CHALLENGES OF SECURITY AND TRUST IN AVIONICS WIRELESS NETWORKS

Raja Naeem Akram, Konstantinos Markantonakis, Royal Holloway, University of London. Egham, UK
Sharadha Kariyawasam, Shahid Ayub, HW Communications Ltd. Lancaster, UK
Amar Seeam, Robert Atkinson, University of Strathclyde, Glasgow, UK

Abstract

Avionics networks have a set of stringent reliability and safety requirements. In existing deployments, most of these networks are based on wired technology which provides a high degree of reliability and safety. Furthermore, it simplifies the security management of the network since certain assumptions, including an inability for an attacker to access the network, can be safely made. The proposal for having an Avionics Wireless Network (AWN), currently being developed by multiple aerospace working groups, promises reduction in the complexity of electrical wiring harness design and fabrication, reduction in wiring weight, increased configurability, and potential monitoring of otherwise inaccessible moving or rotating aircraft parts. While providing these benefits, the AWN must ensure that it provides, at a minimum, equivalent levels of safety to those offered by the wired network. Substituting the wired network with a wireless network, even for a specific set of well-defined and non-critical tasks, brings a whole set of new challenges related to assurance, reliability, and security. In this paper, we discuss the security and trust challenges an AWN deployment might face, along with highlighting potential directions for solutions. Furthermore, as a case study we will elaborate on AWN deployment variants especially the wireless as a comm-link. Finally, the paper makes suggestions that set the agenda for security, reliability and trust work that could, if successful, provide an AWN system meeting the required safety standards.

Introduction

Modern aircraft are a collection of highly reliable, efficient and fault-tolerant computer systems and distributed real-time networks. Avionics Data Networks (ADNs) inter-connect multiple avionics sub-systems, enabling data and control messages to be communicated within a predefined time frame and in a predictable manner. A number of time-, mission- and safety-critical functions of an aircraft are dependent upon efficient and reliable communications. Furthermore, even the non-critical functions are dependent upon ADN services. Therefore, an ADN has to provide adequate service and fault-tolerance levels for both the critical and non-critical functions. Managing these two functions can be challenging and providing a deterministic network with guaranteed bandwidth and Quality of Service is pivotal for the ADN's adoption [1].

Traditionally, ADNs are built upon physical connections using wires that connect various avionics systems. Examples of such networks include ARINC 825 [2], ARINC 664/AFDX (Avionics Full DupleX Switched Ethernet) [3], [4] and standard Ethernet. However, the avionics industry is always looking for a more flexible and scalable architecture to support future avionics systems with a broad spectrum of capabilities and performance requirements [5]. One aspect of future digital avionics is the applicability of the Avionics Wireless Network (AWN), in which wireless communication partially replaces the wired network in an aircraft. This has the potential to reduce the design complexity of wiring, harness design and fabrication, reduce the associated weight of wires, increase configurability due to installation flexibility (e.g. for cabin elements) and reduce maintenance cost/time. In this paper, we briefly discuss this emerging trend, and examine selected proposals and deployment architectures to provide the necessary background to the main topic of the paper. Subsequently, we discuss the AWN variant wireless-as-as-comm-link, its rationale and brief design objectives. Finally, we discuss the security and trust challenges AWN has to overcome and provide potential solutions.

978-1-4799-8940-9/15/$31.00 ©2015 IEEE

Aircraft Data Networks

In this section, we briefly discuss a generic architecture for ADNs. The purpose is to build a foundation on which to base the rationale put forward for the AWN proposals.

Brief Introduction

Avionics systems consist of a multitude of sub-systems interconnected using wired technology as shown in figure 1. Different avionics sub-systems are connected with end systems that are then interconnected with a backbone network such as ARINC 429 [6], ARINC 825 [2] or AFDX (ARINC 664 Aircraft Data Network, Part 7) [3], [7].

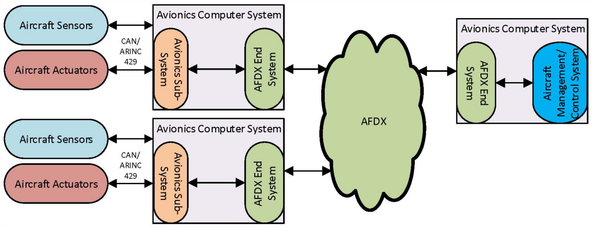

Figure 1. Generic Avionics (Flight-Control and/or Crew) Data Network with AFDX as an Example

For some specific sub-systems, there are sets of sensors and actuators connected on CAN [8] or ARINC 429 buses for flight control systems [9]. The AFDX or similar technology interconnects time- and safety- critical subsystems like environmental control, doors and other utility systems. The AFDX backbone also connects lower criticality subsystems like displays providing safety information to passengers, oxygen masks and triggers of oxygen flow and audio announcements, and it manages the quality of service accordingly. There are some suggestions to move the flight control system to the AFDX [10]; however, the authors at the time of writing are not aware of any such deployment.

In addition to the flight-related network, in a modern aircraft there is also the possibility of having an entertainment network, shown in Figure 2, serving the passengers. The entertainment network can be supported using standard Ethernet technology. Therefore, they do not have to provide a high level of reliability or safety features. Between different avionics systems like flight entertainment and cabin environmental controls, there might be physical separation or stringent firewalls at the gateway between them. In any case, the type and nature of the network configuration is dependent on the deployment scenario and objectives. However, there is a possibility that the flight control network, crew network and passenger (entertainment) network are all supported by the same wired technology, requiring implementation of network segregation with robust gateways and security policies [11].

