AEEC
Together "We Set the Standard."

Prepared By Network Infrastructure and Security (NIS) Subcommittee Network Security WG

Date October 24, 2012

Reference 12-180/ABN-035A lth

Subject **AEEC Technical Application Bulletin**
Considerations for the Incorporation of Cyber Security in the Development of Industry Standards

Abstract

ARINC Standards are used to support the design and development of aircraft systems, avionics, networks, and information security. As broadband connectivity to the aircraft is implemented, and as additional application functions are installed using common communication paths, the need for consistent security principles will be paramount. Security provisions need to be implemented in a consistent way.

The security process begins with a common overview of aircraft security and the proper security considerations provided by ARINC Report 811 with further details provided in the development of additional industry standards.

This Technical Application Bulletin provides cyber security considerations for use in an aircraft environment. It represents the security experience and best practices available at the time of its writing. This document will be updated as the need arises.

DISCLAIMER

THIS DOCUMENT IS BASED ON MATERIAL SUBMITTED BY VARIOUS PARTICIPANTS DURING THE DRAFTING PROCESS. NEITHER AEEC, AMC, FSEMC NOR ARINC HAS MADE ANY DETERMINATION WHETHER THESE MATERIALS COULD BE SUBJECT TO VALID CLAIMS OF PATENT, COPYRIGHT OR OTHER PROPRIETARY RIGHTS BY THIRD PARTIES, AND NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, IS MADE IN THIS REGARD.

NO CERTIFICATION OR WARRANTY IS MADE AS TO THE TECHNICAL ACCURACY OR SUFFICIENCY OF THE DOCUMENT, THE COMPLETENESS, CORRECTNESS, COMPLIANCE, CURRENCY, ADEQUACY, MERCHANTABILITY, FITNESS FOR INTENDED PURPOSE OR SAFETY OF ANY PRODUCTS, COMPONENTS, SYSTEMS, PROCESSES, OR SERVICES (“PRODUCTS”) DESIGNED, TESTED, RATED, INSTALLED OR OPERATED IN ACCORDANCE WITH ANY ASPECT OF THIS DOCUMENT OR THE ABSENCE OF RISK OR HAZARD ASSOCIATED WITH SUCH PRODUCTS. THE USER OF THIS DOCUMENT ACKNOWLEDGES THAT IT SHALL BE SOLELY RESPONSIBLE FOR ANY LOSS, CLAIM OR DAMAGE THAT IT MAY INCUR IN CONNECTION WITH ITS USE OF OR RELIANCE ON THIS DOCUMENT, AND SHALL HOLD ARINC, AEEC, AMC, FSEMC AND ANY PARTY THAT PARTICIPATED IN THE DRAFTING OF THE DOCUMENT HARMLESS AGAINST ANY CLAIM ARISING FROM ITS USE .

THE USE IN THIS DOCUMENT OF ANY TERM, SUCH AS SHALL, MUST OR SHOULD, IS NOT INTENDED TO AFFECT THE STATUS OF THIS DOCUMENT AS A SET OF ISSUES FOR CONSIDERATION OR IN ANY WAY TO MODIFY THE ABOVE DISCLAIMER. NOTHING HEREIN SHALL BE DEEMED TO REQUIRE ANYONE TO INCORPORATE ANY ELEMENT OF THESE ISSUES FOR CONSIDERATION IN ITS PRODUCTS.

ANY USE OF OR RELIANCE ON THIS DOCUMENT SHALL CONSTITUTE AN ACCEPTANCE THEREOF “AS IS” AND BE SUBJECT TO THIS DISCLAIMER.

TECHNICAL APPLICATION BULLETIN
CONSIDERATIONS FOR THE INCORPORATION OF CYBER SECURITY
IN THE DEVELOPMENT OF INDUSTRY STANDARDS
TABLE OF CONTENTS

ATTACHMENTS

APPENDICIES

1.0 INTRODUCTION

Security is a major subject of interest in the airline industry as the volume of aircraft information grows and as this information is transmitted and stored in electronic form using both private and public hosts.

The goal is to implement security provisions in a consistent way. It would be problematic if security were conceived, applied, and ensured differently and inconsistently among the components used in a variety of aircraft architectures. As increased broadband connectivity to the aircraft is implemented and more application functions use common communication paths, the need for consistent security principles will be paramount.

Aircraft operate in a constantly changing and increasingly threatening environment, where attacks on communication and information systems may be launched intentionally to discredit organizations, to disrupt operations, or to do harm. Continuing security, like continuing safety, is dependent upon ongoing operational processes as well as the underlying delivered products/systems.

ARINC Standards are used to support the design and development of aircraft systems, avionics, networks and information security. The more consistently all elements work together over the aircraft lifecycle, the better. The security process begins with a common overview of aircraft security and the proper security considerations provided by ARINC Report 811 with further details provided in the development of additional industry standards.

1.1 Purpose of this Document

The purpose of this document is to provide information to system engineers preparing industry standards for networked systems to ensure that appropriate cyber security provisions are included in emerging systems.

The Network Infrastructure and Security (NIS) Subcommittee, Network Security working group developed this document taking into consideration ARINC Report 811 and ARINC Specification 664, Part 5, as well as other relevant information. This document represents the input from the airline community and others who participated in its development. The reader should take this document into consideration in development of their products and services.

The following actions are recommended:

- Security issues that affect avionics, associated cockpit systems, and cabin systems should be considered thoroughly by those developing standards.
- Company representatives participating in standards development activities should communicate with their in-house security specialists.
- New standards development activities should address how cyber security and common security solutions will be considered.
- ARINC Report 811 and this document should be used by those developing standards to address airline security needs.

1.0 INTRODUCTION

1.2 Background

“Cyber security” is viewed in many ways and is therefore treated inconsistently by people in different disciplines. This inconsistency is exacerbated in the design and development of aircraft systems because the practices related to addressing cyber security include physical facilities, operational and management aspects of security, environmental (i.e., natural or man-made infrastructure threats such as earthquake, storm, and fire), physical attack by human agents, social engineering attacks, direct and indirect cyber attacks, accidents and inadvertent errors on the part of operators. Consideration extends to disaster planning, disaster recovery, and plans for continued operation. Cyber security as commonly practiced focuses heavily on the owner/operator and relatively little on the design and manufacture of the systems themselves.

Industry standards and practices intended for the development and certification of aircraft systems explicitly include consideration for some of these, such as environmental and infrastructure threats of specific types, accidents, and inadvertent errors on the part of operators and maintenance. However, they generally exclude aspects unique to operators and operations, and do not typically address deliberate direct and indirect attacks against onboard cyber systems. This is predicated on the notion that external controls have historically ensured that only well-intentioned individuals and external systems interact with aircraft systems.

1.3 Changes in Aircraft Systems and Equipment

Generally there are two reasons why aircraft systems and related equipment specifications change:

- Aircraft architecture changes require new considerations in the generation of aircraft system and equipment standards.
- New technology requires common adaptations for aircraft not necessarily aligned to the system and equipment standards.

ARINC Specification 664 addresses many aspects of design, architecture, and basic technology that accompany the transition from relatively loosely coupled, vertically integrated systems (identified as “legacy”) to more tightly coupled, service oriented, networks of systems (identified as “emerging”). A consequence of this change is that assumptions made by systems designed for legacy use (while still requiring validation) are often satisfied in different ways, and sometimes are much more difficult to assure in the emerging uses.

For example, legacy system designs assume that while input verification is necessary for integrity and availability of message content, identity of the message originator can be assumed by reliance on wiring definition and installation. This same assumption is often made for network designs, while in fact much of the assurance that the assumption is correct is moving into the realm of network configuration captured in software.

Further discussion and two examples are contained in Appendix C of this document.

1.4 Reference Documents

The background leading to the development of this document may be found in the following ARINC Standards. The latest version applies:

Document	Title
664P5	ARINC Specification 664 Part 5: Aircraft Data Network, Part 5 – Network Domain Characteristics and Interconnection, April 2005
811	ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework, December 2005
827	ARINC Report 827: Electronic Distribution of Software
665	ARINC Report 665: Loadable Software Standards

Further cyber-security reference material can be found in Appendix A of this document.

1.5 How to Read this Document

This document provides guidance for the development of industry standards that require information security. This includes the development of ARINC Standards. The high-level airline security objectives described in ARINC Report 811 are summarized in the left column of Table 3.0. The right column provides additional “general” considerations.

Detailed security guidelines are provided in Attachment 1. These guidelines are loosely aligned with the control families of NIST SP 800-53 Rev 2.

During the preparation of this document, many subjects were discussed for which the group concluded that no meaningful guidance could be provided at this time. In these cases, the expectation is that future revisions of this document will address these issues.

This document was organized so that the body of the document, Sections 1 through 3 can be read in one sitting and that the attachment and appendices can be used as required.

2.0 SECURITY ENVIRONMENT AND ASSUMPTIONS

2.1 Scope, Context and Boundary Definition

The following figure shows some of the documents in development at the time of this writing. These documents address information security considerations in aircraft. Both RTCA SC-216 and EUROCAE WG-72 are producing draft documents that are in various stages of completion. The figure below does not show the intricate relationships between these documents, but rather directs the reader to them. The reader is encouraged to participate in and/or contact the RTCA and EUROCAE organizations directly.

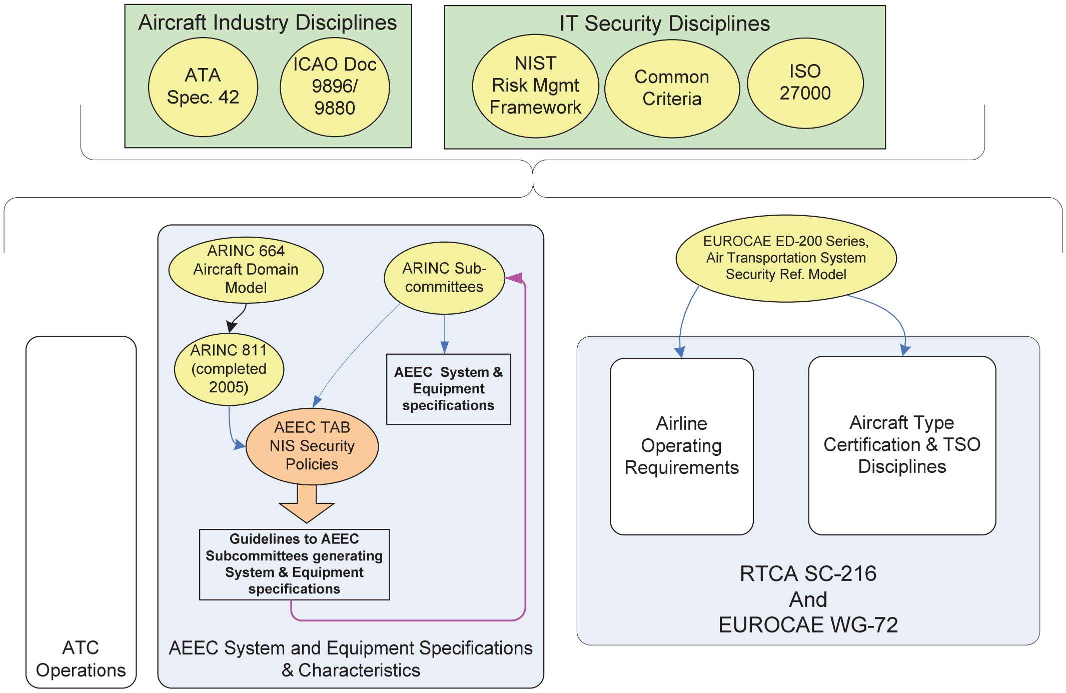
Aircraft Industry Disciplines
ATA Spec. 42
ICAO Doc 9896/ 9880
IT Security Disciplines
NIST Risk Mgmt Framework
Common Criteria
ISO 27000
ARINC 664 Aircraft Domain Model
ARINC Sub-committees
ARINC 811 (completed 2005)
AEEC System & Equipment specifications
AEEC TAB NIS Security Policies
Guidelines to AEEC Subcommittees generating System & Equipment specifications
ATC Operations
AEEC System and Equipment Specifications & Characteristics
EUROCAE ED-200 Series, Air Transportation System Security Ref. Model
Airline Operating Requirements
Aircraft Type Certification & TSO Disciplines
RTCA SC-216 And EUROCAE WG-72

Figure 1 – Relationships among Security Documents

Figure 1 also describes how this document pertains to other industry standards prepared by ARINC, EUROCAE and RTCA. The reader should be aware that Airline Operations and Aircraft Certifications are outside the scope of this document.

