# Design and practical deployment of a network centric remotely piloted aircraft system

Ivan Vidal[1], Francisco Valera[1], Miguel A. Díaz[2], Marcelo Bagnulo[1]

[1] *University Carlos III of Madrid, Av. Universidad, 30, 28911, Leganés (Madrid), Spain*
[2] *IMDEA Networks Institute. Avda. del Mar Mediterráneo, 22. 28918 Madrid, Spain*

***Abstract*—** Remotely piloted aircrafts systems (RPAS) are winning more are more relevance during the last decade since more applications are being enabled by lighter planes with increasing autonomy, higher ceilings and more powerful transmission technologies. The integration of the RPAS as part of the network centric warfare would be a very important milestone to be achieved because of the huge amount of information and capabilities that all these aircrafts can incorporate to the global scheme. This integration is easier for hand held (short range) RPAS since their communications are typically based on digital transmission (like WiFi or WiMAX) but it may not be so obvious for bigger RPAS (long range like tactical or medium/high altitude systems) because their line of sight (LOS) communications are frequently based on analog transmissions. This implies an indirect integration to the network centric warfare by means of the ground control station (satellite communications, when available, may suffer a notorious delay for certain applications). This article presents a recent practical experience, including flight test campaigns, deploying an all-IP communication architecture into one of the most relevant Spanish tactical RPAS, the SIVA, used by both the Spanish Army and the Spanish Airforce during the last ten years. This deployment enables for a cost effective integration of this RPAS (and its natural successor, the MILANO, a medium altitude RPAS) into the network centric warfare by means of direct TCP/IP transmissions over a long range digital LOS channel combined with satellite communications for beyond LOS operations. The proposed design includes network-level security over the radio interfaces, automatic data-link selection, support of remote video terminals and access connectivity towards external IPv6 networks.

Keywords: Remotely Piloted Aircraft System (RPAS), network centric integration, TCP/IP communications

## I. INTRODUCTION

Remotely piloted aircraft systems (RPAS) basically comprises a number of unmanned aircrafts that carry payloads, a ground control station (GCS) that allows the operators to control the system, a communication system to send commands to the planes (flight tele-commands, commands to a video camera, etc.) and retrieve data (telemetry that includes the payload), and supplementary equipment for different purposes (transportation, video terminals, recovery infrastructure, etc.).

The relevance of this type of systems has been increasing along the last two decades due to their huge amount of applications (see [1]). These include both the civil world (farming, photography, coastward, power lines inspection, disaster control, road traffic, wildlife research, pollution control, etc.) and the military world (reconnaissance, surveillance, battlefield management, target designation, artillery adjustment, damage assessment, rescue point marking, etc.).

However far beyond the possibilities as standalone systems, their most impressive capabilities will only be shown when these RPAS are fully integrated within a network centric (netcentric) environment and their payload (including visible images, infrared, radar, audio, chemical or biological sensing, meteorological information, etc.) can be globally shared between the authorized entities (and in the opposite direction, it would also be possible to provide flight commands to the plane from virtually anywhere). This fact has also been sufficiently motivated in the literature (see [2] for instance).

This article describes the practical experience (the results of the two year project called DRONE[1]) enabling one of the most relevant Spanish RPAS to the netcentric warfare. Although the system

[1] The DRONE project has been granted by the Spanish Ministry of Defense:
http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detalleiniciativa.aspx?iniciativaID=74

described in this article is flexible enough so as to be deployed in very different RPAS it has been initially designed in order to be installed into this mentioned RPAS called SIVA (Air Surveillance System [4]) developed by the Spanish INTA (National Institute for Aerospace Technology, [3]) that depends on the Spanish Ministry of Defense.

The SIVA is a tactical system intended for civil and military use, mainly designed for real-time observation missions. The whole system includes several aerial vehicles (see aircraft characteristics on Table 1), a GCS (integrated into a NATO II shelter), a ground launch, recovery and maintenance equipment and finally a remote video terminal (RVT) used for field operations (more information and pictures available in [4]).

The SIVA has been used since 2006 by the 63rd Field Artillery Regiment of the Spanish Army for different missions and exercises, including target tracking, surveillance, disaster evaluation, etc. In addition it is also being used by the Spanish Airforce in the RPA Pilot School since 2012 [5] and has participated in different civil exercises like fire extinction.

The aircraft is equipped with several visible and infrared electro-optical sensors, mounted on a giro-stabilized platform. The video signal together with the rest of telemetry information are transmitted both to the GCS and to the RVT. However it is only possible to send flight commands from the GCS (no upstream flows are allowed from the RVT for security reasons).

Although the experience on the communication system presented in this article has been tested on real flights on the SIVA RPAS it has in fact been designed for the next generation RPAS that is currently under development by the INTA. It is a medium altitude (MALE) RPAS called MILANO [6] which is expected to have the first test flights in 2015.

The main objective of the whole solution is to enable cost effective TCP/IP communications on top of a long range (100-150Km) digital LOS radio channel. TCP/IP is typically used in small hand held (short range) RPAS since their communications are based on digital transmission (WiFi, WiMAX, Bluetooth, LTE, etc.). However, for tactical RPAS like the SIVA or MALEs like the MILANO, with an expected LOS between 20 and 150Km it is not so common to have an active digital radio channel (and the solutions for short range based on WiFi for example, cannot be used in these long range systems). The Spanish tactical RPAS deployed in Afghanistan by the Spanish Army, the PASI[2] (RPAS searcher Mk. II and III from Israel), are based on an analogue LOS transmission (the same as the SIVA until the DRONE project).

