2014 International Conference on Unmanned Aircraft Systems (ICUAS)
May 27-30, 2014. Orlando, FL, USA

HAMSTER – Healthy, Mobility and Security-based Data Communication Architecture for Unmanned Aircraft Systems

Daniel Fernando Pigatto
Inst. de Ciências Mat. e de Comp. (ICMC)
Universidade de São Paulo (USP)
São Carlos, Brazil
pigatto@icmc.usp.br

Guilherme Freire Roberto
Inst. de Bioc., Letras e C. Exatas (IBILCE)
Universidade Estadual Paulista (UNESP)
São José do Rio Preto, Brazil
guilhermefroberto@gmail.com

Leandro Gonçalves
Inst. de Bioc., Letras e C. Exatas (IBILCE)
Universidade Estadual Paulista (UNESP)
São José do Rio Preto, Brazil
leandroblg@hotmail.com

Julio Fernando Rodrigues Filho
Inst. de Ciências Mat. e de Comp. (ICMC)
Universidade de São Paulo (USP)
São Carlos, Brazil
juliofrf@gmail.com

Alex Sandro Roschildt Pinto
Inst. de Bioc., Letras e C. Exatas (IBILCE)
Universidade Estadual Paulista (UNESP)
São José do Rio Preto, Brazil
arpinto@ibilce.unesp.br

Kalinka Regina Lucas Jaquie Castelo Branco
Inst. de Ciências Mat. e de Comp. (ICMC)
Universidade de São Paulo (USP)
São Carlos, Brazil
kalinka@icmc.usp.br

Abstract— **Embedded systems are computer systems that are part of a larger system providing generally monitoring and real-time control for the entire system. They provide a set of pre-defined tasks, usually dedicated to a real time application, and have special requirements. These systems are considered critical when failure events may jeopardize lives or high-value assets. Usually these systems operate with frequent information exchange between the inner parts of the vehicle or between the vehicle with ground stations or also with other vehicles. Due to the fact that they are real-time systems, this communication generally requires low latency and security mechanisms that guarantee the basic requirements of a critical scenario, such as confidentiality, integrity, authenticity and availability of communication channels. Furthermore, there is the concern about the vehicles modules/components safety (also known as "health"), which may present malfunctions, whether intentional (attempted attacks) or not, which can lead to vehicle accidents. Given this increasing need to ensure communication and operation of unmanned vehicles plus the desirable characteristic of increasing connectivity in these scenarios, this project proposes the complete specification of a data communication architecture based on safety and mobility concepts. The principal scenario of development will be the aerial, but we expect to obtain a flexible architecture which will be portable to other scenarios of unmanned vehicles, such as ground and water. The specification of the HAMSTER data communication architecture also contributes to the integration of new heterogeneous aircrafts in the airspace, once the requirements for the certification process are being considered.**

Keywords — data communication architecture; unmanned systems; UAS; UAV; security; mobility; HAMSTER

I. INTRODUCTION

In the past few years, the development of Unmanned Aircraft Systems (UAS) has increased, which allowed the existence of many different types of aircrafts. These aircrafts should be integrated into the airspace in order to operate and execute the necessary missions. For this, it is essential that communications elements meet healthy, mobility and security requirements, increasing the aircraft overall capabilities and, consequentely, allowing the aircrafts to be certified and integrated into the airspace, obbeying the specific rules determined by each country.

This proposal introduces HAMSTER, the HeAlthy, Mobility and Security based data communication archiTEctuRe. The main objective of our architecture is to help developers of unmanned aircrafts to efficiently implement communications in UAS by considering the internal and external communications. Other objectives have also been considered during the definition of the proposal.

This paper is organized as follow: Section II characterizes the Critical Embedded Systems; Section III characterizes Unmanned Aircraft Systems; Section IV specifies Communications in UAS; Section V presents the Related Works; Section V points out the objectives of this proposal; Section VI presents and characterizes the HAMSTER architecture; and Section VII finalizes with several conclusions.

II. CRITICAL EMBEDDED SYSTEMS

Embedded systems are computational devices responsible for dedicated functions that are typically embedded in wider (computational or not) systems. Barr [3] defines an embedded system as a combination of software and hardware designed to perform a specific task, or a system based on embedded microprocessor that operates as a subsystem of a bigger system. Berger [1], more focused on hardware, defines an embedded system as a processing unit, which consists of an integrated circuit attached to a printed circuit board.

In embedded systems area, some of them can be classified as critical. The avionics and automotive domains are classic examples where cost, short production cycles and dependability requirements, robustness, security, control emissions and the specific demands of each scenario influence in obtaining a final product [34]. Due to the high investment in research in this area, loss of such a product involves considerably high financial losses.

These systems are considered critical when failure events may cause loss of life or loss of high-value assets. Thus, it is common that these systems operate with frequent information exchange between the inner parts of the vehicle or from the vehicle with ground stations, or even with other vehicles. Once they are real-time systems, this communication generally requires low latency and security mechanisms that guarantee the basic requirements of a critical scenario, such as confidentiality, integrity, authenticity and availability of communication channels.

The critical embedded systems have been widely researched academically and commercially. Examples of this class of systems are unmanned vehicles, which can be of three main types: air, water and ground. The experiments presented in this article have the unmanned aerial vehicles and internal communication of sensors in an aircraft as the experimental environment. The objective is to identify possible interferences due to the density of wireless sensors communicating with a single central module and the consequent possibility of Denial of Service (DoS). The following subsections discuss UAVs and WSNs (Wireless Sensor Networks) in details.

III. UNMANNED AIRCRAFT SYSTEMS

An unmanned aerial vehicle is a driverless aircraft that is capable of flying autonomously or via a remote control. It is one of the most important examples of critical embedded systems. These systems are generally composed of: navigation sensors and microprocessors that allow the aircraft to travel by autonomously; communication systems that allow greater flexibility to change its course on-the-fly; and a fixed control station to provide more accurate control to the aircraft [35]. It can also be defined as a powered aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry lethal or nonlethal payloads [36].

UAVs usually perform a wide variety of functions, both for the military and to civilian rule, due to their maneuverability which allows them to collect information from hard to reach places, such as in case of environmental disasters. They also help with faster and financially less expensive acquisition of data if compared to common manned aircrafts.

The autonomous control system of a UAV is composed of key technologies, such as [37]: high speed processor; high precision integrated navigation system; air data system; anti-disturbance and standard data link system; take-off and landing system; environment awareness system; collision avoidance system; and payload technologies. In order to monitor these hardware devices, it is useful the distribution of wireless sensors over the aircraft, which will send real-time monitoring information to a central module. Thereby, the master module may give feedbacks to the control system on-the-fly.

An unmanned aircraft system (UAS) is typically composed by aircrafts, one or more ground control stations (GCS) and/or mission planning and control stations (MPCS), payload and communications links.In addition, many UAS include launch and recovery subsystems, transport subsystems, and other equipment for maintenance, communication subsystems, among others.

The main subsystems of a SANT and their functions are described below.

