

Dependencies Between Development (ARP4754A) and Production (Part 21, Subpart G) of Safety-Critical Avionics Equipment

Klaus Fritz and Nikolaus Kurz
Diehl Aerospace GmbH

Eric Peterson
Electron International II Inc

Rolf Buese
Diehl Aerospace GmbH

ABSTRACT

Avionics equipment, especially for safety-critical systems, is developed by means of a series of design steps, propagating and refining requirements through a number of hierarchical levels, from the aircraft level, through system and sub-system levels, down to equipment, subassemblies and individual components (see SAE ARP4754A [11]). At each development level, accompanying safety assessments (e.g. per SAE ARP4761 [12]) are performed to derive safety requirements which ensure compliance to the overall safety requirements determined by the aircraft and systems functional hazard assessments (FHAs). The safety related requirements of all development levels flow through the process down into the individual equipment specifications and are ultimately implemented in the equipment design where the design data is approved for the certificated aircraft (or engine) type.

The equipment production process builds the equipment according to this approved design data. Safety assessment methodologies assume that each produced aircraft is equivalent to the type design. Conformity of the manufactured equipment, to the approved type design data, is therefore paramount to airworthiness and safety of each aircraft.

To ensure conformity, the avionics production process is monitored by a quality system, i.e. a process of inspections and testing to verify conformity to the design data and to approve the manufactured items up to approval of the fully assembled equipment which is individually certificated through an authorized release certificate (e.g. FAA Form 8130-3, EASA Form 1 [5, 8].)

For structural parts, or simple components, function is directly related to their physical properties. Conformity demonstration based on these properties is adequate and straightforward. For complex subsystems or components, in particular for avionics, the function is almost entirely emergent, i.e., not directly related to any physical property of the implementation. Conformity to type design, and verification thereof, must therefore go beyond the implementation, to include functional properties. This however, requires more knowledge about the product than just drawings and bill of materials. Despite the importance of the data shared between the development and the production processes, very little guidance is available regarding the nature of these data, and the methods used to develop an adequate production process quality system.

This paper is an attempt at defining the process and methods potentially required to develop the production process quality system, in particular the conformity verification activities, and the data required from the development processes. The production quality system is considered the continuation of the safety process within the development process.

The scope of this paper is limited to Avionic systems equipment, although in some places aircraft level aspects are mentioned. This paper is concerned about the safety aspects derived from ARP4754A interacting with the production process, referring to a "quality system" as per 14 CFR/IR Part 21, subpart G [2, 4, 7, 8]. Production related quality aspects (e.g. ensuring advantageous production yield supporting business related objectives) are not the subject of this paper.

CITATION: Fritz, K., Kurz, N., Peterson, E., and Buese, R., "Dependencies Between Development (ARP4754A) and Production (Part 21, Subpart G) of Safety-Critical Avionics Equipment," *SAE Int. J. Aerosp.* 6(2):2013, doi: 10.4271/2013-01-2122.