In addition, it has been required to enable fine-grained security policies into the system so as to be able to have a flexible configuration for the different data flows and to include IPv6 support into the GCS in order to be able to open the system to the native IPv6 available in the Spanish military network.

The rest of the article is organized as follows. The second section introduces the general framework of the deployment, presenting the requirements imposed to the RPAS architecture so that it can be properly integrated into a netcentric scenario. Section three describes the most relevant components of the IP communication architecture that enables the mentioned integration. The last sections include details about the practical development and the validation field campaigns.

---

[2] PASI: http://www.ejercito.mde.es/materiales/otros/UAV.html

## II. FUNCTIONAL REQUIREMENTS FOR THE IP COMMUNICATION SYSTEM

Figure 1 shows the most general communication use case with the different elements that are required to be supported by the communication system. As it has been mentioned in the introduction the solution has been designed and tested in the framework of the Spanish Ministry of Defense project DRONE (together with the INTA and Erzia Technologies S.L.) whose main objective was the deployment of a TCP/IP oriented communication architecture for the future MILANO RPAS. This system is currently under development and both the MILANO GCS and the LOS solution have been tested on flight campaigns using the SIVA to demonstrate the netcentric capabilities of the RPAS.

In order to make this possible, it was required as part of the project the migration of the currently available radio PCM communication system existing in the SIVA to a new digital modulation based system (band S for video and data transmission and UHF for flight instructions), enabling new LOS communications capable of supporting IP data packets.

The most relevant requirements imposed by the MILANO RPAS from the INTA to the IP communication architecture can also be deduced from this Figure 1:

- The communication architecture must be aware of the following elements
    - One or several aircrafts.
    - One or several GCS.
    - Dual communication channel per aircraft (two data paths), one of them for LOS communications (band S for video and data transmission around 4 Mbps and UHF for flight instructions with a low bitrate) and the other one on band Ku for satellite communications (around 1Mbps). A data-link selection mechanism should be provided.
    - One or several RVTs capable of receiving the LOS signal in the operation field.
- For redundancy purposes, two versions of the payload (at different rates) must be sent simultaneously from the RPA equipment: a first version through the LOS data link, incorporating high quality video from the aircraft camera and a redundant lower-rate version that is forwarded to the same destination using the satellite data-link. It is the responsibility of the operator working in the GCS to choose the telemetry to visualize. In the opposite direction the LOS data-link will always be preferred when available (the tele-commands will not be sent using both data-links).
- Cooperative flight is not required for two or more of these tactical or MALE aircrafts due to the type of mission they typically accomplish, but the system must be ready to support multiple LOS communications for the common situation of having a plane ready to take-off and another one ready to land.
- The whole system must have an external IPv6 connection to the Spanish military defense network. This connection enables the inclusion of the video and the remotely sensed information (the payload) into the netcentric architecture. Once the RPAS participates in the netcentric warfare model, it can also consume information coming from external sources (other sensors, command and control information, etc.), so that benefits are mutual.
- Due to the multiple possible payload consumers (with possible different authorizations for different sensors, or video, infrared, etc.) the system must be capable of defining fine-grained security policies. All the communication should be protected, including aircraft, GCS and RVT (and external payload consumers or flight operators when available).

## III. IP COMMUNICATION SYSTEM DESIGN

This section describes the architecture and functionalities of the TCP/IP communication system that has been designed for the MILANO.

### *A. Architectural design*

Our system illustrated in Figure 1, supports the real-time exchange of data traffic between endpoints in the GCS and a number of RPAs. Each MILANO RPA can deploy a number of sensors, such as a synthetic-aperture radar, a charge-coupled device camera, a forward looking infrared camera and electronic warfare equipment. These sensors are connected to a Data Acquisition Unit (DAU), which processes the information received from these devices and sends it towards a control workstation in the GCS. The control workstation provides a graphical interface that allows monitoring the real-time data received from the RPA (i.e., telemetry). This equipment can also be configured to redistribute this information to any appropriate equipment in the GCS if required (or to any external device). Additionally, the control workstation can be used to command the RPA, generating data traffic (i.e., tele-command) towards the appropriate elements in the aircraft system, i.e., the camera and the aerial vehicle control module.

The MILANO RPA communicates with the GCS by means of a LOS data-link. Additionally, it incorporates a satellite data link, which allows maintaining data communications in the presence of connectivity failures in the LOS data link. These data links are made available in the RPAS by means of specific subsystems (i.e., the LOS subsystem and the satellite subsystem in Figure 1), which are not part of the design of the TCP/IP communication system presented in this paper. However, we want to emphasize that our system incorporates a management mechanism that enables automatic switching between the available data channels depending on a set of policies that can be independently defined for each RPA. Additionally, the communication system also supports the deployment of a number of remote video terminals. These are modular video and data systems that enable the reception of the telemetry information by mobile units located within the LOS coverage area.

The communication system has been organized in a set of different IP subnets. Although this approach may raise the cost of the final solution, as it requires the usage of router equipment in the GCS and the RPA, and increases complexity in terms of configuration and management with respect to a solution based on layer-2 switches, it introduces significant advantages. First, it isolates the traffic exchanged within the GCS from the traffic that is internal to the RPA, hence limiting the traffic transmitted via the radio channel. Second, it enables the deployment of network-layer security mechanisms, to protect GCS-RPA communications transparently to end systems and applications. This solution enhances the regular data-link encryption if available and in any case enforces the netcentric model supporting direct end-to-end encryption from the RPA to any payload consumer. Third, it facilitates the implementation of mechanisms for automatic data-link selection, taking into account the different communication technologies available at the RPAS (e.g. LOS and SATCOM). Finally, this approach provides a flexible design that allows evolving each subnet independently (e.g. to introduce new equipment, technologies and services in the GCS and RPAS), without affecting devices and applications operating in other subnets.

