Journal Paper

Secure Wireless Avionics Intra-Communications the SCOTT approach

Paper presented at DecPS 2018 (held in conjunction with Ada-Europe 2018, 18-22 June, Lisbon, Portugal).

Ramiro Robles*

Jose Neves

*CISTER Research Centre

CISTER-TR-190205

2018/12

Secure Wireless Avionics Intra-Communications the SCOTT approach

Ramiro Robles*, Jose Neves

*CISTER Research Centre
Polytechnic Institute of Porto (ISEP P.Porto)
Rua Dr. António Bernardino de Almeida, 431
4200-072 Porto
Portugal
Tel.: +351.22.8340509, Fax: +351.22.8321159
E-mail: rasro@isep.ipp.pt, jose.neves@gmv.com
https://www.cister-labs.pt

Abstract

This paper presents the objectives and architecture of the use case of secure wireless avionics intra-communications of the European Project SCOTT (secure connected trustable things). SCOTT aims to build trust of the Internet of Things (IoT) in industrial applications. SCOTT addresses multiple issues such as security, safety, privacy, and dependability across 5 industrial domains: automotive, aeronautics, railway, building and healthcare. The aeronautics use case focuses on the application for active flow control based on dense wireless sensor and actuator networks (DWSANs) to draw conclusions about security, vulnerabilities and safety in the general field of wireless avionics intra-communications (WAICs). The paper presents preliminary conclusions of the vulnerabilities and security solutions across different entities and layers of the aeronautics IoT architecture.

Secure Wireless Avionics Intra-Communications: the SCOTT Approach

***Ramiro Samano-Robles*[1] *and José Neves*[2]**

[1]*Research Centre in Real-time and Embedded Computing Systems, Porto, Portugal; email:rasro@isep.ipp.pt*

[2]*GMVIS SKYSOFT SA, Lisbon, Portugal; email:jose.neves@gmv.com*

Abstract

This paper presents the objectives and architecture of the use case of secure wireless avionics intra-communications of the European Project SCOTT (secure connected trustable things). SCOTT aims to build trust of the Internet of Things (IoT) in industrial applications. SCOTT addresses multiple issues such as security, safety, privacy, and dependability across 5 industrial domains: automotive, aeronautics, railway, building and healthcare. The aeronautics use case focuses on the application for active flow control (AFC) based on dense wireless sensor and actuator networks (DWSANs). Topics about security, vulnerabilities and safety in the general field of wireless avionics intra-communications (WAICs) will be addressed. The paper presents preliminary conclusions of the vulnerabilities and security solutions across different entities and layers of the aeronautics IoT architecture.

Keywords: WAICs, security, vulnerability, IoT, Bubble.

1 Introduction

The number of wireless links is growing exponentially. It is estimated that nearly 25 billion devices will be online by 2020 [1]. A high percentage of these devices will use wireless links. Wireless is expanding to areas previously reluctant to this type of communication. In aeronautics, wireless is just recently gaining acceptance for on-board applications. This late adoption is due to reliability and interference issues. Wireless is starting to be used on board for systems that conventionally used only wireline infrastructure (i.e., as replacement of wires). It will also be used for applications which are now only possible thanks to the wireless component (e.g., indoor localization). Recent interference and reliability studies with state-of-the-art wireless standards (see [2]) suggest the feasibility of a relatively new research area called wireless avionics intra-communications (WAICS) [3]. Examples of potential applications of WAICs are: structure health monitoring, fuel tank sensors, automatic route control based on optimized fuel consumption and weather monitoring, automatic turbulence reduction or active flow control, flexible wiring redundancy design, logistics, and in-flight entertainment.

The avionics industry will experience a wireless revolution in the years to come. The concept of “flyby-wireless” [4] opens several issues in design, configuration, security, trustiness, and interference control. Wireless networks are inherently prone to security and privacy threats due to their broadcast nature. Eavesdropping by unintended parties on board or outside the airplane is one of the main issues, which requires appropriate encryption, coding and/or authentication schemes to be minimized. Man-in-the-middle (MiM) and denial of service (DoS) attacks can prevent sensor information about aircraft health from reaching the control cabin, thus posing a threat to the safety of the plane, leading to mal-functioning. Intentional and unintentional jamming can also increase the risk of failure and lack of communication in aircraft. All these vulnerabilities and risks need to be properly studied, so that potential countermeasures can be implemented.

This paper deals with security in the domain of aeronautics of the European ECSEL project SCOTT (secure Connected Trustable Things) [5]. The aeronautics use case exploits the application of active flow control (AFC) using dense wireless sensor and actuator networks (DWSANs) to design secure communications across different layers and entities of the architecture. The objective is to increase the technology readiness level (TRL) of secure wireless solutions in the avionics industry.

SCOTT is a project that aims to boost trust, security, safety, privacy and dependability of the Internet of things (IoT) in industrial applications. SCOTT envisions a trusted, industrial-compliant cloud connectivity for IoT, with high energy efficiency and autonomous operation. SCOTT uses the concept of Bubble from the predecessor project DEWI [6]. The Bubble is a high-level abstraction of an industrial WSAN with enhanced interoperability, dependability, standardized access to sensor readings, and cross-domain development [7]. SCOTT foresees an ecosystem of communicating bubbles in different industrial use cases.

This paper is organized as follows. Section 2 presents the objectives of the aeronautics domain of the project. Section 3 presents the advances with respect to the state of the art. Section 4 presents the application of active flow control and its architecture. Section 5 presents the physical entity model. Section 6 deals with the functionality model. Section 7 presents preliminary vulnerability and security analysis. Section 8 presents the conclusions of the paper.

2 Objectives and measurable indicators

The objectives of the aeronautics domain (Figure1) are [5]:

- Ensure that WAICs are secure, trustable and safe (reduce identified vulnerabilities and security threats in the project of wireless solutions by up to 90%).
- Construct gateways between WAICs and the internal networks of commercial aircraft enforcing multi-level and multi-metric security, privacy and safety.
- Increase fuel efficiency by replacing cables and using dense-WSANs for turbulence and skin drag control.
- Conduct a study of vulnerabilities and potential attacks to the new hybrid wireless/wired avionics infrastructure. Propose countermeasures with a trade-off analysis between complexity and risk.
- Provide guidelines to stakeholders on how to solve common problems of security, privacy, and trustiness.
- Help in the adoption of WAICs in industry (including standardization and certification issues).
- Enable the use of semantics interoperable middleware tools for the development of advanced fleet management and smart avionics applications.

