Certification Authorities Software Team (CAST)

Position Paper CAST-3

Guidelines for Assuring the Software Aspects of Certification When Replacing Obsolete Electronic Parts Used in Airborne Systems and Equipment

Completed June, 1999

NOTE: **This position paper has been coordinated among the software specialists of certification authorities from the United States, Europe, and Canada. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Guidelines for Assuring the Software Aspects of Certification When Replacing Obsolete Electronic Parts Used in Airborne Systems and Equipment

Abstract

This paper proposes guidelines and an approach for assessing and ensuring that the replacement of electrical and electronic parts used in aircraft electrical systems and equipment is addressed safely from the software perspective in the certification process while minimizing manufacturer and operator costs and schedule impacts. Many electronic components used in already certified aircraft systems and equipment are no longer being manufactured, that is, are obsolete, and this paper proposes an effective and efficient approach for ensuring the software aspects of certification for replacement of these parts in existing airborne systems and equipment.

Keywords

electronic, electrical, part, component, device, obsolete, replacement, similarity

1. INTRODUCTION TO SOFTWARE GUIDELINES FOR OBSOLETE ELECTRONIC PART REPLACEMENT

Many electronic components used in already certified aircraft systems and equipment are no longer being manufactured, that is, are becoming obsolete, and this paper proposes an effective and efficient approach for approving the replacement of these parts in existing systems and equipment.

1.1. PURPOSE

This paper proposes guidelines and an approach for assessing and ensuring that the software aspects of replacing electrical and electronic parts used in and by aircraft electrical systems and equipment are addressed adequately in the certification process while minimizing airframer's, airborne system manufacturer's and aircraft operator's costs and schedule impacts.

Sections 2 and 3 also offer some guidelines for hardware aspects and system aspects when replacing these parts. The hardware and system aspects are discussed primarily from the aspect of potential effects on the software. The system Aviation Safety Engineer (ASE) or designee would still need to address additional issues.

The intent of the paper is to provide guidelines which will ensure that the replacement of obsolete electronic parts is accomplished without affecting airborne system reliability and integrity and aircraft continued operational safety by assuring that the replacement part satisfies its requirements and does not adversely affect other components (including software) of the system nor aircraft safety (i.e., achieve an equivalent level of safety as the obsolete part).

1.2. SCOPE

This paper may be used by certification authority engineers and designees (for example, DERs – Designated Engineering Representatives) as an approach for assessing the needed effort by a manufacturer to replace obsolete parts in airborne electrical or electronic systems and equipment with new parts and to re-certify the aircraft system. It may be used by the applicants, manufacturers and their vendors for preparing a plan for the replacement of obsolete parts and re-certification of the system or equipment.

This approach could also be used for non-airborne equipment that interfaces with aircraft whether by satellite, voice, radio, transponder/receiver or Datalink operations. The only difference being that the applicant may be a regulatory agency or a service provider to the regulatory agency.

1.3. BACKGROUND

Rapid advances in electronics technology has resulted in many faster and less expensive electronic components. These advances have also resulted in manufacturers determining to close down the production lines of many older electronic components used in already certified aircraft systems and equipment. Additionally, electronic parts manufacturers are producing fewer parts that meet the environment qualification standards of military parts (e.g., MIL-STD-883). This results in the airframers and electrical system developers having to replace these components, especially once their "buy" of the components is running low. Although this is not unusual and, in fact, is done continually by the applicants and certification authorities, the fact is that there will be substantially more and more of these replacements that must take place. This can result in tremendous costs to the operators, manufacturers and developers of these components and the systems in which they are used.

1.4. REFERENCES

Following are references and other sources of information that may be useful in assessing electronic part replacement in aircraft applications.

[1] FAR/JAR 23.1301, 23.1309, 25.1301, 25.1309, 33.28 and Appendix A - FAA and JAA regulations most often associated with the software aspects of aircraft electronic/electrical systems and equipment.

[2] FAR 21.93, 21.95, 21.97, 21.99 - FAA regulations associated with changes to type design for TC aircraft and systems.

[3] FAA Advisory Circular AC/JAA AMJ 25.1309.1A - FAA and JAA policy associated with fail safe design of electrical systems and equipment and software.

[4] FAA Advisory Circular AC/JAA AMJ 25.1309.1B {Draft, not yet approved} Intended update of [3]

[5] FAA AC 20-115B, *RTCA DO-178B* - FAA policy which invokes RTCA guidance for software compliance in multiple CFR Parts.