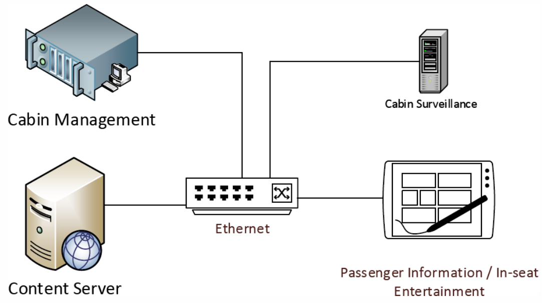

Figure 2. Generic Avionics (Cabin) Data Network

Whatever the deployment topology and the communication technology used, one element is common; the physical wire that connects two or more avionics subsystems. Wiring an aircraft can be costly in that it includes wiring harness designs, cable fabrication and the associated cost of additional weight. Potentially, wires and related connectors represent 2-5 percent of an aircraft's weight [12]. Wiring harness design determines wire routes while providing separate routing paths for redundant wiring to provide robust redundancy. As the wiring of an aircraft is a time- and labour-intensive activity, post-deployment upgrades or installation of new wire routes or avionics subsystems may be costly [13]. As reported by [12], roughly 30 percent of wires are potential candidates for wireless substitutes. Therefore, potential of a wireless solution, possibly in a limited deployment in an aircraft, has reasonable prospects.

Avionics Wireless Network

In this section, we briefly discuss the Avionics Wireless Network (AWN), its different proposed formats, and include a short discussion of work related to AWN and/or security in AWN. In this paper, when we mention AWN our comments are restricted to networks that are on board an aircraft and do not include air-to-ground, air-to-satellite, or air-to-air communication. Our discussion also does not include passenger communication (Wi-Fi) if present in an aircraft.

Brief Introduction

We define an AWN as an aircraft network that for inter-connectivity between its different components deploys some wireless technology instead of using physical wires. Based on this, we can classify AWNs into four overlapping deployment architectures that are briefly discussed below:

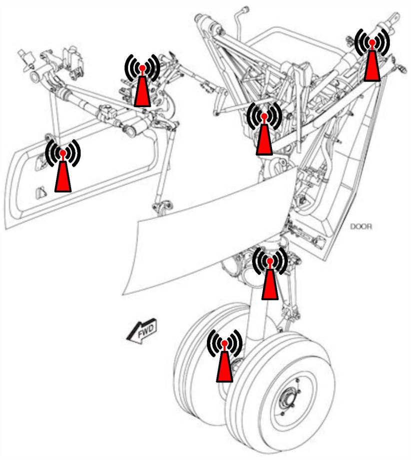

Figure 3. A Generic Front Landing Gear WSN

Wireless Sensor Networks (WSN): A WSN is a collection of intelligent and autonomous agents capable of monitoring physical or environmental conditions. The WSN nodes record the designated data and communicate via a wireless medium to a collection (or sink) of nodes that then communicate over wireless or wired media to the required destination. Such networks are particularly useful in aircraft design if we need to monitor moving and/or rotating parts; for example, landing gear monitoring systems [12] or engine health management [14].

Figure 3 depicts a generic architecture for deploying a WSN to collect safety-related data from the landing gear and communicate it to the pilot. The sink node can be connected to an AFDX end system and the data collected is communicated, using a wired network, to the aircraft cockpit. A WSN is beneficial in such environments as it does not require extensive cabling to function and to communicate data back to the aircraft network. Furthermore, aircraft WSNs do not have to be connected with the aircraft network. They can simply be independent networks that collect and store flight-related data, and an on-ground maintenance crew can offload this data for effective and efficient aircraft management.

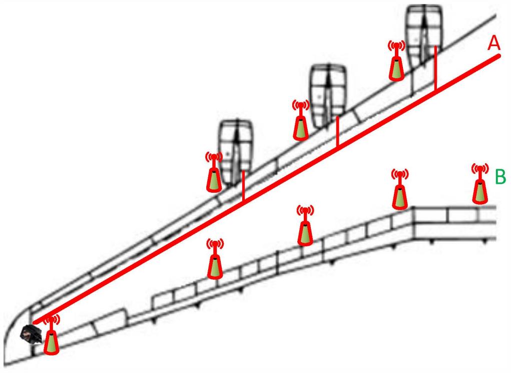

Figure 4. Generic View of Wired and Wireless Hybrid Network Over an Aircraft Wing

Dissimilar Redundancy Network (DRN): Aircraft networks must be fault-tolerant. This design requirement mandates aircraft designers to build redundant components and wiring harnesses. Aircraft designers try to route the wires from physically different locations as much as possible and as permitted by the aircraft geometry. However, building redundant networks based on the same technology might be susceptible to “common mode failures". This might have a very low probability but a potential for common mode failure cannot be neglected.

Figure 4 illustrates a potential deployment architecture that can provide redundancy through dissimilar network technologies, which might enhance the overall reliability [15] in some critical situations compared to “identical redundancy" [16]. In Figure 4, the wired network is represented by label ‘A’ and the wireless network by label ‘B’.

Inflight Entertainment Network: One of the least critical networks on-board an aircraft is the Inflight Entertainment Network (IFE). The objective of this network is to provide individual passengers with multimedia content and flight information (if deployed). We have already depicted the IFE in Figure 2, and

Figure 5 illustrates the same network but with wireless as the medium of communication [17].