The figure shows that the document takes input from other industry bodies and produces an output that may be fed back into that body. This is necessary to maintain commonality of security solutions. As security controls are specified by one industry standard it is important that they be used consistently.

2.2 Security Environment Assumptions and Presumptions

All assumptions used in writing an industry standard should be explicitly spelled-out and related consequences documented in context. Assumptions are statements that require validation to allow for applicability in context. The validation can only be performed by the applicable organization that designs, operates or regulates the topic of assumption.

All presumptions used in the writing of an industry standard should be explicitly called out and related consequences documented in context. Presumptions are statements that need no validation as they are axiomatic in nature and self-evident.

Further discussion can be found in Appendix D of this document.

2.3 Specification Philosophy and Security Environment

The development of industry standards for aircraft systems and equipment is, by necessity, not an exercise in homogeneous top-down design. The explicit goal of such specifications is to create equipment which provides benefits through various aspects of commonality regardless of the aircraft or installation in which they are employed. In essence, to build pre-existing components that can be used in new aircraft and frequently existing aircraft. A successful standard allows for some significant common characteristics (e.g., interoperability, equipment interchangeability, operational commonality) while at the same time not forcing too many restrictions in implementation.

It is important to note that risks and externalities for the system are not the same as risks and externalities for the aircraft. Industry standards may be incomplete in this respect. Therefore, implementers are expected to convey as much information as possible about their assumptions and understanding of these attributes at the system level. In this way system integrators will not miss critical external security dependencies, constraints or requirements.

This communication has historically been achieved by the collaboration of product integration experts and other specialists in the area of system standards development. These experts will, of necessity, work from two perspectives. One perspective addresses the specification itself. The other looks at planned or possible usage of the specification in product lines. The specification is public; the planned usage is often private – or at least not revealed in detail. Hence the planned usage does not appear in the specification, although it may be offered as a clarifying example or may simply be part of private validation exercises by participants in order to satisfy themselves of the relevance and usefulness of the specification for their needs.

The net result of this situation is that development of industry standards has served the industry reasonably well. However, this situation may not hold as security becomes a consideration due to variability in the target environment, the architecture of systems, evolution of the threat environment, and unstated or even unexplored assumptions about the security properties of the environment.

When security is highlighted as a general consideration the current practices tend to become significantly less effective. This is due primarily to:

- A security control baseline may not exist for a particular system or for the systems with which it interfaces. When technology changes (say, from data buses to networks) implicitly introduce “security” issues, the question of what to do about these issues relative to external parties may be impossible to resolve other than by simply making “assumptions”, which may or may not leave those parties with an unacceptable security “burden”.

- Aircraft system designers may not be trained or experienced in cyber security. By the same token, cyber security specialists typically have little to no experience in the unique aspects of aircraft systems, including system dependencies and solution feasibility. As a result, the knowledge gap between the two disciplines can lead to disparate expectations and proposals that fail to achieve design objectives. There is, unfortunately, little remedy for this except time and effort – with the knowledge that things will mature and improve over time.

Since this maturation within the industry takes time and progress is required in the interim, it is important that:

- Participants involved in the development process include those experienced in system design, cyber security, and operations.
- Assumptions or assessments of risk and external factors be discussed and documented. In particular, be as clear as possible on all assumptions related to security.
- What needs to be specification (normative) and what can remain commentary or background (informative) be segregated. It is not necessary that all problems or issues be resolved in the system specification. It is necessary that those that are recognized and not resolved be documented. Documentation of details – resolved and unresolved – is more important to overall success than is resolving every issue.
- System/system dependencies, system / operator dependencies, and other external factors (for example, TSA or other regulations affecting airport or aircraft security) be noted and differentiated.

3.0 GENERAL CONSIDERATIONS

Table 3-1 reproduces the Airline Security Objectives from ARINC Report 811. It augments the objectives with additional considerations.

Table 3-1

ARINC Report 811 Airline Objective	**Considerations for the development of industry standards**
Aircraft systems should use common security controls as much as possible.	Ultimately, security functions and attributes are implemented in systems and integrated with system functions, and are therefore the responsibility of the system designer. The work of the Network Infrastructure and Security (NIS) Subcommittee is to monitor, encourage, and specify the use of common security controls.
The overall cost of aircraft system security controls should be minimized. Cost factors to consider include development, operation, and maintenance costs.	“Minimization” has to be considered relative to the risk being mitigated. Arbitrarily limiting controls due to cost may be penny-wise and pound-foolish. In particular, failure to address a risk that is unique to a piece of equipment by declaring responsibility for mitigation to be “external” may place an inordinate burden on the specification user or integrator. The specification developer should acknowledge and consider the equipment’s contribution to a security risk that must be mitigated in order to successfully deploy the system. The cost, difficulty, and reliability of mitigation within the system should be weighed against the impact of transferring that mitigation requirement to the integrator or end user.
Aircraft systems should employ multiple security controls to mitigate each significant threat.	Overall, this reduces “brittleness” of designs, helps to ensure continued security operation after the failure of individual controls, and contributes to regulatory compliance and safety objectives by eliminating common mode and single-point failures. Note that multiplying controls does not automatically mean increasing security. Redundant systems with the same weakness possess a common mode failure. Security vulnerabilities in a design or implementation often exhibit that same characteristic. Independence of design and implementation, especially when applied to defense in depth, is necessary for “multiple” controls to be effective.
Development, operation, and maintenance of security controls for aircraft systems should fit within the existing aircraft lifecycle.	ARINC Specification 664 Part 5 introduces the concept of aircraft domains where aircraft systems and networks can be grouped according to common characteristics. ARINC Report 811 uses this domain concept and introduces the notion of the aircraft being in various configuration life-cycle states (heavy or line maintenance, etc.). In addition, ARINC Report 811 introduces an influential element for managing security as the “operating” mode of the aircraft equipment and systems. Aircraft systems and equipment may be in one of three modes: Normal Operational Mode Non-Normal Operational Mode (e.g., not-operating properly, “failed”) Maintenance Mode It is the expectation that aircraft cyber security policies will vary depending on the configuration life-cycle state of the aircraft and “mode” of the aircraft systems and can be referenced to the Aircraft Network Domain structure described in ARINC Specification 664 Part 5.
Security solutions for new systems should require as few changes as possible to existing systems.	This is another aspect of the goal of incremental improvement, this time applied to systems rather than organizations.

3.0 GENERAL CONSIDERATIONS

ARINC Report 811 Airline Objective	**Considerations for the development of industry standards**
Security controls for aircraft systems should be flexible in order to permit them to be used within a variety of different policies and procedures.	Controls built into a computer system are a compromise between mandatory enforcement of the designer's security vision and airlines' needs to tailor aircraft and systems to suit their operational needs. From a certification perspective, the dividing line tends to be drawn between issues of continuing airworthiness, for which limited options typically exist, and issues recognized as not contributing to continuing airworthiness. There is little reason to believe that this situation needs to change overall with respect to security. Security controls should, therefore, be developed with a clear sense of what is required for airworthiness and what is not. When airworthiness is not an issue, it should be possible for airlines to tailor security controls to conform to their own preferred policies.
Aircraft systems should provide effective operation to users performing authorized actions.	It is widely recognized that security controls, which are viewed as interfering with the legitimate user, are substantially harder to enforce and more likely to be actively circumvented by the user than are controls that don't “get in the way”. The ultimate interference with the user is to deny a legitimate user access to the system or function they need to perform their job. In addition, if the same user is critical to the on-time performance of an aircraft, the cost impact of a false denial may quickly outweigh the impact of a security failure in that area – especially in the eyes of an airline.
Aircraft systems should be designed to allow for regular adoption of new security controls and technology.	The design of systems is always a trade among many characteristics. It is impossible to anticipate what new controls and technologies may be required in order to design for them. On the other hand, the use of some technologies implicitly includes the prospect of limited effective life. For example, any control that relies on cryptography should be assumed to have a finite, and relatively short, service life, requiring frequent refresh of keys and relatively frequent (compared to aircraft service life) update of obsolescence-prone algorithms. Becoming aware of the inherent life limitations of some security technologies can provide insight into the best way to modularize designs in the hope of somewhat “future-proofing” them.
Security controls for aircraft systems should require minimal administrative and operational overhead.	It is advantageous that all controls operate with a minimum overhead because overhead is costly, and once overhead infrastructure is put in place it becomes an impediment to improvement. More specifically, security controls that are not themselves “game changers” should require minimal additional overhead and ideally no additional infrastructure.
Security controls for aircraft systems should not inhibit airline mission accomplishment (i.e., delivery of passengers from point A to point B).	This is, of course, subject to the question of what risk any given control mitigates. It may be entirely appropriate for a control to inhibit the airlines' mission if the alternative is to expose the passengers, crew, and aircraft to unacceptable safety risk.
Security controls for aircraft systems should be based on open standards.	This is a way of helping to increase usage of common controls (COTS). It also reduces the tendency to implement “security by obscurity” - the idea that a security control is effective by virtue of its design or implementation details being secret. It is recognized that most secrets can't remain secret forever, and any control that relies on long-term protection of a secret is probably not going to be secure. This is especially true where the secret is a design secret.

3.0 GENERAL CONSIDERATIONS

ARINC Report 811 Airline Objective	**Considerations for the development of industry standards**
Security controls for aircraft systems should protect airlines, manufacturers, and suppliers from threats that may affect their commercial image.	Security risk assessments should consider threats that may affect the commercial image of the airlines and the entire industry. There is a tendency to downplay the effect of system malfunctions where it is recognized that no safety impact is involved. However, what the safety expert deems to not be a concern is not necessarily what a member of the flying public would conclude. It's important to not be alarmist; neither should concerns be ignored just because they are held by non-experts.
Security controls for aircraft systems should not compromise the safety of the aircraft.	Security controls are implemented in aircraft systems, which like all aircraft systems must be shown to be effective at performing their intended function and not interfering with the safe continued operation of the aircraft.
Security controls for aircraft systems should mitigate the risks to aircraft systems to a level that is acceptable based on airline business needs.	Security controls used to mitigate risks to continued airworthiness should mitigate these risks to a level defined by airworthiness requirements. Obviously, meeting airworthiness requirements for certification is the responsibility of the certification applicant. Developers of specifications and standards, however, can potentially make that task of ensuring continued airworthiness more difficult or even impossible by failing to consider certification aspects even if they're not explicitly responsible for producing a certified design.

In addition, ARINC Specification 664 Part 5, Section 4, discusses security considerations for airborne networks in the context of the aircraft systems domain model, along with a discussion of security policies and requirements definition (Appendix D) and information about the characteristics of systems that would generally be allocated to each domain (Appendix I).Additional information intended for system designers and specification writers is provided there.

4.0 STANDARDS DEVELOPMENT AND SUPPORT

This document is expected to be useful in the development of all types of systems. It will be particularly useful to determine what security provisions need to be applied to a new system and the related industry standard(s) being prepared. This includes the development of ARINC Standards. The goal of this coordination is twofold: to allow common security solutions to be used and to reduce duplicating efforts. The information provided in this document is intended to augment ARINC Report 811 which introduces cyber security to applicable areas of aircraft operations and maintenance.