A. The control station

Normally located in the soil, but may also be suspended in the air, the control station is the control center operations and also the human-computer interface in UAS. It is also the place where, occasionally, the missions are preplanned [40, 41].

From the control station operators communicate to the UAV via communication systems in order to operate the various existing types of payload and acquire information

related to the aircraft. This information can be payload data, status of the subsystems of the UAS, location data, among others.

The control station is also responsible for communication with external systems. This type of communication can help in the acquisition of climate data and transfer data to and with other systems on a network, for example, which may be important to perform certain missions.

B. Payload

The type and performance of loads are driven by the needs of the business unit. These can range from a few types [40]:

- Relatively simple subsystems that consist of a fixed lens camera with no stabilization technology, weighing approximately 200 g;
- Video systems with a higher capacity range using lens with focal length and more zoom options, greater image stability and with pan and tilt functions, weighing around 3-4 kg;
- High power radars including their power supplies, weighing up to 1000 kg.

More sophisticated UAVs may carry a combination of different types of sensors within a payload module. The data obtained by these various sensors can be processed and integrated to provide more accurate information or information that can only be obtained with the use of more than one sensor [42]. For instance, images of a color camera, images of a thermal camera and possibly a radar system, which can be fused to obtain more complete information.

This information can be used in real time by the aircraft, sent in real time to the control station or be stored internally in the UAV for later access.

C. The air vehicle

The type and performance of the air vehicle is mostly determined by the needs of the operational mission. The most important task of the aircraft is transporting the payload of the mission to its point of application, in addition to carrying the subsystems needed to make it work [40]. These subsystems include the link of communication, stabilization apparatuses and control of the aircraft, fuel, electrical power supplies and basic structure and necessary mechanisms for the launch and recovery of aircraft.

Other determining factors in designing the configuration of the aircraft is the operational range, speed and endurance required for mission execution. From this, the amount of fuel to be loaded will also be determined. The speed requirement will determine whether to use a "lighter than air aircraft" or a fixed or rotary wing aircraft.A military monitoring mission, for example, requires a fixed wing aircraft to operate at high altitudes and high speeds, which should also have a proper takeoff runway.

D. The navigation system

For most operations with UAVs it is necessary that operators know the location of the aircraft at any time. It may also be necessary that the aircraft "knows" its own location in case of the need for an autonomous flight. This requirement may be part of a mission running or an emergency return to the control station after the occurrence of a failure in any of the systems. For this operation to be fully autonomous, i. e. without any communication between the aircraft and control station, a self-sufficient navigation equipment must be loaded on the aircraft.

In the past, this meant that the aircraft would have to load a sophisticated, complex, expensive and heavy Inertial Navigation System (INS), or a less sophisticated and cheaper INS, but with requirements of frequent position updates from the control station via communication links.Currently, with the availability of GPS systems that access position information from a network of satellites, the problem is solved. The current GPS systems are extremely lightweight, compact and relatively inexpensive, and continuously provide positioning information, which associates information with a simple INS and is able to reveal the location of an aircraft accurately.

Non autonomous operations, i. e. where communication between aircraft and control station is practically continuous or where there is risk of blockage of the GPS system, alternative means of navigation can be used. These methods include [40]:

- Radar tracking. In this case, the aircraft is equipped with a transponder which responds to a radar scanner issued by the control station, so that the position of the aircraft is found by the operators on the ground.
- Radio tracking. In this case, the behavior of the radio signal that carries data from the aircraft to the control station is monitored by determining the location of the aircraft from the time information needed for an encoded signal to be exchanged between the aircraft and the control station.
- Direct calculation. In this case, the integration of data about the speed and elapsed time of flight allow the calculation of the position of the aircraft.

E. The system launch, recovery and transportation

Some techniques of launching, rescue and recovery aircraft can be [40,41]:

- Launch. It is necessary for the aircraft that do not have an ability to takeoff/landing autonosmously or do not have access to a track surface and adequate length. It normally comprises a ramp on which the aircraft is accelerated with the aid of a trolley driven by a system of elastic rubber or compressed air to the aircraft reaches the required speed.

- Recovery. This feature is also usually necessary for aircrafts not capable of takeoff/landing autonomously. It is usually implemented in the form of a parachute, installed in the aircraft and that is fired at a suitable height above the landing zone. In addition, airbags can be used as a means of absorbing impact energy.
- Transportation. Unless the aircraft is light enough for manual transport, a transport is needed to carry the aircraft to the proper places.

F. Communication links

The main requirement for the communication system is to provide the link of data between the control station and the aircraft. The transmission medium most used is radio frequency. The tasks of the data links are generally [40, 41, 42]:

- Uplink (from the control station to the aircraft):
  - Send the flight plan to be stored in the aircraft.
  - Send commands to flight control in real time to the aircraft when necessary to pilot it remotely.
  - Send control commands and payload elements related to execution of the mission.
  - Send updated positioning information for the aircraft.
- Downlink (from the aircraft to the control station):
  - Send positioning information of the aircraft to the control station when needed.
  - Upload images and/or data generated with the execution of the mission to the control station.
  - Sending information about the status of the aircraft, such as fuel level and engine temperature.

Besides the mentioned subsystems, other subsystems usually compose a UAS [40]. Among them, the interfacing subsystem responsible for defining the protocols used and the communication interfaces between the various subsystems, the subsystem interfacing with other systems, as the name implies, defines how the SANT should communicate with other systems (for example, ground and air vehicles or satellites); support equipment subsystem that maintains reserves of supplies like batteries for replacement; and the transport subsystem, responsible for transporting all other subsystems to the place of execution of a mission.

IV. COMMUNICATIONS IN UAS

There are three main types of communications in UAS. In this work, by making reference to them, the following classifications and their abbreviations are adopted: (a) in-vehicle communication (IVC), (b) airplane-to-airplane communication (A2A), and (c) airplane-to-infrastructure communication (A2I).

Communication is one of the biggest challenges in designing systems with multiple UAVs, which is crucial for cooperation and collaboration among them. When all UAVs are directly connected to an infrastructure, such as a control station or a satellite, the communication among UAVs can be performed through this infrastructure. However, based communication infrastructure restricts the capabilities of an UAS. One solution to this problem is the adoption of ad hoc networks between UAVs. To the extent that the number of UAVs in a UAS increases, the projection of efficient network architectures emerges as a vital issue to be resolved.

Beyond the direct communication among UAVs in an UAS it is possible and very oftenly implemented a communication link with the control station, being this communication direct or mediated by a satellite [43]. In some approaches, the airplane-to-airplane communication can also be realized through infrastructure, which introduces some new problems. First, each UAV must be equipped with a more expensive and complex hardware to enable communication with the control station or satellite. Another disadvantage of this structure is the network reliability of communication. Due to changing environmental conditions, movements of aircraft and terrain relief, UAVs may have trouble maintaining communication with the infrastructure. Another problem is the restriction of range between the UAV and the control station. If a UAV is outside the coverage area of the control station, it will be disconnected. An alternative communication solution for multiple UAVs is the use of ad hoc networks among UAVs, known as FANETs (Flying ad hoc networks). While only part of the UAVs are within range of the control station or satellite, all UAVs are part of an ad hoc network, which, in turn, enables everyone to communicate with the control station by communicating with other UAVs.

