COLLECTION, STORAGE, PROCESSING AND MOVEMENT OF AIRCRAFT DATA USING A VALIDATED AND SECURED MEANS

CURTIS RIHN

LARS ROSENBLADE

MARK THOMPSON

TABLE OF CONTENTS

ABSTRACT

The information technology (IT) revolution, combined with the need for maintenance personnel to access information quickly, has resulted in the explosive growth of data in the past decade for all industrial operations. Ubiquitous access to data has become an essential component of Health and Usage Monitoring Systems (HUMS), and multiple mechanisms are being devised to ensure seamless connectivity. To insure this data access in the airborne environment, an integrated security framework is required extending from the airplane to all the users on the ground. Existing software-based solutions or COTS hardware-based products are unable to meet the airborne requirements such as RTCA DO-254 or DO-326. Usage of hardware-based FGPAs and Trusted Platform Modules (TPM) and industry standard security/integrity protocols allows an aircraft/ground network system meeting airborne and security requirements, such as Federal Information Processing Standard (FIPS) Publication 140-2.

Keywords: security, Hardware Security Module, Trusted Platform Module, integrity, authentication.

INTRODUCTION

Over time cyber security has become an integral part of the internet of things. Without certificates authenticating a bank's identification, the confidentiality of a communication or the validity of a stock exchange, having everything connected would not make as much of an impact. Now that aviation is entering this realm of being always connected, these ideals need to be implemented for communications to and from the aircraft.

No system will be completely secure no matter how adept the software security implementations are. Hardware implementations subject to FIPS PUB 140-2, also known as Hardware Security Modules (HSM), are used at the heart of the most secure software systems as a safe zone for Critical Security Parameters (CSP). CSPs are security related information whose disclosure or modification can compromise the security of an HSM. HSMs are well suited for encryption, storing keys, etc., but are not dynamic. Due to this limitation, HSMs are usually accompanied with a processor and an operating system to provide data functions behind the security firewall.

In the paper, we describe a security implementation specifically for the airplane environment. Our approach applies ground-based security techniques to an airplane server design, enabling increased data availability with industry-leading security.

AIRCRAFT DESIGN CONSIDERATIONS

Hardware Security Modules have demonstrated high levels of security in ground applications such as banking. However, systems to be installed on aircraft have very specific requirements that must be met. As one would suspect, HSMs are neither built nor designed for an aircraft environment. HSMs have no aircraft interfaces, and do not comply with Radio Technical Commission for Aeronautics (RTCA) DO-160, 254, or 178. RTCA DO-160 outlines the environmental design and test requirements for hardware to be put on an aircraft. The other two RTCA documents, DO-254 and DO-178B, define the hardware and software design processes and documentation levels to meet the certification requirements set by the FAA and/or other regulatory authorities. Table 1 is taken from DO-254 as an example of the level of documentation needed to put hardware on an aircraft.

TABLE 1 RTCA DO-254 HARDWARE DESIGN DOCUMENTATION

(RTCA, Inc., 2000)