Because the ARINC Standards development process is collaborative, everyone is encouraged to engage those within their companies (i.e., airlines, avionics suppliers, airframe manufacturers) who are knowledgeable in cyber security matters. The NIS Subcommittee is prepared to provide support in these areas.

ATTACHMENT 1 STANDARDS DEVELOPMENT GUIDELINES

This attachment is organized in a way that is generally aligned with the control families of NIST SP 800-53. Also both EUROCAE WG-72 and RTCA SC-216 are currently producing documents that will provide aviation-specific security recommendations and the resulting documents should be used as they become available.

Standards developers and systems implementers are forced to make assumptions about the security environment in which the equipment will operate. Some of these assumptions and presumptions are tabulated in appendix D of this document.

Standards developers should be able to employ techniques that reduce the impact of failures, reduce mandatory reliance on systems that may be vulnerable, and add protection layers to reduce the exposure of potentially vulnerable components.

Standards developers should also use care to mandate only what is needed by the specification to achieve its functional objectives, and leave the developers and operators free to develop and integrate individual systems into the aircraft and operations architecture to meet their own specific safety and efficiency requirements.

1.1 Access Control Including Identification and Authentication

1.1.1 Access Control

Access control is well established as a concept and method of limiting access to sensitive data or resources in IT systems. The aircraft environment presents some unique challenges with respect to access control and what occurs when access control fails. Failure, which can result from causes such as forgotten passwords, improper system configuration, or failure of the authentication process, could result in a denial of service. In the case of airline operators, the inability to access key systems could have a critical impact on their operations. Mitigating the risk of access control failure by creating emergency access privileges to override existing controls should be closely monitored for abuse and effectiveness of the access control provided.

For airline operators, the challenges of effective access control are complicated by the large number of potential users at different locations, complex crew scheduling patterns, and numerous onboard systems. If each system employs a unique authentication design, crew members could be required to manage multiple credentials securely and effectively. This creates the risk of credentials being compromised when they are documented.

Standards developers should remember that other systems with similar needs may be on the airplane, and, consider the impact on an:

- Airline, if multiple systems implement unique authentication designs.
- Individual crew member, if multiple systems implement unique authentication designs.

Regardless of the challenges, authenticating users of the system may be required, depending on the sensitivity of the information within or traversing the system. For access to sensitive information it is recommended that the individual accessing be identified and recorded in logs along with the actions performed. Some industry standards or laws may require this individual user logging, for example personal or medical information privacy laws and the Payment Card Industry Data Security Standards (PCI-DSS).

In contrast, regulations do not generally address system requirements for many types of system functions that are common in the IT industry. Simply providing access controls as system functions may in fact add to an airline's regulatory burden since the airline industry is currently much more heavily regulated with respect to maintenance operations than are most industries, particularly with respect to auditable records. Implementing mandatory controls within systems does not necessarily result in a compensating cost or efficiency offset for airlines, which may already implement external controls in approved processes for the same purpose.

Guideline: The provision of controls in airborne systems and functions that airlines are required to maintain, or which affect use of or access to systems, should be considered within the context of the whole airline maintenance and operational process. When possible, it is preferable (as recommended in ARINC Report 811) to provide such controls as options for each airline to adopt and tailor as their unique fleet mix and operational needs dictate.

> **Rationale:** It may be reasonable that airlines with adequate external controls be able to opt-out of built-in security controls. By the same token, well-designed controls may be able to be shown by airlines to be able to compensate for the elimination of other controls in order to improve efficiency, reduce cost, or improve reliability of their security process.

1.1.2 Identification and Authentication

As functions are deployed that communicate using the IP protocol suite, it becomes essential to ensure that such functions authenticate themselves with assurance appropriate to the environment in which those functions exist. In general, the more open the network hosting the function, the greater the need for system-administered identification and authentication (as opposed to physical or local access controls). *Identification* refers to the entity (human or system function) requesting access presenting a credential, i.e., "this is who/what I am". *Authentication* is the process of validating that credential against a database of previously established credentials. Once authentication occurs, authorization decisions can be made.

It should be noted that authentication functions should not be implemented as a blocking control where there is a possible impact to safe operation of the aircraft. Care should also be taken to avoid creating failure modes such that an aircraft may be stranded (unable to be dispatched) because of authentication failures. Such situations could occur, for instance, if the maintenance crew is denied access to systems or functions that are required to be maintained in order to dispatch. Operational use cases should be carefully evaluated by individuals having sufficient experience in the operational area to determine appropriate system responses to failed authentication.

A. Guideline: Specification writers and application developers are encouraged to reference NIST SP 800-63, Electronic Authentication Guidance, which provides guidance for selecting among the variety of electronic authentication mechanisms (e.g., passwords, biometrics, physical tokens, etc.) that may be used to perform local or remote authentication of users.

B. Guideline: If the incorporation and use of passwords is specified as an access control method, ensure that a means exists for the proper authority (usually the airline) to manage the passwords in accordance with a reasonable security policy. NIST SP 800-118 provides guidance for password management.

> **Rationale**: The airlines need to actively manage passwords, with effective policies for change, detection of misuse, and revocation in accordance with good practices.
>
> **Assumption**: Other controls may effectively remove reliance on the password as an access control mechanism. For example, some devices may be only accessible from a physically secure area (e.g., E.E. bay, cockpit) in which every user who has access is trusted. Or the account can do no harm (e.g., Read-only) and does not have access to confidential data. On the other hand, the use of passwords may be the method of choice.

C. Guideline: If the incorporation and use of biometrics is specified as an access control method, ensure that a means exists for the proper authority (usually the airline) to manage the biometrics in accordance with a reasonable security policy. This may be accomplished by ensuring conformance to the requirements of NIST SP 800-76.

> **Rationale**: The airlines need to actively manage biometrics, with effective policies for change, detection of misuse, and revocation in accordance with good practices. (NIST SP 800-76-1)
>
> **Assumption**: Other controls may effectively remove the reliance on the biometrics as an access control mechanism. For example, some devices may be only accessible from a physically secure area (e.g., EE bay, cockpit) in which every user who has access is trusted. Or the account can do no harm (e.g., Read-only) and does not have access to confidential data. On the other hand, the use of biometrics may be the method of choice.

D. Guideline: If digital certificates are used to implement an electronic authentication mechanism, the certificates should comply with the guidance in Section 1.3.3 of this document.

1.1.3 Access Control Lists

Access Control Lists (ACL) can be developed as a means of limiting access to people or systems. However, airline employees are not the only people granted regular access to aircraft on the ground. Third party servicing and maintenance personnel often must have access to airplane systems. Access by regulators or other government personnel may also be a requirement. Consideration must be given to how an airline would manage the provisioning and maintenance of user accounts on a global basis for non-airline employees. Note also that the most prevalent current technique uses localized access controls (e.g., airport-specific badging) administered by local authorities to grant access to aircraft.

A. Guideline: If the incorporation and use of access control lists is provided, ensure that a means exists for the proper authority (usually the airline) to manage the access control lists in accordance with reasonable security policies.

> **Rationale:** Access Control Lists (ACL) need to be updated regularly, upon changes in personnel (e.g., hiring, firing) and when the user changes their credentials (e.g., password update or certificate renewal).
>
> **Assumptions:** The ACL is loadable into the system. Also, it is unreasonable to expect users to have different credentials for each aircraft in a fleet.

B. Guideline: Ensure that user accounts are granted access to only such information and resources that are necessary for their defined tasks; i.e., follow the principle of least privilege. (ref. SP 800-53 AC-6).

C. Guideline: If the ACL is shared between the air and ground systems, the time during which the ACL on the ground and ACL on the aircraft differ should be kept to a minimum, and the operator should anticipate how to handle such differences. Standards developers should note that automated, electronic means of ACL loading are strongly preferred to manual loading (i.e., *sneakernet*).

> **Caution:** Regardless of the means chosen to configure ACLs, there must always be an acceptable means to establish that the airplane is properly configured, including being configured with the correct ACL, and to reinstall or otherwise preserve it in the event that the LRUs containing it are replaced.

1.1.4 Shared Accounts

Shared accounts are useful because of the special environment of aircraft being a mobile unconnected network. It may be impractical to consider requiring all access be with individual, non-shared accounts, as is the typical best practice for ground IT systems, due to the requirement of keeping the ACL up to date.

A. Guidance: The specification of access control lists should not preclude the use of shared accounts. Consideration should be given as to how often, or whether, to support updating shared account authentication credentials.

> **Rationale:** Shared accounts are useful for access in which individual user logging is not required and for which a pool of individuals can be identified as having regular and legitimate need for access. On the

other hand, shared accounts are generally not adequate to control access to any critical data such as personal or financial confidential information.

Having different shared account credentials on different aircraft negates the benefits of the shared account. Requiring a user to know or carry two credentials for the same shared account for any length of time is impractical and with passwords is risky, as it encourages writing it down.

Assumptions: The airlines access control needs are specific to the airline.

Caution: If unique user identification and authentication is required, this technique does not provide such unique identification.

B. Guideline: If a system requires authenticated logins, ensure that unsuccessful login attempts are controlled. After a set limit of consecutive failed attempts, the user/account should be locked out for a defined period of time. To prevent a denial of service, the account should not be permanently blocked. The specification should allow the airline to define the lockout period and the maximum number of unsuccessful attempts. (ref. SP 800-53 AC-7)

Assumptions: An individual account is specified by the attempting user. There may be some (e.g., biometric) login mechanisms that have no account selected and therefore there is no account to be locked out.

Rationale: Makes brute-force attempts on an account more difficult.

C. Guideline: If a system requires authenticated user logins, ensure that user login sessions are not usurped by walk-up users or unauthorized users. There are multiple ways to accomplish this, including physical access controls to the login session device. Alternatively, login sessions should time-out after a period of no activity, and should either automatically log the user out or lock the screen and require re-authentication of the current user. (ref. SP 800-53 AC-11)

Rationale: This technique limits the exposure to walk/pick up access to and use the session as if they were the previous user.

D. Guideline: The system should set a limit on the number of concurrent sessions by the same individual user account. The limitation for an information system account may be global, by account, by account type, or a combination thereof. (ref. SP 800-53 AC-10)

Rationale: Concurrent logins may be an indication of unauthorized use of the same account by another user; on the other hand, concurrent logins may be useful by a maintenance technician working in multiple areas of the aircraft when accessing the system via fixed terminals.

E. Guideline: If a system allows for, or may connect to, wireless client devices, the specification for that system should require that wireless devices and external accesses are recognized such that greater security can be applied to them.

F. Guideline: The system shall be able to distinguish access among wireless clients (which may be on or outside the aircraft), network paths originating outside the aircraft (i.e., remote access), and fixed-location wired connections. An assessment should determine if enhanced access controls beyond those used for fixed or wired interfaces are required for wireless or remote access. (ref. SP 800-53 AC-17, AC-19)

> **Rationale:** Access to aircraft systems from outside the aircraft does not benefit from traditional physical and operational aircraft access controls, and therefore greater control may be necessary depending on what those sessions can do.
>
> Wireless access implies greater uncertainty about from where and who is operating the session since no specific physical location can be inferred. As well, all wireless transmissions are more subject to eavesdropping, denial of service and spoofing.

1.1.5 Remote Access

For the purpose of this document, the term remote access refers to electronic interchange between an airplane system and a system not installed on the airplane. Such electronic interchange can, for example, be performed while the airplane is on the ground connected to an airport network or flying and connected via a digital link such as satellite. Note that due to the threats posed by man-in-the middle attacks, connections initiated by an airplane system are included as well as those initiated by the remote operator or system.