The objectives in terms of measurable indicators are:

- To create a repository of tools, reference implementations and links to middleware and reliability studies of avionics infrastructure.
- Demonstrate secure wireless avionics applications covering different scenarios.
- Development of gateways for avionics applications providing secure and trustable protocol translation.
- Improve the performance of wireless avionics by a factor of 10 in terms of spectral efficiency, also to improving energy efficiency and interference reduction.
- Demonstrate via a prototype, standardization and a reference implementation the reliability and trustiness of commercial wireless standards on board aircraft.
- Provide guidelines to aerospace stakeholders on how to improve privacy and security in WAICs.

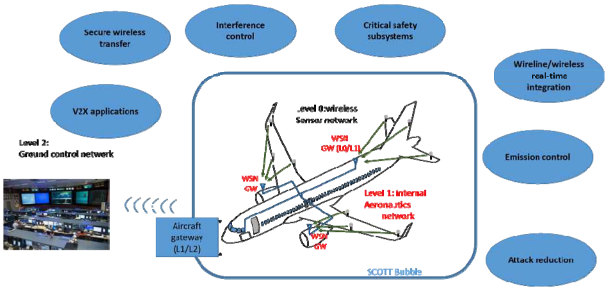

Secure wireless transfer
Interference control
Critical safety subsystems
Wireline/wireless real-time integration
V2X applications
Level 2: Ground control network
.evel 0:wireless Sensor network
WSN GW (L0/L1)
WSN GW
Level 1: internal Aeronautics network
WSN GW
Aircraft gateway (L1/L2)
SCOTT Bubble
Emission control
Attack reduction

Figure 1 Aeronautics objectives

3 State of the art (SoA) and progress

One major potential advantage of using wireless technology in aeronautics is the reduction of wiring, which is a critical issue in aircraft and spacecraft design [8]. Blackhawk helicopters carry almost 2,000 pounds of wires for computers and sensors [9]. Electrical wiring problems cause on average two inflight fires every month as well as more than 1077 mission aborts and over a hundred thousand lost mission hours per year [10]. Each year, navy spends one to two million man-hours finding and fixing wiring problems [11] . Damages on a wired connection can affect not only the system related to the faulty wire, but also contiguous systems which individually would have been fully operational. Therefore, the use of wireless technology is expected to bring considerable gains to the avionics industry in terms of reduction of cables, more flexibility in the design of redundancy links, and faster troubleshooting. Wireless nodes have also the advantage reaching places of an aircraft that cannot be reached by wires. Furthermore, modern WSNs provide self-configuration, RF tolerance, and maintenance troubleshooting that are much more flexible than their wireline counterparts. In critical avionics applications though, wireless links cannot completely replace wired links due to the high reliability requirement. However, they can replace redundant links, thus increasing reliability and flexibility in the design.

In avionics, wireless technology is well known for several applications such as: air traffic management (ATM), telemetry, aircraft-ground control, satellite localization/ communication, identification of friend-or-foe systems, inter-aircraft communications, and radar. In contrast to these applications, which are relatively mature, WAICs have just recently gained attention. Recent results suggest that existing standardized commercial wireless technologies show potential low levels of interference and thus low impact to on-board systems, as well as reliable performance compatible with existing wireline infrastructure. These results have paved the way for new applications for wireless communications in aircrafts.

Security is an important issue in wireless avionics. In comparison with conventional WSNs, the data of an aircraft, particularly related to aircraft health monitoring, is vital for the good functioning, management and safety of a plane. Therefore, the sensor network should be more robust to different types of attacks either from passengers or entities on board, ground or even from other aircrafts. An extensive analysis of different types of security attacks using an adversary model, where the adversary can be internal or external and the attack can be passive or active are available in the literature. Safety and business threats have been identified such as: data integrity, authenticity, confidentiality, link-key establishment, channel jamming mitigation, secure routing, secure location verification, and robustness to node capture (eavesdropping)[12].

SCOTT intends to leverage wireless technology in the aeronautical industry. This means to effectively implement secure and safe wireless technology in real applications to be used by the aeronautics industry. The objective is to bring the concept of IoT to aeronautical applications thus creating a smart, flexible and automatic environment on board and in different elements of the aeronautics industry, including airports, management of infrastructure, flight control, vehicle-to-infrastructure and/or vehicle-to-vehicle communication, turbulence reduction, etc. The aeronautics domain will present a full analysis of vulnerabilities and potential countermeasures for the hybrid aircraft wireless/wireline infrastructure. SCOTT attempts to create a framework for smart avionics development with different levels of security and trustiness that will enable big data analytics and cloud computation for the optimization of aircraft performance, reduction of fuel consumption, controlled interference, and high spectral efficiency.

Several issues will be addressed, including propagation modelling for reliable transmission and reduced leaking or interference, as well as MAC-PHY cross-layer design to reduce conflicts between different subnetworks in the same aircraft and minimize interference to control subsystems. Secure links will be addressed by minimizing transmissions to potential eavesdroppers or unsafe locations either within the same or in other airplanes. Privacy of data will be also addressed by convenient mechanisms and data-context management with ground control.

The aeronautics industry expects huge benefits from the use of wireless technologies. It is estimated that cables constitute over 70% of aircraft weight. The use of wireless links could reduce this figure down to 55%. In addition, technologies such as AFC enabled by DWSANs can help reduce the effect of skin drag, thus further improving fuel consumption efficiency. A reduction of 10% in fuel consumption is translated into several millions of dollars in savings. It is estimated that the use of wireless technologies will bring a 12% reduction in terms of fuel consumption [13]. Further improvements are possible when combined with other technologies such as winglets, carbon fibre fuselage and improved turbine design. The use of cables has one more benefit in terms of cabling planning tasks. It is estimated that these planning tasks have a cost of 2,200 dollars per kg of aircraft [14]. When considering two types of aircraft the estimated savings are the following [15]: A320/B737-900 6,400 kg x 2,200 \$/kg ≈ \$14 million, and A350-900/B787-9 23,000 kg x 2,200\$/kg ≈ \$50,6 million. It is also estimated that 13% of an aircraft operation cost is related to maintenance, reparation and overhaul. Wireless technologies are expected to have a big impact in the reduction of these costs. Automatic configuration, maintenance and troubleshooting can be performed over the air reducing maintenance service costs.