[6] RTCA DO-178B/EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification,* December 1, 1992

[7] FAA Notice N8110.78, *Guidelines for the Approval of Software Changes in Legacy Systems Using RTCA DO-178B.*

[8] FAA Notice N8110.85, *GUIDELINES FOR THE OVERSIGHT OF SOFTWARE CHANGE IMPACT ANALYSES USED TO CLASSIFY SOFTWARE CHANGES AS MAJOR OR MINOR.*

[9] FAA Notice N8110.87, *Guidelines for Determining the Level of FAA Involvement*.

[10] SAE ARP4754, *Certification Considerations for Highly-Integrated or Complex Aircraft Systems,* Issued 1996-11

[11] SAE ARP4761, *Guidelines and Tools for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,*

[12] SAE ARP-xxxx, *Electronic Component Management* {Draft, not yet approved)

[13] RTCA SC-180 DO-TBD / EUROCAE WG-46 ED-xx, *Design Assurance Guidance for Airborne Electronic Hardware* {Draft, not yet approved}

[14] PSG2-21 Revision 5, RTCA SC-189/EUROCAE WG-53 Air Traffic Services Safety and Interoperability Requirements, Subgroup 2 Paper, *Communication, Navigation, Surveillance (CNS) and Air Traffic Management (ATM) Safety Assessment Process,* Draft not yet formally approved

2. CERTIFICATION AUTHORITY SOFTWARE TEAM POSITION

This section and the following subsections define the CAST position for the software aspects of certification for the replacement of obsolete parts in airborne systems and equipment. To summarize, the applicant should conduct a change impact analysis of the part to be replaced in terms of its function(s) within the system, the architecture of the system and the component's role in the architecture, and potential impacts not only on the system but also potential impacts on its software, other system hardware components, system interfaces, the aircraft and its occupants, and operational uses. This change impact analysis will determine the significance of the replacement and the re-verification and re-validation effort necessary to certify the modified airborne system.

2.1. DETERMINING IMPACTS ON THE SOFTWARE

Following is a general process description of activities to perform and document for a change impact analysis:

1. Identify the specific electronic hardware part(s) to be replaced.
2. Perform a change impact analysis to determine the effects of the replacement part on operational requirements, functional requirements, system reliability, EMI, HIRF, system architecture, timing requirements, interface requirements, maintenance requirements, other hardware components, and software.

Note: Hardware replacement parts that could potentially impact the software include: processor (central processing unit - CPU), coprocessor, memory, watchdog timers, memory management units, clock management units, input/output (I/O) devices - busses, A/D converters, D/A converters, bus controllers, signal processors, etc.

3. Identify specific software items and components (requirements, design, architecture, source code modules, object code, linking and loading data, I/O data, memory, timing, scheduling, etc.) affected by the change.
4. Obtain early agreement from the certification authorities for the plans for replacing the part and the change impact analysis. Also, obtain agreement for the data needed to be submitted and/or approved for the change.
5. Identify software verification procedures that must be re-executed to verify that the change did not adversely affect the software (regression testing).
6. Modify identified software items and components as needed to mitigate the effect of the change. Apply change control procedures to any software changes. See also reference [6] RTCA DO-178B / EUROCAE ED-12B, sections 12.1.1, 12.1.5 and 12.1.6.
7. Develop new software verification procedures as needed to verify equivalent software integrity.
8. Execute the software verification procedures to verify the change, to verify no adverse impacts, and to obtain an equivalent level of assurance for the software.
9. Submit agreed-to data to the certification authority. This will usually include a Software Accomplishment Summary that defines the process used for the change and the software life cycle data produced or updated.

Additional guidelines for assessing changes is in references [7] and [8].

2.2 IMPACT CASES ON SOFTWARE

The amount of effort needed to reassure the software depends on the impact of the electronic hardware part replacement on the software. The following 3 sections discuss this further.

2.2.1. NO IMPACT ON SOFTWARE

If there is no impact on the software, there will be no need for additional software effort, unless, of course, the applicant chooses to make some changes to the software that are unrelated to replacing the obsolete electronic hardware part. However, there may still be impacts on other hardware components or systems' aspects (See sections 3 and 4, respectively).