If a remote access interchange can change the configuration of the airplane or can initiate a test sequence or other control function by the system, it should be considered to be a remote maintenance or operational task and is also subject to Maintenance considerations. See Section 1.6 of this attachment.

1.1.5.1 Criticality Considerations

Remote access to a system should be assessed during overall airplane systems design based on the criticality of such system as well as the benefit of such capability for that system.

Guideline: System designers should assess the advantages of implementing remote access against the potential safety impact of the related security threat. For essential systems, the inconvenience of guaranteeing a level of security compatible with the criticality of these systems may outweigh the advantage of such a feature. The system designers should factor-in the security of the ground-to-air data link in the overall safety assessment of this system.

1.1.5.2 Wireless Networks

If the remote connection is established over a ground based wireless network, system designers should ensure that the wireless network access is adequately protected. An example of such protection might be disabling the network during certain flight phases, or disabling Gatelink access at facilities not considered trustworthy.

Guideline: Wireless access should only be enabled in a controlled environment. For that purpose the airplane system should have the capability to turn the wireless access on and off. When this access is enabled, sufficient access security should be enforced to prevent unauthorized access.

1.1.5.3 Multiple Use of Wireless Access

To reduce cost and installation constraint, wireless access on an aircraft may be used for remote access for multiple purposes such as maintenance as well as operational use such as providing network connection to passengers or cabin crew members. It is important that subsystems be able to recognize authorized remote operators or systems requesting connection and grant access only when it is correct and safe to provide such access.

Guideline: If a wireless network can be used for remote access to multiple systems, it is necessary that a device trying to attach to that network be authenticated and authorized. Depending on the condition of the airplane at the time the connection is being established the wireless system can reject device attachment to the network, or a system can reject the remote access by a remote operator or system based on a predefined set of rules. Systems must have the necessary resources and access to adequate airplane parameters.

> **Rationale:** For example: A wireless network used during commercial airline operation could deny access to a maintenance device when the airplane is flying, even if the correct credentials are presented, based on the weight-off-wheel or aircraft flight phases parameters.

1.1.5.4 Remote Access Control

In order to mitigate the security threat to the general airplane network, systems supporting remote access should rely on strong authenticators bound to the role or identity of the remote operator or system to allow establishment of a remote session. Such an authentication function need not be the responsibility of the system itself.

Guideline: Remote access should only be conducted from trusted sources. In order for a system to distinguish between a trusted source and a not trusted source, adequate credentials need to be presented. Please refer to the sections above for guidance on how to specify remote access control.

1.1.5.5 Privacy of Remote Access

A link established for remote access may need to be protected against eavesdropping if valuable information is exchanged during the transaction.

Guideline: Privacy of remote access cannot always be guaranteed by the network itself. For that purpose, the benefits of encryption must be considered.

1.1.6 Mobile Devices and Exposed Data Ports

At the time of this writing there is no industry standard for remote access ports installed on aircraft. Exposed data ports may facilitate maintenance and other activities; however one should also take into consideration the fact that they add an additional level of exposure to security threats. Uncontrolled devices may be inserted into such data ports with or without malicious intent and may alter the behavior of the airborne computer they are connected to.

Guideline: Specification writers and system designers should ensure that remote data ports are protected from physical access by unauthorized personnel.

> **Rationale:** Use of protocols such as Ethernet among airplane systems as well as the intent to unify maintenance tools around commercial laptops has led the industry to deploy standard commercial off the shelf access ports (i.e., RJ45, USB) to provide data connectivity. By ensuring that these ports are physically protected against access by unauthorized users, such as for example passengers or cleaning personnel, an additional layer of defense can be leveraged for access control. For instance, maintenance ports in controlled environments such as the cockpit or electronic bays may provide adequate physical protection. Note that physical protection does not mean that no additional protection is required to systematically meet security and safety objectives of a given system.
>
> Exposed commercial-off-the-shelf ports such as USB may present a vulnerability to systems that would possibly boot or execute the content of the inserted device. In addition, continuing airworthiness mandates tight configuration control of an airplane and new software should not be loaded without a properly controlled and approved process.

Guideline: Computers exposing data ports should not automatically execute or load the content of a device inserted in such ports.

> **Rationale:** USB or RJ45 ports can be used to load new software or content. However, the action should be initiated by accredited operators following a controlled process. In any case, the content of the inserted media should be verified in accordance with the recommendation of Section 1.7 of this attachment. Automatic execution of code contained in an inserted media is strongly discouraged, especially boot-time execution.

1.2 System and Information Integrity

The integrity of an airplane's information system provides assurance that the quality of the system, when it performs its intended function, is in an unimpaired state and free from deliberate or inadvertent unauthorized manipulation. This control family should be reviewed to gain an understanding of how system integrity (SI) may apply to the problem domain.

Generally, SI controls that apply to airborne network environments address flaw remediation, malicious code protection, information system monitoring, security advisories, security function verification, software and information integrity, information input restriction and validation and error handling.

Many of these considerations present design challenges in airborne network environments versus their classic ground based implementations. Non-aircraft implementations generally assume a rate of change to software and data not typical in airborne network environments. Additionally, many confusingly similar controls provided by other existing processes may create a duplication of effort. A good example of a confusingly similar control is input validation. In the software development process, input validation is classically addressed by other existing processes (i.e., SAE ARP-4754, RTCA DO-178B, EUROCAE ED-12) however, information security exploits (i.e., deliberate information manipulation) may not be properly considered. Although the control seems to be a duplication of effort, the type of validation intended by the SI controls require an understanding of known security exploits where input validation can be an effective mitigation strategy. In attacks such as SQL-Injection or Cross Site Scripting (XSS), the attack is designed to circumvent classic input validation approaches. Without knowledge of and attention to these kind of security exploits, traditional best practice aviation systems design would not protect against these well-known types of attacks.

Put another way, if deliberate exploits are possible against airplane networks, it is essential that the designers of the systems and networks be skilled enough in the use of whatever technology they choose to successfully implement robust systems. In the above example, this may mean becoming familiar with and skilled in the design of secure web services if one chooses to use web technology in a design. Being competent in the use of one's chosen technology is traditionally assumed to be a given in this industry. This discussion suggests considerations and issues associated with becoming competent in secure development practices.

The rate of change problem is of particular interest for SI controls because they infer monitoring and remediation unprecedented in the aero industry. Most technologies used to support SI require frequent updates such as anti-virus software and intrusion detection systems or otherwise become ineffective. The reader should pay particular attention to efficiencies gained by the recommended technology relative to the existing environment's ability to support the maintenance activity for the required controls. In cases where control maintenance exceeds the technology benefit, alternate mitigation strategies should be considered.

In addition to the “extra” considerations of the NIST SP 800-53 System and Information Integrity (SI) family controls, the use of these in aeronautical systems can be challenging because:

- The SI family is identified in the operational controls class. In most cases, operations will expect functionality to facilitate implementation of a control and as a result, should be considered in the development of systems.
- The baseline assumptions and implementation requirements for aircraft systems will need to align themselves with this family in addition to other industry standards which may contain confusingly similar objectives as stated above. The appropriate industry standards and the context in which they apply must be provided.
- System and information integrity assurance requirements, as well as functional requirements and design techniques, may differ between the different aircraft system domains described in ARINC Specification 664 Part 5. In these cases, it is especially important to provide detailed considerations that are simultaneously applicable and useful to specifications for systems in all domains.

1.2.1 Public Protocols

Commercial components and designs using IETF RFC-based protocols are of great interest due to perceptions of cost reduction, functionality, and interoperability. In a benign environment, where all interactions with such components and designs are by well-intentioned parties, these objectives may be easily achievable. However, public protocols need to be carefully analyzed for the suitability due to well-known vulnerabilities.

Additionally, there is a high-rate of vulnerability announcements for virtually all products in which the user of the product exchanges information with external and anonymous parties. Such findings result in frequent operational restrictions and product updates to protect the well-intentioned user from people who would use the product vulnerabilities against them. Incorporation of such products into aircraft systems stands to render aircraft similarly vulnerable unless great care is taken to prevent the situation.

Guideline: When considering public protocols, standards developers and system implementers should analyze known and likely vulnerabilities of the public protocol, recommending mitigations or accepting the risks, while acknowledging they are restricted from using typical best practices of the IT industry (such as constant human monitoring and frequent patches) to mitigate them.

> **Caution:** One important thing to remember about the specification or use of any open protocol, design, or product – your adversary almost certainly knows more about its strengths and weaknesses than you do, and is willing to use that knowledge if possible. Conversely, use of private protocol, design, or product does not guarantee fewer security vulnerabilities; in fact, given that public protocols that are constantly scrutinized for vulnerabilities by a large user community,

they can result in a more secure product than a custom one that has not had the same scrutiny.

1.3 System and Communication Protection

1.3.1 Transmission Confidentiality / Integrity

Without adequate protections, communications via air-ground or ground-ground data links may be susceptible to unauthorized disclosure (loss of confidentiality) and/or modification (loss of integrity).

The need for transmission confidentiality/integrity protection is determined based on the results of an information security risk assessment described by ARINC Report 811 (or equivalent assessment), which identifies and assesses the impact of intentional threats. During subsequent security control selection and assessment, it is also important to determine the protocol layers in which it is appropriate to implement protections. For example, application layer security alone may be sufficient to mitigate risk in some cases; whereas other cases may warrant use of application security in addition to transport and/or network layer security.

Note that cryptographic security solutions may be necessary when the application of procedural or non-cryptographic solutions (e.g., checksums) is insufficient to mitigate risk(s) to an acceptable level. However, when employing cryptography, it is important to consider national/international laws regarding import/export/usage (particularly encryption), as well as its potential impact on system performance and airline operations.

Guideline: Protection of IP-based transmissions shall be achieved using either Transport Layer Security (TLS) or Internet Protocol Security (IPsec) as specified in Section 2.5 of ICAO Doc. 9896.

Rationale: Working Group I (WG-I) of the ICAO Aeronautical Telecommunications Panel (ACP) spent several years assessing security protocols suitable for protecting IP transmissions in both air-ground and ground-ground environments. The ICAO ATN/IPS document specifies protocols consistent with Internet RFCs as a way to leverage commercial off-the-shelf (COTS) solutions and exploit economies of scale rather than more costly aero-unique solutions. However, since Internet RFCs allow some degree of flexibility (e.g., crypto algorithm suites), the ATN/IPS document includes requirements that restrict the range of potential solutions as necessary to ensure global interoperability. Although the ATN/IPS requirements are targeted for air traffic management applications, re-use for non-safety applications is consistent with the Common Controls Security Objective, per ARINC Report 811, Attachment 3.

Assumptions: The need to protect specific air-ground or ground-ground data links is determined via an information security risk assessment, per ARINC Report 811 or equivalent assessment.

Caution: Despite the desirability of following ICAO recommendations, this does not resolve the issue of import/export and other laws related to products using cryptography.

Applicable Reference: ICAO Doc. 9896, Manual for the ATN using IPS Standards and Protocols (ATN/IPS).

1.3.2 Cryptographic Key Establishment

Cryptographic key establishment is a secure process by which communicating entities establish a shared cryptographic key. This key is then used with cryptographic algorithms that are used to protect information and communications.

Guideline: When IPsec is used to protect IP-based transmissions, cryptographic key establishment shall be achieved using Internet Key Exchange version 2 (IKEv2) as specified in Section 2.5 of ICAO Doc. 9896.

Rationale: Working Group I (WG-I) of the ICAO Aeronautical Telecommunications Panel (ACP) spent several years assessing security protocols suitable for cryptographic key establishment used in conjunction with IPsec. The ICAO ATN/IPS document specifies protocols consistent with Internet RFCs as a way to leverage commercial off-the-shelf (COTS) solutions and exploit economies of scale rather than more costly aero-unique solutions. However, since Internet RFCs allow some degree of flexibility (e.g., crypto algorithm suites), the ATN/IPS document includes requirements that restrict the range of potential solutions as necessary to ensure global interoperability. Although the ATN/IPS requirements are targeted for air traffic management applications, re-use for non-safety applications is consistent with the Common Controls Security Objective, per ARINC Report 811, Attachment 3.

