The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE

ED-80

April 2000

102 rue Etienne Dolet
92240 Malakoff, France
Web Site: www.eurocae.net

Tel: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net

DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE

ED-80

April 2000

FOREWORD

1. This document, prepared by EUROCAE Working Group 46 "Electronic Hardware", was accepted by the Council of EUROCAE on April 2000.

2. EUROCAE is an international non-profit making organisation. Membership is open to European users and manufacturers of equipment for aeronautics, trade associations, national civil aviation administrations and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.

3. The findings of EUROCAE are resolved after discussion among its members and in co-operation with RTCA Inc., Washington DC, USA and/or the Society of Automotive Engineers (SAE), Warrendale PA, USA through their appropriate committees.

4. This document has been achieved jointly with RTCA SC-180 and is identical to RTCA DO-254.

5. EUROCAE performance specifications are recommendations only. EUROCAE is not an official body of the European Governments; its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.

6. Copies of this document may be obtained from:

EUROCAE
102 rue Etienne Dolet
92240 Malakoff
France

Phone: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
E-mail: eurocae@eurocae.net
Internet: www.eurocae.net

EXECUTIVE SUMMARY

The development and use of complex electronic hardware by the aviation industry has created new safety and certification concerns. In response, EUROCAE WG-46 and RTCA SC-180 were formed. WG-46 and SC-180 agreed to become a joint committee early in the development of this document. This joint committee was chartered to develop clear and consistent design assurance guidance for electronic airborne hardware such that it safely performs its intended functions.

Electronic airborne hardware includes line replaceable units, circuit board assemblies, application specific integrated circuits, programmable logic devices, etc. This guidance is applicable to current, new, and emerging technologies.

The guidance in this document is intended to be used by aircraft manufacturers and suppliers of electronic hardware items for use in aircraft systems. The hardware design life cycle processes are identified. Objectives and activities for each process are described. The guidance is applicable to all hardware design assurance levels as determined by the system safety assessment.

In the development of this document, the committee considered other industry documents including document EUROCAE ED-79/SAE ARP4754, Certification Considerations for Highly Integrated or Complex Aircraft Systems; SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment; and EUROCAE ED-12/RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The use of increasingly complex electronic hardware for more of the safety critical aircraft functions generates new safety and certification challenges. These challenges arise from a concern that said aircraft functions may be increasingly vulnerable to the adverse effects of hardware design errors that may be increasingly difficult to manage due to the increasing complexity of the hardware. To counteract this perceived escalation of risk it has become necessary to ensure that the potential for hardware design errors is addressed in a more consistent and verifiable manner during both the design and certification processes.

As airborne electronic hardware becomes more complex, technology evolves and experience is gained in the application and use of the procedures described in this document, this document will be revised and reviewed consistent with approved RTCA/EUROCAE procedures.

1.1 PURPOSE

This document has been prepared to assist organizations by providing design assurance guidance for the development of airborne electronic hardware such that it safely performs its intended function, in its specified environments. This guidance should be equally applicable to current, new, and evolving technologies. The purposes of this document are to:

1. Define hardware design assurance objectives.
2. Describe the basis for these objectives to help ensure correct interpretation of the guidance.
3. Provide descriptions of the objectives to allow the development of means of compliance with this and other guidance.
4. Provide guidance for design assurance activities to meet the design assurance objectives.
5. Allow flexibility in choice of processes necessary to meet the objectives of this document including improvements, as new process technologies become available.

This document recommends the activities that should be performed in order to meet design assurance objectives, rather than detailing how a design should be implemented.

The philosophy used to generate this guidance document is one of a top-down perspective based on the system functions being performed by electronic hardware and not a bottom-up perspective or one based solely on the specific hardware components used to implement the function. A top-down approach is more effective at addressing safety design errors by facilitating informed system and hardware design decisions, and efficient and effective verification processes. For example, verification should be performed at the highest hierarchical level of the system, assembly, and subassembly, component or hardware item at which compliance of the hardware item to its requirements can be achieved and the verification objectives satisfied.