2.2.2. PARTS REPLACEMENT WITH INSIGNIFICANT IMPACT ON SOFTWARE

Based on the change impact analysis of section 2.1, hardware replacements that only have a insignificant impact on the software may require only minimal software effort with established change control procedures and quality assurance. To reduce the applicant's risk, however, the applicant should coordinate with the certification authority early in the project to ensure that they agree that the impact on software is insignificant. See also references [7] and [8].

2.2.3 PARTS REPLACEMENT WITH SIGNIFICANT IMPACT ON SOFTWARE

Based on the change impact analysis of section 2.1, hardware replacements that have a significant impact on the software (that is, require a modification(s) to the software) may require a more substantial software effort. For significant modifications to the software, RTCA DO-178B/EUROCAE ED-12B (or acceptable alternative means of compliance) and current certification authority policy should be applied. See DO-178B, section 12.1. The applicant may also wish to upgrade the entire system to the most recent amendments of the FAR/JAR and current certification authority system policies. The applicant should coordinate with the certification authority early in the project to ensure their means of compliance for the software aspects of certification will be acceptable.

2.3. RESOLVING IMPACTS ON THE SOFTWARE

As stated in the general process description of section 2.1, impacts and effects on the software should be resolved by identifying those specific software components affected, modifying those components as necessary to facilitate the change, and re-verifying the software and modifications. Depending on the significance of the impact of the change and the software level of the affected functions, the type and amount of software data and assurance needed will vary. The applicant should obtain early agreement with the certification authority for their means of compliance to support the change and provide the agreed-to level of assurance and data.

2.4. RE-ESTABLISHING THE SOFTWARE ASPECTS OF CERTIFICATION

For no effect and insignificant impacts on software (e.g., "small, simple changes" per reference [7]), especially for medium and low software levels (Levels C, D, and E) systems and equipment functions, the certification authority may chose to delegate approval of the change or perform only minimal oversight. For significant impacts, the certification authority may chose to delegate some data approvals or to review and approve all modified software components and data themselves. Normally a Plan for Software Aspects of Certification (PSAC), Software Configuration Index (SCI) and Software Accomplishment Summary (SAS) will be submitted to the certification authority for approval of the software aspects. See also reference [9].

3. HARDWARE ASPECTS

The process for assessing the impact on other hardware components will be similar for hardware as for software except that additional considerations, such as environmental qualification testing (per DO-160D or alternative), will probably always be required unless the applicant can demonstrate similarity of the replacement part with its predecessor. Also, as mentioned earlier, parts manufacturers are producing fewer parts that meet the more stringent military standard durability and environmental requirements, such as temperature range, voltage range, shielding, etc.

The level of effort for the hardware aspects of the obsolete part replacement will depend on the complexity of the part, its impact on other components and the ease with which the applicant can demonstrate equivalent reliability and integrity of the part and system and continued operational safety of the aircraft. For simple parts that can be qualified by similarity and/or exhaustively tested, the level of effort should be minimal. However, for new technology parts that are dissimilar and have significant impacts on other components, the level of effort may be substantial. The applicant and system developer should consider these when analyzing alternative replacements for the obsolete part.

A general description for assessing the hardware impacts of the replacement part is:

1. Identify the specific electronic hardware part(s) to be replaced.
2. Perform a change impact analysis to determine the effects of the replacement part on other hardware components, interfaces, performance and maintenance, and environmental qualification aspects. Also, determine the effects on the fail-safe design, hardware architecture, redundancy, and safety and reliability aspects.
3. Identify specific affected hardware components and data and other effects of the change.
4. Obtain early agreement from the certification authorities for the plans for replacing the part and the change impact analysis. The proposed means of compliance should ensure equivalent (or better) reliability, integrity and level of safety. Also, obtain agreement for the data needed to be submitted and/or approved for the change.
5. Identify test and analysis procedures to be executed to verify and validate all impacts and effects of the replacement part.
6. If other parts need to be replaced or modified because of the effects of the replacement part, perform a change impact analysis for those parts.
7. Develop new verification and validation procedures as needed to ensure all replacements and modifications and their effects are tested or analyzed.
8. Execute the verification and validation procedures to ensure at least equivalency to the obsolete part and to ensure there are no unforeseen adverse impacts or effects, and document the results.

9. Submit agreed-to data to the certification authority.

3.1. FORM, FIT AND FUNCTIONALLY INTERCHANGEABLE

For replacement parts that are form, fit and functionally interchangeable with the obsolete part, of similar technology and which meet environmental qualification requirements, the level of effort should be minimal. Coordination with and visibility by the certification authority should also be minimal. In fact, the replacement would likely be classified as minor, as defined by reference [2], and only require visibility and submission of substantiating evidence after the effort has been completed. However, the certification authority may still request to review the change impact analysis results, qualification by similarity report or environmental qualification testing results and other test data that demonstrates part interchangeability and non-interference with other electronic parts.