Assumptions: None.

Applicable Reference: ICAO Doc. 9896, Manual for the ATN using IPS Standards and Protocols (ATN/IPS).

1.3.3 Public Key Infrastructure (PKI) Certificates

Asymmetric cryptographic algorithms, such as those used to implement digital signatures and key establishment schemes, use a pair of mathematically related keys and one-way functions, which are easy to compute using one of the keys but very difficult to solve without knowing the related key. To ensure security, one of the keys must be kept private and protected from compromise, while the other key may be distributed publicly. Since a public key may be stored and distributed using non-secure means, it is important that the relying party (i.e., the user or application relying on the public key) be able to trust that the public key is authentic.

A public key infrastructure (PKI) provides a trust framework, and a Certificate Authority (CA) is a trusted PKI entity that binds a public key with the identity of the entity for which the key pair was generated. The binding occurs when a CA digitally signs the content of the public key certificate. Prior to using the public key contained in a certificate, a relying party: 1) validates the CA’s digital signature to ensure that the certificate is authentic (i.e., the public key is associated with the entity identified in the certificate) and that it has not been modified during storage or distribution; and 2) may check a Certificate Revocation List (CRL) or use some other means to verify that the certificate has not been revoked.

In general, commercial certificates and CRLs comply with the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile as specified in RFC 5280.

Guideline: X.509 public key certificates and certificate revocation lists (CRLs) shall comply with the certificate and CRL profiles specified in ATA Spec 42.

> **Rationale**: The Air Transport Association (ATA) Digital Security Working Group (DSWG) developed a certificate policy for use in the civil aviation community. ATA Spec 42 includes certificate and CRL profiles that are suitable for aeronautical applications and interoperability with an aerospace industry bridge. These profiles provide greater specificity than, but do not conflict with, Internet RFC 5280. Existing ARINC Standards (e.g., ARINC Specification 822) and ICAO Doc. 9896, ATN/IPS, reference ATA Spec 42.
>
> **Assumptions**: (1) The scope of this policy is inter-organizational communications protected using a certificate-based security solution (e.g., IPsec); however, re-use of the policy for intra-organizational communications (e.g., within an airline) has the potential to minimize key management infrastructure and key management life cycle costs. (2) An analysis is performed to ensure that compliance with ATA Spec 42 is consistent with organizational practices and/or regulatory requirements.
>
> **Applicable Reference**: ATA Spec 42, Aviation Industry Standards for Digital Information Security.

1.4 Certificate Management

This section addresses certificate management based on a PKI as outlined in Section 1.3.3 of this attachment. Avionics development programs and related industry standards should take into consideration the operational aspects of PKI and not force airlines into implementing a process that is incompatible with ground PKI implementations or, worse yet, a new process for every new component placed on aircraft that requires a certificate.

If specifications employing cryptography are written before the key management standards solidify (as indeed some already have been), they should carefully consider how to define their own key management requirements with sufficient isolation from their function so that they need not require extensive modification when key management standards emerge, and ideally so that they are relatively agnostic to the key management process overall. This requires careful documentation of assumptions, constraints and requirements pertaining to key usage.

ATTACHMENT 1
STANDARDS DEVELOPMENT GUIDELINES

For many airlines, placing digital certificates on aircraft may be a completely new concept presenting multiple challenges. Some of these are:

1. Airlines may have limited knowledge of PKI.
2. In most airlines (if not all) PKI is managed by the IT security division, rather than aircraft maintenance.
3. Airlines will need to determine how to incorporate, coordinate or integrate IT functions, to the extent necessary, with aircraft maintenance functions, roles and responsibilities within their unique business organization.
4. Airlines will need to determine / verify each division's roles and responsibilities (Corporate Security, IT Security, Aircraft Engineering, Aircraft Maintenance, etc.)
5. Airlines will need corporate, legal and security policy review of PKI.
6. Airlines will need to address the differences between device certificates and personal certificates.
7. Airlines will have to support multiple dissimilar methods of generating and installing digital certificates onto avionics components (possibly including device key pair generation on aircraft avionics and on ground systems).
8. Airlines will need to determine the device certificate vetting process.

While the above items mention what airlines need to consider, it provides insight into what the operators will be faced with and what industry standards should consider.

1. Developers should make it possible for airlines to clearly and cleanly establish roles and responsibilities to the extent necessary such that airlines can accomplish item 3 above.
2. Developers should be aware of the device certificate vetting process required by CA suppliers. (ref. ATA Spec 42)

Also mentioned in Section 1.3.3 above, airlines need to determine whether they will be implementing an internal versus external PKI for certificate use. While there's any number of reasons an airline might choose one over the other, the important point is that standard development should not preclude either approach. Should an airline elect to outsource (external) their PKI with a Certificate Authority (CA) supplier there are contractual requirements placed upon the airline by the CA supplier. These requirements are expected to be supported by the avionics solution, from a software, hardware and procedural aspect. It is possible that a poorly developed standard and/or implementation would not allow for, or would not meet, one or more of these requirements and therefore present implementation and/or operational issues for airlines.

Certificates are used for a number of different functions, such as verifying identity and encrypting messages. ATA Spec 42 defines many digital security guidelines that should be taken into consideration when developing standards that either will use or in some way be part of a PKI solution. Chapter 3 – Implementation Guidance on the use of PKI in the Civil Aviation Industry was specifically written to help system developers and standards bodies tasked with implementing and operating systems using cryptographic components.

ATTACHMENT 1
STANDARDS DEVELOPMENT GUIDELINES

A. Guideline: When specifications either directly implement or interface to a digital certificate solution they need to follow the ATA Spec 42 guidelines.

Rationale: ATA Spec 42 details the PKI requirements and specifications for the civil aviation industry.

Caution: ATA Spec 42, Chapter 3 addresses implementation guidance, but there are areas that are not covered. Also there are some standard PKI practices that may not work in airplane systems.

Assumptions: Each CA supplier has its own unique practices, extensions, and unique characteristics. ATA Spec 42 is the civil aviation industry standard and is assumed to provide a common framework.

Applicable Reference: ATA Spec 42, Aviation Industry Standards for Digital Information Security.

B. Guideline: Best practice is that private keys are never transported to an avionics component. If this is not possible, a solution to securely generate and deliver keys must be provided, since no such capability exists in general.

Rationale: The entire process from key pair generation to certificate (and possibly private key) installation onto the aircraft must be secure. A system's security is only as strong as its weakest link. It does little good to generate a high-strength key pair and certificate only to have a poorly implemented and highly vulnerable transfer to the aircraft.

Caution: Some avionics may not be able to meet the requirements for, or have the capability to, generate a public/private key pair necessary for the digital certificate process. Therefore a ground based system may be required to perform this function which presents a number of issues, such as secure transport of the private key onto the avionics component, and ensuring that this private key has the appropriate security.

Assumptions: Secure transport of the private key (and certificate) onto an avionics component cannot assume a new line maintenance classification as the airlines may not be able to support such an approach.

C. Guideline: Transfer to and installation of certificates on avionics components must be performed by line maintenance personnel, not IT personnel.

Rationale: There are both regulatory and possible Union issues that would not allow IT personnel to install (data load) anything onto an aircraft. Similarly aircraft mechanics will not be managing the airline's corporate PKI implementation.

Caution: At most airlines (if not all) PKI is managed by security in the IT division and therefore secure transport capabilities of the certificate (and possibly private key) onto an avionics component needs to incorporate this handoff capability.

Assumptions: An automated update process may not exist. While this does not preclude the development of such a process, in its absence, the cost of labor should be considered. In addition, designers should not assume the existence of initialization keys that can be used to secure the transfer of new keys.

D. Guideline: Standards developers working in this area need to be aware that there are external standards and process requirements that must be met by avionics components that utilize digital certificates.

Rationale: Digital certificate IT (and CA supplier) requirements do extend into the avionics component and must be considered in avionics development programs and therefore specified in industry standards.

Caution: A number of these requirements are based on the CA supplier's Certificate Policy (CP) which is a legally binding document. These documents are unique to each CA, so care must be taken when examining information from a specific CA in order to develop industry standards.

Assumptions: Aircraft configuration control processes must be maintained.

E. Guideline: Given there is currently no defined aircraft certificate system at the time of this writing, there needs to be informal coordination and strong consideration of the number of keys an airline may be forced to maintain.

Rationale: If every new component on the aircraft that requires a certificate also requires its own certificate with its own unique process airlines will be faced with an unmanageable situation.

Caution: Individual standards developers have no visibility into or control of how many other systems use certificates on the airplane.

Assumptions: Airlines are prepared to maintain digital certificates and keys.

F. Guideline: Standards developers need to consider the nature of digital certificates, their limited life spans and need to be changed quickly if revoked for whatever reason, and allow for as easy as possible replacement/renewal in specification development.

Rationale: Airlines must have the flexibility to load new certificates without the burden, timeframes and expense associated with the controls surrounding a software part number role. Probably the most obvious example that demonstrates this requirement is a private key compromise that renders the certificate useless, forces its revocation and immediately requires an airline to issue a new certificate.

Caution: This guideline specifically addresses digital certificates that the operators are expected to be responsible for. There may be other digital certificate types on an aircraft that are outside the scope of this guideline.

Assumptions: The avionic equipment supports digital certificate replacement.

G. Guideline: Best practice is that certificates should be renewed according to ATA Spec 42.

Rationale: IT industry best practice is that certificates be renewed every 3 years.

Caution: Certificate renewal should be able to be coordinated with aircraft maintenance activity in order to minimize the impact to the airline.

Assumptions: None

1.5 Security Logging

Aircraft manufactures have different cockpit and operational philosophies, and airlines expect event and maintenance logging to be consistent within any aircraft type. Unfortunately, the specification of overall aircraft or system logging requirements is currently the responsibility of the system(s) integrators, typically the airframe manufacturer. However, at the specification level, some high-level guidelines for security logging may be provided as discussed in this section. That said, it also means that security logging needs to be an integral part of any other kind of event logging or parameter monitoring, because in many instances security events cannot be clearly differentiated from normal operation or non-security-related failure. In such cases it may be that a security-related event may reveal itself in a more thorough examination.

It is highly desirable that security logging be consistent and standardized across aircraft types and systems.

1.5.1 Specifying Security Control Logging Requirements

On the system level it is important to discriminate between pure security control functions and those which serve the aircraft functionally in a more general sense; that is, they may contribute to security but are present in the design for some other reason. When something happens to a security function, it may be valid to conclude that the most likely cause is of interest to “security” rather than to reliability in general. “Security event logging” is fairly easy to address for these functions. One example of a function that is inherently related to security is authentication for purposes of access control. Apart from that general case however, there is no definition, let alone a standard definition, for a “security event”. Therefore it’s up to the specification writer to provide information to the implementer(s) concerning the identification of behaviors or other symptoms that constitute failures in or violation of security policies that are or should be defined for a system.

Some external regulations or standards may require logging, for example financial processors or personal privacy laws. See IFE Security Event Logging Use Case for an example based on considering the requirements from the PCI Council around processing credit card data.