FANETs can be considered as a special kind of MANET (Mobile Ad hoc Networks) and VANET (Vehicular Ad hoc Networks) [41]. However, there are some differences between FANETs and other networks:

- The degree of mobility of the nodes in FANETs is much greater than the degree of mobility in MANET or in VANET nodes. While in MANETs and VANETs the nodes move embedded in people and cars, respectively, in FANETs the nodes are embedded on an aircraft in flight.
- Due to the high mobility of nodes in FANETs, the topology changes more frequently than the network topology in MANETs or even in VANETs.

- The existing ad hoc networks existing are intended to establish peer-to-peer connections. FANETs also need peer-to-peer connections for the coordination and collaboration of UAVs. Consequently, FANETs need to support peer-to-peer communication and still manage traffic information to send them to monitoring stations.
- Typical distances among nodes of a FANET are much longer than in MANETs and VANETs [44]. Thus, the communication range in FANETs must also be greater than other networks. This fact directly impacts the radio links and employed hardware elements.
- The systems of multiple UAVs may include different types of sensors and each sensor may require different strategies for data distribution.

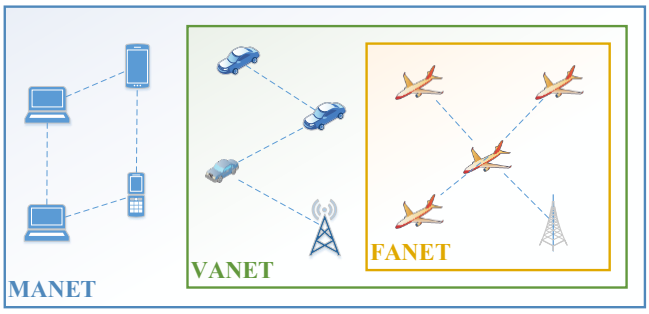

Figure 1. MANET, VANET and FANET. Adapted from [41].

Ad hoc networks are classified according to their utilization, implementation, communication and mission objectives [41]. By definition, FANET is a kind of MANET and there are many similarities between them.Furthermore, FANETs can also be classified as a subset of VANET, which, in turn, is also a type of MANET. This relationship is illustrated in Figure 1.

Considering all the existing concern with communication FANETs and considering that this is a key factor for the operation of UAVs in the airspace, this work focuses on the specification of links, technologies, protocols, mechanisms and cryptographic algorithms to be applied to A2A and A2I communications, which are directly connected to FANETs, and also the IVC communication.

V. RELATED WORKS

This section presents an overview of the use of data communication architectures in critical embedded systems as a way to facilitate the development of such systems and, in the case of unmanned aircraft, enabling their integration into the airspace. This integration relies on an adaptation of the standards set by specific organizations such as the FAA (Federal Aviation Administration) of the United States and ANAC (National Civil Aviation Agency) in Brazil. In United States, the inclusion of an aircraft to the National Airspace System (NAS) must meet a series of requirements, including issues related to Sense and Avoid (SAA), which try to "imitate" the knowledge and perception of a human pilot in relation to abnormalities with the aircraft or obstacles that may arise on the fly [1, 2].

Unmanned aerial systems are just one example of critical embedded systems. Embedded systems are computer systems that are part of a larger system generally providing monitoring and controlling in real time for the entire system [1, 4, 12, 24, 32]. They provide a set of pre-defined tasks, usually dedicated to a real time application, and have special requirements. These systems are considered critical when failure events may cause loss of life or loss of high-value assets. In some applications, such as in aviation, critical embedded systems must have low failure rates as a catastrophic failure each 10^5 to 10^9 hours of operation [31]. Examples are multicore and multiprocessor systems that are becoming common in embedded systems and further increasing software complexity [8]. Even so, they are becoming more and more common in home and professional environments to control and / or manage information. Therefore, allowing them to be easily inserted into their specific space (e.g. air space) is one of the challenges in the area.

In addition to air scenario, there are the terrestrial and aquatic scenarios, the latter divided into surface and underwater vehicles. In all of them, except for some particular characteristics of each scenario, communication and fault tolerance requirements are highly desired and therefore the communication that provides complete management of the tasks performed by such systems is one of the key factors in designing a critical embedded system .Even systems that perform tasks of gathering information and are not sensitive to real time, i.e. they do not need to send information at run time to a base station or other systems operating nearby, they have the need for proper storage of information collected within the system to prevent thefts, manipulations by malicious entities or loss of such information.

This project aims at the complete specification of a data communication architecture applicable to critical embedded systems of any kind. However, in order to guide the steps of definition and development, this project will focus on unmanned aerial vehicles, also known as UAVs. The adoption of an environment and implementation of a detailed study of your requirements will allow the architecture contemplates more specific features, always focusing on architecture components modularization for future adaptation to different application scenarios of these systems.

The reason for the choice of the air scenario is due to the fact that it is more critical than other scenarios (terrestrial and aquatic). UAVs typically reach speeds considerably

higher than those achieved by terrestrial and aquatic vehicles, which leads to the conclusion that if a solution implemented for aircraft works satisfactorily even with the influence of the speed factor in a scenario where the operations are performed at high speeds certainly the proposal will be functional and applicable to environments where speeds hit by vehicles are usually lower, which leads us to believe that few or no modifications would be required for other classes of vehicles. Certainly other factors should differentiate ground and water vehicles from aircrafts, such as the density of vehicles, which must be greater in the case of ground vehicles. However, the aim of this study should be evaluated initially on aircrafts and at the end of the project, case studies with aquatic and grund vehicles can be run as a research complement.

Although the speed factor being considered as an element impacting the final result of communication, this project should make an assessment of this and other factors in environments with and without mobility. The work presented in [23] is a performance evaluation of routing protocols for mesh clustering applications of UAVs, covering technologies aimed at the fast and secure sharing of information between vehicles and base stations and vehicles with other vehicles that make up the unmanned aerial system (UAS). The tests are performed in two ways: with the vehicles in movement and with the vehicles stationary in the air, since the UAV used in the work are quadrotors. Four mesh routing protocols are evaluated in these two scenarios. The performance of the open802.11s protocol was the best of all, followed by BATMAN Advanced, by the OLSR and, finally, by the BATMAN protocol. The first two, in conclusion reached by the authors, are best suited for applications that require the combination of several UAVs forming a squadron of aircrafts. However, these tests were run with low speed aircrafts (quadrrotors) reaching approximately 1 m/s. This project aims to design an architecture that includes aircrafts of all types and characteristics, including those that reach higher speeds to perform specific missions.