3.2. PART REPLACEMENT WITH MINOR IMPACTS ON OTHER PARTS

For replacement parts that have minor impacts or no effects on other parts, are of similar technology and meet functional and environmental qualification requirements, the level of effort and coordination with the certification authority should also be minimal. The replacement would likely be classified as minor, as defined by reference [2], especially if there is no impact or effects outside the system, such as operational characteristics, performance characteristics or maintenance procedures. Data and substantiating evidence would likely be submitted only after the effort has been completed. However, the certification authority may still request to review the change impact analysis results, qualification by similarity report or environmental qualification testing results and other test data that demonstrates system functionality and non-interference with other electronic parts.

3.3. PART REPLACEMENT THAT SIGNIFICANTLY IMPACTS OTHER PARTS

For replacement parts that have significant impacts and effects on other parts, are of new technology (for aircraft applications), have additional and/or different functionally than the obsolete part, and/or have effects on operational, performance or maintenance procedures for the system, the level of effort may be substantial and early coordination with the certification authority is encouraged. The applicant should present their change impact analysis results and plans for ensuring intended function, equivalent reliability and integrity, and equivalent (or better) level of safety and continued operational safety. It would likely be classified as a major change, as defined by reference [2], and may require submission of "substantiating data and necessary descriptive data for inclusion in the type design."

Depending on the impacts, this data may include requirements and design data, environmental qualification test results, and system laboratory, ground and flight test. The applicant should coordinate with the certification authority all affected aspects of the part replacement that are affected with the various certification authority discipline specialists (i.e., electrical systems and equipment, flight test, structures, propulsion, etc.)

and submit the data in a timely manner to ensure an effective and efficient certification effort.

4. SYSTEM CONSIDERATIONS

The replacement of an obsolete electronic part may also have an impact on the airborne system or equipment in terms of safety, reliability, functionality, performance, operations, maintenance, EMI, HIRF, lightning, and/or other system aspects.

If the hardware part is being used in an identical manner (form, fit and functionally interchangeable) and has the same anticipated reliability and environmental qualities as its predecessor, it is unlikely that the replacement will have impact on these system attributes. However, if the part is used differently, has added functionality, impacts other systems, hardware or software, or requires changes to other components of the system or its operational use, then more effort, certification authority visibility, and assurance will be necessary. The following subsections discuss some of these aspects.

In addition to the potential impacts of the replacement part on the software and hardware aspects, there may be impacts on system characteristics, other interfacing systems, or operational or maintenance procedures. For the change impact analysis from the system perspective, the applicant should focus on potential system effects of the replacement.

For replacement parts with a system impact, the certification authority may require that the applicant upgrade the system to current regulations, policy and guidance for environmental qualification, electro-magnetic emissions or interference (EME/EMI), lightning, HIRF, and human factors.

From the system perspective, the applicant should perform a change impact analysis to determine the impact of the proposed change (replacement part) on the system, system interfaces, human factors, operational use, etc.

A general description for assessing the system impacts of the replacement part is:

1. Identify the specific electronic hardware part(s) to be replaced.
2. Perform a change impact analysis to determine the effects of the replacement part on system aspects including: safety, reliability, functionality, performance, hardware architecture, operations, environmental qualities, maintenance, interfaces within the system and with other systems; and other system's aspects.
3. Identify specific hardware components and specific effects on system's aspects and other systems, and identify documentation and data affected.
4. If other parts need to be replaced or other parts or systems modified because of the effects of the replacement part, perform a change impact analysis for those parts.
5. Identify test and analysis procedures to be executed to verify and validate all impacts and effects of the replacement part(s) and modifications, including, as applicable for the significance of the change, laboratory test, ground test and flight test.