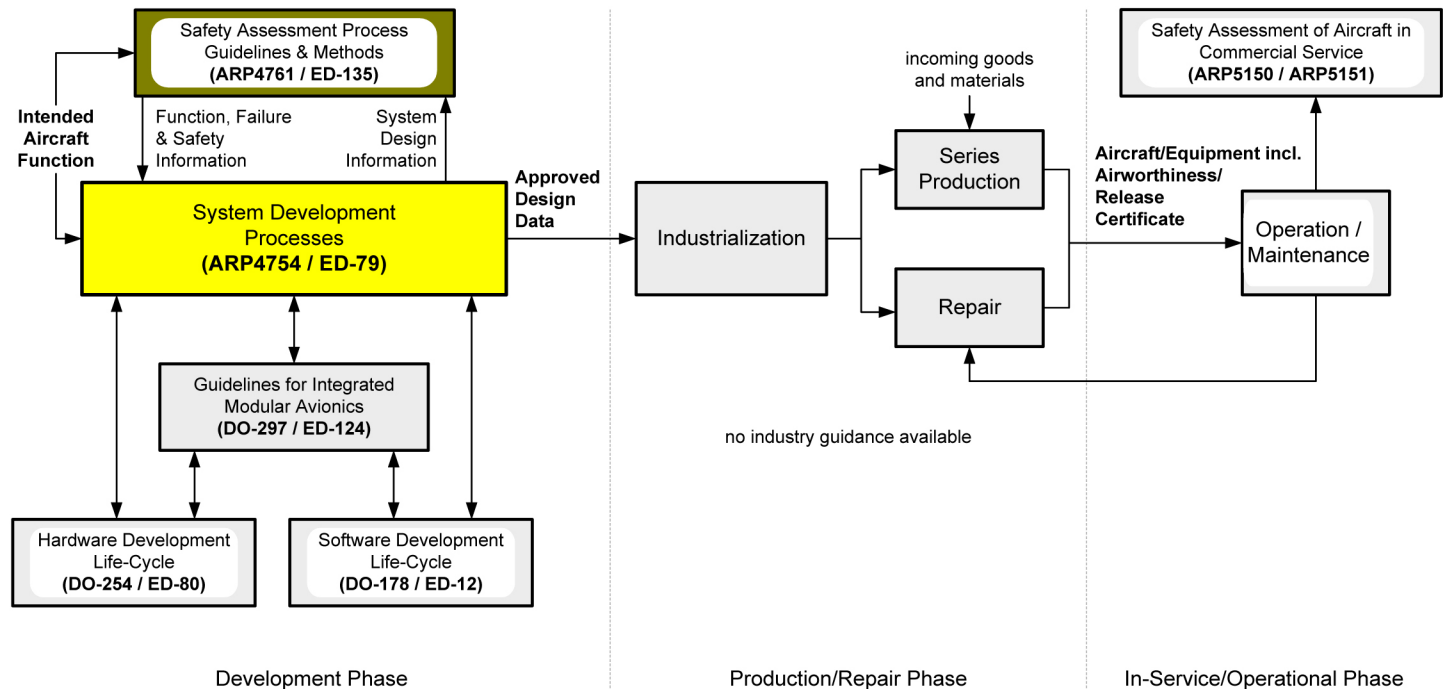


Figure 1. Life-Cycle Phases and Industry Guideline Overview.

THE AVIONICS EQUIPMENT LIFECYCLE

The life-cycle of aircraft, systems and equipment comprises of the development phase, the production phase and the in-service/operational phase (see Figure 1). The phases are accomplished by different organisations reacting to their associated regulations:

The development phase is accomplished by the applicant for the type certificate, (holder of a design organization approval (DOA) under EASA rule). Application for type certificate is regulated by 14 CFR/IR Part 21, subpart B [2, 7], while the technical requirements are given prescribed in 14 CFR Part 25/CS-25, with the important safety regulation for avionics equipment in particular given in §25.1309 [1,3,7].

The production phase is accomplished by a holder of a production organization approval (POA) regulated by 14 CFR/IR Part 21, subpart G [2,4,7,8].

The continued airworthiness activities during the in-service/operational phase, including repair, are accomplished by the holder of the maintenance organization approval (MOA) regulated by 14 CFR/IR Part 145 [9, 10].

Within the in-service/operational phase, there are two levels of activities: Maintenance (exchanging a failed unit with an operational unit), and repair (exchanging parts within a unit). The latter requires a new authorized release certificate and is, by nature, similar to a reduced production process. Within this context, repair activities will therefore be considered as part of the production process.

Figure 1 is derived from ARP4754A [11] showing the industry guidelines available for the individual phases.

Development Phase

The development phase of aircraft, systems and equipment is an integral and iterative process comprised of a development stage and a verification stage (e.g. ARP4754A [11], figure 5, 6), accompanied by an integral safety process.

Development stage

Within the development stage, concepts at aircraft level are detailed into aircraft and system level specifications, which are then detailed down into the equipment level specifications (incl. hardware and software specifications). Those are the basis for the implementation and integration to an avionics equipment product.

Verification stage

The verification stage ensures complete and correct implementation and integration of intended functions from equipment, through system up to aircraft level.

Safety process

As per industry guidelines (e.g. ARP4754A [11]), the development process is accompanied by integral safety processes at each of the function development levels (Figure 2).

The safety process ensures generation and identification of safety features required to show compliance to safety requirements at each level (e.g. ARP4754A [11], figures 5, 7).

The derived safety requirements are provided into the development process, are therefore implemented into the design and verified during the verification stage. Safety specific verification of the implementation and integration of

the safety related requirements is performed during the safety verification process and associated analyses.