1.2 SCOPE

This document provides guidance for design assurance of airborne electronic hardware from conception through initial certification and subsequent post certification product improvements to ensure continued airworthiness. It was developed based on showing compliance with certification requirements for transport category aircraft and equipment but parts of this document may be applicable to other equipment.

The relationship between the system life cycle and the hardware design life cycle is described to aid in the understanding of the interrelationships of the system and hardware design assurance processes. A complete description of the system life cycle, including system safety assessment (SSA) and validation, and the aircraft certification process is not intended.

Certification issues are discussed only in relation to the hardware design life cycle. Aspects concerning the ability to produce, test, and maintain the hardware item are addressed only as they relate to airworthiness of the hardware design.

The guidance in this document is applicable, but not limited to, the following hardware items:

1. Line Replaceable Units (LRUs).
2. Circuit Board Assemblies.
3. Custom micro-coded components, such as Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs), including any associated macro functions.
4. Integrated technology components, such as hybrids and multi-chip modules.
5. Commercial-Off-The-Shelf (COTS) components.

Additional considerations that refer specifically to COTS components are included in Section 11 since COTS component suppliers may not necessarily follow the design processes described by this document or provide the necessary hardware design life cycle data.

This document does not attempt to define firmware. Firmware should be classified as hardware or software and addressed by the applicable processes. This document assumes that during the system definition, functions have been allocated to either hardware or software. RTCA DO-178/EUROCAE ED-12 provides guidance for functions that are allocated to implementation in software. This document provides guidance for functions that are allocated to hardware.

NOTE: This allows an efficient method of implementation and design assurance to be determined at the time the system is specified and functions allocated. All parties should agree with this system decision at the time that the allocation is made.

Assessment and qualification of tools used for hardware item design and verification is addressed in Section 11.4.

This document does not provide guidance concerning organizational structures or how responsibilities are divided within those structures.

Environmental qualification criteria are also beyond the scope of this document.

1.3 RELATIONSHIP TO OTHER DOCUMENTS

In addition to the airworthiness requirements, various national and international standards for hardware are available. In some communities, compliance with these standards may be required. However, it is outside the scope of this document to invoke specific national or international standards, or to propose a means by which these standards might be used as an alternative or supplement to this document.

Where this document uses the term “standards”, it should be interpreted to mean the use of project-specific standards as applied by the airborne system, airborne equipment, engine, or aircraft manufacturer. Such standards may be derived from general standards produced or adopted by the manufacturer. Guidance for standards is provided in Section 10.2.

1.4 RELATED DOCUMENTS

EUROCAE ED-79/SAE ARP4754, Certification Considerations for Highly Integrated or Complex Aircraft Systems, as a source of development guidance for highly integrated or complex aircraft systems.

SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, as a source of safety assessment methods to be used in the hardware design assurance process.

EUROCAE ED-12/RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification, as the complementary document for software development assurance.

EUROCAE ED-14/RTCA DO-160, Environmental Conditions and Test Procedures for Airborne Equipment, may be used by equipment designers as the primary environmental test standard for hardware item qualification.

1.5 HOW TO USE THIS DOCUMENT

This document is intended to be used by the international aviation community. To aid such use, references to specific national regulations and procedures are minimized. Instead, generic terms are used. For example, the term “certification authority” is used to mean the organization or person granting approval on behalf of the country responsible for certification. Where a second country or a group of countries validates or participates in this certification, this document may be used with due recognition given to bilateral agreements or memoranda of understanding between the countries involved.

The guidance in this document represents a consensus of the aviation community and is a collection of the best industry practices for design assurance of airborne electronic hardware. To take into account the process developed in this document, the intent was to produce guidance that should be applied to complete new hardware designs and subsequent changes. Guidance for hardware previously developed to other processes is addressed in Section 11.1. It is understood that means other than those described herein may be available to and be used by the applicant.