Considering the significant increase in aircrafts for applications in precision agriculture, national security (military missions), environmental monitoring and domestic, and aiming to maximize the connectivity of these aircraft, some studies have done tests using the new version of the IP protocol, IPv6 . The work [10] proposes a secure mobile-based solution using IPv6 for ground vehicles, primarily by requiring authentication for network access and then making use of the standard NEMO (Network Mobility) and a combination of IPsec/IKEv2 for safe data control and exchange.This solution applied to ground vehicles has proven to increase the connectivity and security of information transmitted, provided by IPv6 features and desirable in the applied context. However, in most cases, the speeds reached by air vehicles are higher than those achieved by ground vehicles and it would be desirable to determine whether the use of IPv6 in UAS is feasible. This project aims to adopt IPv6 in order to use the new standard suggested and its advantages over IPv4, which is in obsolescence. However, it should be reviewed as it is known that the IPv6 protocol imposes a number of safety features that make its performance be considered lower than the IPV4 [7, 15]. This is because IPv6 has treated security as one issue inherent to the protocol, which is not done by IPv4.

Also in the context of IPv6 applied to ground vehicles, the work presented in [9] evaluates the use of pseudonyms in IPv6 communication applications for ITS (Intelligent Transportation Systems), which aim to deliver entertainment on the road.The use of pseudonyms is a current approach to preserve location privacy, but the tests performed showed a degradation in performance due to frequent change of IP address. Thus, two protocols have been proposed to solve the problem. The result proved possible to achieve confidentiality and integrity, but does not provide location privacy, a desired requirement for ITS applications. Concerning the proposal of this project, the use of pseudonyms can be applied to aircraft in situations of domestic applications with small UAVs, for example, it is desirable location privacy, a factor to be contemplated in tests with lower mobility scenarios during the validation process of the proposed architecture.

The work of [27] presents an architecture that allows the addition of network devices or protocols minimizing the impact on existing software. This is a desirable feature of any architecture developed with the aim of critical embedded systems, as well as minimizing the effects on other layers can be useful in portability for vehicles of different application scenarios. However, the proposed work does not consider essential safety aspects and does not perform a check of aircraft components for anomalies that may have been caused by malfunctions or failures of the same or even arising from attacks by replacing modules modified by third parties. Attacks via GPS are already common and can be highly damaging to aircrafts using GPS receivers for location purposes [17]. The authentication of modules and received signals is one way to help reducing attacks on UAS and also is adopted as design requirement of this project.

In [33] it is possible to verify a proposed modularized hardware architecture for small UAVs, including the use of a Service Oriented Architecture to enhance the performance of the solution and facilitate communication. The use of modularity offers clear advantages in the decoupling modules and facilitating the replacement of these to accommodate different applications. Similarly, in the work [14] a modular architecture based on services is presented for small UAVs.The features are divided into distributed elements, also called services, which are interconnected by a middleware.However, none of the proposed architectures considers large UAS, which is currently desirable, since certain aircraft applications require more robustness to enable the execution of tasks that involve various operations and, in some cases, require hardware elements of larger size and/or heavier. This proposed project addresses a complete data communication architecture for UAS composed by

heterogeneous UAVs. Heterogeneity is a feature on distributed systems of all types, including real-time and critical embedded systems.

The article published in [30] details the platform software architecture known as the Berkeley UAV. It successfully demonstrates the vision-based autonomous navigation to avoid obstacles and validate concepts linked to the control to execute collaborative tasks, i.e., to form squadrons of UAVs. This is a modular architecture due to the already known advantages in developing modularized systems. However, adopting the idea of a more generic architecture that addresses heterogeneous UAS, this proposal differs from the aforementioned article as it aims to define and specify parameters, protocols, mechanisms and links focused on UAS of various types.

All papers are concerned with the modularization architectures, show different characteristics in mobility and do not worry, most of the time, about security and "health" of vehicle components. In some cases, they only address small aircrafts, which represents the exclusion of a large part of existing aircrafts and are currently employed to implement more robust missions.

Considering these circumstances, this project has the main goal to specify a data communication architecture for unmanned heterogeneous aircraft systems, with a view to increasing the mobility and flow of data exchanged between the various elements of the SANT. This architecture also pursues increased security of internal and external modules in vehicles and base stations. For this, a protocol for authentication of hardware modules is proposed and protocols such as IPv6 should be evaluated and, according to the results, adopted for the architecture. Moreover, the concept of 3-D wireless networks should be incorporated into the project as a way to increase the possibilities of exchanging information between the components of the UAS [13]. The objectives of this research will be presented in the next section and details about the architecture will be presented in the section of development.

The growing use of UAVs should cause them to become common, happening to be marketed more widely. In this scenario, the architecture proposed in this work will facilitate the development of automated systems for UAVs, allowing these vehicles to be inserted and incorporated more easily into airspace, contributing to its spread. Moreover, incorporating security can also facilitate the certification process of these UAVs with responsible agencies.

VI. OBJECTIVES

The main objective of this work is the specification and validation of a complete data communication architecture for unmanned aircrafts focusing on "health" and secure components and increased mobility in modern UAS. To achieve the main objective, some specific objectives were defined:

- Propose and specify a data communication architecture that addresses all types of communication existing in the context of modern UAS, making the specification of links, technologies, protocols, mechanisms and cryptographic algorithms to be applied;
- Propose a mechanism for expanding the safety of the aircraft through the creation of a protocol/system to examine the "health" and the authenticity of all internal and external components of the aircraft and the ground station.For this, a central security unit (CSU) is proposed and also a mechanism to assess the authenticity of the CSU is provided;
- Propose an architecture that uses 3-D wireless networks to increase the mobility of elements involved in modern UAS, facilitating, for example, rescue and military operations;
- Obtain an architecture that facilitates the integration of unmanned aircrafts into airspace, contributing to its spread;
- Expand the data communication architecture for terrestrial and aquatic vehicles, generating specific case studies;
- Obtain breakthrough results for publications in recognized events in the area.

VII. HAMSTER: HEALTHY, MOBILITY AND SECURITY-BASED DATA COMMUNICATION ARCHITECTURE

The first step to assist in the specification of a communication architecture is to identify the parts of a UAV and ground station that present critical real-time requirements, allowing appropriate approaches for each of these parts to ensure proper operation of the aircraft. Illustrated in Figure 2 is an inside view of the aircraft and the ground station with modules organized according to the need for low latency, medium latency or no real-time constraints.

From the organization presented above, the next sections discuss the proposal of this project separated into two parts: the first deals with issues of "health" of the components and the security of the communication, and the second addresses the requirement for strong mobility in UAS.

A. "Health" and security of components

This subsection is divided into two parts. The first one addresses a policy of the use of components of the aircraft and the second one addresses an authentication protocol which will also check the "health" of components.

1) Components usage policy

One of the first steps to ensure the safe operation of a vehicle and to facilitate their integration into the airspace should be the redefinition of some components usage policy.

A few parts of an aircraft receive proper care to ensure that the modules are authentic and have not been replaced or tampered with by a third party. The current policy adopted by most aircraft manufacturers uses a concept of "Accept all" which trusts in all components embedded in an aircraft. This proposal suggests the adoption of the approach "Deny All", which denies the authenticity of all mechanical components and peripherals attached to the vehicle until the opposite is proved, which can result in safer vehicles (security) against some types of attacks.