Data Section	Hardware Life Cycle Data ①	Objectives ②	Submit	Level A	Level B	Level C	Level D
10.1	Hardware Plans						
10.1.1	Plan for Hardware Aspects of Certification	4.1(1,2,3,4)	S	HC1	HC1	HC1	HC1
10.1.2	Hardware Design Plan	4.1(1,2,3,4)		HC2	HC2	HC2	NA
10.1.3	Hardware Validation Plan ③④	4.1(1,2,3,4); 6.1.1(1)		HC2	HC2	HC2	NA
10.1.4	Hardware Verification Plan	4.1(1,2,3,4); 6.2.1(1)	S	HC2	HC2	HC2	HC2
10.1.5	Hardware Configuration Management Plan	4.1(1,2,3,4); 7.1(3)		HC1	HC1	HC2	HC2
10.1.6	Hardware Process Assurance Plan	4.1(1,2,4); 8.1(1,2,3)		HC2	HC2	NA	NA
10.2	Hardware Design Standards						
10.2.1	Requirements Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.2	Hardware Design Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.3	Validation and Verification Standards ③	4.1(2)		HC2	HC2	NA	NA
10.2.4	Hardware Archive Standards ③	4.1(2);5.5.1(1); 7.1(1,2)		HC2	HC2	NA	NA
10.3	Hardware Design Data						
10.3.1	Hardware Requirements	5.1.1(1,2); 5.2.1(2); 5.3.1(2); 5.4.1(3); 5.5.1(1,2,3); 6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC1	HC1
10.3.2	Hardware Design Representation Data						
10.3.2.1	Conceptual Design Data ③	5.2.1(1)		HC2	HC2	NA	NA
10.3.2.2	Detailed Design Data	5.3.1(1); 5.4.1(2)		⑤	⑤	⑤	⑤
10.3.2.2.1	Top-Level Drawing	5.3.1(1); 5.4.1(2); 5.5.1(1)	S	HC1	HC1	HC1	HC1
10.3.2.2.2	Assembly Drawings	5.3.1(1); 5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.3	Installation Control Drawings	5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.4	Hardware/Software Interface Data ③	5.3.1(1); 5.5.1(1)		HC1	HC1	HC1	HC1
10.4	Validation And Verification Data						
10.4.1	Hardware Traceability Data	6.1.1(1); 6.2.1(1,2)		HC2	HC2	HC2 ⑥	HC2 ⑥
10.4.2	Hardware Review and Analysis Procedures ③	6.1.1(1,2); 6.2.1(1)		HC1	HC1	NA	NA
10.4.3	Hardware Review and Analysis Results ③	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	Hardware Test Procedures ③	6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC2	HC2 ⑦
10.4.5	Hardware Test Results ③	6.1.1(1,2); 6.2.1(1)		HC2	HC2	HC2	HC2 ⑦
10.5	Hardware Acceptance Test Criteria	5.5.1(3),6.2.1(3)		HC2	HC2	HC2	HC2
10.6	Problem Reports	5.1.1(3); 5.2.1(3); 5.3.1(3); 5.4.1(4); 5.5.1(4); 6.1.1(3); 6.2.1(4); 7.1(3)		HC2	HC2	HC2	HC2
10.7	Hardware Configuration Management Records	5.5.1(1); 7.1(1,2,3)		HC2	HC2	HC2	HC2
10.8	Hardware Process Assurance Records	7.1(2); 8.1(1,2,3)		HC2	HC2	HC2	NA
10.9	Hardware Accomplishment Summary	8.1(1,2,3)	S	HC1	HC1	HC1	HC1

In addition to the traditional design requirements for hardware and software, RTCA now recognizes the urgency for security on aircraft and has released new security standards. The standards are covered in documents DO-326A, DO-355, and DO-356. These standards put more emphasis on security during design, production, manufacturing, and while in operation. Simply put, designing secure systems for aircraft requires a unique mindset and a commitment to the aerospace process.

Due to design safety considerations of aircraft, there has always been a barrier between data the aircraft produces and the forever changing applications that use the data. The data is important to a whole myriad of entities and comes from a myriad of sources of varying Design Assurance Levels (DALs). For example, there is engine data for engine manufacturers, error reports for maintenance personnel, aircraft heuristics for airlines and lessors, etc. The Data itself is agnostic to the DAL requirements stated in DO-254, 178, and 356. It is the connections to other aircraft hardware which determines the DAL. For example, hardware normally capable of receiving data from the Aircraft Control Domain[1] cannot have software running that can be upgraded without going through the long certification process that is DO-178 Category C or higher. Once the data is isolated from the aircraft interface, a processor can view the data and be lower category such as D or E. This allows for more flexibility on the applications and on the processors. The increased flexibility allows the applications to adapt and grow with the data.

TABLE 2 DO-254 HARDWARE DESIGN ASSURANCE LEVEL DEFINITIONS

(RTCA, Inc., 2000)

System Development Assurance Level	Failure Condition Classification	Failure Condition Description	Hardware Design Assurance Level Definitions
Level A:	Catastrophic	Failure conditions that would prevent continued safe flight and landing.	A: Hardware functions whose failure or anomalous behavior, as shown by the hardware safety assessment, would cause a failure of system function resulting in a catastrophic failure condition for the aircraft.
Level B:	Hazardous / Severe-Major	Failure conditions that would reduce the capability of the aircraft or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a large reduction in safety margins or functional capabilities, physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.	B: Hardware functions whose failure or anomalous behavior, as shown by the hardware safety assessment, would cause a failure of system function resulting in a hazardous/severe-major failure condition for the aircraft.
Level C:	Major	Failure conditions that would reduce the capability of the aircraft or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities, a significant increase in flight crew workload or in conditions impairing flight crew efficiency, or discomfort to occupants, possibly including injuries.	C: Hardware functions whose failure or anomalous behavior, as shown by the hardware safety assessment, would cause a failure of system function resulting in a major failure condition for the aircraft.
Level D:	Minor	Failure conditions that would not significantly reduce aircraft safety, and which would involve flight crew actions that are well within their capabilities. Minor failure conditions may include: a slight reduction in safety margins or functional capabilities, a slight increase in flight crew workload, such as routine flight plan changes, or some inconvenience to occupants.	D: Hardware functions whose failure or anomalous behavior, as shown by the hardware safety assessment, would cause a failure of system function resulting in a minor failure condition for the aircraft.
Level E:	No Effect	Failure conditions that do not affect the operational capability of the aircraft or increase flight crew workload.	E: Hardware functions whose failure or anomalous behavior, as shown by the hardware safety assessment, would cause a failure of a system function with no effect on aircraft operational capability or flight crew workload. For a function determined to be Level E, no further guidance of this document need apply, however, it may be used for reference.