A. Guideline: Specification of security event logging requirements and objectives should be done as part of any specified security control functionality. This includes any required protection of the logged data from “tampering” or unauthorized access. Also what constitutes a “security event” should be included as part of the security control specification. The following types of security events should be considered, some of which may overlap existing maintenance events:

- Authentication failures and successes

- Unexpected inputs where inputs from unauthorized sources can't be ruled out
- Loading of new security data (ACL, keys, firewall rules, binaries, etc.) – noting that this overlaps basic airplane configuration management.
- Disabling/enabling of interfaces or functions
- User login/logout events (related to authentication successes)
- All events requiring privileged access
- Access to the security log or other sensitive data
- All actions taken by administrative or root accounts
- Access denied errors

Rationale: As specifications require and specify security controls, the security event logging requirements need to be explicitly stated as part of the security control functionality, and NOT be left to the implementer, which might lead to inconsistent implementation.

Caution: At the present time, there is no recording system or functional specification for central "security logging" on commercial aircraft.

Assumptions: The developer has the expertise to specify the security event logging requirements of the security control that they specify.

B. Guideline: For every recorded security event, at least the following metadata should be recorded along with it:

- User identification (if applicable and available)
- Type of event
- Date and time
- Origination of event
- Identify or name of affected data, system, or resource.

Assumptions: At least the recording entity has access to the date and time.

1.5.2 Aircraft Function, (Normal) Logging

In contrast to the specified logging requirements of security functions, the implementer of "normal" aircraft functions has always been required to monitor and log "events". Currently, almost all aircraft types contain systems that are recording a significant amount of data in various systems, sometimes specifically collected from a large group of other systems, which report either on demand or at a certain repetition rate. Note that the existence of a system that records data does not imply the existence of a useful recording standard for that system.

Many types of "events" are already being recorded by specific systems and equipment. Some of these types are:

- Aircraft conditions, consolidated into reports (system status, health, etc.)
- Regular (widely constant rate) system data

- Cockpit voice/Aircraft internal sound
- System Failures or abnormal “out-of envelope” behavior
- Flight conditions
- ATN/ATC data communication
- Crew Observations
- Maintenance Actions
- Passenger Usage (Billing and Accounting)
- Etc.

Guideline: The specification writer of “normal” aircraft functions should specifically consider and direct the implementer to specifically consider, intentional disruption as part of the overall logging requirements of more normal, classical events.

Rationale: Current world events require that security be a part of everyone’s thinking and, for the system designer and equipment implementer, system exposure to intentional disruption must be included in the evaluation. Each specification and/or piece of equipment should consider the unique characteristics of the target environment and log events that may be part of intentional disruption upstream of their inputs.

Caution: The intent or root cause behind failures is not usually obvious – it may in fact not be possible to distinguish between “simple” failure or malfunction and deliberate disruption or malicious manipulation. As is typical in such instances, the specific reasons behind a failure may only become obvious through investigation. In the case of maintenance activities, this is often accomplished through Fault Isolation Procedures. In instances where a cause is not obvious from an observed effect, fault isolation may serve to clarify whether a particular event or failure was due to malicious (i.e., security-related) activity or is simply a random or other non-security related failure. Reliance on one clear indication for reporting is to be preferred over multiple records of a suspicious nature.

Assumption: The action to take when a security event has occurred is properly part of an airline security policy. Implementers should take care not to assume too much about what action airlines “should” take beyond resolving the effect on equipment health or aircraft airworthiness.

1.5.3 Recording Feasibility

The feasibility of storing and downloading security event records should be considered. In an aircraft environment, the availability and capacity of communications links is limited. In addition the ability to store security event records prior to downloading off the aircraft is limited.

Common approaches to IT security logging involve the recording and analysis of massive amounts of data, usually because “normal” IT system behavior is poorly defined. No one knows what constitutes “normal” behavior, and security violations may be indistinguishable from normal system activity without the collection and correlation of large amounts of data. When dealing with duly authorized individuals who are behaving in unauthorized ways, there may in fact be no clear distinction between "normal" and "abnormal" behavior.

Conversely, aircraft in general do not have the extremely large storage capacity required for such data collection, the bandwidth to move such amounts of data from aircraft to ground, nor the personnel available to airlines to collect and analyze it all – if in fact the data were to exist and be recorded.

Guideline: System specifications should provide guidelines and insight into what recording is feasible, and developers should design systems and functions in ways that provide clear symptomatic indications of failures or violations.

Rationale: Aircraft systems' nominal behavior should be far better understood and controlled than all but the most rigorously defined and monitored IT systems. If system designers follow "normal" design practices for aircraft systems, avoiding the inclusion of unintended or non-required functionality, the declaration and enforcement of network traffic to a degree similar to "legacy" wiring (in which all connections and signals that are not specified are not impossible to create), and overall monitoring of out-of-spec behavior, it should be possible to collect far more reliable data in far less quantity. Since system designers know the system expected behavior in detail, they're in an excellent position to identify anomalous behavior.

Assumptions: Even with advances in technology, storage in avionics systems and equipment is limited, certainly more limited than IT systems. Fortunately, as shown above, good design practice and attention to the limits of intended system behavior and "normal" input characteristics can yield useful records in far lower volume than in a typical IT application.

Caution: It is emphasized that attempts to mandate data logging must be supported by justification – why it is necessary; what it is going to accomplish; what other costs (collection, storage, analysis) must be incurred to make it useful and who is going to use it. It is easy to do something on the basis of "good practice" of another industry only to have it become a waste of effort because no ultimate user ever emerges for it. This is an area in which airline operations experience should provide significant input.

1.6 Maintenance

Today, maintenance operations on an aircraft are policed by official accreditation of mechanics to perform a defined set of tasks with appropriate recording of all actions (usually on paper). Continuous airworthiness relies on this accreditation and recording and assumes that unauthorized personnel cannot access aircraft or disrupt maintenance activities. Access to the aircraft is usually controlled by appropriate physical security, e.g., badging and area access controls; verification of aircraft ID is usually by checking a physical attribute such as tail number or nose number; authorized work orders detail maintenance actions; and the results of any maintenance action is recorded. If any of these processes are replaced by any innovative methods offered by networking or remote access, careful consideration of security measures should be made to establish equivalent levels of access assurance, identification of both initiator and recipient of a maintenance action and accurate and timely recording of all actions.

Trends going in the direction of an always-connected-airplane may offer opportunities to provide always-on maintenance links allowing remote troubleshooting or data gathering.

When specifying such features, specification writers should pay special attention to the consequences of a security breach on one of these links. If an airplane system can be accessed remotely, then the mechanic's accreditation mentioned earlier must be replaced by adequate security controls.

At a minimum, specifications should identify any special considerations implementers should be aware of regarding installation design or maintenance procedures.

For a further discussion, see Section 1.1.5, Remote Access, of this attachment.

1.7 Media Protection: Security Considerations for the Distribution of Software

NIST SP 800-53 Media Protection focuses on the physical media used to transport data to be loaded into a system from one computer or handler to another. However, with the availability of broadband access to aircraft, media-less data loading is now possible. This section focuses on the content of load-media rather than the media itself as appropriate content protection is applicable whether an actual physical media is used or not.

Security aspects of distribution of software cannot be restricted to equipment only. A system level approach is necessary to identify all the stakeholders in the trust chain from the computer from which a piece of data is generated to the target equipment onto which it is loaded. Implementers are expected to understand the implication of their particular equipment or interface within the security chain in order to make recommendations.

Media which is sensitive to security concerns should be treated appropriately. Such media include media used to load new software on airplane loaders (physical MSP per ARINC Report 827) and media used to load data to and from an airplane system (fault reports, flight plans, entertainment content).

While data loaded into non-essential systems does not require protection as far as airplane safety and airworthiness is concerned, it must be recognized that certain non-essential systems deal with data that need to be protected as they are either private (airline maintenance data, passenger manifests, credit card information, etc.) or protected by copyright laws (entertainment content). In addition, software parts in general are proprietary and should be protected from inadvertent or unnecessary disclosure.

Security provisions for the distribution and configuration management of aircraft software are the responsibility of AMC Working Groups for Field Loadable Software (FLS) and Electronic Distribution of Software (EDS). Recent new aircraft designs (i.e., Airbus A380 and Boeing 787) have increased numbers of software part numbers and have implemented differing security mechanisms for the distribution and configuration management of those software parts.

ATTACHMENT 1
STANDARDS DEVELOPMENT GUIDELINES

As broadband access to the aircraft, e.g., Gatelink, and network connectivity to onboard systems increases, the possibility of software data loading remotely across these broadband links, eliminating the manual loading procedures performed by the technician onboard the aircraft, becomes very attractive to aircraft operators. These new software data loading pathways will require a rethinking of the security and configuration management practices currently in use.

ARINC Report 811 provides a three-step process for evaluating the need for security measures and should be applied to the area of software distribution and loading.

1.7.1 Media Format and Distribution

Guideline: Standards should not impose media protection or distribution guidelines that differ from ARINC Report 827 as it may create incompatibility and additional burden on operators.

Rationale: ARINC Report 827 provides for both signatures and encryption as an option. Depending on the level of data security required for the particular application being distributed both encryption and digital signature may be used.

Caution: Note that neither the international legal ramifications nor issues of key management on aircraft are addressed in this recommendation.

1.7.2 Authentication

Guideline: Standards should require any media used to load data into systems to have their content protected against tampering and unauthorized loads. The use of digital signatures to authenticate and validate the origin of the data being distributed is encouraged to be in accordance with ARINC Report 827.

Rationale: A digital signature on data that is being distributed will reduce the likelihood that intentionally corrupted data will remain undetected.

Caution: Verification of digital signatures requires the receiving entity to hold the public certificate of the signing entity. Certificate management is described in Section 1.4 of this attachment.

1.7.3 Confidentiality

Guideline: Standards should require media containing confidential information to use encryption using cryptographic algorithms and key lengths appropriate to the length of time that the data must be protected.

Rationale: Confidential information on portable media should be protected from a media transporter/handler's accidental or illicit inspection or copying. Revealing information to those transporting the media, who cannot be assumed are permitted to view it, should be avoided. A seal or envelope containing the media only indicates tampering but does not prevent it.

Assumptions: Keys to decrypt and the associated decryption algorithm are available on the destination aircraft system.

Caution: Note that neither the international legal ramifications nor issues of key management on aircraft are addressed in this recommendation.

1.7.4 Integrity

A. Guideline: Standards should require media containing confidential information to be protected by a digital signature in order to provide an integrity check to reduce the likelihood of undetected intentional modification.

Rationale: Any on-board system receiving confidential information should be able to verify that this data comes from an authenticated source. For example, when loading a new Wi-Fi key, one wants to be sure it is not fake. Confidential information on portable media should be protected against undetected intentional modification in addition to the legacy practice of protection against unintentional corruption. (A simple checksum does not protect against intentional collision; that is, finding a new string that produces the same checksum. Transmitting the checksum, simple or not, with the content does not protect against malicious modifiers modifying the checksum value itself.)

Assumption: A certificate to check the signature is available on the destination system.

B. Guideline: When requiring malware protection/detection upon insertion of mass storage media, the reader should be aware that the use of commercial signature-based virus and malware detection programs to validate content of media is an efficient way to prevent malware propagation only on COTS operating systems which have demonstrated sensitivity to such attacks.

Rationale: Most systems on board aircraft rely on proprietary operating systems for which there is no known malware development activity. Since signature based anti-virus software rely on signature files or database to detect malware, the usage of such software on airplane is not recommended as it needs to be regularly updated to be kept up to date, often every 24 hours, sometimes more often. As most aircraft systems remain completely separated from commercial networks (i.e., Internet or airline private network), the update of such anti-virus software could often only be done via portable media and would create additional unwanted scheduled maintenance activity thus increasing greatly the cost of ownership of such systems. In addition, aircraft life could span up to 25 years and it is unrealistic that a commercial anti-virus company would accept to contract or guaranty updates for such an extended period of time. In that case, even if no changes are made to the system during that time, the anti-virus itself would need to be changed thus resulting in additional maintenance activity, potential configuration changes and possible impact on the certification of the airplane.