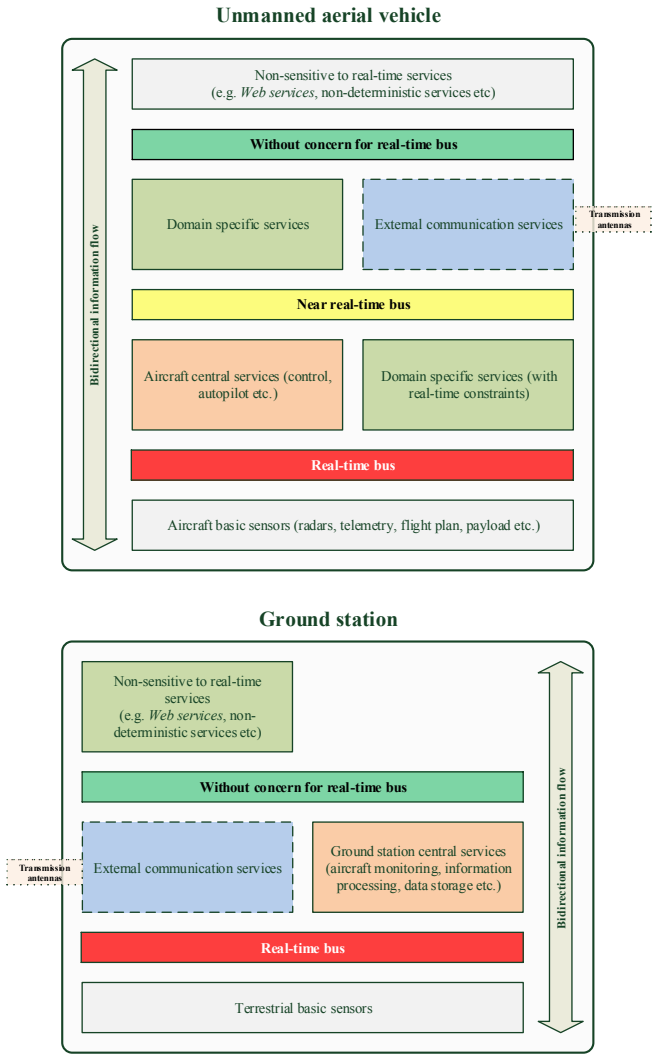

Figure 2. Parts of a basic UAV and a ground station with the buses defined according to the need for speed.

The categorization of modules is therefore crucial for this new security model to be applied to air vehicles. There are various peripheral devices and modules that comprise a UAV and each one of them requires different levels of security (safety), which leads to the necessity of a classification module according to the criticality of the function performed thereby. This proposal suggests the categorization in primary and secondary modules as illustrated in Figure 3. As it can be seen in Figure 2, the communication architecture of the UAV that is the basis for this proposal has three communication buses: real time (red) whose latency is expressed in the order of milliseconds and is focused on the essential parts of the aircraft for its safe operation (e.g. basic sensors); near real time (yellow) whose communication time is in the order of tens of milliseconds, comprising modules less critical but still sensitive to real time (e.g. communication with other vehicles, which may be a feature operant at low latencies, but is not still as critical as the autopilot, which, in situations of failures requiring abort the mission, can operate without communication with other vehicles or ground stations), and the bus without concern for time real (in green) that allows the use of services with non-deterministic times that are not essential to the operation of the basic functions of the aircraft.In the case of the ground station, the organization follows the same idea, but only with a real-time bus and another without concern for real-time, considering that the functions performed by the ground station should be limited to sending information/commands of highest criticality to the aircraft and communicating with others via Internet. The latter situation may not require real time communication channels.

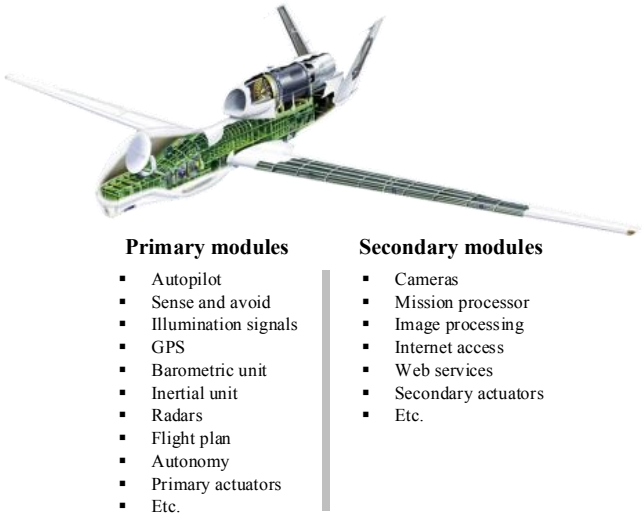

Figure 3. Example of a brief categorization of existing modules in an UAV according to the criticality of the functions performed on the aircraft.

In primary modules are those modules that are considered essential components for the aircraft to fly, to be aware of its location and be able to perform an emergency landing safely, even without the fulfillment of a mission that

could be underway, i.e. modules such as autopilot, GPS receiver, and barometric/inertial units are examples of modules classified as primary. In contrast, modules that add not essential functions to the UAVs are classified as secondary modules. When abnormal behaviors are detected in any sub-assembly of the aircraft, the operation of the primary components of the plane is not affected and the secondary module that showed the abnormal behavior is disabled. It is also blocked all packets sent by the module, since this behavior may be consist in a security attack. This implies that all primary modules are authenticated before the flight starts, otherwise the aircraft must not proceed to takeoff. However, the secondary modules do not necessarily need an authentication before takeoff.

In addition to protecting against malicious attacks still exists the possibility of identifying anomalies from the time of use of the components. With time, pressure, collisions and personal use of aircraft components, natural degradations may occur. Therefore, mechanisms that identify the existence of unusual behaviors should aid in the safety of the aircraft in general, even with a consequent abort of a mission for reasons of physical integrity of the aircraft. These concepts are strongly linked to the area of sense and avoid (SAA), which, although not part of this project, will be considered as an element to be incorporated to the architecture in the future. This enhanced security module of each aircraft assists in obtaining safer aircrafts and therefore more apt to be inserted into the airspace.

Another concept associated with the idea of authentication modules is to create user profiles. When a mission is coupled to the aircraft, it must go through an authentication process, which assigns different access permissions to the modules of the aircraft. This concept is similar to that used in modern operating systems where an administrator user can install and remove programs, for example, without restrictions, unlike a visitor user, who has access to the execution of the programs installed and is not allowed to install/uninstall new programs. In the context of UAVs, this concept adds a layer of security that allows blocking the use of certain modules on one level located below of the software layer, ensuring that specific modules are blocked from certain classes of users. This specification is intended to prevent unauthorized access. Even if there is a single effective user of UAVs, no other user (whether or not an attacker) will have privileged access to information or modules of the UAV.