AIRCRAFT SECURITY

To date, aircraft security has been addressed by system segregation, DAL and, for communication systems, by the obscure formats of the systems. The antiquated norm of "security by obscurity" on aircraft is no longer sufficient. It has been acknowledged that air to ground systems such as ACARS have not been hacked because it would require extensive knowledge and insight of ARINC 429, and the implementation of the communication stack of certain applications. Today's pervasiveness of IT, and the use of COTS components, makes the barriers to implementation knowledge much lower. Better security standards need to be set from the conception to operation of hardware. Bringing FIPS PUB 140-2 level 3 approved HSM on to the aircraft is a necessity that can no longer be delayed.

[1] (ARINC, 2005)

Security Algorithms and Authentication

Security can be broken into three key areas: confidentiality, integrity, and availability. Guarding from improper information modification or destruction as well as ensuring information non-repudiation and authenticity is arguably the airplane industry's top priority. Integrity is generally authenticity and validity rolled into one. Authenticity is done with some kind of public key infrastructure (PKI) such as RSA, ECDSA, etc. These cryptographic methods create a public key and private key. As their names suggest, the public key is made to be circulated in the public domain and the private key is what was referred to before as a CSP, and therefore, should never be exposed. The difficult part of PKI is getting the public key from a trusted source. Once the public key is sent over the web it is subject to change or other malicious activity. To mitigate these types of threats a trusted third party is needed to do the due diligence on each entity to make sure the key pair identifies them correctly. This trusted third party is referred to as a certificate authority (CA). For instance, a CA could be at the manufacturing facility of a unit to authenticate it before being shipped to the customer. Once the CA authenticates an entity, it issues a certificate. Now anyone who trusts this CA can verify the unit is trusted by the CA, which inherently means they can trust the unit.

Validity comes into play when sending or receiving data to/from the airplane system. The data is validated using different algorithms such as SHA or HMAC to generate a unique signature for the data. In congruence with authentication the data is validated to prove it was not altered, who it came from, and who its intended target was. To prove the data was not altered the receiving party can run the same algorithm on the data and see if the signature provided matches the signature given by the authenticated source. This proves validity of the data sent.

As mentioned before, the largest burden of PKI is vetting the entity behind each unique key. A CA, in theory, is an entity trusted by everyone. They will do the due diligence to make sure the entity is who they say they are. After the vetting process the entity can pass out the certificate certifying the public key. In a machine to machine environment the due diligence is much easier. During any hardware's manufacturing process a unique key pair can be derived and certified, thus validating the legitimacy of the unit. This is widely used in the other industries, such as in the automobile industry and can be applied to airplane systems.

Design & Development

Based on the aircraft design considerations and aircraft security requirements, Thompson Aerospace set out to develop an aircraft system to improve the availability of aircraft data while imposing security standards appropriate to the application. As a result, Thompson Aerospace has a patent-pending solution that is able to meet all the requirements for collecting, storing, processing, and moving data on commercial aircraft in a secure manner. We are presenting this type of implementation as a practical example of a solution.