4 Application case: Active Flow Control based on dense WSANs

The objective of the Bubble AFC is to employ a wireless sensor-actuator and communication bubble for suppression of the turbulent flow and delaying the BL (boundary layer) transition. The sensor network will detect the low-pressure region on the upper wing surface. The position of BL transition zone will be defined, selecting the appropriate actuators to be activated. At the same time, and based on the sensor values, the set of conditions for operation of the actuators (e.g., frequency, amplitude) will be calculated based on existing data (pre-set data). The selected actuators are activated to manage the turbulent flow on the wing surface. The data is stored. A new sensor reading is collected, and the cycle is repeated. The stored data can be analysed to assess system operation during, for example, different flight profiles or moments (e.g., take-off, landing, and cruise). Ground systems can interact with the sensor-actuator and communication bubble to get the data recorded during the flight and process this information to determine actuation plans and analyse the data of the whole fleet.

There are several challenges in the interconnectivity and how to achieve the desired objective in a dependable manner, whilst minimizing energy expenditure. The WSAN requires sensor measurements at high frequency and in a synchronous manner, to be able to correlate sensor readings, especially from sensors in close proximity. The WSAN also needs deal with failures of sensors, and this can be approached by employing reliable data transmission and data delivery mechanisms and also by employing data processing strategies that can deal with sensor failures.

It is important to boost the use of wireless communication systems on board to enable the deployment, as soon as possible, of technologies like Structural Health Monitoring (SHM) and Active Flow Control. To achieve this goal, these wireless networks and sensor systems need to communicate and interact with the main data buses of the aircraft. Hence, the specification of bi-directional bridges between different types of technologies is required. This is still the case if wireless technologies are used as the main data bus of the aircraft. Different wireless networks, with different delivery deadlines and different underlying technologies must operate together without possibility of interference. Bridge protocols and interfaces must be specified considering the constraints of the different networks.

The AFC system uses an architecture with a set of polygonal patches, each patch with a regular grid/array of sensors and actuators. These patches will be located mainly on surface of the wings of the aircraft, and potentially on other surfaces of the fuselage. The objective is to control the turbulence region across the aircraft and reduce losses. All the sensors and actuators inside a single patch will be wired together sharing a single communication and control point. The patches will communicate wirelessly with a relay or access point located conveniently in the aircraft to ensure good communication with several patches. Each patch will be enabled with some sort of intelligence to provide management of all the sensors and actuators inside the patch and to provide convenient communication link with the sink and the control unit inside the Bubble. The architecture of AFC is therefore a hybrid of a wireless and wireline sensor network, which is the most convenient for this application. The information generated by each sensor will be collected by the control unit of each patch (node) which will provide some preliminary filtering, fusion and aggregation functionalities. The refined information will be then relayed towards the control unit (Gateway or relay node). Based on this collected information and based on different flight profiles, the AFC system will decide the type of actions to be performed by the set of actuators on each patch. Each of the flow control actuators is a piezoelectric device (synthetic jet actuator –SJA- or Fliperon). These actuators can delay the turbulence BL and thus help in counteracting the dragging effect in response to the measured information and according to flight profiles.

The size and number of patches, as well as the number of sensors/actuators per patch is optimized using a simulator. These parameters are function of the accuracy of the active flow control system, the range of the wireless technology selected, and the data rate of the wireless sensor nodes. All sensor/actuators nodes will be powered via cables. The patch will be provided with some power saving features too. For example, when a sensor information or actuation is not required from some patches, they can be powered down until they need to be used again, thereby saving energy.

The architecture proposed for the AFC system is relatively new in aeronautics, as it constitutes a hybrid design with wired and wireless components. The number of sensors for this application is expected to be large, more than in common WSNs, being deployed over a relatively small area. This brings up the issue of interference, if each sensor was to be enabled with an individual wireless connection. To solve this, our approach presents an architecture where groups of sensors wired together form a patch that will act as a single wireless transmitter. Each patch will be provided with smart self-configuration and control. Figure 2 shows the possible embodiment of a regular design of sensor and actuators inside a patch. Each patch will have a radio transceiver and a control unit with some intelligence. This node will be in charge of organizing the processing and operations inside the patch, as well as filtering, fusing, and aggregating data to be sent towards the wireless node.

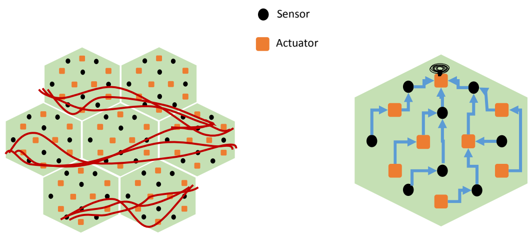


Figure 2 Patch concept for AFC

Another aspect is the interconnection of WAICs into the avionics internal systems as shown in Figure 3. The proposed solution has to be able to pass reliably the traffic from/to the wireless sensor/actuator network to the internal avionics network under different QoS constraints. In general, the AFDX (Avionics Full-Duplex Switched Ethernet) network (or ARINC664) has more stringent QoS requirements, therefore the solution must include an appropriate scheduler that will ensure these QoS constraints of the AFDX traffic are met or conveniently addressed when transported to/from the wireless domain.