As commented in section II, an important design requirement to enable netcentric operations was to enable data communications between the RPAS and external IPv6 networks belonging to the Spanish Ministry of Defense. On the other hand, the TCP/IP communication system must support legacy equipment that is already available for MILANO that only supports IPv4. To accommodate both

requirements, the design incorporates stateless NAT64 [7] translation functionalities in the GCS router, which will provide the boundary between the RPAS network and external IPv6 networks.

### *B. Network level security*

The architecture of communication system designed for MILANO includes security support at the IP layer, i.e., IP security (IPsec), to protect data communications between the RPA and the GCS. The definition of IPsec includes a number of specifications, although the base architecture is described in [8]. The main advantages of using this technology in the communication scenario addressed in this paper can be summarized as follows:

- IPsec security is implemented at the network layer (either in conjunction with IPv4 and IPv6), hence it is transparent to endpoint applications at the RPA and the GCS, which do not need to be updated.
- It is a comprehensive security solution, providing authentication, confidentiality, integrity and anti-replay.
- It is a flexible solution, which allows deploying security at different granularity levels, as it is required, protecting host-to-host communications or all the traffic exchanged between two network locations. In addition, it supports the use of different security protocols and algorithms.

According to the architectural design illustrated in the previous subsection, all the data traffic exchanged between an aircraft system and the GCS traverses their corresponding IP routers, i.e., the RPA router and the GCS router. Taking this into account, the security solution that has been designed for the TCP/IP communication system, consists of deploying a set of protected communication tunnels between the RPA router and the GCS router. Each communication tunnel will be implemented by means of IPsec in tunnel mode, using the *encapsulating security payload* (ESP) protocol [9], which enables confidentiality, integrity, data origin authentication and anti-replay features. These IPsec tunnels allow protecting all the data traffic exchanged between the GCS and the RPA, transparently to any legacy or new endpoint applications or equipment (e.g. SAU, aircraft camera or GCS workstations) which do not require software or hardware updates. In section IV the overhead introduced by IPsec will be measured in the flight campaign.

Figure 2 illustrates the security solution that has been considered for the communication system of MILANO RPAS. As it can be observed from the figure, telemetry is protected by means of an IPsec tunnel established between the RPA router and the GCS router via the LOS data link. Additionally, according to the system requirements described in section II, the design includes another IPsec tunnel to protect the redundant telemetry information that is transmitted at a lower rate through the satellite data link. On the other hand, the approaches to support RVT equipment and to protect data traffic originating at the GCS and terminating at the RPA, present certain particularities that need special consideration, and will be covered in subsequent subsections.

### *C. Support Remote Video Terminals*

The support of Remote Video Terminals requires enabling the reception and processing of telemetry by mobile units within the LOS coverage of the RPA. In this respect, a candidate option that was considered to support the one-to-many communication introduced by the use of RVTs (or many-to-many in case of simultaneous operation of several RPA), was to use multicast technologies at the network level to deliver data traffic from each RPA to the GCS and RVTs.

However, this approach was discarded in the final design because, although [8] describes the use of IPsec for unicast and multicast traffic, classical IPsec security associations provide point-to-point protection, and the security provided by the cryptographic algorithms of IPsec is not general enough to be applicable to one-to-many and many-to-many security associations, as in the case of multicast (see [10]). Although extensions to IPsec have been defined by the IETF for multicast traffic[3], in our design we decided to implement a simple approach based on unicast and classical IPsec security associations, aiming at facilitating a practical deployment that avoids the introduction of additional or complex multicast-related mechanisms, and taking into account that the use of RVT equipment may not be required in every mission.

The integration of the RVT into the security solution presented in this paper is depicted in Figure 2. In the communication system presented in this paper we use a unicast scheme to support the delivery of telemetry from the RPA to the GCS. To guarantee that a RVT, within LOS coverage of the RPA, can process the data traffic originating at the aircraft system, we simply clone in the RVT equipment the IP addressing assigned to the GCS. Additionally, it will be necessary to provide the RVT with the cryptographic keys that are required to execute IPsec security procedures on the data traffic received from the RPA. In our solution, the configuration parameters corresponding to the different IPsec tunnels are dynamically generated during the pre-flight phase, and are offloaded to the RVT equipment (if any is to be used during the mission). By configuring the RVT equipment with the same IP addressing and IPsec parameters that are available in the GCS, the RVT can gain access to the telemetry information transmitted from the RPA, providing that it is within the radio coverage of the LOS data link.

Finally, we want to mention that in the current version of the TCP/IP communication system, cryptographic keys are changed before every mission, but not during the flight. Our future work will address the analysis of alternatives to support automatic key expiration and renewal, to cope with those cases where the flight duration encourages limiting the amount of information that is exposed to potential attackers encrypted with the same keys.

### *D. Data-link selection*

The design of the TCP/IP communication system presented in this paper incorporates a mechanism that enables automatic data-link selection (LOS or satellite) for the delivery of IP traffic, based on a set of policies that can be independently defined for each aircraft system. This mechanism could be used to independently govern data-link selection both for tele-command and telemetry traffic.