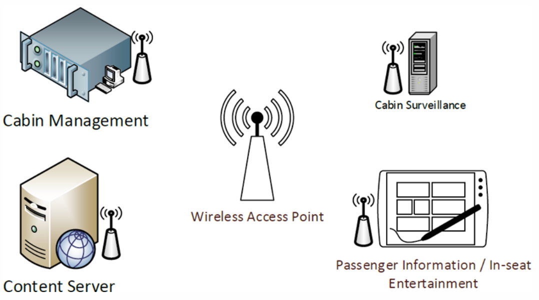

Figure 5. Wireless Passenger Entertainment • ••• ork• •

Building a wireless network for passenger entertainment can enable an adaptive cabin configuration and/or customisable services.

Wireless as a Comm-Link: In this type of AWN, a wireless communication network replaces the wired link between avionics computing modules. The protocols and the network architecture above the data link layer can still be the same, only at the physical layer, the data is communicated via a wireless medium rather than a wired medium. As shown in Figure 6, wireless connectivity only substitutes the wires that interconnect the avionics sub-systems.

For a more complex deployment, multiple avionics systems might interconnect with each other via a switch. In this case, the depiction in Figure 6 would be same except the wireless link would be between the (selected) avionics systems and the switch. One thing to note is that data paths (routing in a predefined manner) might be handled by the avionics systems and wireless technology is only used to transmit data packets between two points. If there is a redundancy in the wired network then it can be substituted for a redundancy in the wireless network where both data paths are over wireless, unlike the DRN. This deployment has the potential to replace selected wired networks on board an aircraft without any major modifications to existing applications/systems. The proposal discussed in the subsequent sections is more or less compatible with this deployment model.

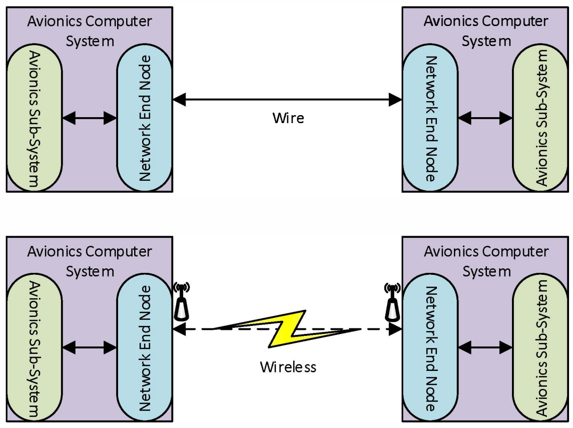

Figure 6. Generic Representation of Wireless as a •••••••••••••••••••••••••••••• omm•Link

The discussion in this section was restricted to AWNs based on their deployment architectures and how they utilise wireless communication to establish connectivity. For discussion on AWN classification based on data rate and system locations, please refer to [12].

Related Work

Wireless Sensor Networks and wireless technology itself have gained substantial attention in both the academic community and industry. They are well studied for their security and trust issues and several proposed solutions have been put forward. There is some work in the public domain that is associated with wireless networks on board an aircraft. However, at the time of writing, the authors were not aware of any work addressing concerns related to the security of such networks in an aircraft.

One of the initial discussions around AWNs was in the WSN deployment model [18], [19] that proposed a sensor network to monitor engine health. Wireless technology has also been proposed for aircraft maintenance systems [20]. Security and trust have also been subject to some analysis by both the academic community and industry. A brief overview of aircraft information security and some improvements were proposed in [21]. Security assurance research encompassing airplane production to operation was presented in [22], [23]. A general discussion on the security issues related to the aircraft network and aircraftsâĂŹ connectivity with the Internet is discussed in [24], while [1], [11] discuss the impact of the WSN and related security concerns deployed in the aircraft. Security and safety are intrinsically linked to each other in general and specifically in the context of the aviation industry [25]–[27]. The application and impact of cryptography, especially public key cryptography for avionics networks, was evaluated in [28].

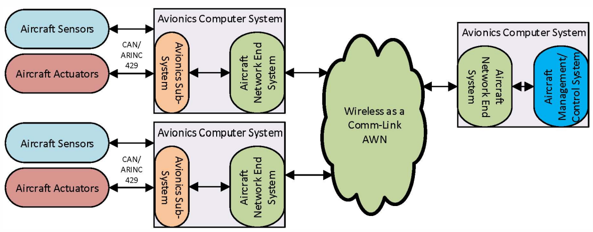

Figure 7. Generic Architecture of an Aircraft Network with AWN as Wireless as a Comm-Link

The treatment of security and general deployment of AWNs based on wireless-as-a-comm-link has not been extensively analysed, either by the academic community or industry. However, general guidelines and experience in designing wired aircraft networks and WSN are still worth mentioning, as current and related future work is based on them.

AWN Case Study

In this section, we will discuss an example of a potential wireless comm-link AWN. This is then considered as a running example for related security and trust issues faced by an AWN in the context of this paper. Figure 8 illustrates the generic architecture of an aircraft network with an AWN deployment.