The project developed by Pires [38] is the implementation of a communication protocol between a mission-oriented sensors array (MOSA).This is a plug-and-play mechanism (SSI) for coupling a payload to the rest of a system of an unmanned aircraft. It is part of the work to implement the communication protocol (SSP) and the selection/modification of hardware adapters responsible for data communication. Since MOSA is an external module to the aircraft, it is desirable to authenticate it before the mission execution. In the authentication phase, it must be associated with a particular usage profile, which, as already mentioned, is a policy of using the resources available in the UAV. This process of authentication and allocation of profile guarantees the safety of the aircraft component against attacks made by MOSA, for example, but is applicable to any other component or device that has been coupled to the aircraft.

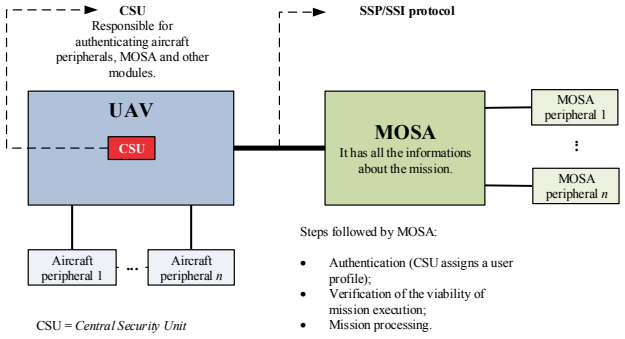

Figure 4. Example of integration between the work published in [22] and the proposed communication architecture.

In the illustration of Figure 4 it is possible to see the steps performed after coupling MOSA to the aircraft and the authentication step through CSU (Central Security Unit), which will have its operation detailed in the next section. It is important to note that MOSA specific peripherals, which will be embedded in the aircraft as part of the payload, are not authenticated because they are directly connected to the MOSA and are not aware for the aircraft.

This access policy assigned to each user must make use of cryptographic algorithms suitable for embedded or real-time sensitive environments, which is closely related to the work done by the owner of this proposal during the Masters course, which consisted on a performance evaluation of cryptographic algorithms running on embedded prototype, which aimed at establishing which algorithms are best suited for such an environment and identify the overhead generated by them in communication and, consequently, in the overall system performance [18, 19, 20, 21, 25, 26, 28, 29].

2) Protocol structure

To protect the aircraft from attacks coming from malicious components connected to it, this proposal suggests some steps that should ensure that all components act as expected. For this, some procedures are proposed and detailed below.

When we plan to implement more stringent security policies of the components of a vehicle, it is necessary to ensure that they are all authentic, so when one of them fails or presents an abnormal behavior, others will be prevented from sending information to it.Furthermore, these policies must be applicable even on the fly, considering that climate change, for example, may affect the behavior of the

components. Plus, each component must contribute to the general aircraft safety increase. In order to apply these methods and requirements, it is assumed that at the system startup or after the aircraft hardware changes, the CSU module remains in a safe state. It will still be responsible for storing a table of public keys of all vehicle components, operating similarly to a Certification Authority (CA), which has the goal of making sure that a public key belongs to an entity (person, router or network) [11]. Each module (or component) will store a hash table of the keys to see if it is corrupted.

During boot of the vehicle, a phase of mutual authentication should occur with the CSU. It checks the database credentials of all modules, the criticality of them, and even if there is some kind of access restriction. There is also the possibility to decide whether a module should be initialized or not during the verification stage. The following steps will be authentication and exchange of encrypted messages to establish a secure channel for the exchange of information between modules and CSU.

After this handshake, three situations are expected:

- The module that is trying to authenticate and CSU have not been tampered with;
- The module has been tampered with and therefore has not been authenticated:
    - If it is a module of primary type, the aircraft should not take off;
    - If it is a module of secondary type, communication with the same is interrupted and a notification can be sent to a control station.
- The module that is trying to authenticate realizes that CSU is not authentic, and must notify the other components about it.

From the point of view of communication security, an ideal situation would be if all modules could authenticate with others. However, this method would cause an overload in the system, since the increase of modules in the aircraft would cause an exponential increase in the number of exchanged messages. To solve this problem there exist the e-voting protocols, such as [6]. In the case of the CSU module not being authentic, protocols such as those presented in [5] can be used. This model can be further expanded according to the needs of the aircraft, including a negotiation mediated by the CSU to create a secure channel of communication between modules. A graphical representation of processes performed during the authentication module with CSU can be seen in Figure 5.

Besides abandoning IPv4 protocol to IPv6 to take place which itself is safer, issues that may compromise the safety of an aircraft (or vehicles in general) should be considered and addressed in the proposal of a communication architecture for its validity and contribution be effective. The proposal presented in this project aims to include certain steps to verify the authenticity of the existing modules in a UAV and allow to extend features and functionality as needed by the scenario and the application, which consists of an innovative proposal.

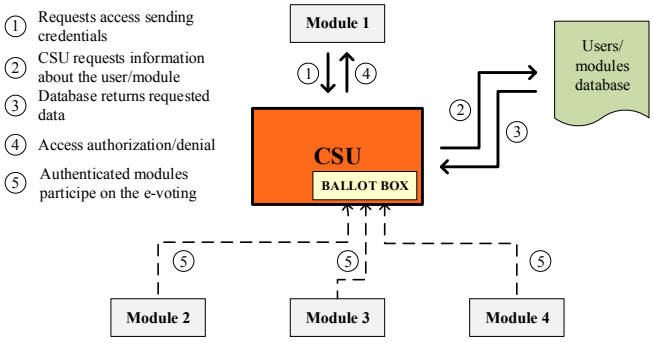

Figure 5. Phase of authentication of modules with CSU.

B. *Mobility*

One of the main characteristics for the proposed architecture regarding to mobility is creating a distributed architecture, i. e., that addresses the various elements (aircraft, ground stations, support vehicles, terrestrial sensor networks etc.) that make up a UAS and the establishment of all types of possible communication in this type of scenario. The concept of 3-D wireless networks should be considered in defining the architecture. These networks consider merging the digital world with the physical world allowing the exchange of information among individuals and objects with data services. For example, in military scenario modern 3-D wireless networks can be used to connect aircraft, troops and fleets allowing greater exchange of data between them and ensuring the security of sensitive information that may be exchanged. This new paradigm introduced by 3-D wireless networks meets the needs of scenarios where UAVs are applied [13].

Another topic to be evaluated within the context of this proposal is the use of IPv6, which aims to increase the innate mobility [7]. It is known that the increase of devices connected to networks today was one of the reasons that boosted the use of IPv6. In the context of avionics there is an increase of works that adopt the concept of ubiquity, because all the elements involved in a modern UAS often have a specific address and are considered communicating elements when carrying out missions. The adoption of IPv6 is a tendency in all areas, especially those that can benefit from the most basic advantages of the new protocol, as is the case with this proposal in terms of mobility and security.