However, to honor the requirements described in section II, our design explicitly deactivates the execution of this mechanism for data traffic transmitted from the RPA to the GCS (i.e., telemetry), restricting its usage to the traffic delivered from the CGS to the RPA (i.e., tele-command). The reason for this is that, according to the specified design requirements, the DAU transmits two simultaneous versions of the telemetry information to the GCS, one through the LOS data-link and another through the SATCOM data-link.

On the contrary, data-link selection for data traffic originating at the GCS and terminated at the RPA is performed by the automatic management mechanism supported by our system. In our design, the quality of each data-link available in the RPA for incoming traffic is continuously monitored. In this respect, several metrics can be used, such as the strength of the received signal (i.e., the automatic gain control or AGC), packet loss or link delays. This information is collected by a management entity

[3] IETF Multicast Security (msec) working Group (now concluded): http://www.ietf.org/wg/concluded/msec.html

running at the RPA router, the central component of the TCP/IP architecture in the RPA. Taking into account this information, and according to a set of preconfigured policies that may differ for each RPA, the management entity may decide that another data-link should be used to deliver tele-command traffic to the RPA. In this case, the management entity contacts a management agent running at the GCS router to trigger a data-link switching procedure. The management agent enforces the decision taken by the management entity, configuring the new data-link for tele-command. In addition, our design allows an operator, working in the control workstation of the GCS, to override decisions instructed by the management entity, and enforce, during the flight, the use of any of the available data-links for tele-command traffic.

Figure 2 illustrates the security scheme used by the TCP/IP communication system to protect the delivery of tele-command information. As this information can only be transmitted through one of the available data links (LOS or SATCOM), and data-link selection is automatically governed by the management agent running at the GCS router, the proposed solution utilizes a single IPsec tunnel between the GCS and the RPA. This way, packets originating at the GCS and terminating at the RPA are encapsulated by the GCS router and forwarded through the tunnel towards the RPA router. The management process in the GCS router changes the forwarding table of the router, to configure the next hop in the IPsec tunnel towards the RPA router, either via the LOS data-link or the satellite data link. This way, the management process can enforce the usage of the selected data-link at the GCS router.

## IV. Implementation and Practical Deployment

This section covers the details corresponding to the implementation and practical deployment of the TCP/IP communication system presented in the previous section. This system has been developed using specific hardware and software platforms that are described next.

The RPA router has been built using a rugged PC/104 system, with an Intel Core 2 Duo 1.86 GHz processor, 2 GB memory and 4 GB flash disk. The system includes 2 GbE ports, allowing connecting the LOS and satellite subsystems, and mounts a PCIe/104 Ethernet switch with 4 GbE ports, which can be used to connect the different IP compliant components available at the RPA (the number of available ports can be increased by stacking additional PCIe/104 Ethernet switches as necessary). The GCS router has been deployed using a barebone computer, with an AMD Athlon II X2 3 GHz processor, 8 GB memory, 500 GB hard disk and 3 GbE ports, which allow connecting the LOS and satellite subsystems in the GCS. The GCS router provides a data-link to external IPv6 network, and implements stateless NAT64 functionalities Tayga[4]. Both the RPA and GCS routers deploy an operating system Debian GNU/Linux 6.0.6 i686. IPsec security was enabled in both routers using the Debian package *ipsec-tools* 0.7.3[5], which was used to configure the communication tunnels depicted in Figure 2. A prototype of the RVT system was implemented using a laptop with an Intel Core 2 Duo 2.4 GHz processor and 2GB memory. This laptop deploys the same operating system as the RPA and GCS routers and includes the support of IPsec. It also includes a system of virtual machines VirtualBox[6], which has been used to execute a virtualized version of the control workstation that is installed in the GCS. This way, telemetry can be processed and visualized by a RVT user.

The management processes that provide automatic data-link selection (see section III.D) have been implemented using Java 1.6.0_18. Although our design can support this functionality both for tele-command and telemetry data traffic, the design requirements presented in section II for the MILANO

[4] Tayga, a stateless NAT64 implementation for Linux: http://www.litech.org/tayga/
[5] IPsec utilities for Linux, package ipsec-tools, http://packages.debian.org/squeeze/ipsec-tools
[6] Oracle VM VirtualBox, https://www.virtualbox.org

RPAS restrict the use of automatic data-link selection to tele-command traffic. Therefore, our implementation deploys a management entity in the RPA router and a management agent in the GCS router.

In the current implementation, the management entity monitors the quality of the LOS data-link in the RPA by continuously checking the AGC level, which is obtained from the LOS subsystem. To avoid oscillations in data-link selection, a hysteresis function applied to the AGC values governs the decision process. If the average AGC falls below a predefined threshold, the management entity triggers a change to the satellite data-link; this change is undone in case that the quality of the LOS data-link is recovered. Changes are requested to the management agent running at the GCS router, which enforces the decisions instructed by the management entity if they are not overridden by the operator.

The implementation of the TCP/IP communication system was integrated into the SIVA. Several ground tests were scheduled to verify the appropriate operation of the communication system to support data traffic exchange between the INTA applications running at the RPA and the GCS. This traffic, in the case of SIVA mainly includes telemetry originated by the DAU, and tele-command sent towards the aircraft camera and the control module, and it is all real-time traffic over UDP. Ground tests also allowed us to verify the security procedures, the correct execution of the RVT, the automatic data-link selection mechanism and the external connectivity with IPv6 networks. It is important to emphasize that, although the SIVA RPAS does not include a satellite link, we validated the automatic data-link selection mechanism by introducing artificial attenuation in the LOS link and checking the appropriate execution of the management processes at the RPA router and the GCS router.