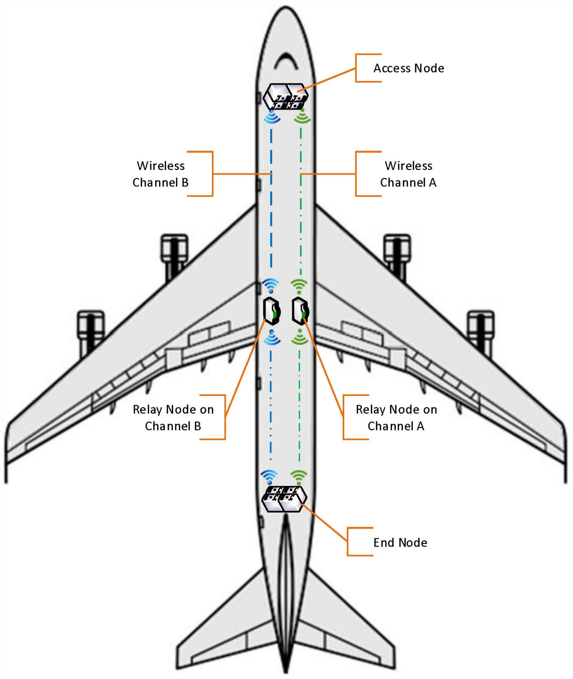

Figure 8. Generic AWN Architecture

Basic Architecture

As discussed before, a wireless-as-a-comm-link AWN should be a seamless replacement of a wired connection in the existing aircraft network. Figure 8 depicts a simple representation of an AWN with three types of AWN nodes.

- Access Node: A node that is connected to the existing aircraft network (wired network), which can be an AFDX and/or avionics data bus. This node acts as an interface to the AWN that connects with the main aircraft systems, through which the avionics systems can communicate with the end devices (e.g. sensors, actuators, displays, etc.).
- End Node: A node that is connected to one or more of the end devices such as sensors, actuators and displays. It acts as an interface node connecting the end devices with the AWN and with the rest of the avionics system.
- Relay Node: A node that connects the access and end nodes. In a multi-hop connectivity, relay nodes act as the communication conduits between the access and end nodes. Relay nodes only interface with the access and end nodes and only avionics systems can connect with them.

There are two communication paths, represented as “wireless channel A and B" and each path may have relay nodes (one or more). The actual wireless band and communication channel are dependent on the deployment environment and any related specification/standardisation for such networks at the time of deployment. From the security point of view, band and communication channels are important, especially as related to wireless jamming and Denial-of-Service (DoS) attacks. In this paper we do not investigate the details of different bands and communication channels; however, we do discuss attacks related to them. To provide dissimilar redundancy (in a limited sense), individual wireless links can be on different bands and channels.

Security and Trust Challenges

In this section, we discuss the threat model, along with potential attacks on and security objectives of an AWN.

Threat Model

The threat model in this section consists of two elements related to an adversary. The technical capability of an adversary and his/her objectives are discussed individually in the sections below:

Adversary's Capability: An adversary's capability is based on his/her technical knowledge and the financial support he/she has to achieve a particular attack. The adversary in the context of the AWN has the capabilities listed below:

- Has the ability to receive and transmit data on any wireless link, regardless of the underlying technology being deployed.
- Has knowledge of the AWN's inner workings. There is no design element that is unknown to the adversary.
- Can monitor network activity while the aircraft is on the ground or in the air.
- Has the ability to inject traffic only onto a limited set of communication (wireless) links on board an aircraft.
- Can acquire AWN nodes, either new nodes from the manufacturer or a recycled node (decommissioned node).
- From a computational point of view, the adversary has more resources than individual nodes on the AWN.

The limitations imposed on the AWN adversary are listed below:

- Does not have the capability to break any cryptographic algorithms, as long as they are deployed in a standard/recommended manner.
- Does not have physical access to the AWN nodes while they are in operation on board an aircraft.
- Does not have access to the aircraft system that is connected to the AWN.

Adversary's Objective: Based on the adversary's capabilities, an adversary might aim to achieve one or more of the goals listed below:

- Reduce the network efficiency (transmission capability) over a particular link.
- Modify the commands or instructions in a manner that allows the adversary to achieve his/her goal; for example, turn off the entertainment system.
- Compromise an AWN node (or nodes), so the adversary can read all the communication data (unencrypted)
- Introduce an AWN node into the network as a trusted node, then collect vital network and aircraft information from this (introduced) node.
- Depending upon the criticality of the aircraft systems that are connected with the AWN, try to effect his/her operations.

Challenges to the AWN

In this section, we discuss some of the well-known attacks that could potentially occur in the AWN environment. We also briefly explain what the AWN can do to avoid the listed attacks.

ARP Spoofing Attack: In communication networks, ARP (Address Resolution Protocol) spoofing attacks involve an adversary trying to associate his Media Access Control (MAC) address with the IP address of a genuine node. The AWN environment can avoid this by building a strong predefined binding of an MAC address to the IP address. In addition, the MAC address can be bonded with the node authentication based on asymmetric cryptography.

MAC Spoofing: In this scenario, an adversary changes the MAC address of his or her device to that of a genuine device. The adversary will then try to connect to the network in such a manner that other devices (or networks) will consider it the genuine device (whose MAC address it is spoofing). As discussed in the previous attack, if the MAC address is bonded to the node authentication based on asymmetric cryptography then the potential of success for this attack is very low.

Replay Attack: An adversary captures a message or a communication session, which he or she then replays back to one of the original participants. The purpose of this is to trick one the original participants into accepting the adversary's device as the genuine communication partner, with which previous communication was established. If each wireless link (access node and relay node, or end node and relay node) in the AWN environment is encrypted with a session key (generated at the start of the session), replaying messages from a previous session will not succeed. If the adversary replays messages from the same sessions, the communicating entities can detect the replayed messages either due to repeated message indicators, failure of the message to decrypt properly, and/or message sequence number.