4.1 Overview of the architecture

The main physical entity of the SCOTT AFC system is a regular array of wired sensors and actuators also called patch. A possible configuration of this patch and an array of patches are shown in Figure 2. The patch can have hexagonal, rectangular or in general a polygonal shape, depending on the needs of coverage over the aircraft. The patch is mounted over the surface of the fuselage and mainly the wings of the aircraft, where turbulent flow is expected to be formed, particularly at high vehicle speeds and high values of angle of attack (AoA). We recall here that the objective of the dense SAN (sensor and actuator network) implemented by means of patches is to track the formation of turbulent flow and attempt to delay the separation of the boundary layer using actuation policies for different flight profiles or moments of an aircraft mission. All the sensors and actuators inside the patch are controlled by a master unit, which is in charge of intra-patch management, signal relaying, data aggregation, data fusion, compression, and protocol conversion. The sensors and actuators can be connected using a real time technology that can have several characteristics or topologies. One potential configuration is using a microprocessor board controlling one subset of sensors and actuators inside the patch. A network of microprocessors is deployed inside the patch, with a real time transmission technology such as CAN (Controller Area Network) or ARINC 664. Intra-patch routing algorithms can be implemented to allow the information of different sensors to be collected reliably and in real time by the master unit.

Each patch in the network has a wireless transmission unit that is used to communicate with a wireless gateway

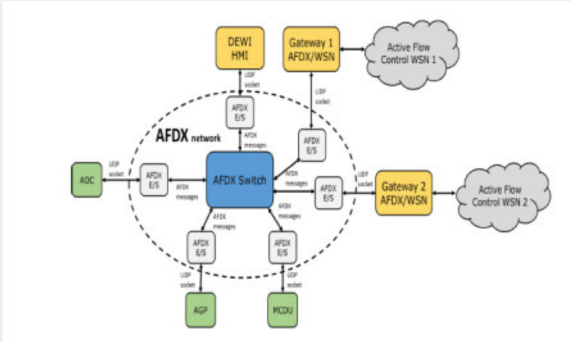


Figure 3 Interconnection with an aeronautical internal network (AFDX)

located conveniently in the aircraft to maximize coverage with a set of distributed patches (see high level architecture displayed in Figure 5). The patch is the basic unit of the proposed AFC system, as it provides modularity, scalability, flexible implementation, as well as advanced management and troubleshooting. Close loop operation occurs at three levels:

1. Directly at the sensor and actuator microprocessor control level to deal with the fast (short term) and spatially correlated variations of the turbulent flow to be sensed.
2. At the level of the internal aeronautics network (see Figure 3). A control unit for the network of patches resides in the internal control operation of the aircraft. The decisions of the medium-term turbulence statistics are taken directly in this close loop control unit on-board the aircraft.
3. All the relevant measurements for different moments of an aircraft mission are relayed from the aircraft to ground control. Ground control contains a database of actuation policies that are optimized over different types of aircraft at different times of the year, routes and weather conditions. This level of control allows operators to optimize routes, as well as actuation policies based on big data analytics that will become more reliable over longer periods of time and with more data of sensor and actuation policies.

5 Physical entity model

Patch of sensors and actuators. The basic unit of the AFC system consists of a regular set of sensors and actuators that communicate with each other in a mesh array or in star formation with a master control unit. The intra-patch communication technology can be real-time or with high reliability to transport all the sensor readings to the master unit, as well as any actuation control policy back from the master unit to the actuators. Each patch has a wireless communication module that allows transmission with an access point or with other patches depending on the configuration. Patches are also allowed to relay the information of other patches towards the destination if necessary. The control unit can also process the sensor data across time and space inside the patch. Other functionalities of the patch include filtering, encoding, encryption, compression, etc. One potential configuration is using a microprocessor board controlling one subset of sensors and actuators inside the patch. A network of microprocessors is deployed inside the patch, with a real time transmission technology such as CAN (Controller Area Network) or ARINC 664.The intra patch communication technology can use secure routing to avoid malfunction or an attack.

Wireless gateway or WAICs access point. This entity implements the PHY and MAC layer transmission and organisation of the WAICS radio technology for communication with patches. The gateway translates the wireless protocol to the internal wireline aeronautics network of commercial aircraft. This translation has several challenges due to the different nature of the unreliable and unsecure wireless world in comparison with the real-time internal avionics network. Part of the analysis is how to make secure this translation from the wireless domain to the wireline real-time operation of the commercial aircraft.

Internal actuation policy control unit. This entity is in charge of the collection of the medium-term statistics of the collected flow information from the network of patches across the entire aircraft. Therefore, it can be used to calculate actuation policies that optimize the delaying of the BL separation for the whole airplane. In this problem it is evident that the whole performance and stability of the aircraft as well as aerodynamic efficiency, and monitoring of other stability issues of the airplane come into place. In addition, for security purposes it is possible to implement intrusion detection, misbehaviour tracking, redundancy coding, authentication of patches, authorisation of actuation policy control, etc.

Ground operator and actuation policy database back end servers. This entity is in charge of the actuation control and optimisation across different aircraft. It is intended to provide airline operators with a means to control, analyse, collect and process sensor data of different routes and aircraft. This processing aims to obtain (using cloud computing tools, for example) optimised actuation policies according to the time of the year, route, type of aircraft, weather conditions, etc. In a generalized scenario, this entity provides consolidated access to sensor and actuation control information for wireless avionics applications. Several security mechanisms can be used in this external access to aircraft information such as authorization, authentication, encryption, tunnelling, intrusion detection, privacy labelling/control, etc.

5.1 Aircraft architecture

The aircraft comprises several systems with different functions defined to achieve several product goals (see Figure 4):

1. Aircraft Control Domain (ACD): contains functions required to maintain the aircraft airworthy providing control to pilot or breathable environment to passengers. Any fail or malfunction jeopardizes the aircraft.
2. Airline Information Services Domain (AISD): used by airline to operate the aircraft providing maintenance information and software and databases updates.
3. Passenger Information and Entertainment Services Domain (PIESD): contains those functions used by passengers during the flight like games, internet connection and access to media.