The primary goal of the Thompson system is to increase the availability of aircraft data while adding security functions to that data. Security could be added to existing aircraft data systems as a bolt-on solution, acting as a gateway between aircraft devices and the ground. However, given the disjointed nature of aircraft data systems, such a solution would be heavy and require a large number of components, both critical negative factors in aircraft design. Fortuitously, the embedded HSM (eHSM) solution was designed to coexist on the same silicon as high-performance processors, meaning that an eHSM could be incorporated into a multi-functional server at negligible weight/cost. This enables the Thompson solution to add the security capabilities at the same time as adding greatly expanded data handling functional capabilities via the server processors, interfaces and memory. The eHSM is basically an FPGA which is programed for specific cryptographic and aircraft interface tasks while providing interfaces internal to the server. The FPGA also has a trusted module at its disposal. Trusted modules

come from the Trusted Computing Group standard. They call for an ASIC capable of using RSA for authentication purposes. This hardware or equivalent[2] is widely used in the automobile industry.

Figure 1 shows the architecture of our system, including two eHSMs, designated eHSM1 and eHSM2, that are designed to meet FIPS PUB 140-2 level 3, as well as DAL category C for DO-356 and 254. Having two eHSMs allows our system to physically isolate date interfaces, if required, or to increase the DAL level of data that is routed through both of them when orthogonal security engines are employed. This system forces the information to always pass through both eHSMs to be authenticated and validated. Each eHSM is designed for communicating with a specialized entity. For instance, when data comes through the processor (P3) connecting to the ground, it uses standard secure protocols such as IPSEC or TLS to connect. The eHSM1 serves as the root of trust for communication between the ground and the aircraft. This situation is analogous to the commercial use of the HSM talked about earlier. eHSM1 takes advantage of a FIPS PUB 140-2 level 3 certified TPM to house the CSPs and do the RSA authentication aspect of the eHSM. The eHSM1 Encryption Engine uses AES-128 and SHA-256 for the confidentiality and validity of the information being sent to and from the ground.

eHSM2 connects to entities in or around the aircraft via WiFi, Bluetooth, or wired connections. eHSM2 is specialized for on-aircraft communication and uses the Encryption Engine to house an Access Control List (ACL) and a SHA-256 engine. The Encryption Engine leverages an ECDSA trusted module for the authentication of each user or machine that connects with the system. Once the information passes into the dual eHSM implementation and is vetted, the data can be pre-processed by one of the two processors attached to eHSM2. These processors do not need to meet high DAL or FIPS requirements because they are isolated from the aircraft systems, allowing the customer to choose a standard operating system. More importantly the customer can run their own applications. These applications can be updated much more seamlessly and manageably. This is due to the fact that data cannot leave the unit without passing through an eHSM. An eHSM will be installed on the downstream and upstream allowing the data to be validated and authenticated in either direction. The endpoint of the data will also be authenticated using a certification system.

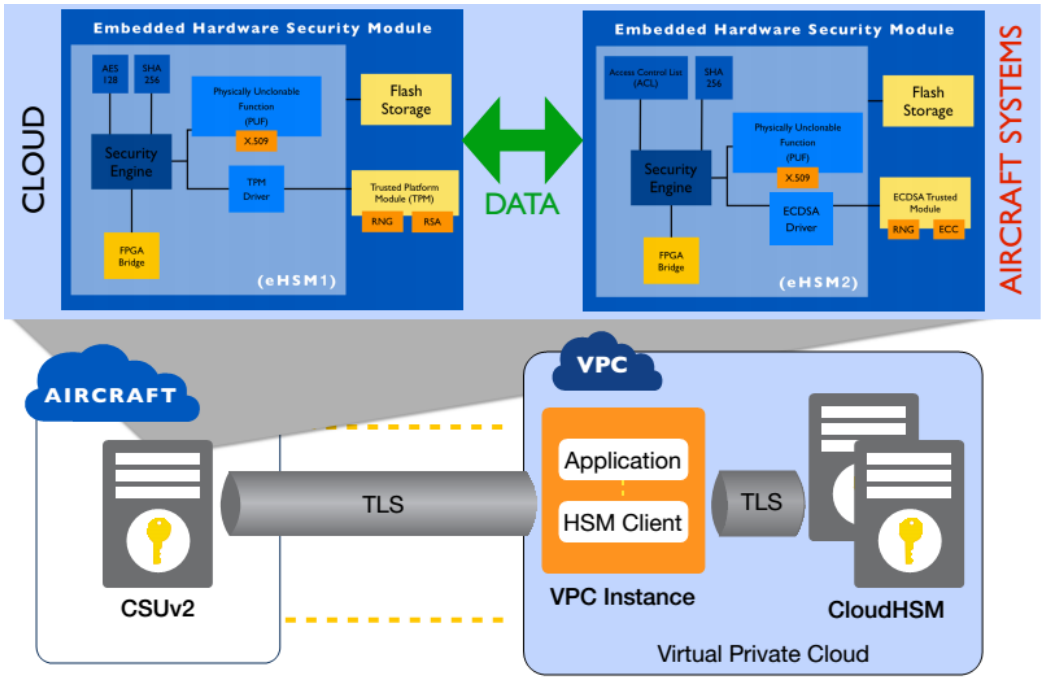

FIGURE 1 EHSM CONFIGURATION

(Rihn, 2015)

[2] Equivalent refers to how the device meets all the requirements for a TPM except it may use a different cryptographic algorithm such as Elliptical Curve Cryptography.