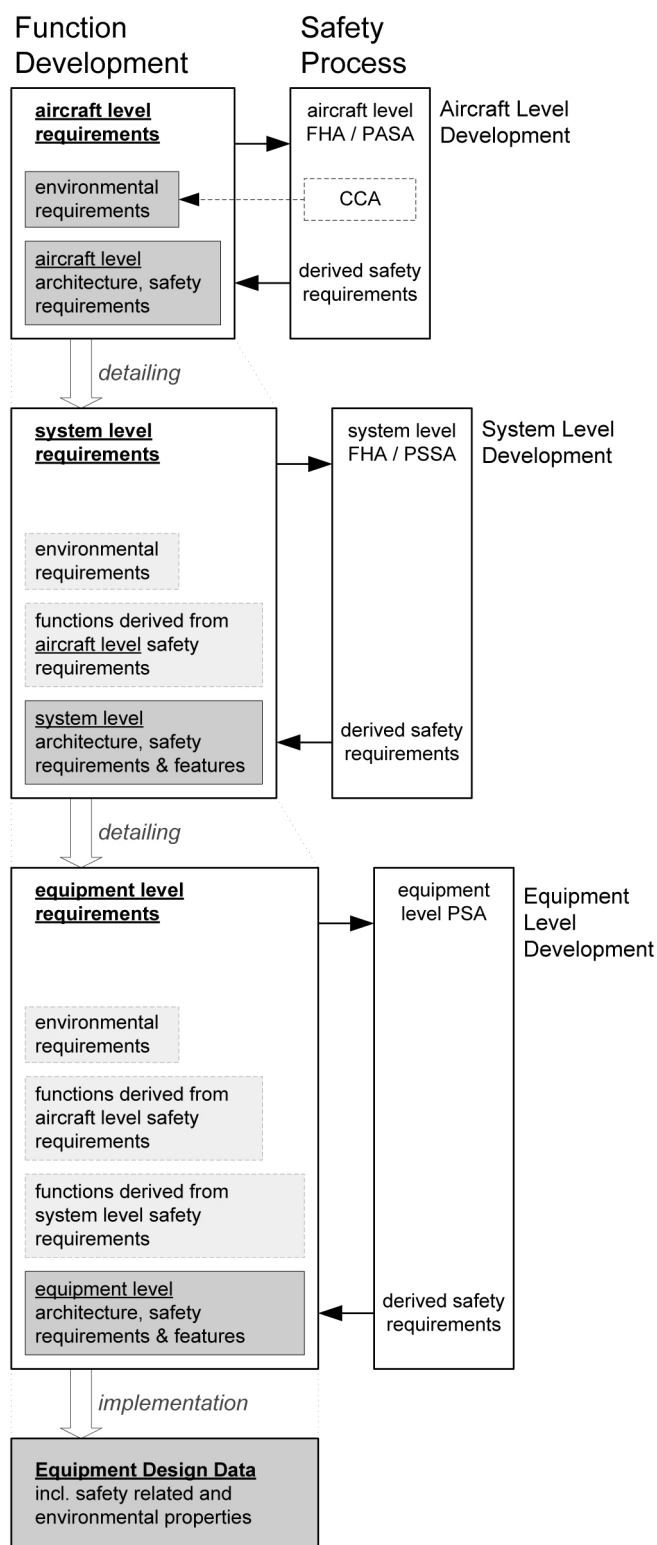


Figure 2. Safety Requirements from all Levels flow into Equipment Design Data.

At aircraft level, the aircraft concept, architectural and functional requirements are subjected to the safety process (e.g. FHA, PASA) which identify or generate derived safety requirements. The common cause analysis performed at aircraft level (including PRA, ZSA, CMA) contributes environmental requirements for non-normal operation (e.g. vibration levels following an engine failure, loss of cooling temperature environment), which could also be considered safety related requirements at this level.

Those aircraft level requirements are detailed into system level requirements and again, at the system level, subjected to the safety assessment process, generating derived safety requirements specific for this level. The safety related requirements generated at the aircraft level may also become more detailed at system level.

The same process applies when the system requirements are detailed into equipment level requirements. The requirement set for the equipment level requirements now contains derived safety requirements from the aircraft and system levels as well as safety related environmental requirements. The safety assessment performed at equipment level contributes additional derived safety requirements.

Requirements from all levels of the development process including the safety related flow into the lowest equipment item. Within the flow of safety related requirements from aircraft level down to equipment level requirements, relevant requirements of those safety related functions or features or environmental requirements should be identifiable as safety related and traceable through the levels of development (ARP4754A [11], section 5.3.1.1).

From equipment level, the requirements, including the safety related requirements, are implemented into the design represented by build data comprised of hardware and software with specific or emergent properties.

In the build data, however, all of implemented functions and features are treated equally. After implementation, it is not recognizable to what extent a particular component or property supports aircraft and system safety, or serves another purpose such as reliability, operability, maintainability or manufacturability.

Certification and approval of design data

Documented accomplishment of processes and evidence of verified compliance at each level (aircraft, system and equipment level) generally leads to certification of the aircraft type (see also Figure 5).