Finally, to verify the operation of the SIVA RPAS with the new TCP/IP communication system during real flights, several campaigns were conducted, being the last one by the end of 2013, in the military base *Conde de Gazola* (Leon, Spain), which belongs to the Spanish Army. Figure 3 shows the original mission planning that was uploaded to the SIVA RPA. As it can be observed from this planning, the RPA should circumnavigate the military base a number of times following a square trajectory, and then should move away to a different flight area. However, we want to mention here that, due to NOTAM (Notice to Airmen) constraints, the mission planning was modified in-flight and the trajectory was limited to waypoint 13$^{th}$, where the RPA was instructed to return back to the military base for landing.

Figure 4 shows the throughput of the telemetry information received by the GCS router, during a period of the flight that covers the aircraft landing. The continuous line represents the throughput of the telemetry information transmitted via the LOS data link, which is protected by means of IPsec. On the other hand, the dotted line below this one reflects the traffic load corresponding to the same information after decryption at the GCS router. The average throughput of the IPsec protected telemetry during the flight was 1.174 Mbps, and the overhead introduced by IPsec security was around 7.7%, representing an affordable cost. Eventual falls on the telemetry throughput shown in the figure correspond to short periods of loss coverage in the LOS data-link. However, we want to emphasize that the TCP/IP communication system, designed and implemented in this work, successfully supported the data traffic exchange between the GCS and RPA while the LOS data-link was active, and that, in any case, these short eventual losses of LOS coverage did not prevent the appropriate operation of the RPA.

## V. Conclusion

In this article, we present the design of a TCP/IP communication system that enables the integration of the future MILANO RPAS, an aircraft system under development by the Spanish INTA, to the

network centric warfare. The proposed design supports the data exchange between a GCS and a number of RPAS, providing at the same time advanced functionalities, such as network-level security over the radio interfaces, automatic data-link selection, support of remote video terminals and access connectivity towards external IPv6 networks. The TCP/IP communication system has been implemented using existing hardware and software platforms, available in the marketplace, and has been integrated into a RPAS owned by the INTA, i.e. the SIVA. This integration allowed us to verify the appropriate operation of the system, by means of different ground tests and with a real flight, during a campaign conducted in the military base *Conde de Gazola* (Leon), belonging to the Spanish Army. The whole system has been delivered to the Spanish Ministry of Defense at a very limited cost as opposed to other existing RPAS solutions, which was one of the objectives of the DRONE project. Our future work will address the evolution of the communication system with new functionalities, such as the design and implementation of a comprehensive network management architecture for the MILANO RPAS, and exploring different alternatives to support automatic key management, including in-flight key renewal, between the RPA, the GCS and any involved RVTs.

## ACKNOWLEDGEMENTS

This work has been partially granted by the Spanish Ministry of Defense through the DRONE project (DN8644-COINCIDENTE-10032110042). The authors want to acknowledge the INTA and Erzia Technologies S.L. personnel that participated in the DRONE project for the fruitful collaboration and excellent work. The work of Francisco Valera has been partially funded by the Spanish Government through the MINECO eeCONTENT Project (TEC2011- 29688-C02-02).

## REFERENCES

[1] R. Austin. “Unmanned Aircraft Systems. UAS Design, development and deployment.” Wiley and sons, April 2010. ISBN: 978-0-470-05819-0

[2] T. Samad, J. S. Bay, and D. Godbole, “Network-centric systems for military operations in urban terrain: The role of UAVs,” in Proc. IEEE, Jan. 2007, vol. 95, no. 1, pp. 92–107

[3] INTA. Instituto Nacional de Técnica Aeroespacial “Estaban Terradas”. Available online (Apr. 2014): http://www.inta.es/

[4] SIVA. Air Surveillance System. Instituto Nacional de Técnica Aeroespacial “Estaban Terradas”. Available online (Apr. 2014): http://www.inta.es/doc/programasaltatecnologia/avionesnotripulados/siva_web.pdf

[5] J.L. Expósito. “The Spanish UAV pilots will be instructed in Matacán”. Revista española de defensa. N. 289. Nov. 2012. Spanish Ministry of Defense. ISSN 1131-5172. Available online (Apr. 2014): http://www.defensa.gob.es/Galerias/documentacion/revistas/2012/red-289-uas-matacan.pdf

[6] MILANO. Instituto Nacional de Técnica Aeroespacial “Estaban Terradas”. Available online (Apr. 2014): http://www.inta.es/doc/programasaltatecnologia/avionesnotripulados/milano_web.pdf

[7] X. Li, C. Bao, F. Baker, "IP/ICMP Translation Algorithm", Internet Engineering Task Force, RFC 6145, Apr. 2011.

[8] S. Kent, K. Seo, “Security Architecture for the Internet Protocol”, Internet Engineering Task Force, RFC 4301, Dec. 2005.

[9] S. Kent, “IP Encapsulating Security Payload (ESP)”, Internet Engineering Task Force, RFC 4303, Dec. 2005.

[10] S. Frankel, S. Krishnan, “IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap”, Internet Engineering Task Force, RFC 6071, Feb. 2011.

## BIOGRAPHIES

IVAN VIDAL (ividal@it.uc3m.es) received the Telecommunication Engineering degree in 2001 from the University of Vigo, and the Ph.D. in Telematics Engineering in 2008 from the University Carlos III of Madrid. He is currently working as visiting professor at Universidad Carlos III de Madrid. His research interests include multimedia networking, IP Multimedia Subsystem (IMS) and Information-Centric Networking (ICN). He has been involved in several international and national research projects related with these topics, including the EU IST MUSE, the spanish MEDIANET project and the Spanish Ministry of Defense project DRONE. He has published several papers in magazines and conferences, lately in the areas of mobility support in IMS networks and ICN management.