FIPS 140-2 controls the physical security, and makes sure the cryptography used is through approved algorithms or security functions set forth by National Institute of Standards and Technology. The physical security of the unit must adhere to 140-2 during manufacturing and in operation. The eHSM meets FIPS 140-2 level 3 which provides several physical security features above and beyond level 3. An example of this would be the Encryption Engine's immunity to differential power analysis (DPA). DPA is an exploit used to gain CSPs by probing the power during cryptographic computations, and then making deductions based on the data collected. With enough of this data CSPs can be revealed on an unprotected integrated circuit. The unit uses tamper evident seals and coatings to show when someone has attempted to gain access to the unit and a resin is used on the eHSM integrated circuits. Level 3 also requires a high probability of detecting and responding to tampering by zeroizing all plaintext CSPs. In addition, the ASIC used as the TPM and the ECDSA trusted module both have tamper detection zeroizing functions built in..

Manufacturing and Provisioning

A critical aspect of incorporating security at this level is ensuring the integrity of the process throughout manufacturing. The private keys must retain their confidentiality. The Security Engines, shown in Figure 1, come with physically unclonable functions (PUF), which allows for the creation of a unique identifier when it is loaded. How this works is that a function to derive the key is stored rather than the key itself, so no key is stored on the chip. The key derived from the PUF can be bound to a certificate through the CA.

Both the TPM and ECDSA Trusted Module come with unique keys built in as well. The unique public keys will be sent to the manufacturing commercial HSM to get certified by the CA. An example of this can be seen in Figure 2 below. The digital signature algorithm used is ECDSA. This algorithm is used by the HSM to create certificates for client public keys with the HSM's private key. The certificates are sent back to the client and the HSM public key is sent to all the units who want trust that HSM's certificates. This can be hierarchical in the sense the HSM can be certified or signed by a private key further up in the chain.