Man-in-the-Middle (MITM) Attack: The aim of a MITM attack is establish secure and/or trusted connections between two entities by an adversary in such a manner that both of the genuine entities do not know of the existence of the adversary in the middle. The adversary has the capability to read unencrypted messages and can modify them as required. In the AWN environment, when new sessions are established, entity authentication is based on asymmetric cryptography. All entities involved in this process have an existing knowledge of the credentials of the communicating entity (via predefined knowledge of the public keys of the communication partners). This pre-existing knowledge, a secure challenge-response based entity authentication and session key generation make it difficult for an adversary to successfully mount an MITM attack.

Compromising a Node: An adversary takes control of an AWN node, either because he or she has physical access to the device and exploits a vulnerability to gain control, or by remotely exploiting the node. In either case, the objective of the adversary is to gain control of the node; if successful, the adversary can read all communications in plaintext (intended to be handled by the respective node) and modify the communication. This attack enables an adversary to become an active part of the AWN, which poses a severe risk for the AWN and the potential safety of the aircraft. To avoid such attacks, physical access to the nodes should be limited (and controlled, giving access only to authorised staff) and no connection or communication packets should be processed without data origin authentication. Furthermore, all fail-safe and/or fail-back states should be as restricted as possible to avoid any unforeseeable situations.

Introducing Decommissioned Node: In this scenario, the attacker gains access to a decommissioned node and tries to reverse-engineer it to retrieve any node-specific secret values, such as security parameters and cryptographic keys. The attacker then clones this information into a malicious node and then tries to introduce the node to an active AWN on board an aircraft. Protection against this potential scenario is to avoid using the same security-sensitive parameters and cryptographic keys in all of the AWN nodes across the same aircraft or within a fleet of aircraft. All cryptographic keys should be unique to an individual node and communication link (whether logical or physical). Furthermore, AWN nodes should be tamper-resistant to avoid any data retrieval as far as possible. Finally, at the time of decommissioning, the security credentials of the decommissioned nodes should be blacklisted so no-one can use these credentials to authenticate to the AWN network.

Eavesdropping on the Communication Channels: An adversary listens to the communication medium; however, the concern is not whether an adversary can listen or not, since it is very difficult to avoid eavesdropping on a wireless channel. Rather, we are only concerned with what information an adversary can gain from eavesdropping. If the adversary does not gain any additional knowledge of the network or the aircraft functions after eavesdropping on the communication channels, we would consider that the network is secure. To provide this, all communication between logical and physical links in the AWN is encrypted using unique session keys that expire at the end of each session, where a session is a single aircraft flight.

Packet Redirection Attack: In this attack, an adversary captures a packet, changes its destination address and injects it back into the communication channel. If the adversary swaps the destination and sender's addresses then the sender will receive the message back. This is referred to as a reflection attack and we consider it a variation of the packet redirection attack. For an AWN that uses unique session keys per communication channel, changing the destination would not be useful as the destination node will drop the packet because it cannot verify the integrity of it. Reflecting the same packet back to its sender will only increase the load on the sender node, which can easily verify whether the packet was intended for it or not.

Denial of Service (DoS) Attack: For communication networks, one of the most difficult attacks to avoid is the Denial of Service (DoS) attack. In this attack, an adversary stresses either the communication channel or the computational capability of the target node to the extent that it either downgrades to no-security state to maintain the Quality of Service (QoS) or stops functioning properly (dropping large numbers of packets, with QoS degradation and potential shutdown). It is difficult to completely avoid a DoS attack; however, having dissimilar redundancy and the potential to change wireless channels (to predefined values) can limit the impact of such an attack.

Random Frame Stress Attack: In this attack, source and destination address are kept the same but all other data fields of a packet are randomly changed to see whether it induces any errors when the target node processes the information. This attack is usually successful when the target node processes the packet, encounters an error and tries to recover in a manner in which it does not have to drop the packet (for QoS reasoning, as an example). However, in an AWN the data load of the communication packets can be protected by cryptographic integrity making, so any modification in this field would be detected. For remaining fields, if they do not conform to the predefined structure, the node would simply drop the packet before processing it.

Wireless Jamming: In this attack, an adversary tries to block all communication on wireless frequencies. The adversary's aim is to disrupt wireless communication. An AWN may deploy individual links on different channels on different frequency bands (like 2.4Ghz and 5Ghz). However, a multi-spectrum frequency jammer can be used to jam not all but a limited segment of the AWN. It is easy to detect an attack, and a frequency change might give a limited reprieve, but an attacker can easily overcome this.

Forcing Inflight Network Reconfiguration: Aircraft networks have preconfigured architectures with no dynamic reconfiguration. This is assumed to also be true for the AWN and configuration of the network should be done within a safe and secure environment. During the flight, such a critical operation should be prohibited to avoid any unforeseeable issues. Furthermore, if an authorised user can do it, an adversary may also have the potential to achieve this. Therefore, reconfiguration of the AWN should only be carried out when the aircraft is not airborne, and only after environmental sensors have provided a trusted proof that the aircraft is stationary, on the ground and in a safe/secure location.

The attacks and potential risk scenarios discussed in this section are by no means an exhaustive list. However, they provide a representative list of potential issues that an AWN has to overcome for its safe deployment in an aircraft environment.

