3], or game applications[2]; but it represents a huge problem when you consider critical applications such as an aircraft or a satellite. In this context, it is necessary to take into account the certification of the final software, and to integrate the tool chain used for design in the standardization process followed in such a specific field.

2.1 Aeronautical software design

In this paper, we consider the certification process followed by the aeronautical industry when new embedded software has to be designed for a specific purpose. Several standards have to be met. We will focus on the two most closely related to our topic: DO 178 C [4] and DO 331 [5].

2.1.1 DO 178 C: Software Considerations in Airborne Systems and Equipment Certification

In 2012, RTCA released the third version of the DO 178 document which gives guidance for airborne system certification. This new version takes into account the latest developments in terms of model driven approaches for software system design. The emphasis is placed on model driven approaches that are able to automatically generate software code by taking as inputs only high level models which represent the different features and behaviors of the final system. It introduces in particular the possibility to validate such a system by using formal methods in order to reduce the amount of testing for the validation of the final product. This is a major improvement for aeronautical engineers which significantly changes the way aeronautical systems are designed and produced.

2.1.2 DO 331: Model-Based Development and Verification

In addition to DO 178 C, another standardization document, DO 331, deals with tools and methods used to automatically generate software and to validate these high level models in line with initial system specifications. In this document, advanced verification methodologies are introduced. RTCA recommends the use of three different technologies to ease the verification process: model checking, formal proofs and code assertions [6]. These three techniques have been used for a long time in different engineering fields and are mature enough to be introduced into complex environments such as aeronautical certification and validation processes.

2.1.3 Model driven approaches for UAS design

These new techniques to model and certify an aeronautical system can be integrated into the global process for UAS design. This integration will have two main advantages for engineering. Firstly, the UAS design step will be facilitated thanks to modularity and reusability of model driven design approaches. Secondly, the certification of the global UAS system will be able to take advantage from formal validation techniques dedicated to work with inputs such as high level models. In the next sections of this article, we highlight how a model driven approach first developed for aeronautical design purposes can be extended to the UAS field. We will outline the effectiveness of such an approach and we will illustrate it through a case study: the SUANET project.

3. Integration into the civilian airspace: a complex topic

In this section, we focus on a specific UAS issue: how to integrate UAS into the traditional airspace? UAS integration into the civilian airspace can be considered from different points of view (path planning [7], communication compatibly[3], certification, etc). We will focus solely on the certification issue in this article. It means that if a company wants to deploy a UAV swarm in the civilian airspace it needs to justify that its system is fully compliant with the certification process of any aircraft in the same civilian airspace.

Indeed, this task can be complex, given that an aircraft has a lot of certification documents to produce before being cleared to fly in the civilian airspace. Thus, if a traditional testing

[2] See http://interfacedesignforgames.blogspot.fr/2010/04/week-10-uml.html for details.

[3] See http://www.rockwellcollins.com/Landing/Convergence/-UAS-in-civil-airspace.aspx for details.

Paper Inc

approach is followed for UAS certification it can result in a huge amount of testing being required. This is why model driven approaches have a lot to contribute for certification processes of UAS, by enabling designers to avoid some of the traditional testing steps by using, for instance, formal methods for validation.

3.1 Taking advantage of aeronautical model driven approaches

Different proposals have been made for the certification of complex aeronautical systems. UAS ought to take advantage of the numerous research projects that have been conducted in this area by both public and private companies.

Different specific issues have been considered in the literature. For instance, [8] have introduced model-driven development to enhance command and control capabilities of an aircraft. [9] have been conducting model-driven development for IMA (Integrated Modular Avionics). [10] have considered the consequences of model-driven development for the whole product line process of an aircraft. However, these examples are always dedicated to one specific issue of the aircraft development. We can cite [11] which discusses a global model driven process for aerospace systems, but we cannot find in the literature a similar approach dedicated to the aeronautical field.

This is why we would like to cite [12] where we have introduced a new model driven methodology for fast prototyping of generic aeronautical systems. We have illustrated this methodology in the development of a new embedded router for future aeronautical communications [13].

By taking advantage of previous research contributions in the aeronautical field which have already shown their capabilities, we believe it is possible to accelerate the UAS certification process.

Thus, we have chosen, in the next sub section to describe a specific French project (SUANET: Secure UAV ad hoc network). Its objectives are to integrate a UAV swarm into the French civilian airspace by considering mature and advanced model driven design approaches.