In cases where examples are used to indicate how the guidance might be applied, either graphically or through narrative, the examples are not to be interpreted as the preferred method.

Section 11 discusses additional considerations for specific known cases where some of the objectives of Section 2 through Section 9 may not be satisfied. These considerations include guidance for the use of previously developed hardware, COTS component usage, product service experience, and tool assessment and qualification.

Appendix A provides guidance for the necessary hardware design life cycle data based on the hardware design assurance level that is being implemented.

Appendix B contains guidance on design assurance techniques for hardware used in implementing Level A and B functions which should be applied in addition to the guidance in Section 2 through Section 11. Appendix B may be applied for hardware of design assurance Levels C and D at the applicant’s discretion.

The Glossary of Terms as used in this document is contained in Appendix C. Appendix D contains a list of acronyms that are used in the document and spells out their complete names.

A list does not imply that its elements are in any way complete or that all elements are relevant to any specific product.

Notes are used in this document to provide explanatory material, emphasize a point, or draw attention to related subjects, which are not entirely within context. Notes do not contain guidance.

The word “should” is used when the intention is to provide guidance. “May” is used in conjunction with optional text.

This document uses the term “hardware item” to describe the electronic hardware which is the subject of the document.

The qualifier “hardware” is to be assumed throughout the document unless specifically stated otherwise. When the term “requirements” is used it is assumed to mean “hardware requirements”. A system or software qualifier will always be specifically stated, such as “system requirement”.

NOTE: Various industry advisory documents and aviation requirement documents do not always use harmonized terminology. For example, Federal Aviation Regulations (FAR) 21 and Joint Aviation Requirements (JAR) 21 use the term “product” to mean an aircraft, aircraft engine, or propeller. Document SAE ARP4754/EUROCAE ED-79 uses the term “product” to mean hardware, software, item or system generated in response to a defined set of requirements. The reader is advised to be aware of these and other differences in the use of terminology. This document uses the definitions in the glossary.

1.6 COMPLEXITY CONSIDERATIONS

Although various classifications of the term “complexity” are used to describe electronics, such as simple, complex and highly complex, the differentiation between these classifications is not rigorously defined. Defining differences in complexity herein is based on the feasibility and level of difficulty necessary to accomplish acceptable verification coverage by deterministic means.

Hardware should be examined hierarchically at the levels of integrated circuit, board and LRU for complexity, including addressing functions that may not be testable, such as unused modes in multiple usage devices and potentially hidden states in sequential machines.

A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior.

When an item cannot be classified as simple, it should be classified as complex. An item constructed entirely from simple items may itself be complex. Items that contain a device, such as an ASIC or a PLD, can be considered simple if they meet the criteria of simple as described in this section.

For complex items, the proposed means of providing design assurance should be agreed to by the certification authority early in the hardware design life cycle to mitigate program risk.

For a simple hardware item, extensive documentation of the design process is unnecessary. The supporting processes of verification and configuration management need to be performed and documented for a simple hardware item, but extensive documentation is not needed. Thus, there is reduced overhead in designing a simple hardware item to comply with this document. The main impact of this document is intended to be on the design of complex hardware items.

1.7 ALTERNATIVE METHODS OR PROCESSES

Methods or processes other than those described in this document may be used to provide hardware design assurance. These methods and processes should be assessed based on their ability to satisfy the applicable regulations. Alternative methods or processes should be approved by the certification authority prior to their implementation. In lieu of direct comparison with the applicable regulations, the applicant could use the following guidance to reduce program risk while evaluating alternative methods or processes by comparison to this document.

