6.6 ACS Duplication

6.6.1 Supplier Intellectual Property

Airlines expect to be authorized to use and copy the ACS parts that are required to maintain the authorized configuration of their aircraft. Therefore, the owner of the software intellectual property rights is expected to grant the right to an airline to copy software that the airline is authorized to use, provided the airline respects the following needs of the supplier:

- Protect the intellectual property rights contained in the software
- The software will be used by the airline only in applications that are authorized by the software supplier

6.6.1.1 Airline Responsibilities

Airlines and their designees should hold, use, and copy software in conformance with the guidelines of this document and are expected to provide adequate assurances to the intellectual property owner that the software is not used or copied for purposes other than those permitted. The airline should maintain a list of LSPs for which permission to duplicate is authorized.

Airlines should maintain a process in which copied and distributed software is traceable to the original airline source (i.e., master copy) from which copies were made. The original airline source could be a file transferred electronically or a physical media obtained from a software supplier or aircraft manufacturer.

The airline's rights to duplicate may be transferred from the airline or training device manufacturer to a maintenance provider (MRO).

6.6.1.2 Airframe Manufacturer Responsibilities

To assist the operators with software configuration management, airframe manufacturers should obtain rights to copy software from the LSP suppliers for all SFE and SPE software delivered on an aircraft.

When the airframe manufacturer issues a SB for approved use of a new software part, the airline should be granted the rights to copy the new software.

6.6.1.3 Responsibilities of Other Parties

An airline, training device manufacturer, or airframe manufacturer may duplicate software for distribution to a remote location. A third party may distribute software as defined by the license agreement when the Supplier has granted Rights to Copy.

6.6.1.4 Designee Responsibilities

Any maintenance provider acting as a contractor of an airline should protect the integrity and security of the intellectual property; this should be addressed in a contract or negotiated with the supplier.

6.6.2 Copyright

It is the practice of most suppliers to copyright their software. Applicable copyright regulations should be adhered to in any duplication procedures instituted by an airline.

The ACS supplier is expected to a make clear distinction of what constitutes airline rights to copy and what constitutes copyright protection.

6.6.3 Duplication Process and Tools

The airline is responsible for using a software copying process and tools that will not alter the software image. The copy process should provide a means to ensure that the copies created are identical to the software being copied. Failure to make an exact copy could result in the LSP failing to load. Airlines desire a standardized process for duplicating LSPs, minimizing the use of different duplication processes from multiple LSP suppliers.

Integrity checks and bit image comparisons should be used to ensure that the software image has not been altered during the duplication process. Some examples of integrity check are:

- CRC – Cyclic Redundancy Check
- MDS – Message Digest Algorithms
- SHA – Secure Hash Algorithms

6.6.4 Quality Assurance Program

The software quality assurance procedures should be defined and described in an accepted quality management system.

6.6.5 Integrity

To ensure the integrity of all copies of software parts, the CRC or other integrity check methods should be used in compliance with ARINC Report 665.

The software (MSP or LSP) is processed with the appropriate integrity algorithm to yield a check value. When the software is copied, the copy integrity check value is compared with the master software part check value. If the two check values do not

agree, then an error has been made in the copy operation, and the software part is unserviceable.

The integrity check value used for software loading is independent of the integrity check used to duplicate software. Various software tools are available to calculate various forms of integrity checks.

Even if the software part does not conform to ARINC Report 665, a CRC or other integrity check value can be generated for any file using various software tools. The software part supplier should provide the integrity check value (and the method used to calculate the value) upon request.

6.6.6 Virus Considerations

The ground systems used for software distribution, duplication, and storage should be protected against malicious data such as viruses.

Most aircraft systems are protected against viruses during normal operation by unique file formatting, including the integrity check, which prevents software loading if data has been altered. Furthermore, the unique architecture of airborne systems generally prevents virus execution. More information on integrity checks can be found in Section 5.6.1.

COMMENTARY

Training devices may allow data loading using different methods than the data loading methods used on actual aircraft. As a result, some virus protection strategies that may exist in the aircraft data loading process might not be available on the training device.

7.0 SOFTWARE STORAGE

7.1 General

Software parts have attributes that make them different from hardware parts. Appropriate storage facilities, planning, and support infrastructure, compatible with each operator's operations are required for software parts.