Usage of such software is hence discouraged and should only be considered for systems running an operating system whose vulnerability to malware is left exposed.

Assumption: Malware sensitive operating system features such as auto-run on insertion of load media (USB thumb drives or CD-ROM) are detected and remediated (i.e., disabled) during the vulnerability analysis of a system supporting such an operating system.

1.7.5 Availability

Guideline: Standards should require media containing confidential information to be traceable from handler to handler. Implementers should consider whether or not the specified LRU needs physical access controls around its media access ports.

Rationale: Even if data is encrypted, stealing the media allows attackers all the time they need to crack it. Some of the public may also steal it simply for the value of the media itself. (e.g., high density flash drives).

Assumptions: Media containing confidential information is not left on the aircraft in a publicly accessible state such that a passenger could remove it. Airline or maintenance crew accessing non-public areas of the aircraft have other mitigating access controls and are vetted by other procedures, which may permit the designer of equipment placed in such non-public areas to have no physical access controls around loadable media in their equipment. As an example, equipment installed in the cockpit may expose a standard data load port (e.g., USB, RJ45, etc.) with no additional physical protection if it can be shown that adequate protection of cockpit access itself is controlled through a procedural protection.

1.8 Configuration Management: Updates to User Modifiable Elements

To be added in a future revision.

APPENDIX A REFERENCE MATERIAL

The following table provides reference material for considering cyber security.

ARINC 664P5	ARINC Specification 664 Part 5, “Aircraft Data Network, Part 5 – Network Domain Characteristics and Interconnection”
ARINC 811	ARINC Report 811, “Commercial Aircraft Information Security Concepts of Operation and Process Framework”
ISO/IEC 15288	ISO/IEC 15288, “Systems and software engineering – System life cycle processes”, Feb 2008
ISO/IEC 15408	ISO/IEC 15408:1999, “Information Technology – Security Techniques - Evaluation criteria for IT security, Part 1: Introduction and general model”, First Edition, 1999-12-01.
ISO/IEC 15408	ISO/IEC 15408:2005, “Information Technology – Security Techniques – Evaluation criteria for IT security, Part 1: Introduction and general model”, Second Edition, 2005-10-01
ISO/IEC 27001	ISO/IEC 27001, “Information technology – Security techniques – Code of practice for Information security management “, June 2005
ISO/IEC 27002	ISO/IEC 27002, “Information technology – Security techniques - Information security risk management”, June 2008
ISO/IEC FDIS 27003	ISO/IEC FDIS 27003, “Information technology – Security techniques – Information security management system implementation guidance”, 2009
ISO/IEC FDIS 27004	ISO/IEC FDIS 27004, “Information technology – Security techniques – Information security management – Measurement”
ISO/IEC 27005	ISO/IEC 27005, “Information technology – Security techniques – Information security risk management”, June 2008
SP 800-12	NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, 1995, currently available from: *http://csrc.nist.gov/publications/nistpubs*
SP 800-27	NIST, Special Publication 800-27, Engineering Principles for Information Technology Security, June 2004, currently available from: *http://csrc.nist.gov/publications/nistpubs*
SP 800-30	NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems”, July 2002, currently available from: *http://csrc.nist.gov/publications/nistpubs*

APPENDIX A
REFERENCE MATERIAL

SP 800-37 NIST, Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004, currently available from: *http://csrc.nist.gov/publications/nistpubs*

SP 800-39 NIST, Special Publication 800-39, DRAFT Managing Risk from Information Systems: An Organizational Perspective, April 2008, currently available from: *http://csrc.nist.gov/publications/nistpubs*

SP 800-53 NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”, Feb 2005, currently available from: *http://csrc.nist.gov/publications/nistpubs*

SP 800-57 NIST Special Publication 800-57, “Recommendations for Key Management”, Aug 2005, currently available from: *http://csrc.nist.gov/publications/nistpubs*

SP 800-97 NIST Special Publication 800-97, “Guide to IEEE 802.11i”, June 2006, currently available from: *http://csrc.nist.gov/publications/nistpubs*

NSA IATF NSA IATF, “Information Assurance Technical Framework”, Sept 2002

RFC4949 IETF, RFC4949, Internet Security Glossary, Version 2, August 2007, currently available from: *http://www.rfc-editor.org/rfc/rfc4949.txt*

CC 3.1 Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 3, July 2009, currently available from: *http://www.commoncriteriaportal.org/thecc.html*

44 U.S.C. Title 44, US Code, §3502, currently available from: *http://uscode.house.gov/search/criteria.shtml*

ATA Spec 42 Air Transport Association, Spec 42, Aviation Industry Standards for Digital Information Security, Revision 2009.1

PCI DSS 1.2.1 Payment Card Industry (PCI) – Data Security Standard: Requirements and Security Assessment Procedures, currently available from: *https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html*

APPENDIX B GLOSSARY FOR AERONAUTICAL INFORMATION SYSTEMS SECURITY

Many terms in this document have been adopted from ARINC Report 811. This Glossary has then been further developed for a number of reasons. The initial realization was that two communities, namely the Aircraft Safety and the Aircraft Security communities, do not share a common understanding of some of these terms. Hence it was of paramount importance to avoid misinterpretations between them. Equivalently, the terminology used in the Aircraft Engineering and IT-Systems Engineering community is also quite different and it was often necessary to explain the terms used by the respective group.

Information Security has evolved in the commercial industry over many years, so definitions of terms have been established in many forums. Among those are ISO, IETF, or Common Criteria, to name a few international ones. National definitions are even more widespread, addressing the subject often from a more local perspective. This glossary is the attempt to consolidate, to the extent possible, all major definitions and to bring them into the aeronautical context. It provides abbreviations, explanations, and recommendations for use of aircraft information system security terminology. The terms and definitions provided are those accepted by RTCA SC-216/EUROCAE WG-72.

To avoid confusion, the same term or definition should be used whenever the same concept is mentioned. To improve international understanding, industry standards should use terms in their plainest, dictionary sense. This includes the use of well-established terms from industry standards documents. Private or newly made-up terms should be avoided. Terms that are proprietary, or that create a bias toward a particular security technology or mechanism versus other, competing techniques that already exist or might be developed in the future should also be avoided. Since many of these terms have been used extensively in the Information Security community, considerable effort has been made to identify the source.

Accreditation

The authorization of an Aeronautical Information System to process, store, or transmit information, granted by a management official (e.g., from a regulatory agency). Accreditation is based on an assessment of the management, operational, and technical controls associated with an Aeronautical Information System. (adapted from: NIST SP800-37)

Aeronautical Information System

The set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information involved in all aspects of aircraft operations. Note that this includes supplier’s information systems supporting the development of onboard system software and data. (adapted from: Title 44 U.S.C., §3502)

Aircraft Type Certification

The legal recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other document as required by national laws and procedures. In particular, certification of a product involves:

a. The process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety.
b. The process of assessing an individual product to ensure that it conforms with the certified type design.
c. The issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with paragraph (a) or (b) above. (SAE ARP 4754, "Certification")

Airworthiness

The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function. (SAE ARP 4754)

Assessment

A systematic evaluation of an aircraft, aircraft system, item, and its requirements. (SAE ARP 4754)

Assumptions

Statements, principles, and/or premises offered without proof. (SAE ARP 4754)

Completeness

Completeness of a requirement statement means that no attributes have been omitted and that those stated are essential. Completeness with respect to another requirement statement means completeness within the scope and attributes of the other statement. (adapted from: SAE ARP 4754)

Consistent

Consistency between requirements statements means the attributes are in agreement within the scope of the intended purposes. A design specification is consistent with the requirements if neither contradicts the other. A power budget summary is consistent with a design specification if a quantity in the budget that refers to the design specification is equal to the quantity implied by the design specification. (EUROCAE ED-202)

Data

Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. (Brinch Hansen, Operating Systems Principles, 1973, Prentice Hall)

APPENDIX B
INFORMATION SECURITY GLOSSARY

Defense in Depth

An architectural feature in which a security function is accomplished by more than one countermeasure such that an attack would require vulnerabilities in multiple countermeasures. (EUROCAE ED-202)

Denial of Service

The prevention of authorized access to resources or the delaying of time-critical operations (NIST SP800-27A)

Function

In any architectural context, when an element achieves a stated objective, that objective is a function. (EUROCAE ED-202)

Impact

Qualitative indication of the magnitude of the adverse effect of a threat condition. (EUROCAE ED-202)

Information

Information is the (subjective) interpretation of data. (Computer Security, 2nd edition, Dieter Gollmann, 2005, Wiley)

Item (Aircraft)

Any equipment, line replaceable unit, or line replaceable module. All items are characterized by a hardware definition and, where appropriate, a software definition. (SAE ARP 4754)

Malware

Malicious software that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim. (adapted from NIST SP800-83)

Objective (Security)

A statement of intent to counter identified threats threat scenarios and/or to satisfy identified organization security policies and assumptions that have been levied by a security assessment, internal or external. Security objectives specify the security problem and goals for the security countermeasures. (EUROCAE ED-202)

Operations

In any architectural context, when two or more elements cooperate to achieve a stated objective, that objective is an operation. (EUROCAE ED-202)

APPENDIX B
INFORMATION SECURITY GLOSSARY

Requirement

An identifiable element of a function specification that can be validated and against which an implementation can be verified. (EUROCAE ED-202)

Risk

Exposure to the possibility of harm. The risk of an event is a function of the severity of the adverse event and the threat likelihood of that event. (EUROCAE ED-202)

Security Environment

Generic term encompassing the operational and development environments.

Security Level

A classification of the effectiveness of a security countermeasure, its ability to reduce the likelihood of threat scenarios. A classification of the rigor and discipline in performing the supporting assurance processes needed for the development, implementation, operation, or management of a security function, based on the threat condition classifications associated with aircraft-level functions mitigated or controlled by the security function/countermeasure. (EUROCAE ED-202)

System (Aircraft)

A combination of interrelated items arranged to implement a specific aircraft-level function or group of functions. (SAE ARP 4754)

System (Information)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note that information systems consist of people, processes, and technology. (NIST SP800-53, Rev.2)

Trust

Trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel. *http://safevote.com/papers/trustdef.htm*

Validation

The determination that the requirements for a product are sufficiently correct and complete. (SAE ARP 4754)

Verification

The evaluation of an implementation of requirements to determine that they have been met. (SAE ARP 4754)

APPENDIX B
INFORMATION SECURITY GLOSSARY

Virus

A self-replicating program that runs and spreads by modifying other programs or files. (NIST SP800-61)

Vulnerability Assessment

Generic term encompassing the two existing methods, knowing vulnerability analysis or vulnerability testing, used during the evaluation of the development and anticipated operation of the aircraft/ system/ item that could be exploited by a threat source.

APPENDIX C GUIDANCE ON STANDARDS DEVELOPMENT

C-1 Specifying Aircraft Systems and Equipment Standards

System and function standards should consider the following:

- Aircraft architecture changes require new considerations in the generation of aircraft system and equipment standards.
- Adoption of new technologies requires common adaptations for aircraft not necessarily aligned on system and equipment standards.

C-1.1 Example 1

The benefits of transition from point-to-point, point-to-multipoint, and shared isolated data bus structures to networks can be lost or greatly diminished if appropriate consideration is not given in the new or altered specifications for systems.

For instance, in the specification of maintenance tooling, the data bus model transitioned from aircraft to shop fairly easily. Whether the LRU being maintained is located in a shop fixture or on an aircraft with wiring to fixed sources is largely immaterial, even though the connectivity to “live” external systems in the shop may only be to a shop tool and on the aircraft may be to a large number of other LRUs – possibly including maintenance tooling, and possibly indirectly through maintenance system LRUs on the aircraft. But the converse, the introduction of networks on aircrafts, may dramatically change the interactions of an LRU when installed compared to the interactions in the shop with a tool.