3.2 SUANET project objectives

In this project, started in September 2013, and planned to last for 36 months, we are planning to study the possibility of transferring model driven technologies from traditional aeronautical areas to UAS. The objective is to increase the confidence we will have in the final UAS and to accelerate the certification process with the French Civil Aviation Administration (DGAC[4]). In this project, ENAC (the French Civil Aviation University) has joined with a French company DELAIR TECH located in Toulouse. DELAIR TECH[5] is specialized in the design of UAVs with a dedicated payload. Each customer can choose a specific application to deploy inside the UAV. Different examples of UAV applications have already been developed such as surveillance, communication networks and aerial photography.

Given that different applications can be investigated with such a UAS; we chose to illustrate specifically how a swarm of UAVs can improve video surveillance of geographic areas affected by natural disasters (for instance fire, storm, typhoon, etc.). Thus, in the SUANET project, we will design a complete communication architecture for the whole UAV swarm and the ground station control. We will also investigate the interconnection with external networks such as the national security network. This connection with external networks and the requirement of communication between the different UAVs of the swarm imply that we will have to focus our research on new secure communication solutions. These solutions would need to be light enough to be integrated on a mini-UAV but robust enough to avoid any malicious behaviors from the environment.

3.2.1 Video surveillance application

Figure 1 describes this video surveillance scenario where different UAVs communicate with each other depending on their position in the area. For instance, DT2 acts as a communication relay if DT1 and DT3 cannot directly communicate. The different monitoring data is exchanged with the ground station which collects this data and can transfer some of it to the external network for collaborative purposes.

3.2.2 Mini-UAV characteristics

The miniaturization feature of DELAIR TECH's UAVs (DT-18 UAV) is an important characteristic to take into account in the development of the final solution. Their small size must be taken into account when designing the system in terms of CPU, energy consumption or means of communication.

Figure 2(a) illustrates the legacy communication antenna used between the ground control station and DT1 of our video surveillance scenario to remotely pilot the UAV swarm and receive the observed data. Figure 2(b) describes the HMI

[4] DGAC: « Direction Générale de l'Aviation Civile » which is equivalent to FAA (Federal Aviation Administration) or EASA (European Aviation Safety Agency) but at a French scale.

[5] DELAIR TECH company website: *www.**delair-tech**.com/*

provided by DELAIR TECH to plan missions of the UAV swarm.

Table 1 describes the main technical characteristics of DT-18 UAVs[6].

Table 1: DT-18 UAV characteristics

Characteristic	Value
Model	DT-18
MTOW	< 2kg
Payload	250g
Range	100km
Cruise speed	50km/h
Wind	up to 45km/h
Photo	5 to 10cm resolution
Video	20cm resolution
Infra-red video	30cm resolution
Real-time transmission	up to 15km. Extension to 100km
Autopilot	Delair-Tech technology
Onboard computer	payload and communication control, 1GHz
Field deployment	< 10 minutes
Price	15 k€

In the next section, we will demonstrate how a model driven approach initially developed for aeronautical purposes can be instantiated for the UAS environment. We will give specific examples on how it can be applied in the SUANET project. Modularity and reusability of the UAS will be highlighted and technical solutions to provide security and means of communication within a swarm of UAVs will be investigated.

4. Case study: transition of a model driven design from the aeronautic field to the UAS environment

4.1 Model driven methodology principles

The previous methodology we designed to develop generic systems for aeronautical purposes (see [12] for details) is built on the following three steps:

1. **Partitioning step:** this is the architecture design where each (or a set of) feature(s) of the global system is (are) grouped into the same functional partition;
2. **Design step:** for each functional partition we produce one high level model which represents the behavior of the different agents and processes acting together;
3. **Transformation step:** based on an auto-generator of software code we are able to transform the high level model into software code in C language.

Step 1 has to be manually written, the most efficient approach is to produce a Software Requirement Specification (SRS) file detailing the different behaviors of the final application.

For step 2, we use Mathworks Simulink and Stateflow tools[7] to model the different partitions. Their graphical features help the designer to fast generate high level behaviors. An example of high level models is described in Figure 3. In this step, we can already work on the certification process because it is possible to use formal validation techniques directly on the high level models. This material can be also used by the development team as part of the final certification documents it needs to produce to the regulator (Federal Aviation Administration or European Aviation Safety Agency in our context). For instance, Stateflow is able to detect any dead state in the high level model which will correspond to a dead code in a traditional design approach. The main difference is in the rapidity which with we are able to detect this dead state: with a high level model tool it is automatically analyzed whereas in a traditional approach only the developer is able to detect it by manually reviewing the final code.