ACLSPs may be stored on many types of media and stored on many different devices at many locations depending on business needs. This section outlines the most important of these storage locations with respect to the airline's business processes.

Aircraft delivered with loadable hardware may include a spare set of ACLSPs stored on media or on-aircraft MSDs. The media may be contained in designated storage location on-aircraft or off-aircraft. ACLSPs that are stored on physical media or MSDs should be considered spare parts that do not affect airworthiness. The ACLSP becomes part of the aircraft installed configuration when it has been successfully loaded into the target hardware.

7.2 On-Aircraft Storage

In general, the ACLSPs stored onboard an aircraft should be maintained current for that aircraft configuration, including any alternate configurations. Obsolete or superseded ACLSPs should be removed from the aircraft to avoid configuration management issues.

There are instances where it may be advantageous to store future or superseded ACLSPs as well as the current ACLSPs on the aircraft. For example, during an ACLSP configuration change, the airline may store both the future ACLSPs and the current ACLSPs, until the modification can be scheduled for installation.

If an Airworthiness Directive or a safety related issue directs removal of obsolete or superseded software, then ACLSPs should be removed from all on-aircraft storage locations.

7.2.1 Onboard Mass Storage Device

Onboard MSDs with file server capabilities are often used to store ACLSPs. Onboard software load functions may load software from an MSD. To maximize the effectiveness of MSDs, it is recommended that the ACLSPs configured to each aircraft be loaded on the MSD. Obsolete or superseded ACLSPs should be removed.

Onboard MSDs should contain a full set of ACLSPs required by any possible configuration for that aircraft, including software for all interchangeable and intermixable configurations. Airlines may choose to hold a superset of all current ACLSPs on replacement MSDs to have a single MSD configuration across multiple aircraft.

Aircraft configuration management is maintained by ensuring that the correct ACLSPs are installed in the correct target hardware locations on the aircraft according to the operator's configuration control documentation. However, business and regulatory concerns may drive the need for similar configuration control methods for configuring onboard MSDs. For example, an AD could require software to be replaced or removed for safety of flight reasons. See Section 6.0 for more details.

7.3 Off-Aircraft Storage

All software distributed electronically or on media should originate from one or more secure off-aircraft storage locations. A process must be developed to identify how maintenance personnel can obtain parts for onboard loading from the storage locations.

Off-aircraft software storage can apply to ACLSPs and HCLSPs (used for hardware modification). The general term LSP is used where processes may apply to either type of software.

If an Airworthiness Directive or a safety related issue directs removal of obsolete or superseded software, then ACLSPs and HCLSPs affected should be removed from all off-aircraft storage locations. One must also ensure that stock and spare target hardware be sanitized if preloaded with software affected by the Airworthiness Directive.

7.3.1 Ground-Based File Server

A ground-based file server may be used as a media backup or as a means to store and distribute LSPs electronically within an airline for installation on an aircraft or in a component shop. Multiple ground-based file servers may be utilized to support ground operations.

To maximize the effectiveness of a ground-based file server, the LSPs applicable to an airline's fleet of aircraft should be available on the file server. The file server may be included in the operator's released configuration control process.

The airline or maintenance provider should ensure the security of file servers. The access to the server should be limited to those requiring access for operational reasons. When transferring software (i.e., from a ground-based file server to another location), a change log should be maintained as a part of the file server management process to assist with distribution troubleshooting or security events. The file management process should also provide a means for tracking the EDS from the server to an onboard MSD.

7.3.2 LSP Storage Vault

An LSP storage vault is a type of ground-based file server used to store LSPs electronically in a permanent central repository. An LSP storage vault is used by an airline SCL to perform physical configuration management and control of LSPs. SCL processes are generally used to manage this storage (see Section 5.5). Most LSP duplication and distribution activities performed by airlines should occur from master images stored in the LSP storage vault. Airlines may implement multiple instances of an LSP storage vault from which to perform duplication and distribution activities. Processes are needed to verify the integrity of stored LSPs and to reconcile the contents of multiple vaults.

LSP storage vaults should have the capability to prevent access to LSPs that have been removed from aircraft via an Airworthiness Directive.

Aircraft manufacturers, suppliers, and training providers may also have SCLs and associated LSP storage vaults. However, those processes are outside of the scope of this document.