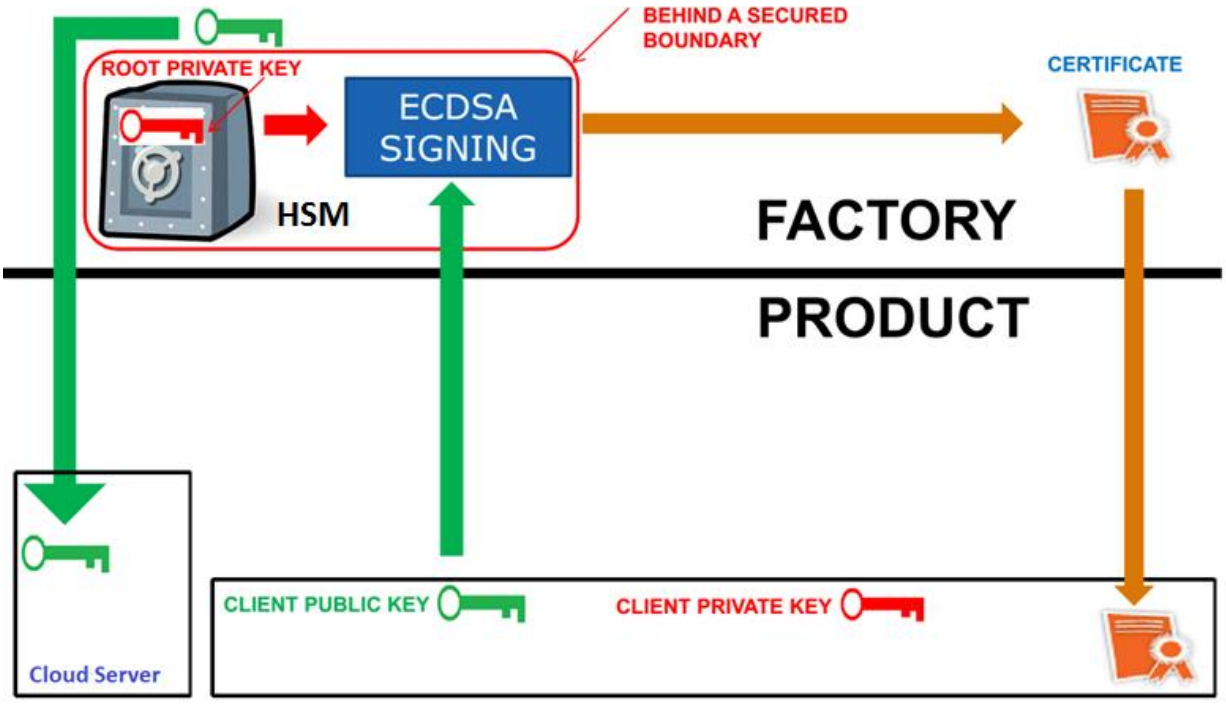

FIGURE 2 CERTIFING KEYS DURING MANUFACTURING

(Dean, 2014)

CONCLUSION

In the future, security of airborne systems will require standard solutions common to ground-based secure systems. Existing solutions assume that personnel will not mishandle the keys or data. Some existing systems assume that obscure links, such as ACARS, will prevent attacks by their specialized nature, or that system isolation is adequate. These types of assumptions will not be acceptable to regulatory agencies or data users as the data and its use become more integral to airplane operations.

As a result, cryptographic systems will be necessary for all systems on and communicating with an aircraft. These systems need a vetted authentication method to allow for host and client checks before data is sent. Thompson Aerospace has designed an architecture to provide security functions to an appropriate level, while improving data availability utilizing hardware-based cryptography and isolation to permit COTS data processing. With the availability of inexpensive, powerful and convenient secure data, the airplane industry can move into the world of big data with confidence.

REFERENCES

Airlines Electronic Engineering Committee. (2005, April 12). Aircraft Data Network Part 5: Network Domain Characteristics and Interconnection. Annapolis, Maryland, USA.

ARINC. (2005). *664P5: Aircraft Data Network Part 5 Network Domain Characteristics and Interconnection.* Annapolis, Maryland: ARINC.

ARINC. (2013). *842-1: Guidance for Usage of Digital Certificates.* Annapolis, Maryland: ARINC.

Dean, A. (2014). *CryptoAuthentication.* Atmel.

National Institute of Standards and Technology. (1994, November 9). FIPS PUB 191: Guideline for The Analysis Local Area Network Security. Gaithersburg, MD, USA.

National Institute of Standards and Technology. (2001, May 25). FIPS PUB 140-2: Security Requirments for Cryptographic Modules. Gaithersburg, MD, USA.

National Institute of Standards and Technology. (2001, November 26). FIPS PUB 197: Advanced Encryption Standard (AES). Gaithersburg, MD, USA.

National Institute of Standards and Technology. (2004, February). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Gaithesburg, MD, USA: NIST.

National Institute of Standards and Technology. (2012, March). FIPS PUB 180-4: Secure Hash Standard (SHS). Gaithersburg, MD, USA.

National Institute of Standards and Technology. (2012, June). NIST Special Publication 800-121: Guide to Bluetooth Security. Gaithersburg, MD, USA.

National Institute of Standards and Technology. (2013, July). FIPS PUB 186-4: Digital Signature Standard (DSS). Gaithersburg, MD, USA.

Rihn, C. (2015). *ARINC 848 Presentation: Aircraft Information Technology made Straightforward and Secure.* Irvine, CA: Thompson Aerospace.

RTCA, Inc. (2014). *DO-326A: Airworthiness Security Process Specification.* Washinghton D.C.: RTCA, Inc.

RTCA, Inc. (2000). *DO-254: Design Assurance Guidance For Airborne Electronic Hardware.* Washington D.C.: RTCA, Inc.

RTCA, Inc. (2014). *DO-355: Information Security Guidance for Continuing Airworthiness.* Washington D.C.: RTCA, Inc.

RTCA, Inc. (2014). *DO-356: Airworthiness Security Methods and Considerations.* Washington D.C.: RTCA, Inc.

Soja, R. (2014). *Automotive Security: From Standards to Implementation.* Freescale.

Thompson, M. S. (2008). *Patent No. US20100195634 A1.* USA.

Thompson, M., Coolidge, T., Rihn, C. M., & Rosenblad, L. E. (2014). *Patent No. 62/050,177.* USA.