Considerations for evaluation of alternative methods or processes may include:

1. Where used instead of processes prescribed by this document, processes satisfying one or more of the objectives of Section 2 through Section 9 should show an equivalent level of design assurance.
2. The effect of the proposed alternative methods or processes on satisfying the hardware design assurance objectives should be assessed.
3. The effect of the proposed alternative methods or processes on the life cycle data should be assessed.
4. The rationale for using the proposed alternative methods or processes should be substantiated by evidence that the methods or processes will produce the expected results.

1.8 DOCUMENT OVERVIEW

Figure 1-1 is a pictorial overview of the sections in this document, and some of their relationships to each other and to other related processes. There is no intent to show data flow but rather to show which sections and external processes are related.

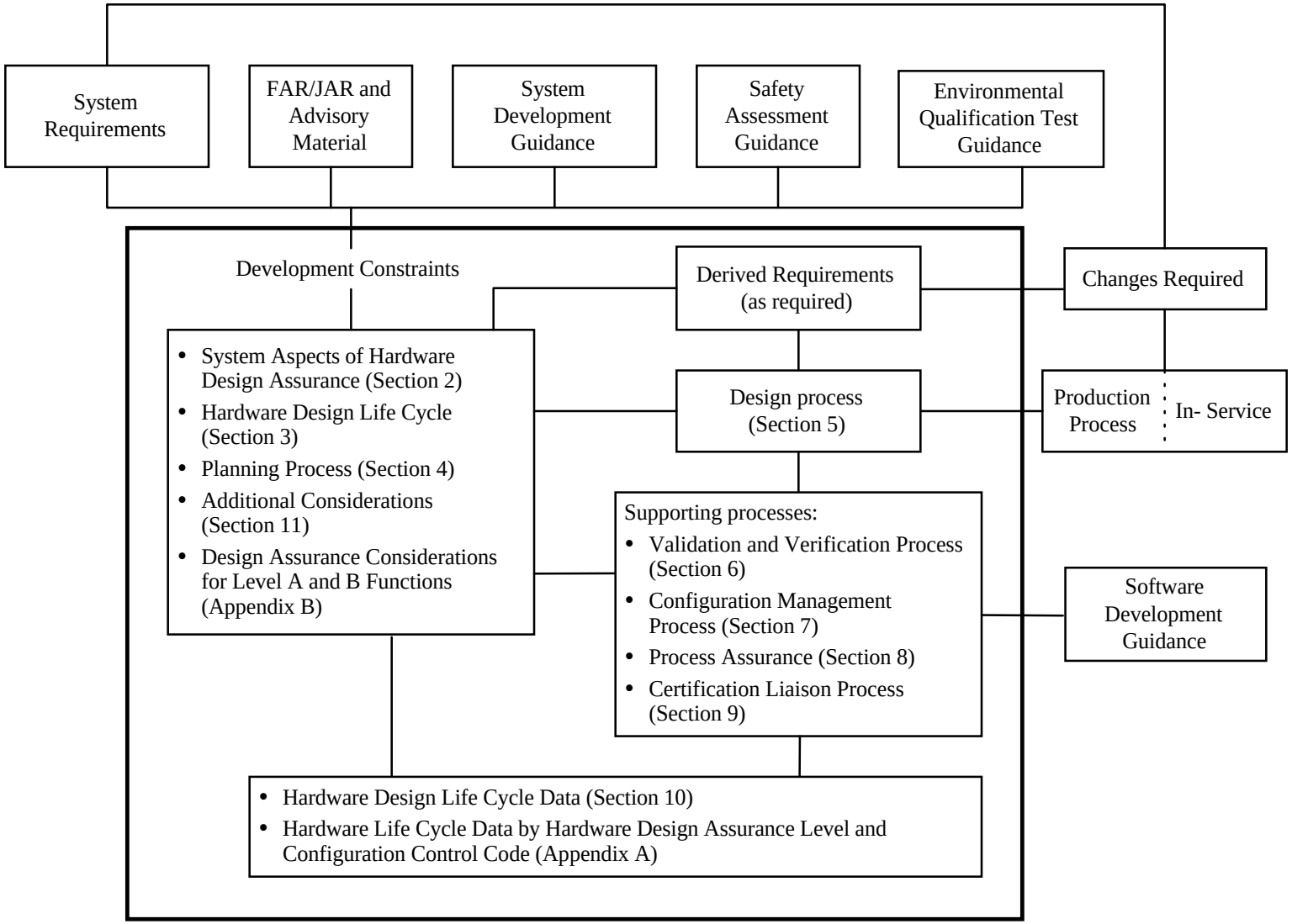


FIGURE 1-1: DOCUMENT OVERVIEW

CHAPTER 2

SYSTEM ASPECTS OF HARDWARE DESIGN ASSURANCE

Hardware design assurance begins at the system level with the allocation of system functions to hardware and the assignment of their corresponding system development assurance levels.

A single system function may be assigned to a hardware item, to a software component or to a combination of hardware and software. Safety requirements associated with the function are addressed from a system perspective, a software perspective and a hardware perspective to determine the level of reliability and the level of assurance necessary to satisfy these requirements.

Figure 2-1 illustrates the relationships of the system development process for airborne systems and equipment and safety assessment, hardware development, and software development processes.