Design data of the aircraft, system and equipment required for series production is approved as part of the certification of the aircraft type.

Design data is the information required to produce identical copies of the certificated aircraft and its components (e.g. ARP4754A [11], chapter 4 and figure 3). Design data may contain build data, as well as requirements and data for the production process, for the product verification (e.g.

correctness, completeness, conformity), and formal criteria (e.g. configuration data). As detailed above, it contains safety related data and properties (see Figure 2).

Design data generally refers to an implementation description of requirements developed within the development process and is of different character as data normally produced within the development process (e.g. requirements, analyses and verification procedures and evidence).

Industry guidelines (e.g. ARP4754A [11]) are not specific about contents and character of the design data required for series production of an aircraft type. As the design data is considered the interface to series production, this paper attempts to detail data required for series production of Avionics equipment and verification of conformity.

Production Phase

The production phase of the aircraft and its equipment consists of an industrialization stage and the production stage (Figure 3). Following completion of each production process step and verification of conformity, the product is finally approved by issuing the release certificate associated with the serial number of the product. The product is airworthy and may be released into the in-service/operational phase.

It seems adequate that the industrialization and production stages including the associated outputs (processes and means) should adopt the general principles of the development standards guidelines of ARP4754A [11], e.g. development assurance, traceability, configuration control, etc., since the inputs (i.e. approved design data) as well outputs (i.e. released products) are associated with type or airworthiness release certificates. However, the discussion of subjecting production with general principles of the development process is not subject of this paper.

Industrialization stage

The industrialization stage uses the approved design data, which is a formal output of the development phase associated with the certificated aircraft type. This data is used to develop the production process and the means required for the series production of the product. It is also used to develop the quality system required to verify conformity of each serial product to the approved design data.

Similarities between the system/equipment development process and methods including the safety process and the industrialization process including the quality process are established in the following chapters of this paper.

Production process and means

The development of the production process and associated means is primarily based on the build data included in the approved design data. It involves also the product breakdown, supply chain and purchasing of incoming goods and materials, as the associated definitions need to be considered for the development of the quality system.

Details of the industrialization of production processes and means are beyond the scope of this paper. This paper will focus on safety processes within the development phase and the associated quality processes within production phase.

Quality process and means

The development of the quality process and associated means is comprehensive and requires the build data, the essential properties and the definitions of the production process and means. The activity is interactive and iterative with the development process of the equipment and of the production concerning verifiability of the conformity.

The quality process needs to consider completeness and correctness of the build process as well as failures which may occur with the components, sub-assemblies or during the final assembly of the equipment. The nature of the failures may be random or systematic (common mode). As per the regulation, the quality system needs to ensure conformity of the released product to the approved design data.

The quality system is integral with the series production process, and needs to cover the full process, e.g. from the supply of commercial-off-the-shelf items (components or sub-assemblies not developed and produced to aerospace standard processes) and supply of (aerospace) sub-assemblies up to the final assembly of the “black box” product.

A systematic approach using different methodologies may be required for the development of a quality system to ensure detection of any potential non-conformities and failures prior to release of the product to an airplane operation. The overall approach should identify which deficiency may be detectable by which inspection or test. An attempt to depict suitable methods and analyses is provided further below in this paper.

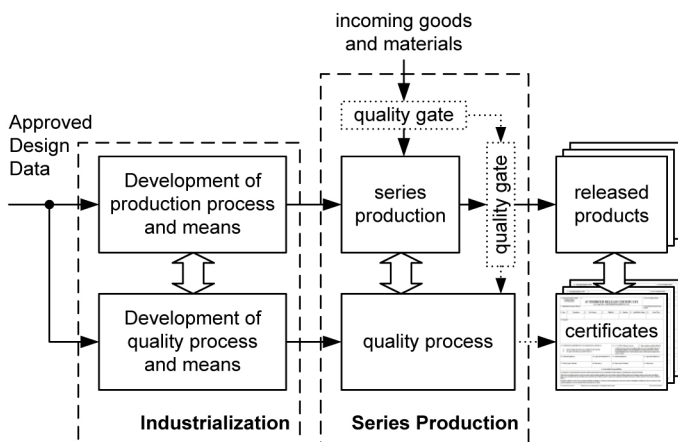


Figure 3. Industrialization and Series Production.

Series production

An example of the integral production and quality process is depicted in Figure 4. Parts and components may be assembled to sub-assemblies in different processes (e.g. “process 1” and “process 2”) prior to the final assembly to a black box (e.g. “process 3”). The sub-assemblies are approved for conformity (completeness and correctness) within a process quality gate both considering the confirmed work instructions (completeness) and verification results (correctness) of quality means.