In step 3, we used GeneAuto [14], an Open Source generator to generate the final C language software taking as input high level models and providing source codes in C language. This step can also improve the certification process given that, if your auto-generator is certified, you validate that the final source code is compliant with the features modeled at step 2, and then you do not need to manually realize extensive testing on the final source code. Please note that GeneAuto is certifiable but not certified at this time. However, several commercial tools exist in the industry to convert high level Simulink or Stateflow models to certified embedded code. However, they are all proprietary, expensive and with narrow freedom for the end users, this is why we did not select them in the SUANET project.

[6] Additional information can be found at http://www.delair-tech.com/wp-content/uploads/2012/10/DT-18-Datasheet-EN.pdf.

[7] See www.mathworks.com for details.

PaperCept Inc

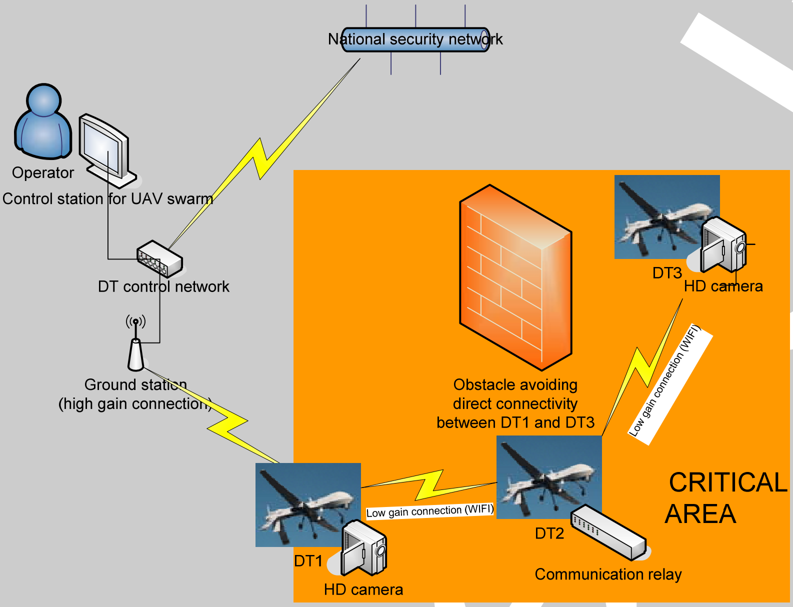

Figure 1: video surveillance use case in the SUANET project

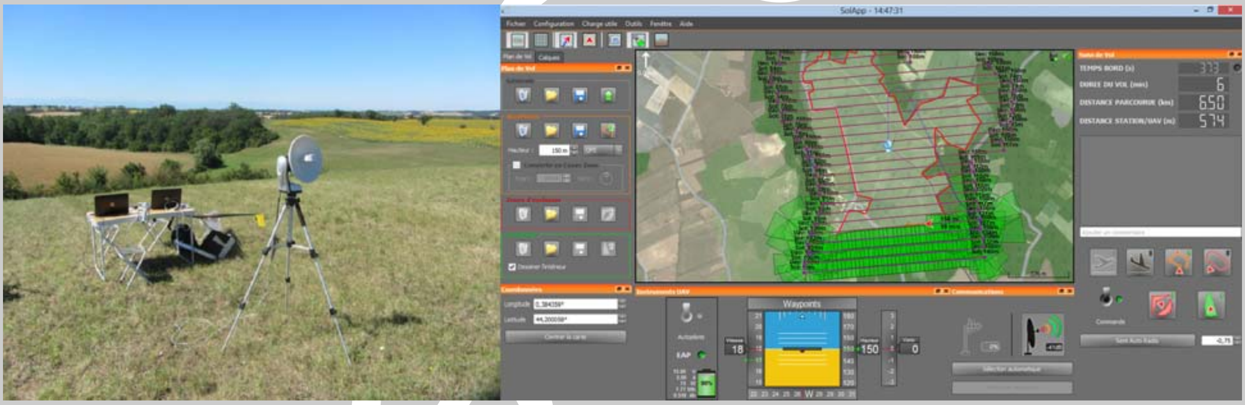

Figure 2: (a) ground control station to remotely pilot the UAV swarm (b) HMI to plan UAV missions (Pictures copyright DELAIR TECH Company, 2013)

After step 3, please note that there is still important work to do in order to generate a final binary compliant with the UAS hardware where you intent to deploy your system designed with this methodology. This part of the process is outside the scope of our UAS certification issue and will not be described in this article (details are provided in [12] for the aeronautical field).