AWN Security and Trust Objectives

In the previous section, we analysed the AWN environment in the context of potential risk scenarios and how adequate prevention measures could be implemented. In this section, we will discuss the security and trust objectives set for the AWN environment.

Communication Confidentiality: Communication over any physical or logical links should have confidentiality. The content of the communication is significant, not the communication itself. From an adversary's point of view, he or she may still be able to view the data being communicated but cannot make sense of it. Each communication link, whether logical or physical, should have a unique session key. In the AWN environment, it is recommended that session keys expire at the end of each flight.

Communication Integrity: Communication between any two nodes, linked via either physical or logical channels, should have strong integrity. The integrity of the contents of the communication (data) can be achieved using strong cryptographic mechanisms. Depending upon the deployment, the integrity mechanism can be either part of the confidentiality or a separate process. If it is a separate process, then the integrity process will also have its own unique session key.

Node-to-Node Secure Channel: Individual pairs of nodes that have a direct wireless connection, for example in the case of access node to relay node, relay node to end node and relay node to relay node, should have a unique secure channel. This channel can be used for communicating system information and to disseminating any network announcements.

Ingress-to-Egress Secure Channel: Any data entry and exit point should have a unique secure channel. An example of such a channel is between an access node and end node. It is technically a logical channel and all the relay nodes in between cannot read the contents of a communication. Relay nodes take the encrypted data and forward it to the required destination.

Asymmetric Cryptography-based Entity/Node Authentication: Individual nodes, when they establish a secure channel with their pre-defined partners, should include node authentication. The authentication process should be based on challenge-response mechanisms using asymmetric cryptography.

Remote Node Trust Verification and Validation: Any node in the network or a trusted external entity should be able to verify the current state of an AWN node. In this objective, AWN nodes can be interrogated to provide proof that the current state (both hardware and software states) of the node is trustworthy.

Trusted Boot for AWN Nodes: AWN nodes should have a trusted boot mechanism to verify and validate that the node is booted into a secure and verifiable trusted state. During the node authentication and secure channel establishment, a node might have to produce a proof that validates its trusted state. Any malicious or accidental changes to the secure state of a node should be detected and reported in a secure manner, so maintenance staff can take adequate measures to protect the overall AWN network.

Link High-Availability: Wireless channels are susceptible to environmental and malicious interference. Therefore, at the time of designing the deployment of the AWN environment for a particular aircraft, adequate measures should be taken to avoid any environmental interference. Furthermore, necessary measures should be taken to detect and notify network administrators of any malicious interference.

Secure Fail-Back Mechanism: In all likelihood, some of the AWN nodes will fail either in an operational or a security context. In any context, the fail-back mechanism should be as restrictive as possible. The rationale behind this restriction is to avoid providing a potential opportunity to an adversary to infiltrate the AWN environment through the fail-back mechanism. Furthermore, it is challenging to predict all possible failures that an AWN node might experience, so from a security point of view, a restricted fail-back mechanism is preferable.

Holistic Approach – From Manufacturing to Decommissioning

A better approach to security is to embed security into the system from the beginning. Therefore, for the AWN environment, security-related measures have to be incorporated, managed and followed at every lifecycle stage. In this section, we walk through the lifecycle stages of the AWN node and environment and list the actions that should be taken and actions that should be avoided.

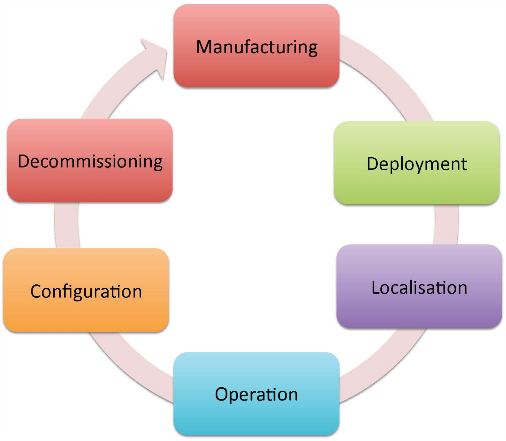

Figure 9. AWN LifeCycle

Manufacturing: Security must be taken into account at the manufacturing stage of the nodes. The manufacturing stage is concerned with the creation of the hardware and the associated core operating system. At this stage, the important elements are to build all security-related functions and disable any reprogramming or debugging functionalities.

Deployment: At the deployment stage, the board is manufactured and securely delivered to the aircraft manufacturer, who then starts to build it for a particular role in the AWN environment. Each of these boards can be built as access/end nodes or relay nodes. At this stage, a secure operating system is installed and security parameters should be initialised or configured. Also, necessary care should be taken at this stage to avoid any disclosure of security parameters to malicious entities.

Localisation: In this stage, the AWN environment is up and running but under the control/management of the aircraft manufacturer. Either the airline can keep it in this setting or they can take ownership of the network. This stage configures the AWN environment to the needs of its user (i.e. airline and/or aircraft maintenance crew/company). Necessary precautions should be taken to avoid any information disclosure or compromise that enables an adversary to be included as a trusted entity in the AWN configuration.

Operation: During the flight, the AWN would be in “Operation" stage. This is a lock-down stage of the

AWN's lifecycle. At this stage, no security parameters should be allowed to be changed.

Configuration: During the lifetime of the AWN, modification may be required in the form of either network configuration or removal and inclusion of AWN nodes. Before the AWN moves to configuration mode, its mode transition should require strong authentication. Only trusted users or entities should be allowed to authenticate to the AWN in this stage.