COMMENTARY

Electronic distribution from aircraft manufacturers and suppliers to airlines is assumed to occur from a secure storage location.

7.3.3 Shop Loader MSD

Shop loaders are used by operators to preload target hardware off the aircraft. Many shop loaders have MSDs. Shop loaders are considered to be maintenance support equipment.

To maximize the effectiveness of shop loaders with MSDs, the software applicable to each target hardware to be pre-loaded should be available on the shop loader MSD.

7.3.4 Portable Loader MSDs

Portable loaders are used for loading software into target hardware both off-aircraft and on-aircraft. Many portable data loaders have MSDs. Portable loaders are considered to be maintenance support equipment.

To maximize the effectiveness of portable loaders with MSDs, the LSP applicable to each hardware target loadable by the portable loader should be available on the MSD.

7.3.5 Media Storage

LSPs are often stored on physical media (e.g., floppy disk, CD-ROM). Physical media (MSPs) may be part numbered to assist configuration control of the media. Physical media may contain multiple LSPs. Operators using MSPs must manage the correlation of LSP numbers to the associated MSP numbers. Operators should have processes to ensure media is stored and handled properly for each media type.

7.4 Binder/Storage Box

Aircraft manufacturers may deliver new aircraft with media storage containers (e.g., binder, storage box) for storing LSP media. The aircraft operator may choose to store the physical media on the aircraft or to remove the media from the aircraft.

Some airplanes types may require the entire suite of software to remain on the aircraft as part of the Type Certificate. Airlines should research and adhere to their governing regulatory requirements.

Media storage containers are considered maintenance support equipment. The operator should develop processes for the management of the storage containers stored either on or off the aircraft.

To maximize the effectiveness of media storage containers, the LSPs applicable to each aircraft that will be loaded from physical media should be available in these media storage containers.

8.0 AIRCRAFT CONFIGURATION MANAGEMENT OF ACS

8.1 General

The airline is responsible for the total configuration management of the aircraft as it is utilized within the airline's business. This responsibility includes ACS which is part of the type certified configuration of the aircraft as well as ACS that is not part of the aircraft type certified configuration. Airlines have a choice to manage all ACS in the same manner or establish different processes for both types of ACS.

Following are the fundamental elements of ACS configuration management:

- Establishing an authorized software configuration for each aircraft that follows the allowable certified configuration options
- Establishing processes to ensure that all aircraft conform to the authorized software configuration following any maintenance activity that may affect the software configuration.

Efficient processes for ACS configuration management are vital to an airline's business. ACS configuration management processes can impact other maintenance processes, including inventory control, purchasing, supply chain logistics, maintenance planning and execution. Newer, more complex aircraft with higher quantities of ACS will likely require different configuration management processes than older aircraft did. It is expected that existing configuration management processes for legacy aircraft will evolve to the new process described here over time. For description of the previously defined configuration management process, refer to the original release of ARINC Report 667.

Flight training device manufacturers, users, and operators should employ this guidance as applicable when installing ACS in simulation devices. More guidance on flight training device simulator software can be found in ARINC Report 610.

8.1.1 Configuration Management Vocabulary

The following definitions and figures are provided for proper understanding of the content that follows. The figures show the relationships between hardware and software

Interchangeability: The ability of an item (e.g., SW part, HW part) to replace another one without alteration and fulfill the same requirement. The form, fit, and function remains exactly the same when an alternate choice of hardware or software is made.

Compatibility: The ability of software to properly function in a target hardware environment.

Mixability: Mixability refers to compatibility of the hardware and software between two or more different hardware units or systems.

S1000D: An industry standard for the data format of Technical Publications expressed in XML format. Examples are: AMM, IPD, and SB. IPD is the electronic form of what is currently referred to as an IPC.

Certified Configuration Authority (CCA): The FAA/EASA Part 25 authority data issued by the TC or STC Holder that defines all allowable certified hardware and software modification options that are applicable to each aircraft system.

Airline Configuration Reference (ACR): The in-service configuration management system for the airline's fleet. This reference should capture the required configuration for each aircraft in the fleet and each ACLSP with associated hardware that is authorized to be installed regardless of regulatory requirements.

Functional Item Number (FIN): A FIN identifies an item performing a function within a system. A FIN is unique for the whole Aircraft.