Silva [39] is implementing a control system for a VTOL (Vertical Take-Off and Landing) focused on aid to minimize drift when applying pesticides in crops, or in reducing the

scattering of products outside the area of pre-defined application. The autonomous VTOL must follow a manned aircraft collecting information about the drift through specific sensors, sending commands to course correction and product application to the manned aircraft. The stems can vary according to the wind, temperature, and other conditions, so it is desirable to use a smaller plane to track the applicator product and assist in applying correction to obtain a most effective, economical and less drift end result. The illustration in Figure 6 shows the different types of communication existing in the scenario proposed by Silva. This project will provide a complete specification of these three types of communication, which shows the importance of the interaction between the work in development to the research group and for the field. The development of HAMSTER will be divided into segments wich will be dealing with a concern of the proposal. These segments will be: i) IVC communication; ii) A2A communication; iii) A2I communication; iv) security (which also includes security and healthy); and v) mobility. This segmentation will allow a parallel development of the architecture, despite the fact that every part may influence the development of other parts. At the end, all the segments will be fused and the HAMSTER architecture will be obtained and validated using, for instance, the OMNeT++ Network Simulation Framework.

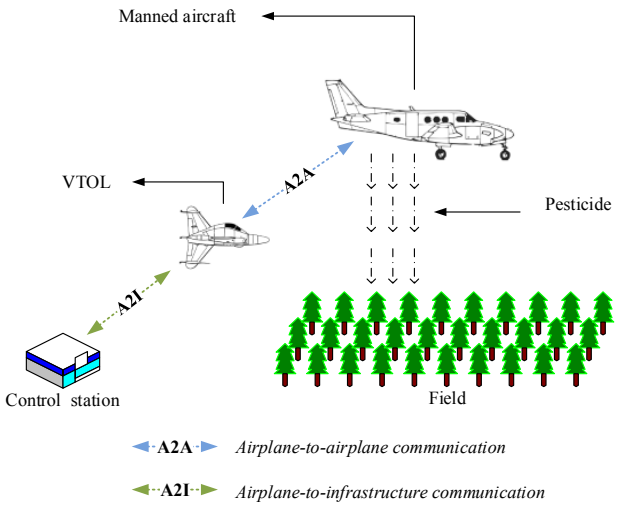

Figure 2. Types of communication existing in the scenario proposed by Silva [39].

VIII. CONCLUSIONS

The main result expected with this project is to obtain the complete specification of a data communication architecture that considers aspects of security and mobility, two requirements increasingly desirable in the context of critical embedded systems. The focus is on the development of unmanned aerial vehicles, but it is expected to obtain an architecture also applicable to other scenarios, such as unmanned ground and water vehicles. Thus, we aim to facilitate the certification process of these vehicles to become able to operate in the airspace, on highways or in the aquatic environment and, consequently, being more commercially exploited.

IX. ACKNOWLEDGEMENTS

The authors acknowledge the support granted by CAPES, CNPq and FAPESP (processes number 2012/16171-6 and 2012/08498-5).

REFERENCES

[1] BERGER, A. S. Embedded systems design: An introduction to processes, tools, and techniques. Lawrence, KS, USA: CMP Books, 2002.

[2] Curtis W. Heisey, Adam G. Hendrickson, Barbara J. Chludzinski, Rodney E. Cole, Mark Ford, Larry Herbek, Magnus Ljungberg, Zakir Magdum, D. Marquis, Alexander Mezhirov. A Reference Software Architecture to Support Unmanned Aircraft Integration in the National Airspace System. In Journal of Intelligent & Robotic Systems, 69:41–55, August, 2012.

[3] Barr M (1999) Programming embedded systems in C and C++. O'Reilly Series. O'Reilly.

[4] DOUGLASS, B. P. Real time uml: Advances in the uml for real-time systems (3rd edition). Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 2004.

[5] Hiroaki Kikuchi, Junji Nakazato. Modint: A Compact Modular Arithmetic Java Class Library for Cellular Phones, and its Application to Secure Electronic Voting. Security and Protection in Information Processing Systems, p. 177-192, 2004.

[6] Horng-Twu Liaw, A secure electronic voting protocol for general elections, Computers & Security, Volume 23, Issue 2, March 2004, Pages 107-119, ISSN 0167-4048.

[7] IPv6.br | Portal sobre IPv6 do NIC.br. Disponível em: <http://ipv6.br/> Acesso em: 16 Fev 2013.

[8] J. Kouloheris. Future of System Level Design. In panel discussion of First IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, October, 2003.

[9] Jong-Hyouk Lee, J M Bonnin, Fernando Pereniguez Garcia, Antonio F Skarmeta Gomez. Use of Pseudonyms in IPv6 ITS Communication: Performance Degradation and Exposure New Identity with Security Protocols, International Workshop on IPv6-Based Vehicular Networks, IEEE Intelligent Vehicles Symposium 2012 (IV'2012), June 2012.

[10] Jose Santa. Continuous IPv6 Communications in a Vehicular Networking Stack for Current and Future ITS Services. In 2012 IEEE Intelligent Vehicles Symposium Workshops, 2012.

[11] KUROSE, J. F.; ROSS , K. W. Computer networking: A top-down approach. 5 ed. Addison Wesley, 2009.

[12] LAVAGNO, L.; MARTIN, G.; SELIC, B. Uml for real: Design of embedded real-time systems. Norwell, MA, USA: Kluwer Academic Publishers, 2003.

[13] Li, P.; Pan, M.; Fang, Y. Capacity Bounds of Three-Dimensional Wireless Ad Hoc Networks, Networking, IEEE/ACM Transactions on, vol.20, no.4, pp.1304-1315, Aug. 2012.

[14] López, Juan; Royo Chic, Pablo; Barrado, Cristina; Pastor Llorens, Enric. Modular Avionics for Seamless Reconfigurable UAS Missions. In: Digital Avionics Systems Conference, 2008. DASC 2008. IEEE/AIAA 27th. IEEE, 2008. p. 1. A. 3-1-1. A. 3-10.

[15] Narayan, S.; Kolahi, S.S.; Sunarto, Y.; Nguyen, D.; Mani, P. Performance comparison of IPv4 and IPv6 on various windows operating systems, Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on , vol., no., pp.663-668, 24-27 Dec. 2008.

[16] National Institute of Standards and Technologies. 4D/RCS: Reference Model Architecture for Unmanned Vehicle Systems Version 2.0. August, 2002.

[17] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, New York, NY, USA, 75-86. 2011.

[18] PIGATTO, Daniel Fernando. Segurança em sistemas embarcados críticos - utilização de criptografia para comunicação segura. 2012. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) - Instituto de Ciências Matemáticas e de Computação, University of São Paulo, São Carlos, 2012. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-06092012-154011/>.

[19] PIGATTO, D. F. ; SILVA, N. B. F. ; BRANCO, K. R. L. J. C. . Avaliação e Comparação de Desempenho entre Algoritmos de Criptografia de Curva Elíptica com El-Gamal baseados nas Bibliotecas MIRACL e RELIC. In: Escola Regional de Redes de Computadores (ERRC), 2011, São Leopoldo, RS. Escola Regional de Redes de Computadores (ERRC). Porto Alegre, RS: Sociedade Brasileira de Computação - SBC, 2011. v. 9. p. 113-116.