FRANCISCO VALERA (fvalera@it.uc3m.es) received the Telecommunication Engineering degree in 1998 from the Technical University of Madrid (UPM), and the Ph.D. in Telecommunications in 2002 from the Univ. Carlos III de Madrid (UC3M), where he is currently a tenured associate professor. He has been involved in several national and international research projects and contracts related with experimental facilities, protocol design, inter-domain routing, protocol engineering, next generation networks and multimedia systems, serving there as PI, work package leader and also as coordinator. Dr. Valera has published over 60 papers in the field of advanced communications in magazines and conferences. He has also has participated in the scientific committee, organization and technical review in different national and international conferences.

MIGUEL ÁNGEL DÍAZ (miguelangel.diaz@imdea.org) received the Bachelor's Degree in Computer Science and Engineering in 2014 from the University Carlos III of Madrid. In 2012 he received a scholarship from University Carlos III to perform research on RPAS, which he continued until his incorporation to IMDEA Networks. In this company he is a candidate to the PhD degree in telematics engineering. His current work is focused on Internet measurements, android application implementation and cybersecurity.

MARCELO BAGNULO (marcelo@it.uc3m.es) received en electrical engineering degree from the Universidad de la Republica Oriental del Uruguay and a PhD degree in Telecommunications from Universidad Carlos III de Madrid. He is an associate professor at the Telematics Department at Universidad Carlos III de Madrid. He is co author of over a dozen IETF RFCs and over 50 academic papers.

| | SIVA | MILANO |
|---|---|---|
| **Span** | 5.81m | 12.5m |
| **Length** | 4.02m | 8.2m |
| **Maximum Take-Off Weight MTOW** | 300kg | 1000kg |
| **Payload** | 40 | 150kg |
| **Autonomy** | 7h | >20h |
| **Speed** | 115-190 km/h | 230km/h |
| **Range** | 100-150km (L.O.S.) | B.L.O.S. (SATCOM) |
| **Ceiling** | 13,000feet | 26,000feet |