Software Location ID (SLID): Software Location Identifiers identify where software is installed in the aircraft for purposes of confirming that the aircraft is in the proper configuration.

Airline Generated Change (AGC): Any change from system suppliers or airlines that have no accompanying SB. An example is an airline created UMS change.

8.1.2 Configuration Accountability

It is important to establish the accountability for the software configuration of an aircraft from time of delivery of that aircraft to an airline customer through its entire life cycle. This section clarifies those accountabilities.

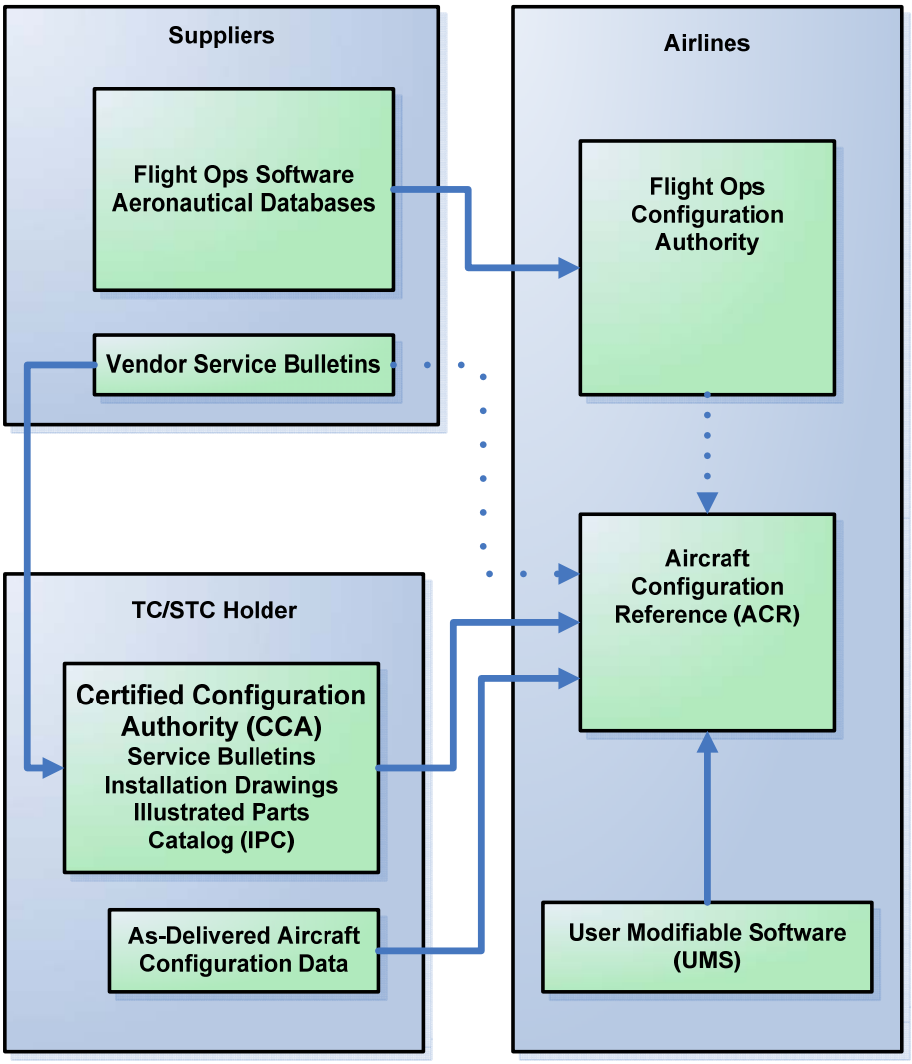

Figure 8-1 – Configuration Authority Responsibilities

TC/STC holders have the responsibility for the CCA for their respective aircraft or systems through the life of the aircraft. They are responsible for identifying the TC or STC configurations available to airlines. This will include the SB references that replaced one certified configuration with another.

The aircraft manufacturer provides “as-delivered” configuration data to airlines that identifies the configuration of the aircraft at time of delivery and is used as the baseline for the ACR. IPC/IPD data is then updated by the TC/STC holder on a regular basis. **ARINC Specification 843:** *Aircraft Software Common Configuration Reporting* defines the process and format for generating a software configuration report from an aircraft or a mass storage device

The airline is responsible for the ACR for any changes to the aircraft after delivery, for the entirety of time they operate the aircraft.