One aspect of this change is that ARINC 615A data loaders needed to include the concept of “finding” the LRUs on the network so that LRU addresses would not have to be standardized explicitly by type and that loader tools would not need to be pre-programmed with LRU addresses. In a networked Information System, this is a potential security risk. Since the standards explicitly assumed trusted wiring and trusted network configurations, this was not treated as a security risk in the standards. However, when portable equipment is attached to aircraft networks, when is it valid to assume that the equipment can be trusted solely by virtue of the network connection? Is it appropriate for a portable computer to be used for this, particularly when it must “discover” the same information that an attacker would require, i.e., what systems are available on the network?

Embedded onboard loaders, on the other hand, may easily (and possibly even by manufacturer requirement) be pre-programmed to “know” each and every legitimate LRU by type and address when installed. Some LRUs may even change their addresses when on the aircraft versus in the shop. This consideration was addressed in the protocol to allow for both aircraft loaders and shop loaders operating differently and loading the same LRU running the same code. Similar considerations should be given relative to some aspects of security, but often tend to be glossed over as left to the system- or aircraft-integrator to address.

Furthermore, and directly relevant to security, the LRU executing the protocol “trusts” the asserted identity of the loader on the other end of the network and no provision is made for verification. In other words, if an LRU receives a message per the protocol it assumes that the source of the message is legitimate. Whether this assumption places an undue constraint on aircraft architectures and operations is debatable. What is undeniably true, however, is that it remains a constraint that must be addressed externally, not only external to the LRU, but external to the specification because the specification does not address it. If an integrator wants to use the specification, this external constraint must be satisfied. If an integrator cannot or will not address this constraint, the standard cannot be used. Therefore, to ensure the broadest application of standards, it behooves all parties to create standards that fit emergent needs rather than only the needs of past generations of aircraft architectures.

C-1.2 Example 2

The current and anticipated use of cryptography to support authentication of communicating systems or of data and confidentiality of communications between systems or of data at rest is rapidly growing in aircraft systems. With cryptography comes an inescapable issue to be dealt with: secret keys. Whether cryptography is based on symmetric ciphers or asymmetric ciphers, protecting secret keys from disclosure is intrinsic to its successful use.

Also inescapable is that there is no standardized means for addressing the use of such secret data in the operational context of airlines, aircraft maintenance or aircraft systems. Each time a specification incorporates the use of cryptography it introduces a need to handle secret keys, and there are probably as many ways to solve that problem as there are uses of cryptography. Sometimes it is inherently necessary to transport secret keys (for instance, when symmetric keys must be shared). Other times it may not be necessary to transport the secrets, but it is necessary to physically verify the holder of a credential (for instance, in PKI when a certificate must be signed). Sometimes keys may be treated as operational data; other times it may be more appropriate to treat them as software parts. Sometimes certificates may simply be trusted without checking for revocation; other times it may be desirable to verify the continuing validity of a certificate.

Each situation is different, and some time will inevitably elapse before appropriate standards are developed to address all the needs in specifications that survive to be incorporated in operational systems. The risk is that there will be a divergence of methods proposed for handling secret keys, confidentiality requirements, and key-related processes, and that this divergence will result in excessive costs and operational complexity for airlines.

APPENDIX D SECURITY ENVIRONMENT ASSUMPTIONS AND PRESUMPTIONS

This appendix provides assumptions and presumptions related to the security environment of an aircraft Information System and its interfaces. These assumptions and presumptions are based on in-service experience. They should be considered for the entire aircraft life cycle per ARINC Report 811.

D-1 Security Environment Assumptions

This paragraph provides assumptions related to the security environment of the aircraft information system and its interfaces. All assumptions used in writing a standard should be explicitly called out and related consequences documented in context. Assumptions are considered statements, which need validation for their context to allow for applicability. The validation can only be performed by the applicable organization that designs, operates or regulates the topic of assumption.

The following list is a sample list of security environment assumptions that may be used in specification generation:

- Ground Network Infrastructure

  In the development of a standard the contribution of any ground network infrastructure of all Air Transport organizations (Aircraft Operators, Maintenance and Repair Organizations, Airports, Air Navigation or Communication Service Providers) should be considered as a layer of defense relative to the aircraft infrastructure, which is not accessible by an unauthorized user. Consequently these ground infrastructures should be secured commensurate to the assumed level. These organizations should maintain the security at the same level throughout the life of the infrastructure and those of the serviced aircraft.

  It should be assumed that ground networks are adequately managed and controlled to protect against threats such that they maintain the cyber security for systems and applications using the network, including information in transit.

- Remote access

  All remote access points (wired or wireless) as well as wireless access to equipment installed on the aircraft shall be considered a threat relative to the aircraft.

- Line Replaceable Units, Items, or Modules

  Since tampering with equipment requires a specific power source, connectors and expertise to communicate with the equipment, LRU/LRI/LRM tampering is not considered as a threat. It is recommend, however, that LRU/LRI/LRM tampering be considered in a physical security risk analysis is outside the scope of this document.

- Indirect attack

  Personnel from all organizations involved in the Air Transportation System, although well trained, and qualified, may make errors to be considered. Some of these errors may influence the security level of a system specified. An analysis should identify negligent acts, omissions or misuse as operational vulnerabilities and assess the associated threat (e.g., mobile device already corrupted when used by an authorized user).

D-2 Security Environment Presumptions

This paragraph provides presumptions related to the security environment of the aircraft information system and its interfaces. All presumptions used in writing a standard should be explicitly called out and related consequences documented in context. Presumptions are considered statements, which need no validation as they are axiomatic in nature and self-evident.

D-2.1 Aircraft Zones and Physical Access

The following table summarizes the accessible/inaccessible zones. An area “Accessible to an unauthorized user” is neither controlled by the manufacturers nor the operators – thus the level of control can only be estimated. An area “Inaccessible to an unauthorized user” is an area under control by either the manufacturers or operators, where:

- A security procedure is applied to permit access to the physical zone,
- A physical zone access verification control is applied (e.g., badge),
- And users are trained / informed about the security procedures to be applied during the access to the zone / network access / information.

Aircraft Zones	Controlled Access	Operations Area secured access	Flight Deck restricted access
Cockpit			X
Forward avionics bay			X
Aft avionics bay			X
Cabin (including toilets, showers, etc.)	X		
Aircraft entry area	X		
Flight Crew Rest Compartment			X
Cabin Crew Rest Compartment	X		
Cargo hold		X	
Landing Gear bay, Wheels		X	
Engines		X	
Apron in aircraft vicinity		X	

D-2.2 Mobile Devices

Mobile devices are devices not installed on an aircraft (e.g., USB key, CD-ROM, DVD, laptop.), intended to be used on the aircraft and to return outside of the aircraft after use. All mobile devices should be considered accessible to unauthorized users.

Considered are:

- Mobile devices of all the organizations (Manufacturers, operators, MRO, Airport, Service Providers and Suppliers) which can be connected to the aircraft,
- Mobile devices used to load equipment in maintenance shops,

- Mobile devices used to trouble-shoot, test and manufacturing of equipment in maintenance shops and/or production lines.

D-2.3 Personnel

Personnel from all organizations (Manufacturers, Operators, Maintenance Repair Overhaul centers, Airport, Service Providers and Suppliers) are considered “well intentioned” with respect to the security of the Air Transportation System. However, it is also the case that personnel with inside knowledge and access are in a position to cause more damage than outsiders. Although this document discusses security controls, it is recognized that it is more difficult to fully mitigate the additional risk from insiders. Mitigating specific risks from insiders is an operational security issue, although the security features will be of use in this context.

D-2.4 Communication of information

Aircraft are connected to the ground and other aircraft through a variety of different communication means. Some of the communication means operate in a regulated environment, such as Air Traffic Control or Navigation related systems, while others are solely operated under the authority of aircraft operators and their service providers:

Communication of information	Accessible by an unauthorized user (including remote access)	Inaccessible by an unauthorized user
Communications aircraft-ground via Gatelink (e.g., WIFI, GSM, GPRS)	X	
Communications aircraft ground via radio (e.g., HF, VHF, SATCOM,)	X	
ACARS	X	
Communications between Airframe mfg, MRO, suppliers, airline, ANSP	X	
Navigation aids (e.g., VOR, DME, ILS)		X
Communications between aircraft in flight (e.g., TCAS, ADS-B)		X

D-2.5 Attacker Profile

Attacker profiles are primarily defined with the following attributes:

- The expertise of the attacker
- The knowledge of the attacker of the target
- The resources available to the attacker

The following threat levels (or attacker profiles) were derived from the Information Assurance Technical Framework (IATF) of the US National Security Agency (NSA), which in turn draws from other materials and discussions with subject matter experts throughout the Information Systems Security Organization (ISSO):

APPENDIX D
SECURITY ENVIRONMENT ASSUMPTIONS AND PRESUMPTIONS

- **T1.** Inadvertent or accidental events (e.g., tripping over a power cord).
- **T2.** Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening).
- **T3.** Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).
- **T4.** Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations).
- **T5.** Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., international terrorists).
- **T6.** Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation).
- **T7.** Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis).

APPENDIX E IFE SECURITY EVENT LOGGING USE CASE EXAMPLE

The following use case was submitted by Panasonic Avionics.

An IFE system has many reasons to log data independent of security reasons including: passenger usage, fault data, reliability data such as temperature profiles, advertisement activity, and passenger surveys. Once securing the IFE system is considered, traditional security logging requirements from the ground IT industry begin to apply. And then with the addition of the handing of credit card data for purchases within the IFE system, security standards from the Payment Card Industry (PCI) Council mandates even more logging.

It is also worth noting that some international privacy laws require treating medical or even personal information as secure as financial information, which can extend secure or protected treatment to a passenger manifest list, frequent flyer database, meal preferences, or ‘special needs’ requests.

The PCI Data Security Standard (Requirement 10.2) requires logging of the following events:

- All individual accesses to cardholder data, including (Requirement 10.1) linking such access to each individual user.
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts

The latter three are good practice for any secure system. It is only the first that presents a unique requirement, though it could be generalized as “access to *sensitive or protected* data” which could then apply to some passenger related data.

It is just this requirement, to link actions to individual users, that presents a challenge on board an aircraft. Refer to Appendix 1 Section 1.1.4 on Access Controls for further considerations. It is only practical to consider maintaining an ACL with individual user accounts on board an aircraft if a reliable, low-cost, and moderately speedy communications link exists between the aircraft and the ground (e.g., Gatelink).

And for each event, the PCI standard (Requirement 10.3) requires logging of the following metadata:

- User identification
- Type of event
- Date and time
- Origination of event
- Identity or name of affected data, system, or resource.

The above should be considered as guidance to be carried into standards for every avionics system capturing security audit data.

APPENDIX E
IFE SECURITY EVENT LOGGING USE CASE EXAMPLE

Furthermore, PCI standard (Requirements 10.6, 10.7) requires reviewing logs “daily”, and that the [log] audit trail be retained for at least one year.

This requirement is impractical to support even within an IFE system which can have Terabytes of storage. Such storage is usually dedicated to entertainment content. In addition, typical maintenance actions of removing and replacing LRUs on the plane would make it very difficult to maintain any audit data still on the LRU and associate it properly with the aircraft on which the data was generated. Therefore, proper handling of log data requires at least periodic offloading. Given that there are economic reasons to carry out periodic offloading of financial transactions, it is not unreasonable to expect that the audit logs can be offloaded by the same mechanism and perhaps at the same time. Then the persistence requirement can be much more easily handled by ground systems.

To meet “daily” requirements, logs must be off-loadable for ground-based review daily, or alternative means should be provided to “review” the logs by automatic filtering mechanisms on board, perhaps only sending to the ground (typically by more expensive communications means) any serious event within 24 hours of occurrence.