6. Obtain early agreement from the certification authorities for the plans for replacing the part and the change impact analysis. The applicant should get agreement also on the significance of the replacement and whether current FAA regulations and policy (for example, for EMI, HIRF, lightning, etc.) will be imposed. For changes that are classified as major by reference [2], that is, have an "appreciable effect on weight, balance, structural strength, reliability, operational characteristics, or other characteristics affecting the airworthiness of the product", the applicant should get approval of their proposed means of compliance for the change. The proposed means of compliance should ensure equivalent (or better) reliability, integrity and level of safety. Also, obtain agreement for the documentation needed to be submitted and/or approved for the change.
7. Develop new verification and validation procedures as needed to ensure all replacements and modifications and their effects are tested or analyzed.
8. Execute the verification and validation procedures to ensure at least equivalency to the obsolete part and to ensure there are no unforeseen adverse impacts or effects, and document the results.
9. Submit agreed-to data to the certification authority.

4.1. OBSOLETE ELECTRONIC PART AND SYSTEM SAFETY IMPACTS

If the hardware part is being used in an identical manner (form, fit and functionally interchangeable) and has the same anticipated reliability as its predecessor, it is unlikely that the replacement will have any impact on the system safety assessment. See also references [3], [10] and [11]. However, if the part is being used differently or has added functionality or requires a change to the system architecture or interfaces, then the replacement could have an impact on system safety and a system safety assessment should be performed (or updated) accordingly. This safety assessment should determine the failure conditions and reliability and integrity requirements for the replacement part(s).

If it is determined that the replacement part can have no effect or only a minor effect on the system safety, then, of course, the applicant's effort for re-certifying the system will be minimal. It may consist of only environmental qualification testing (EQT) and non-interference demonstration.

However, replacement parts that impact aircraft or system safety may require a substantial effort. System testing, including flight testing, should be repeated or augmented as necessary to ensure equivalent system safety. Hardware replacements that impact safety should always be coordinated with the cognizant certification authority, especially those classified as a major change by reference [2].

4.2. ASSESSING IMPACT ON SYSTEM FUNCTIONALITY AND PERFORMANCE

Again, if the hardware replacement part is being used in an identical manner and has little or no impact on system functionality or performance, then minimal effort and assurance should be needed to re-certify the system.

However, if the part significantly impacts system functionality and performance, then system testing, including flight testing, should be repeated and augmented as necessary to validate system functions and performance and to ensure equivalent system safety. Hardware replacements that impact system functional and performance requirements should always be coordinated with the cognizant certification authority.

4.3 ASSESSING IMPACT ON OPERATIONAL ASPECTS

If the hardware replacement part has no impact on safety or the operational use or maintenance of the system or equipment, then minimal effort and assurance should be needed to re-certify the system. However, if the part replacement impacts aircraft operational use, aircraft flight manuals, operational manuals or bulletins, minimum equipment lists, dispatch requirements, or maintenance procedures, then additional assurance, testing and certification authority visibility are warranted. Hardware replacements that impact aircraft operational and maintenance requirements should always be coordinated with the cognizant certification authority.

4.4 ENVIRONMENTAL QUALIFICATION / NON-INTERFERENCE

The applicant will most likely always be required to demonstrate that the replacement part meets the current environmental qualification requirements (or at least to the level of its predecessor) of the aircraft and does not adversely interfere with other systems and equipment installed on the aircraft (non-interference). Environmental qualification requirements should be negotiated with the cognizant certification authority. Demonstrating non-interference may require ground and flight test of the modified system to ensure no adverse impact.

4.5. SYSTEM ASSURANCE AND APPROVAL

The applicant should coordinate significant replacement part projects with the certification authority early in the project. They should present their change impact analyses results, identify all impacted system, hardware and software components and characteristics, and propose their means of compliance for assuring equivalent safety for the replacement part. They should also propose the data that will require modification or upgrading and data submission and approval requirements for the project.

The cognizant certification authority should review the applicant's proposal in a timely manner and either propose improvements to the proposal or approve it.

Once all system, hardware and software activities are completed in compliance with the approved plans, the system data should be approved. Data requiring approval by the cognizant certification authority or designee may include plans, requirements, design data, implementation data, assembly drawings, parts lists, configuration indices,

accomplishment summaries, AFM, operational procedures, maintenance manuals or bulletins, and flight and laboratory test results. See also reference [2].

5. SUMMARY AND CONCLUSIONS

When the need arises to replace an obsolete part, the applicant and their developer should use a systematic, disciplined approach to conducting a change impact analysis, identifying all system, hardware and software impacts of the change, mitigating and resolving all identified impacts, reverifying the system and providing visibility and assurance to the cognizant certification authority. This paper describes some of the aspects and considerations that should be addressed by the applicant and offers some guidance for a consistent, standardized approach to assessing and assuring electronic hardware part replacement.