The quality means at this intermediate quality gate, depending on feasibility, may involve testing and inspection to verify properties which may not be accessible at the fully assembled product. Testing may be automated, while inspections follow predefined checklists.

Example 1: Within “process 1”, board stiffener devices may be installed on electronic circuit card assemblies to ensure compliance to non-normal environmental vibration requirements derived from a higher level safety assessment. The quality gate verifies by inspection, that the appropriate devices are installed, and fixed according to the working instructions with appropriate means, e.g. screwed, glued, etc. The conformity verification is performed immediately after the build process step since they are not visible after final assembly and their associated function is not testable. Other properties of this process step (e.g. correct performance and functioning of an electronic circuit) may be automatically tested after final assembly during a black box test.

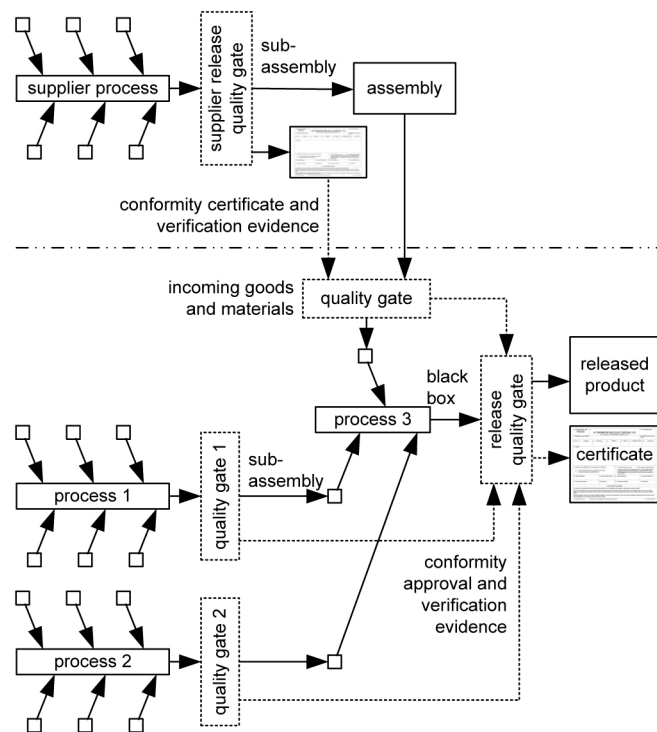


Figure 4. Integral Production and Quality Process.

Sub-assemblies delivered by a sub-tier supplier are produced according to the “supplier process”. A supplier quality gate is defined in coordination with the overall quality system concept and ensures verification of properties which cannot be verified after the final assembly. The supplier provides a conformity certificate along with the sub-assembly. The production goods and materials incoming inspection for this case may be limited to identification of the sub-assembly and acceptance of the certificate and associated verification evidence documentation.

This description refers to sub-assemblies produced by a POA holder or in the sense of the associated processes. If a sub-assembly, a part or electronic component is an “off-the-shelf” component (no process control and no conformity certificate delivered, e.g. by non-aerospace production), the incoming goods and materials quality gate, needs to be coordinated with the overall quality system concept. The identification and any essential property, which cannot be verified during subsequent sub-assembly or final assembly quality gates needs to be verified by the incoming goods and materials quality gate.

The final assembly process (e.g. “process 3”) produces the final product to be released to the aircraft. The release quality gate is the last step of the conformity verification performed on the final product (“black box”).

The release quality gate verifies correct processing of the last production step, external (physical) properties and the operational performance of functions within a normal and non-normal aircraft environment. Configuration items (hardware and software) need to be verified and documented.

The approval process certifying the release of the product into aircraft operation must consider conformity verification approvals of the final and sub-assembly quality gates and collect the overall verification evidence (e.g. completed work instructions, test results, completed checklist forms) associated with the equipment series part number.

In-Service/Operational Phase

The in-service phase represents the operation of the aircraft within a fleet performing the intended functions under the anticipated operational and environmental conditions. This phase is manifold and begins with entry-into-service of an aircraft type. Each aircraft and equipment goes through a life cycle of service operation, failure conditions, maintenance action, and resuming service operation.

The failure conditions may be caused by random failures of components, development errors (common modes), but also by production failures or errors. In-service data including data about identified causal production failures or errors, as well as any experience associated may be valuable to improve both the production process and the quality system - overall to improve safety of the fleet in-service and future aircraft.