The next part of this section is dedicated to illustrating through a specific case study how model driven design can accelerate the development of new systems. For instance, we are going to reuse in the SUANET project some specific parts of a previous design (mainly communication and security features) and thus to take advantage of modularity and reusability of our model driven design approach for the specific field of UAS.

4.2 Modularity

In previous research, based on our model driven design approach, we produced a full compliant secure and safe router for aeronautical communications [13]. This device is able to exchange different types of information between the ground and the aircraft (point-to-point communications) in one or several safe and secure communication tunnels.

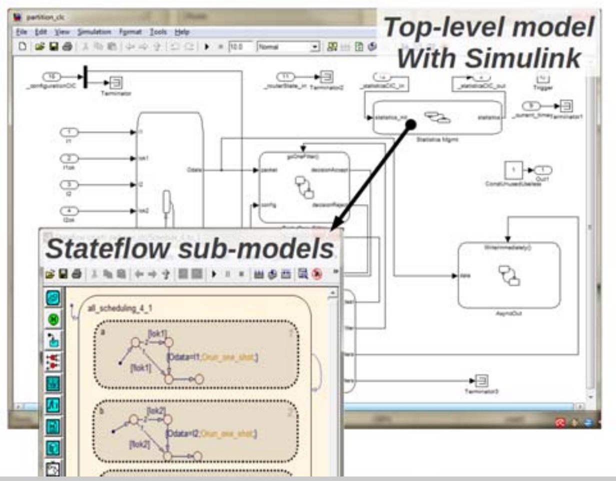

Figure 3: examples of high level models (step 2)

In the SUANET project, the communication paradigm is not point-to-point communications because each UAV which belongs to the swarm can be either one communication relay or an end-device (with surveillance capability in this case) as mentioned in Figure 1. The communication paradigm used to make the UAV swarm communicate is thus a Mobile Ad Hoc Network (MANET) [15] paradigm. Even if the routing function is different in the two paradigms, the aeronautical modular design detailed in Figure 4 will facilitate the final UAS system design. Indeed, specific models such as Piface (i.e. the level 2 network interface) will be derived to be compliant with the new link layer technology (mainly IEEE 802.11 “WIFI” [16] in our video surveillance use case). For the Pfr partition dedicated to filtering, routing and QoS (Quality of Service), a new routing function will be designed to be compliant with the ad hoc feature of the network, but the whole framework of network layer will be maintained. Finally, the global design will be eased due to the global modularity of our model driven design approach. The certification process will also be accelerated given that different parts of the models have already been validated in our previous research.

4.3 Reusability

Model driven design approaches can also enhance software reusability. Indeed, a specific part of the new architecture designed for SUANET will be directly derived from the original aeronautical one: the Pse partition dedicated to enforce the security for the different data exchanged between senders and receivers. In section 3.2, we pointed out how security inside the UAV swarm and between the swarm and the additional networks (control and national security agents for instance) is an important issue. To do so, specific communication functions (such as authentication, integrity or confidentiality) have to be designed. The initial aeronautical Pse partition contains these different features and consequently, can be transfer directly from the original aeronautical design to this specific UAS system. For the same reason as in section 4.2, the certification process will be facilitated given that the different functions and modules of Pse partition have already been validated.

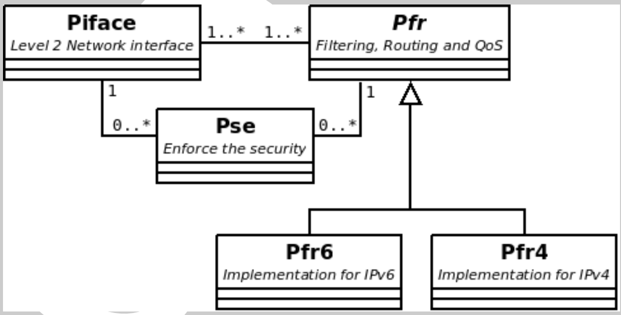

Figure 4: examples of a modular design

5. Conclusion and future work

In this paper, we have addressed the following question: “how can model driven development approaches improve the certification process for UAS?”. As a first step, we introduced model driven development approaches that can be inherited from airspace and aeronautical systems and that could be reused in UAS design. As a second step, we demonstrated how a model driven design can improve UAS system robustness. To illustrate our thesis, a case study, derived from the SUANET research project, was introduced and focused on the main advantages for UAS environments: modularity and reusability.