Table 1: SIVA/MILANO main characteristics

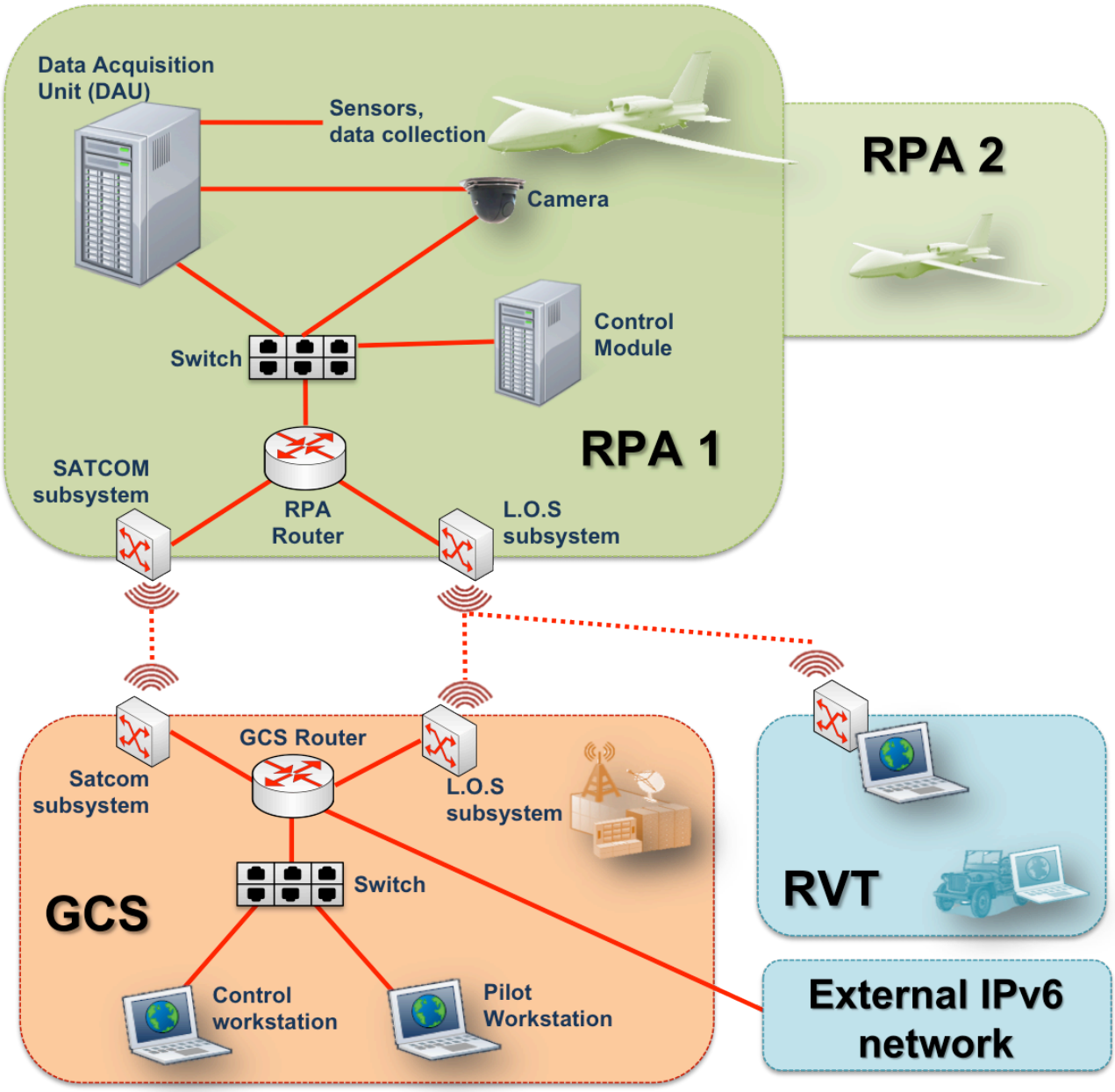


Figure 1: overview of the system architecture

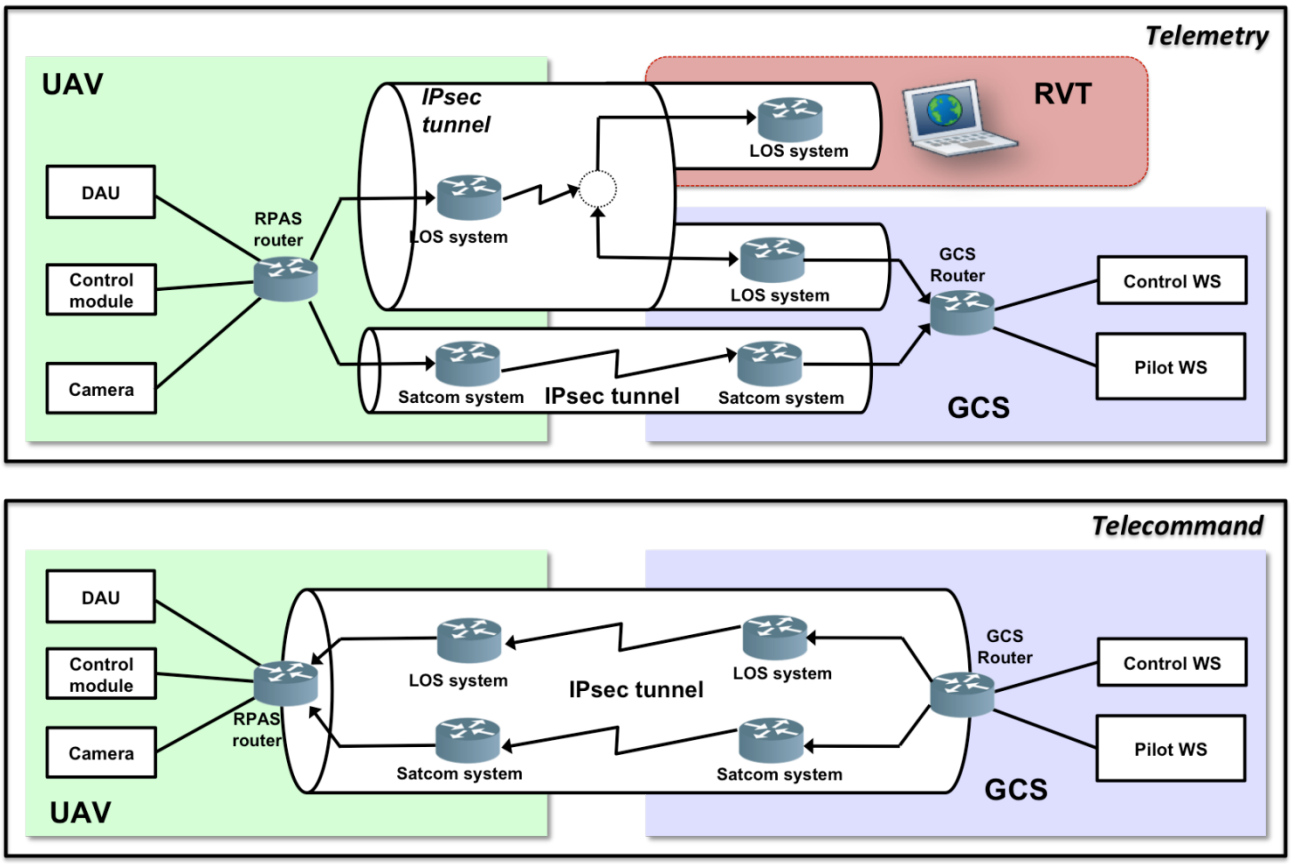


Figure 2: IPsec security for telemetry and tele-command