Decommissioning: At the end of the lifecycle of the AWN node, it should be properly decommissioned. Recycling should be carried out in a manner that ensures all security-related parameters are completely removed and the node itself is entered as a blacklisted node in the AWN configuration.

Future Research Directions

In this paper, we have put forward a foundation for the security and trust services provisioned for and/or by an AWN. However, the discussion is by no means an exhaustive treatment of these challenges. There are multiple aspects of security and trust validation that still need to be analysed and in this section we briefly discuss some of them.

Trusted Boot and Remote Attestation of an AWN Node

Trusted boot is the combination of both secure and authenticated boot processes. The trusted boot process measures certain properties of the succeeding boot component (in the boot configuration) and if the properties do not satisfy the security requirement, it terminates the boot process. In addition, the trusted boot process can provide a validation to a third party about its trusted state, when requested. Part of this future work would be to analyse the existing trust boot architectures and evaluate their suitability for the AWN nodes. Additional services that can be built using the trusted platform would also be explored. Finally, we will look into the performance issues related to the trusted boot, as one of the main objectives is to have a secure and high-performance mechanism.

Secure and Trusted Channel Protocol with Node Authentication

When the AWN environment is powered on, individual nodes will initiate the process to establish a secure and trusted channel with their pre-defined partners. The secure channel will provide the assurance that the data will be communicated under full confidentiality and integrity provisions. In contrast, a trusted channel ensures that each communicating node is secure and in a state that is trusted by its peers (communicating partner nodes). Together this provides the assurance that data will not only be protected when it is in communication between nodes, but also when it is residing (even temporarily) on each of the nodes.

Secure Management Framework

The management process related to the design, development, deployment and maintenance process has to take a holistic approach and security should be an integral component. In future work, we will investigate the security management issues related to such a network and how effectively procedures can be designed that complement the technical (security) part of the AWN.

Security Specification and Evaluation Framework for Airworthiness

Currently, guidance and specifications covering airworthiness and the associated certification process of an IMA do not fully cover emerging security and potentially privacy (passenger-related data) requirements due to the AWN [19]. In this work, we will investigate how existing specifications and guidance can be applicable to the AWN environment and what changes, if any, are required to accommodate the emerging challenges.

Conclusion

In this paper, we outlined the concept of the AWN and its different variants. There is a valid potential for the AWN to be part of an aircraft network; however, detailed analysis and security considerations are pivotal for the success of any of the deployments. In this paper, we defined an adversary model that might target an AWN and listed the adversaryâĂŹs likely capabilities. We also analysed potential risk scenarios that a generic AWN variant might encounter. In addition, we provided potential solutions for each of the risk scenarios that, if adequately implemented, might avert the risk. The paper also details the lifecycle stages of the AWN and discusses what should and should not be done in the context of security to build an overall secure system. Finally, we detailed some exciting future research directions to investigate specific issues related to the AWN. There is no doubt that extensive work is still required before an AWN can be deployed in an aircraft environment and there are plenty of challenges to overcome. The paper sets the scene for the work to be undertaken to make AWNs a robust and secure proposal.

References

[1] R. V. Robinson, K. Sampigethaya, M. Li, S. Lintelman, R. Poovendran, and D. von Oheimb, “Secure network-enabled commercial airplane operations: it support infrastructure challenges”, in Proceedings of the First CEAS European Air and Space Conference Century Perspectives (CEAS), 2007.

[2] Arinc 825-3: General Standardization of Can (Controller Area Network) Bus Protocol for Airborne Use, English, Online, Standard, ARINC, 2015.

[3] Arinc 664: Aircraft Data Network Part 1 -Part 8, English, Online, Standard, ARINC, 2006.

[4] N. E. din Safwat, M. A. El-dakroury, and A. Zekry, “Article: the Evolution of Aircraft Data Networks”, International Journal of Computer Applications, vol. 94, no. 11, pp. 27–32, 2014, Full text available.

[5] D. Schaadt, “AFDX/Arinc 664: Concept, Design, Implementation and Beyond”, SYSGO, Am Pfaffenstein 14, D55270 Klein-Winternheim, White Paper, 2007. [Online]. Available: http://www.cems.uwe.ac.uk/~ngunton/afdx_arinc664.pdf.

[6] Arinc 429: Digital Information Transfer System (dits), English, Online, Standard, ARINC, 2012.

[7] J. Li, L. Zheng, and J. Yao, “AFDX Based Avionic Data Bus Architecture Design and Analysis”, in Autonomous Decentralized Systems, 2009. ISADS’09. International Symposium on, IEEE, 2009, pp. 1–1.

[8] K. Etschberger, Controller Area Network. IXXAT Automation GmbH, 2001, ISBN: 3000073760.

[9] G. F. Bartley, “Digital Avionics Handbook”, in, C. Spitzer, U. Ferrell, and T. Ferrell, Eds., 3rd. CRC Press, 2015, ch. Boeing B-777: Fly-by-Wire Flight Controls, pp. 29–1 –29–14.

[10] B. Harris and B. Tran, “Fiber Optic AFDX for flight Control Systems”, in Avionics, Fiber-Optics and Photonics Technology Conference (AVFOP), 2012 IEEE, 2012, pp. 15–17. DOI: 10.1109/AVFOP.2012.6344056.