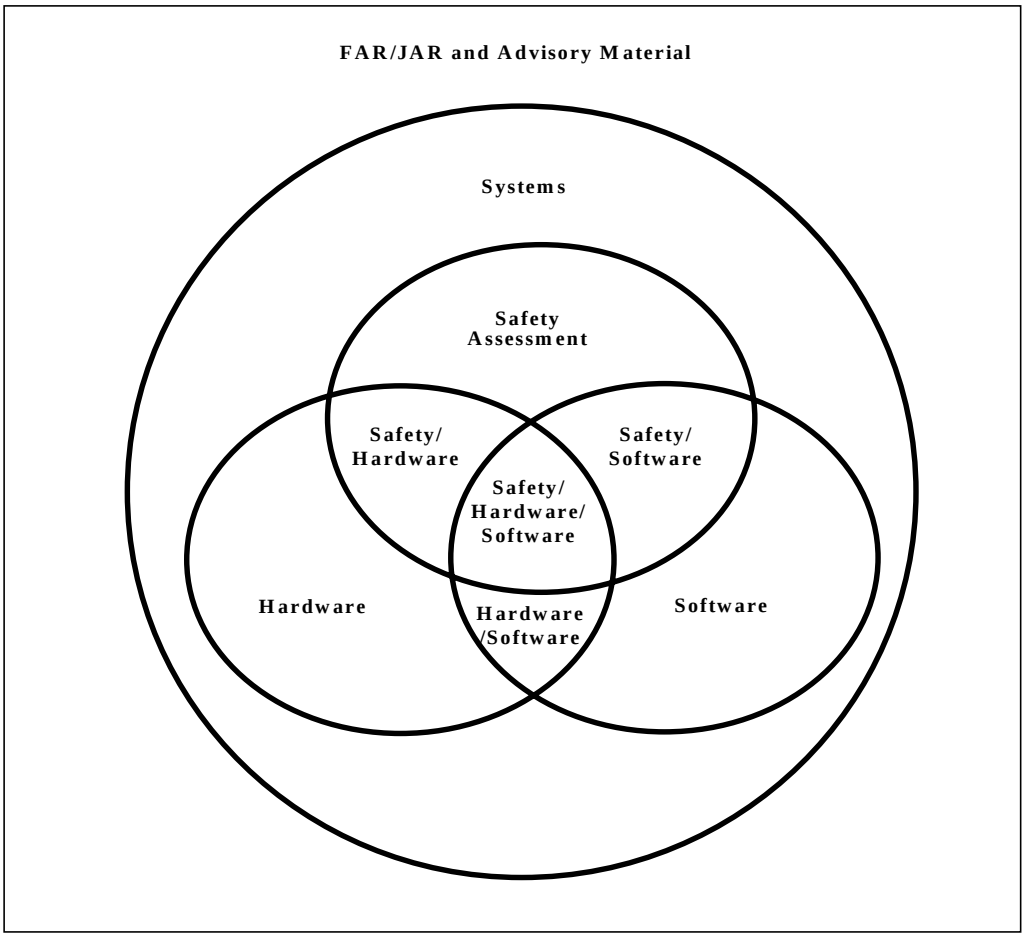


FIGURE 2-1: RELATIONSHIPS AMONG AIRBORNE SYSTEMS, SAFETY ASSESSMENT, HARDWARE AND SOFTWARE PROCESSES

There are four areas of overlap in the figure, Safety/Hardware, Safety/Software, Hardware/Software and Safety/Hardware/Software. These overlaps illustrate the relationship and interactions between these processes where a system requirement may result in requirements within the scope and design assurance guidance of multiple processes. For example, a hardware function that contained safety requirements would involve both the safety assessment process and the hardware design life cycle process.

The overlaps illustrate the need for a coordinated interaction between the processes to ensure that the assurance requirements of the system function are satisfied. The discussion of system or software assurance processes is beyond the scope of this document. However, in coordinating the design assurance for a hardware function, the applicant may wish to take advantage of assurance provided by activities in the systems or software processes.