5.2 Layered model alignment

This section provides the alignment of the physical entity model described in previous subsection with the layered overview of the SCOTT high level architecture. This layered model is closely correlated to the concept of

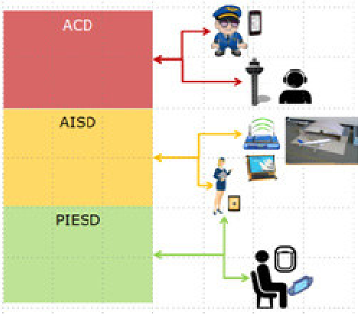


Figure 4 Aircraft domains and users

SCOTT Bubble, which is the basic building block for interoperability and security enhancing for the project. This layered model consists of three levels (one of them optional) that define the intra and extra-bubble space as observed in Figure 5. Level 0 is the wireless domain to provide the last link between the fixed aeronautical infrastructure towards the distributed sensor or object nodes. In the active flow control use case, this wireless technology has actually a hybrid approach using wireline and wireless components under the name of patch. A patch is a wireline entity of sensors and actuators. Each patch uses wireless technology to communicate with the L0 or WSN gateway. The access point is placed on-board the aircraft therefore acting as the translation entity between the wireless domain and the internal network of the aircraft. This internal network of the aircraft acts as the L1 of the SCOTT reference architecture. Many other WAICs applications will use the same approach, particularly those in which the wireless link replaces an existing wireline sensor. In the case of the AFC use case, it is also plausible that L1 is completely independent of the internal network of the aircraft. However, for the sake of covering more generic implementations, it will be multiplexed inside this internal network, which in many current commercial aircraft is a real-time deterministic version of Ethernet technology. This integration into the L1 internal aircraft network, comes at the expense of traffic contention, possible attacks from other points inside the internal network, as well as attacks originated in the wireless network towards other aircraft internal subsystems. This means that the internal critical aircraft network can be subject of an attack coming from the wireless domain, which is a less secure environment. In the SCOTT reference architecture, L1 is an optional level, mainly because in some uses cases it is possible that this interaction with an existing domain network does not exist. The on-board unit acts as the Bubble Gateway, which controls all aspects of the intra-bubble space and provides translation for external user access. This is the boundary of the SCOTT Bubble in aeronautics.

Finally, Level 2 of the reference architecture defines the extra bubble space. L2 is used for external access to the information of Nodes inside the aeronautical Bubble. This is the ground control operation network, where the external user is the airline operator or a smart avionics application collecting information from many different aeronautical Bubbles, inside the same aircraft or located in different aircraft or fleets. The mapping of the aeronautical use case to this layered view of the architecture is shown in Figure 5.

The Bubble is a concept that allows an integration of legacy WSN and local industrial domain technologies into a single point of entry towards the modern Internet cloud. The bubble Gateway can provide transparent access to the objects inside the Bubble, or simply to a summarized version of the information generated inside the Bubble. This concepts allows designers to exercise control over the access to the intra-bubble entities, and therefore enforce higher dependability different from the non-delay sensitive internet-like infrastructure (L2) and also higher security control. In the aeronautics industry, the use of a Bubble confined to one aircraft or sections of the aircraft is a powerful tool to avoid attacks from external entities, while also controlling the permissions granted to L1 internal users. The attacks coming from the passenger entertainment system can also be handled by enabling the bubble gateway with convenient scheduling policies and out-of-band security communication, as well as autonomous operation.

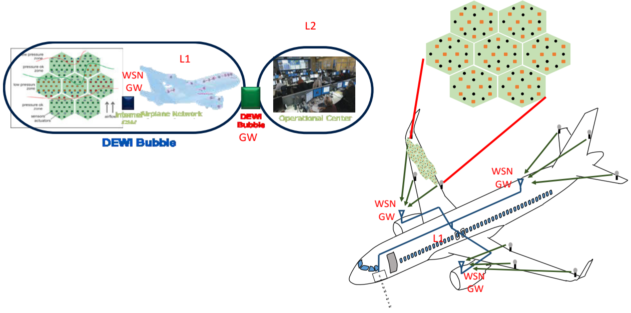


Figure 5: AFC use case architecture

6 Functionality model

The functionality model is derived explicitly from the reference architecture of the project. The explicit functional model for the AFC system is shown in Figure 6, and the hybrid view functional versus layered entity model is shown in Figure 7. Functional layers include: Device Layer (DL), Network Layer (NL), Service Layer (SL), IoT and Virtualization Layer (IOTL), Cloud and application Layer (CAL), and Service Layer Management (SLM) and Cross-Layer Management (CLM).

Each of the physical entities will implement a slight variation of the functional model. The hardware layer in the patch unit focuses on the technology to interconnect sensors and actuators, intra-patch routing, management, compression, redundancy coding, encryption (optionally), authentication, intrusion detection, safe mode operation and troubleshooting. The intra-patch technology is real-time and is used to collect the sensor measurements from the dense mesh of nodes in the master unit of each patch. There are no high-level functionalities here except in the master unit of each patch, which provides protocol translation to the wireless domain.

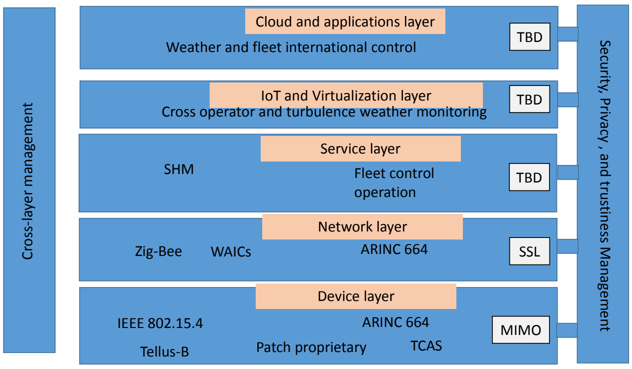
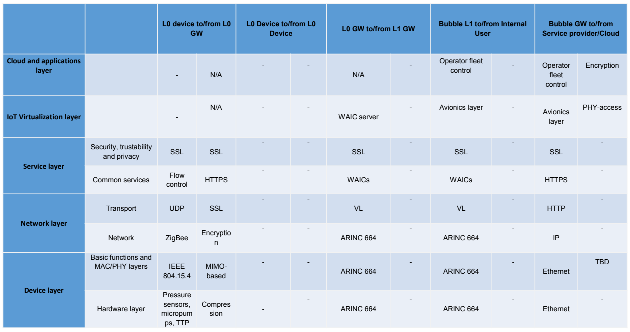