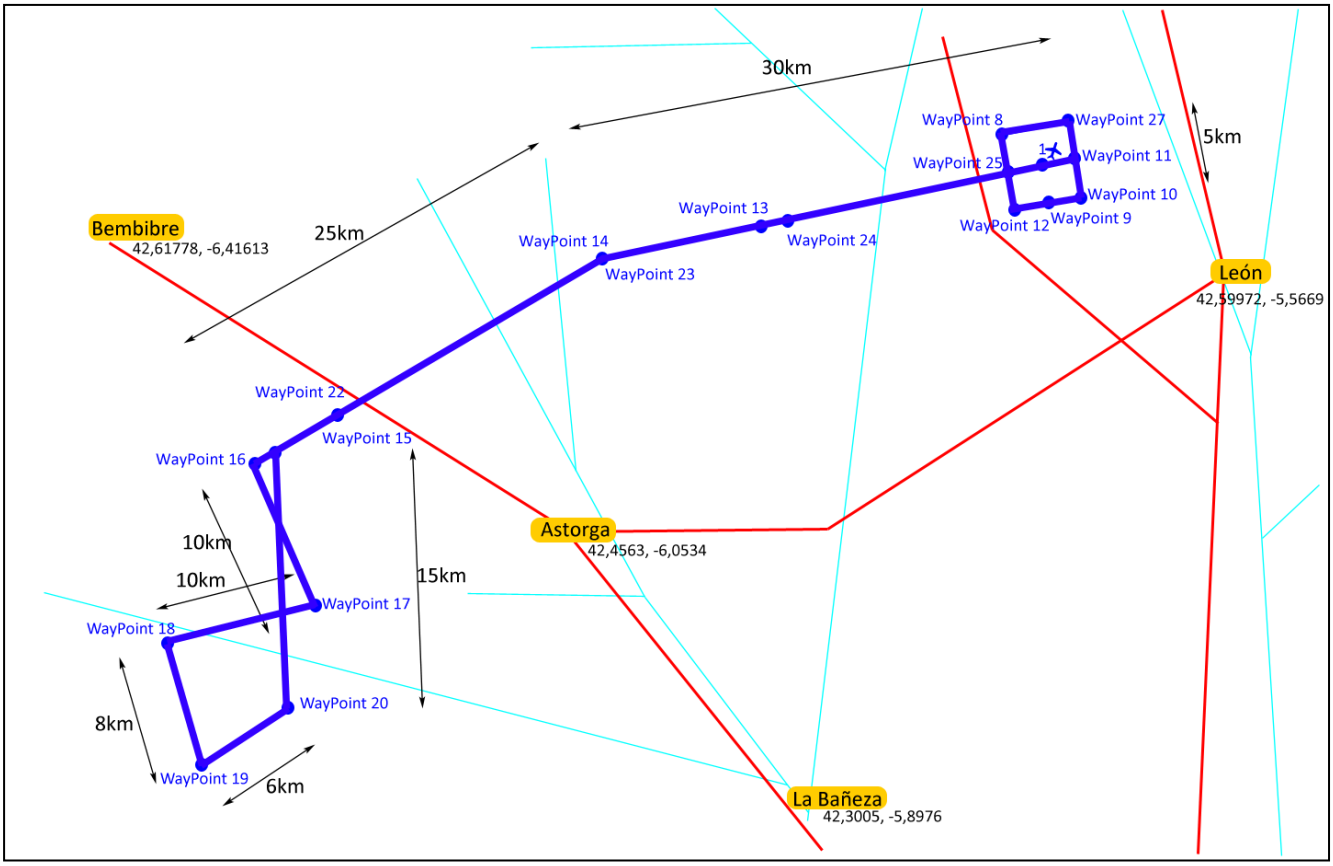


Figure 3: mission planning (INTA mission WayPoints)

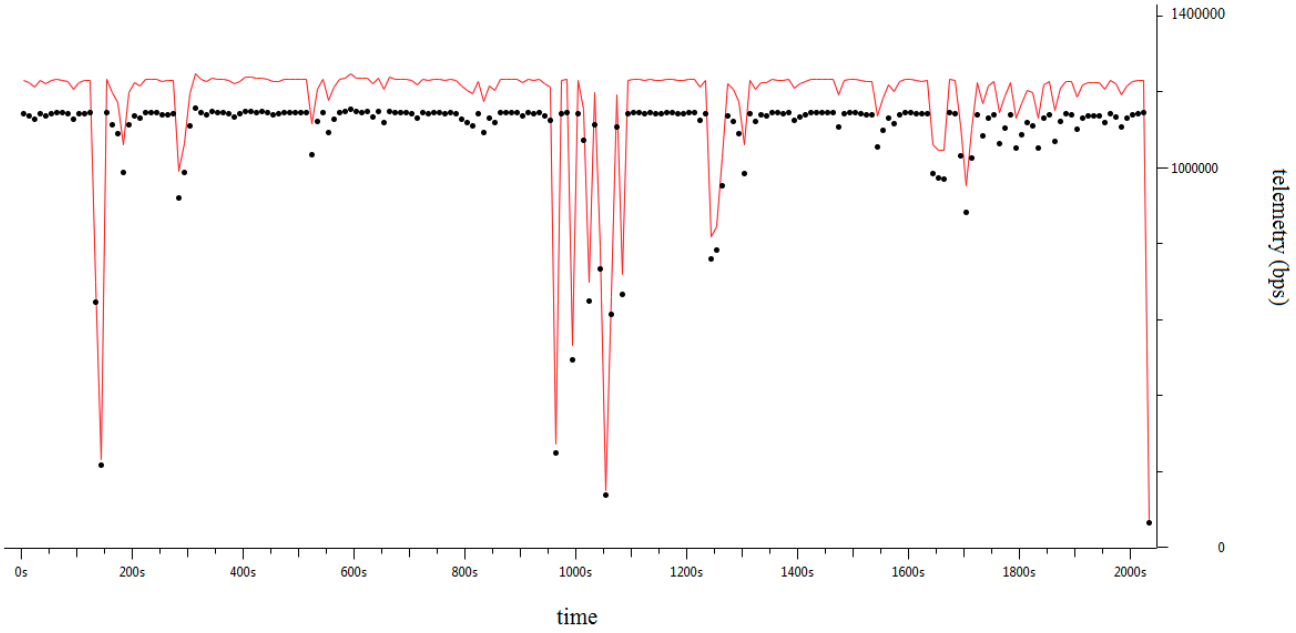


Figure 4: telemetry (video and sensor data) received at the GCS router