The SUANET project has recently started (September 2013) and we still have several tasks to undertake:

1. **Enhance design:** even if model driven approaches enable reusability of previous design, there are sill some specific parts of the design that we need to produce, for instance the dedicated functions to implement MANET routing;
2. **Development of the final UAS:** there is a significant part of the development still to conduct. Indeed, the different partitions identified in section 4 will be implemented on real systems. SABRE Lite[8] is the final architecture identified in the project and some technical adjustments

[8] See http://boundarydevices.com/products/sabre-lite-imx6-sbc/ for details about implementation features.

will be necessary to produce a final binary from the auto generated source files in C language;

3. **UAS testbed:** an exciting part of the SUANET project deals with testing the software solution we proposed in the real environment. We will be able to test our communication and security solutions for UAS with 3 different mini-UAVs from DELAIR TECH company. These tests are planned in the second half of 2014 and they will give a strong validation environment for our methodology and related technical solution.

In a more prospective research work, additional functionalities could be investigated for future UAV swarms. For instance, communications between two different groups of UAV swarms sharing the same mission but not the same goal. We can imagine reconfiguration features of the different groups in terms of number, functionality or positioning. These reconfiguration features require future communication and security components. We need to develop them to enhance the level of service of the final UAS we plan to propose.

6. Références

[1] Grady Booch, Ivar Jacobson & James Rumbaugh, *"OMG Unified Modeling Language Specification"*, Version 1.3 First Edition: March 2000. Retrieved 12 August 2008.

[2] Randy Miller, *"Designing Web Services Using UML"*, 2003 BorCon Conference, Agile Processes Workshop.

[3] Terry Bahill, Jesse Daniels, *"Using objected-oriented and UML tools for hardware design: A case study"*, Wiley Periodicals, Issue Systems Engineering, Volume 6, Issue 1, pages 28–48, 2003.

[4] [DO 178 C] SC-205 DO-178C. *"Software considerations in airbone systems and equipment certification"*. Radio Technical Commission for Aeronautics, 12/13/2011

[5] [DO 331] SC-205 DO-331. *"Model-based development and verification supplement to DO-178C and DO-278A"*. Radio Technical Commission for Aeronautics, 12/13/2011

[6] Gabriella Gigante, Domenico Pascarella, *"Formal Methods in Avionic Software Certification: The DO-178C Perspective"*, Leveraging Applications of Formal Methods, Verification and Validation. Applications and Case Studies, Lecture Notes in Computer Science Volume 7610, 2012, pp 205-215.

[7] Timothy M. Ravich, *"The integration of unmanned aerial vehicles into the national airspace"*, University of Miami School of Law, Free Book, http://web.law.und.edu/lawreview/issues/web_assets/pdf/85-3/85NDLR597.pdf, 2010.

[8] Robert W. Jacobs, *"Model-Driven Development of Command and Control Capabilities For Joint and Coalition Warfare"*, Command and Control Research and Technology Symposium, June 15-17, 2004.

[9] A. Horváth, D. Varró, T. Schoofs, *"Model-driven development of ARINC 653 configuration tables"*, IEEE/AIAA 29th Digital Avionics Systems Conference (DASC), 2010.

[10] H. Dubois, V. Ibanez, C. Lopez, J. Machrouh, N. Meledo, P. Mouy, A. Silva, *"The product line engineering approach in a model-driven process"*, ERTS 2012.

[11] V. Wiels, R. Delmas, D. Doose, P.-L. Garoche, J. Cazin, G. Durrieu, *"Formal Verification of Critical Aerospace Software"*, AerospaceLab Journal, Issue 4 - May 2012

[12] A. Varet, N. Larrieu, *"New methodology to develop certified safe and secure aeronautical software – an embedded router case study"*, 30th digital avionics systems conference (DASC), Seattle, Washington, USA, 2011.

[13] A. Varet, N. Larrieu, *"Design and Development of an embedded aeronautical router with security capabilities"*, Integrated Communication, Navigation and Surveillance Conference (ICNS), Washington DC, Colombia, USA, 2012.

[14] Nassima Izerrouken, Xavier Thirioux, Marc Pantel, Martin Strecker, *"Design and Development of an embedded aeronautical, Certifying an Automated Code Generator Using Formal Tools: Preliminary Experiments in the GeneAuto Project"*, European Congress on Embedded Real-Time Software (ERTS), 2010, Toulouse.

[15] C. Rajabhushanam, A. Kathirvel, *"Survey of Wireless MANET Application in Battlefield Operations"*, International Journal of Advanced Computer Sciences and Applications, 01/2011.

[16] *"IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*. (2012 revision). IEEE-SA. 5 April 2012. doi:10.1109/IEEESTD.2012.61782.