Cross-layer management
Cloud and applications layer
Weather and fleet international control
TBD
IoT and Virtualization layer
Cross operator and turbulence weather monitoring
TBD
Service layer
SHM
Fleet control operation
TBD
Network layer
Zig-Bee
WAICs
ARINC 664
SSL
Device layer
IEEE 802.15.4
ARINC 664
MIMO
Tellus-B
Patch proprietary
TCAS
Security, Privacy , and trustiness Management

Figure 6 Functional entity layered model



		L0 device to/from L0 GW		L0 Device to/from L0 Device		L0 GW to/from L1 GW		Bubble L1 to/from Internal User		Bubble GW to/from Service provider/Cloud	
Cloud and applications layer		-	N/A	-	-	N/A	-	Operator fleet control	-	Operator fleet control	Encryption
IoT Virtualization layer		-	N/A	-	-	WAIC server	-	Avionics layer	-	Avionics layer	PHY-access
Service layer	Security, trustability and privacy	SSL	SSL	-	-	SSL	-	SSL	-	SSL	-
	Common services	Flow control	HTTPS	-	-	WAICs	-	WAICs	-	HTTPS	-
Network layer	Transport	UDP	SSL	-	-	VL	-	VL	-	HTTP	-
	Network	ZigBee	Encryptio n	-	-	ARINC 664	-	ARINC 664	-	IP	-
Device layer	Basic functions and MAC/PHY layers	IEEE 804.15.4	MIMO-based	-	-	ARINC 664	-	ARINC 664	-	Ethernet	TBD
	Hardware layer	Pressure sensors, micropum ps, TTP	Compres sion	-	-	ARINC 664	-	ARINC 664	-	Ethernet	-

Figure 7 Mapping functional vs physical entity

One candidate for intra-patch communication is the protocol TTP (Time Triggered protocol). In the wireless domain for inter-patch communication, several aspects of the functional model are here presented: MAC and PHY communication layers use MIMO (multiple-input multiple output), beamforming, MAC-PHY security, interference rejection, spatial-based authentication, collision resolution by retransmission diversity, multi-packet reception, interference alignment, and dependability control. Optionally, encryption in this link will also be used based on the IEEE 802.15.4 standard. Intrusion detection, and safety hazards identification are also being investigated. Higher layer functionalities include secure routing, tunnelling, patch-authentication using key distribution algorithms, malware detection, and firewall protection to avoid intrusion into the internal network of the aircraft. The inter patch network is focused heavily on secure radio resource management using multidimensional physical and MAC layer diversity (retransmission control), as well as MIMO allocation. Other functionalities in this inter-patch network are troubleshooting, energy management, flow state estimation, and actuation control.

The functionalities in L1 are mainly focused on the scheduling of traffic of the AFC system into the internal commercial real-time network of the aircraft (using the standard ARINC 664). Other functionalities include the following: quality of service control, flow management, secure encryption, traffic analysis to avoid malware intrusion, etc. The Bubble gateway has upper layer functionalities of routing in the internet, sensor data fusion, actuation control/update, sensor node virtualization, tunnelling, authentication of external users, key distribution, intra AFC system management, traffic control, dependability insurance mechanisms for real time internal networks, device management, etc. Secure Socket Layer (SSL) is one of the options in evaluation to be implemented at the L1 and L2 network levels of the aeronautics architecture. An extension of the concept of virtual link (VL) used in the standard ARINC 664 is also under consideration to be used in the wireless domain.

Other associated functionalities to the AFC use case are aircraft collision avoidance using the technology TCAS (Traffic collision avoidance). This refers to the high-level application domain of secure wireless avionics intra communications. The model can also be extended to other structure health monitoring (SHM)-like applications for the aircraft. More details are shown in Figure 7, where some of the interfaces are still under study (TBD- to be defined). The functional view of the reference architecture defines several interfaces between layers as follows:

6.1 Interface DL-NL

The network layer requests the services from the device layer implemented in the patches and the MAC-PHY technology used for the inter-patch communication. The NL is in charge of routing in the network of patches, IP address identification, interoperability with the internal network of the airplane via scheduling, and traffic control. The network layer has also the objective to have a load balance in all the possible AFC networks across the plane, and the matching between the deadlines of the wireline and wireless network. This interface can also host some security functionalities based on IP technology such as IPSEC, tunnelling, secure sockets layer, etc.

6.2 Interface NL-SL

The service layer requests the network layer with the flows of the different patches and wireless networks aggregates of the active flow control system. It is in charge of organizing all the collection of sensor information across the different wireless networks of patches, processing and correcting errors. Intrusion identification is possible by matching the statistics of different networks and comparing to established margins of values. There is also the possibility to detected interference and jammers. Error of the boundary layer tracking or estimation of lift off forces can be used as metrics to estimate malfunction or potential attacks.

6.3 Interface SL-IOTL

The IoT layer allows airliner operator to gather data from aircraft. Authentication of credential of operators, as well as rules for privacy management for integrity or exposure can be implemented in this interface mechanism.

6.4 Interface IOTL-CAL

This interface aims to provide the data of one aircraft to the cloud computing facilities that will calculate optimum actuation policies using the data from different aircraft, airliners and potentially different routes. This will allow us to provide one last level of closed loop control.

6.5 Interface DL-CLM

The main mechanisms for security control in the AFC system are foreseen to be implemented in the MAC-PHY layer. The cross-layer management aims to use this information to improve system performance in different layers. Channel conditions can be used indirectly to estimate flow states and provide redundancy to the sensor information. They can also be used to authenticate, manage and troubleshoot different patches.

6.6 Interface DL-SLM

This interface focuses on the multi-layer security interface with the device layer. Examples of this interface allow MAC-PHY algorithms to identify jammers or directions of eavesdroppers. Node identification using direction of arrival or statistical signal processing are also possible. Redundancy of source and channel coding can be used.

6.7 Interface NL-CLM

In this interface the network layer provides information to cross-layer optimization algorithms, Routes, Addresses, traffic state, quality of service, etc. are some of the metrics and information that can be requested through this interface.