Suppliers of certain systems (e.g., IFE) are responsible to manage the FAA Part 25 or EASA Part 25 system CCA related to their ACS from time of aircraft ticketing through the life of the aircraft.

8.2 Establishing the Airline Configuration Reference (ACR)

8.2.1 Understanding the CCA

The aircraft manufacturer will provide as-delivered configuration data to identify the certified aircraft configuration for each aircraft at time of delivery to the airline.

Modifications to the certified configuration are incorporated through manufacturer or supplier provided SBs or operator originated modifications based upon the STC process, minor modification processes, or operator engineering paperwork (such as EOs). More than one aircraft software part number for a given software function may be certified to be used with a specific target hardware and allowed to be used, just as more than one hardware part number for a given hardware function may be allowed to be installed on a given aircraft.

The CCA provided by the TC/STC Holder (aircraft manufacturer or supplier) to airlines captures the allowable Part 25 hardware and software changes to each aircraft in an airline’s fleet. New changes typically originate in SBs and Airworthiness Directives that once released get incorporated into the CCA as represented by the IPC or equivalent electronic system. The scope of the CCA is typically limited to Part 25-certified components.

The CCA also identifies compatibility and mixability related to software and hardware. The CCA is not intended to fully define the ACR.

COMMENTARY

With the increased use of Integrated Modular Avionics (IMAs) as well as Commercial Off-The-Shelf (COTS) software (such as operating system software), it is believed that Software-Software Compatibility and Mixability dependencies will become more prevalent. Compatibility and mixability checks are often performed automatically by the loadable systems but are also captured in the CCA to ensure compatibility and mixability issues do not arise during the loading process.

In the past, the CCA was documented in the paper-based IPC and SBs. This data is now captured in S1000D IPD and SB Publication Modules.

8.2.2 Creation of the ACR

The Certified Configuration Authority captures the in-service authorized ACS and inter-related hardware configuration for each aircraft in the airline's fleet. The ACR reflects the changes to an airline's aircraft configuration from the original CCA. These changes may include FAA Part 121 ACS and airline-generated UMS not represented in the CCA.

An ACR should use the CCA as an input for defining an airplane's required configuration. It is important to note that there are other sources of configuration information such as airline internal requirements, periodic database updates, UMS, etc.

ACR data primarily defines ACS installed and operating in target hardware. In addition, airlines should consider how ACR data is maintained for onboard MSDs that act as spare parts software storage. It is recommended that each instance of an ACLSP stored in an onboard MSD would be authorized in the ACR. It should be noted that ACS is allowed to be stored on onboard MSDs, even if the software is not also installed in aircraft target hardware as long as the ACS is not obsolete (i.e., not allowed to be installed) or have safety concerns (e.g., as outlined in an Airworthiness Directive (AD)).

An important consideration is whether the airline allows only one software configuration to be installed and maintained by line maintenance or whether choices of compatible HW and SW will be allowed to be made by line maintenance. Use of one configuration is easier to maintain and clear but less flexible during line maintenance repairs. Line maintenance must contact Engineering to install alternate HW and SW in this case.

It is possible that an ACR for Type Design Software (LSAPs) may be separate from the ACR used for Operationally Approved software. For example, an independent Flight Operations Configuration Reference (FOCR) could be established for managing flight operations software. Other Configuration Authorities could exist for items like Aircraft Support Data.

Airlines are encouraged to use software configuration management tools (e.g., an EDMS) to manage their ACR for modern complex aircraft. Many good Commercial Off The Shelf (COTS) products exist that perform this function and can be modified to fit an airline's business process. CCA information can be input into the CM tool as a source for the ACR. It is highly recommended that the CCA information be distinguishable from the ACR information to preserve the integrity of both authorities.

The Software and all relevant documentation (FAA/EASA forms, CoC, etc.) related to the respective Software Part should be linked in the ACR.

8.2.2.1 ACR Software Configuration Data

The following information should, at minimum, be considered for inclusion in the airline's ACR for managing each ACLSP:

- Software Part (ACLSP) Number
- Software Part (ACLSP) Nomenclature
- SLID (if used)
- SLID Nomenclature (if used)
- FIN (if used)