[11] N. Thanthry and R. Pendse, “Aviation Data Networks: Security Issues and Network Architecture”, in Security Technology, 2004. 38th Annual 2004 International Carnahan Conference on, 2004, pp. 77–81. DOI: 10.1109/CCST.2004.1405372.

[12] “Technical Characteristics and Operational Objectives for Wireless Avionics Intra-Communications (waic)”, ITU-R: Radiocommunication Sector of ITU, Tech. Rep. ITU-R M.2197, 2010. [Online]. Available: http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2197-2010-PDF-E.pdf

[13] D.-K. Dang, A. Mifdaoui, and T. Gayraud, “Fly-by-Wireless for Next Generation Aircraft: Challenges and Potential Solutions”, in Wireless Days (WD), 2012 IFIP, 2012, pp. 1–8.

[14] R. Yedavalli and R. Belapurkar, “Application of Wireless Sensor Networks to Aircraft Control and Health Management Systems”, English, Journal of Control Theory and Applications, vol. 9, no. 1, pp. 28–33, 2011, ISSN: 1672-6340. DOI: 10.1007/s11768-0110242-9. [Online]. Available: http://dx.doi.org/10. 1007/s11768-011-0242-9.

[15] E. F. Hitt, “Digital Avionics Handbook”, in, C. R. Spitzer, U. Ferrell, and T. Ferrell, Eds., 3rd. CRC Press, 2015, ch. Fault-Tolerant Avionics, pp. 5–1 –5–25.

[16] J. Downer, When Failure is an Option: Redundancy, Reliability and Regulation in Complex Technical Systems. Centre for Analysis of Risk, Regulation, London School of Economics, and Political Science, 2009. [Online]. Available: http://eprints.lse.ac.uk/36537/1/Disspaper53.pdf.

[17] A. Akl, T. Gayraud, and P. Berthou, “Investigating Several Wireless Technologies to Build a Heteregeneous Network for the in-flight Entertainment System Inside an Aircraft Cabin”, in Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on, IEEE, 2010, pp. 532–537.

[18] B. Nickerson and R. Lally, “Development of a Smart Wireless Networkable Sensor for Aircraft Engine Health Management”, in Aerospace Conference, 2001, IEEE Proceedings., vol. 7, 2001, 7–3262 vol.7. DOI: 10.1109/AERO.2001.931402.

[19] K. Sampigethaya, R. Poovendran, L. Bushnell, Li, R. Robinson, and S. Lintelman, “Secure Wireless Collection and Distribution of Commercial Airplane Health Data”, Aerospace and Electronic Systems Magazine, IEEE, vol. 24, no. 7, pp. 14–20, 2009, ISSN: 0885-8985. DOI: 10.1109/MAES.2009.5208555.

[20] R. Harman, “Wireless Solutions for Aircraft Condition Based Maintenance Systems”, in Aerospace Conference Proceedings, 2002. IEEE, vol. 6, 2002, 6–2877–6–2886 vol.6. DOI: 10.1109/AERO.2002.1036127.

[21] M. Olive, R. Oishi, and S. Arentz, “Commercial Aircraft Information Security-An Overview of Arinc Report 811”, in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, 2006, pp. 1–12. DOI: 10.1109/DASC.2006.313761.

[22] S. Lintelman, R. Robinson, M. Li, D. v. Oheimb, Poovendran, and K. Sampigethaya, “Security Assurance for It Infrastructure Supporting Airplane Production, Maintenance, and Operation”, in Proc. U.S. National Workshop on Aviation Software Systems: Design for Certfiably Dependable Systems (NITRD HCSS-AS), 4-5 Oct 2006, Alexandria, VA, J. Sprinkle, Ed., http://ddvo.net/papers/HCSSAS.html. , 2006.

[23] G. Ladstaetter, N. Reichert, and T. Obert, “It Security Management of Aircraft in Operation: a Manufacturer’s View”, SAE Technical Paper, Tech. Rep., 2011.

[24] N. Thanthry, M. S. Ali, and R. Pendse, “Security, Internet Connectivity and Aircraft Data Networks”, Aerospace and Electronic Systems Magazine, IEEE, vol. 21, no. 11, pp. 3–7, 2006.

[25] S. Brostoff and M. A. Sasse, “Safe and Sound: a Safety-Critical Approach to Security”, in Proceedings of the 2001 Workshop on New Security Paradigms, ACM, 2001, pp. 41–50.

[26] A. Pfitzmann, “Why Safety and Security Should and Will Merge.”, in SAFECOMP, M. Heisel, P. Liggesmeyer, and S. Wittmann, Eds., ser. Lecture Notes in Computer Science, vol. 3219, Springer, 2004, pp. 1–2, ISBN: 3-540-23176-5. [Online]. Available: http://dblp.uni-trier.de/db/conf/safecomp/safecomp2004.html#Pfitzmann04.

[27] M. Paulitsch, R. Reiger, L. Strigini, and R. E. Bloomfield, “Evidence-Based Security in Aerospace: from Safety to Security and Back Again.”, in ISSRE Workshops, IEEE, 2012, pp. 21–22, ISBN: 978-1-4673-5048-8. [Online]. Available: http:/ /dblp.uni-trier.de/db/conf/issre/issre2012w.html#PaulitschRSB12.

[28] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, and J.-U. Bußer, “Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes”, in Proc. of the 7th AIAA Aviation Technology, Integration and Operations Conference (ATIO), http://ddvo.net/papers/AIAA_ATIO.html, AIAA, 2007, ISBN: 1-56347-889-7.