6.8 Interface NL-SLM

The network layer interacts with the security layer management via a set of specific protocols. Tunnelling, virtual links, security layers, etc. are examples of specific implementations of this interface. In the aeronautics use case there is no expected usage of this interface.

7 Vulnerability and attack model(s)

Vulnerability and attack models are being developed for different layers of the aeronautics architecture. A useful reference model used in the SCOTT reference architecture and across the literature of security of IT systems (Common Criteria) is displayed in Figure 8. The important aspect from this framework is to identify the main asset, the associated vulnerability, and potential threats(s). From this information it is possible to define the actions that the stakeholders are willing to implement to reduce risk. The following tables show the vulnerabilities identified so far and potential solutions.

, Table 2, and Table 3 present the vulnerabilities and potential solutions for L0, L1, and L2 layers, respectively. The tables follow the functional model of the SCOTT reference Architecture.

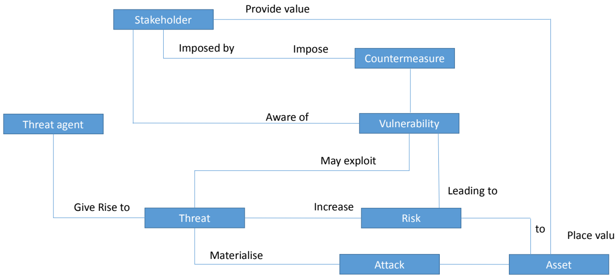


Figure 8 The Common criteria conceptual model for security

Table 1: Vulnerabilities, threats and solutions AFC L0

Layer	Vulnerabilities	Potential solutions
CAL	N/A	N/A
IOTL	N/A	N/A
SL	DDoS	Packet analysis, authentication
NL	DoS, spoofing, MiM	Authentication, encryption,
DL	Jamming, eavesdropping, collision, Integrity.	MIMO, beamforming, blind processing, rotational invariance techniques, multi-objective optimization

Table 2: Vulnerabilities, threats and solutions AFC L1

Layer	Vulnerabilities	Potential solutions
CAL	Spoofing, Identity theft	
IOTL	DoS, latency issues	
SL	Replay attack	
NL	DoS, spoofing, MIM	Authentication, encryption,
DL	Interference, congestion, spoofing	MIMO, scheduling, traffic shaping, authentication, PHY-layer assisted control and sensor aggregation

Table 3: Vulnerabilities, threats and solutions AFC L2

layer	Vulnerabilities	Potential solutions
CAL	Data integrity, lack of privacy, lack of confidentiality, Spoofing, Identity theft	
IOTL	DoS, latency issues	
SL	Replay attack	Firewall L3, tunnelling, Key distribution
NL	DoS, MiM	Authentication, encryption,
DL	Spoofing	PHY-layer assisted control and sensor aggregation, authentication

Figure 9 shows the loop of actuation control and the potential security issues that can be found along that loop and the entities involved in the process of the aeronautics use case. The intra-patch technology can be subject to software and hardware malfunctions, hacking attacks that take over the control of some patches operating system or transmission units. Some software verification, safe-mode operation, or firewalls can be used to avoid these problems inside the patch. The patches aim to reliably collect information of the state of the flow, and also implement the optimum actuation policy with the lowest delay to reduce risks of incorrect operations, or instability of the aircraft. It has been identified in previous deliverables that attacks such as denial of service or jamming that can completely disable the AFC system are not the most serious types of threats, provided the system is identified as unavailable. The most serious threats in the AFC case is when the information collected by the patch has been mismanaged or that its integrity is lost due to man in the middle, spoofing or replay attacks. This means that the control logic of the AFC system will decide actuation policies that are incorrect and therefore will affect the efficiency of the system in terms of loss of lift off forces, reduced efficiency in skin drag reduction, and eventually in fuel consumption increase, reduced range, payload capacity or aircraft speed. Therefore, particular attention will be placed on attacks where the data integrity of the sensors or the loop to disseminate actuation policies is compromised. In the network of patches, MIMO (multiple input multiple output) will be used to construct an efficient way to manage the wireless transmissions to reduce risks of eavesdropping attacks, counteract jamming, identify compromised patches, authenticate and authorize spatially-based transmissions, and provide redundancy to the measurements of the state of the flow aggregated from al the patches across the airplane.

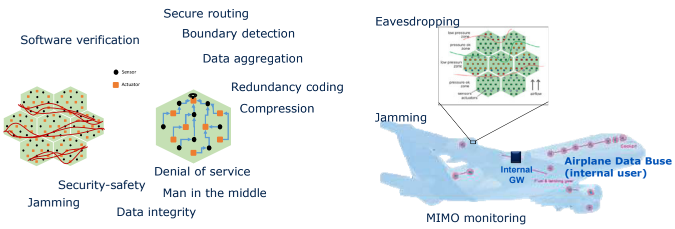


Figure 9 Security analysis of the ACF use case

Currently four attacks and security solutions are being considered in this use case. An interference jamming attack model is being considered using direction of arrival detection, higher layer detection using statistical tools or a simple passive footprint stochastic geometry model to reduce the potential attacks from pre-established directions in the aircraft. This information about the attacker, either active or passive is used in the adaptation, retransmission control, MIMO resource allocation or beamforming solution. These processes are illustrated in Figure 10.

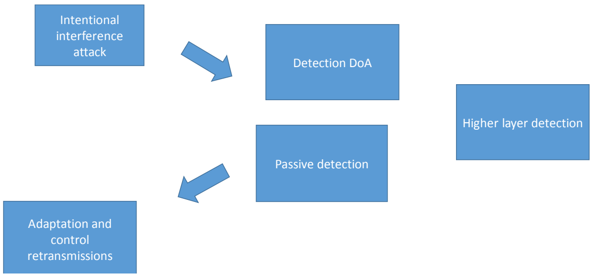

Intentional interference attack
Detection DoA
Higher layer detection
Passive detection
Adaptation and control retransmissions

Figure 10 Interference attack model and countermeasure

Eavesdropping is a passive attack common in wireless applications. When using MIMO to manage the information transmitted in different spatial direction, it is possible to deal simultaneously with the reduction of interference and the leakage of information to insecure directions where eavesdropper might be detected or where there is a high risk. The model is shown in Figure 11.