[20] PIGATTO, D. F. ; SILVA, N. B. F. ; BRANCO, K. R. L. J. C. . Performance Evaluation and Comparison of Algorithms for Elliptic Curve Cryptography with El-Gamal based on MIRACL and RELIC Libraries. Journal of Applied Computing Research (JACR), v. 1, p. 95-103, 2011.

[21] PIGATTO, D. F. ; SILVA, N. B. F. ; SIKANSI, F. E. G. ; BRANCO, K. R. L. J. C. . Aplicação de Criptografia e Assinatura Digital para Prover Comunicação Segura em Veículos Terrestres Não Tripulados. In: II Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2011), 2011, São José dos Campos. II Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2011), 2011. v. 1. p. 1-4.

[22] PIRES, R. M. ; RODRIGUES, D. ; BRANCO, K. R. L. J. C. . MOSA - Mission Oriented Sensor Arrays - Uma Proposta. In: XXXVII Latin-American Informatics Conference (CLEI XXXVII), 2011. Anais do XXXVII Latin-American Informatics Conference (CLEI XXXVII), 2011. p. 1-10.

[23] Pojda, J.; Wolff, A.; Sbeiti, M.; Wietfeld, C. Performance analysis of mesh routing protocols for UAV swarming applications, Wireless Communication Systems (ISWCS), 2011 8th International Symposium on , vol., no., pp.317-321, 6-9 Nov. 2011.

[24] RAVI, S.; RAGHUNATHAN, A.; KOCHER, P.; HATTANGADY, S. Security in embedded systems: Design challenges. ACM Transactions on Embedded Computing Systems, v. 3, n. 3, p. 461–491, 2004.

[25] RODRIGUES, D. ; ESTRELLA, J. C. ; PIGATTO, D. F. ; BRANCO, K. R. L. J. C. . Performance Evaluation of Security Techniques in Web Services. In: 13th International Conference on Information Integration and Web-based Applications & Services (iiWAS), 2011, Ho Chi Minh City, Vietnam. 13th International Conference on Information Integration and Web-based Applications & Services (iiWAS), 2011. v. 13. p. 270-277.

[26] SALLA, G. C. ; SARTIN, A. M. ; PIGATTO, D. F. ; BRANCO, K. R. L. J. C. . Performance Evaluation of Security Communication in Critical Embedded Systems. In: CBSEC (Brazilian Conference on Critical Embedded Systems), 2012, Campinas, SP. II Brazilian Conference on Critical Embedded Systems, 2012. v. 1. p. 54-57.

[27] Sang-Hun Lee; Sanghyun Han; Hyun-Wook Jin. A Configurable, Extensible Implementation of Inter-Partition Communication for Integrated Modular Avionics, Embedded and Real-Time Computing Systems and Applications (RTCSA), 2012 IEEE 18th International Conference on , vol., no., pp.453-458, 19-22 Aug. 2012.

[28] SCHOABA, V. ; SIKANSI, F. E. G. ; PIGATTO, D. F. ; BRANCO, K. R. L. J. C.; BRANCO, L. C. . Digital Signature for Mobile Devices: A New Implementation and Evaluation. International Journal of Future Generation Communication and Networking, v. 4, p. 23-36, 2011.

[29] SCHOABA, V. ; SIKANSI, F. E. G. ; PIGATTO, D. F. ; BRANCO, K. R. L. J. C.; BRANCO, L. C. . DISIMOD Digital Signature for Mobile Devices. In: International Conference on Convergence and Hybrid Information Technology (ICHIT 2010), 2010, Daejeon. International Conference on Convergence and Hybrid Information Technology, 2010. v. 1. p. 1-8.

[30] Tisdale, J.; Ryan, A.; Zennaro, M.; Xiao Xiao; Caveney, D.; Rathinam, S.; Hedrick, J.K.; Sengupta, R.; , "The software architecture of the Berkeley UAV Platform," Computer Aided Control System Design, 2006 IEEE International Conference on Control Applications, 2006 IEEE International Symposium on Intelligent Control, 2006 IEEE , vol., no., pp.1420-1425, 4-6 Oct. 2006.

[31] TRINDADE, O.; BRAGA, R. T. V.; NERIS, L. O.; BRANCO, K. R. L. J. C. Uma metodologia para desenvolvimento de sistemas embarcados críticos com vistas a certificação. In: SBAI '09: Anais do IX Simpósio Brasileiro de Automação Inteligente, 2009, p. 1–6.

[32] WOLF, M. Computers as components: Principles of embedded computing system design. Burlington, MA, USA: Morgan Kaufmann Publishers, 2012.

[33] Zhicheng Deng; Chuanbao Ma; Ming Zhu. A reconfigurable flight control system architecture for Small Unmanned Aerial Vehicles, Systems Conference (SysCon), 2012 IEEE International , vol., no., pp.1-4, 19-22, March, 2012.

[34] Margaria T, Steffen B, editors (2010) Leveraging Applications of Formal Methods, Verication, and Validation, volume 6415 of Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-16558-0.

[35] Nonami K (2010) Autonomous Flying Robots: Unmanned Aerial Vehicles and Micro Aerial Vehicles. Springer, 2{7 pp.

[36] Office of the Secretary of Defense (2005). Unmanned Aircraft Systems Roadmap 2005-2030. URL: http://www.fas.org/irp/program/collect/uav roadmap2005.pdf.

[37] Chen H, Wang Xm, Li Y (2009) A Survey of Autonomous Control for UAV. In: 2009 International Conference on Artificial Intelligence and Computational Intelligence. IEEE, volume 2, pp. 267{271. doi:10.1109/AICI.2009.147.

[38] Pires, R. de M., Rodrigues, D., Branco, K. R. L. J. C., & Trindade, O. (2008). Unmanned Aircraft Systems: Federal Actions Needed to Ensure, Safety and Expand Their Potential Uses Within the National Airspace System. In XXXVII Conferencia Latinoamericana de Informática - CLEI.

[39] SILVA, Natássya B. F.; BRANCO, Kalinka R. L. J. C. "A new concept of VTOL as fixed-wing". ICUAS'13 - The 2013 International Conference on Unmanned Aircraft Systems.

[40] AUSTIN, R. Unmanned Aircraft Systems: UAVS Design, Development and Deployment. Aerospace Series. Wiley, 2011.

[41] FAHLSTROM, P.; GLEASON, T. Introduction to UAV Systems. Aerospace Series. Wiley, 2012.

[42] VALAVANIS, K. P.; OH, P. Y.; PIEGL, L. A. Unmanned Aircraft Systems: International Symposium On Unmanned Aerial Vehicles, UAV, 08. Mathematics and Statistics. Springer, 2008.

[43] FREW, E. W.; BROWN, T. X. Networking Issues for Small Unmanned Aircraft Systems. Journal of Intelligent and Robotic Systems, v. 54, n. 1-3, p. 21–37, 2008.

[44] CLAPPER, J.; YOUNG, J.; CARTWRIGHT, J.; GRIMES, J. Unmanned Systems Roadmap 2007–2032. Relatório Técnico, Department of Defense, 2007.