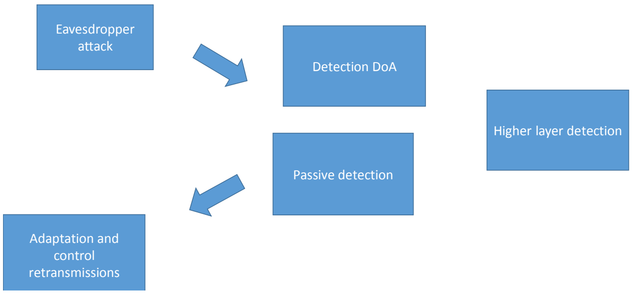


Figure 11 Eavesdropping attack model and countermeasure

Intrusion attack can lead patches to have incorrect or undesirable behaviour, producing data or incorrect feedback to the loop control. Mechanisms are being developed to provide redundancy about the flow state sensed by different patches. These mechanisms are based on a combination of physical MAC and higher layer reasoning processes. The idea is to detect patches that have been compromised and adapt all the network to reduce the influence of a compromised patch. The process is shown in Figure 12.

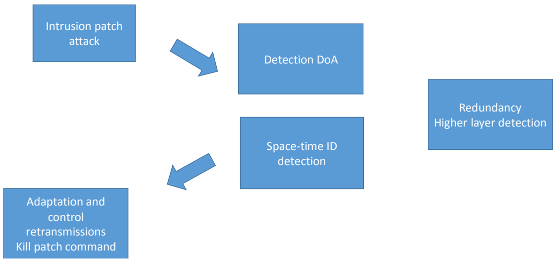

Intrusion patch attack
Detection DoA
Redundancy Higher layer detection
Space-time ID detection
Adaptation and control retransmissions Kill patch command

Figure 12 Intrusion attack and countermeasure model

Higher layer attacks are also being considered. A denial of service attack (see Figure 13) can be launched in the internal network of the aircraft, producing the lack of contact of the patches with the control unit on board the plane. Different approaches are being considered to address this issue, for example the triggering of an autonomous operation by the network of patches, distributed decision making, etc.

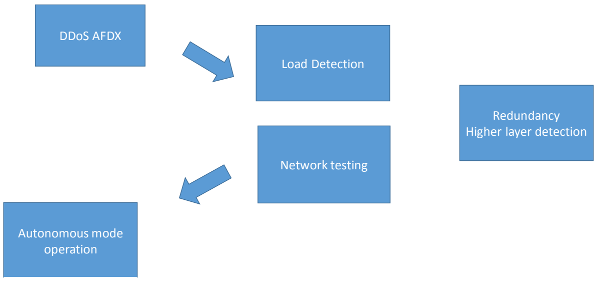


Figure 13 DoS attack and proposed countermeasure model

Conclusions

This paper has presented the architecture of the aeronautics use case for secure WAICs. Interface, objectives, requirements and preliminary vulnerability and security analysis have been conducted. The aeronautics industry will benefit from a detailed security analysis of interfaces in the context of modern IoT systems and architectures. SCOTT expects to cover several aspects in the coming years.

Acknowledgments

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway. Funded also by FCT/MEC, ERDF (European Regional Development Fund) under PT2020, and by CISTER Research Unit (CEC/04234).

References

[1] D. Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything.* Available at http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] N.L. Armstrong and Y. M. M. Antar (2008), *Investigation of the Electromagnetic Interference Threat Posed by a Wireless Network Inside a Passenger Aircraft*, IEEE transactions on Electromagnetic Compatibility, vol.50, no.2, pp.277-284.

[3] ITU (International telecommunications Union), *Characteristics of WAIC systems and bandwidth requirements to support their safe operation*, Working document toward a new technology report.

[4] D. Dang, A. Mifdaoui and T. Gayraud (2012), *Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential solutions*, Wireless Days (WD) IFIP.

[5] SCOTT JU Grant Agreement incl. Description of Action (DoA), ECSEL Joint Undertaking, Grant Agreement No. 737422, Part B, 2017-05-18.

[6] DEWI JU Grant Agreement Annex 1 – Description of Work, 2016-12-16.

[7] R. Samano-Robles, T. Nodstrom, W. Rom, S. Santoja, and E. Tovar (2016), *The DEWI high-level architecture: Wireless sensor networks in industrial applications*, Eleventh International Conference on Digital Information Management (ICDIM), Porto.

[8] J. Liu, I. Demirkiran, T. Yang, and A. Helfrick (2008), *Communication schemes for aerospace wireless sensors*, IEEE/AIAA 27th Digital Avionics Systems Conference, 2008, 26-30.

[9] L. N. Long and S. J. Schweitzer (2004), *Information and knowledge transfer through archival journals and online communities*, AIAA Paper 2004-1264, Aerospace Sciences Meeting, Reno, NV.

[10] S. Field, P. Arnason, and C. Furse (2001), *Smart wire technology for aircraft applications*, Proceedings of the 5th Joint NASA/FAA/DoD Conference on Aging Aircraft, Orlando, FL.

[11] T. Stone, R. Alena, J. Baldwin, and P. Wilson (2012), *A viable COTS based wireless architecture for spacecraft avionics*, IEEE Aerospace Conference, Big Sky MT, pp. 1-11.

[12] K. Sampigethaya, R. Poovendran, L. Bushnell, L. Mingyan, R. Robinson, and S. Lintelman (2009), *Secure wireless collection and distribution of commercial air-plane health data*, IEEE Aerospace and Electronic Systems Magazine, vol.24, no.7, pp.14-20.

[13] D. Graham-Rowe (2009), *Fly-by-wireless set for take-off,* New Scientist, vol. 203, pp. 20-21.

[14] M. Harrington (2011), *Introduction to wireless systems in aerospace applications*, Proceedings of the CANEUS "Fly-by-Wireless" Workshop, Montreal, Canada.

[15] O. Elgezabal (2010), *Fly-by-Wireless (FBWSS): Benefits, risks and technical challenges*, CANEUS Fly-by-Wireless Workshop, Orono, ME, USA.