These relationships and interactions are described further in Section 2.1.1 through Section 2.1.3.

2.1 INFORMATION FLOW

The flow of information between the life cycle processes is shown in Figure 2-2. The following sections describe the flow of information from the system development process to the hardware design life cycle process, from the hardware design life cycle process to the system development process, and between the hardware design life cycle process and the software life cycle process.

NOTE: It is recognized that these are iterative processes and changes will occur throughout the hardware design life cycle.

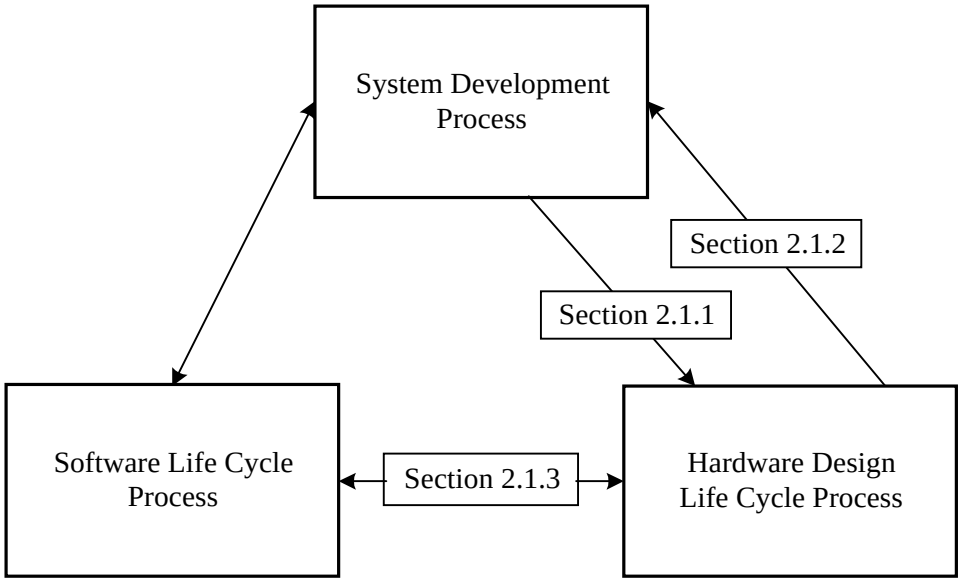


FIGURE 2-2: SYSTEM DEVELOPMENT PROCESSES

2.1.1 Information Flow from System Development Process to Hardware Design Life Cycle Process

This information flow may include:

1. Design and safety requirements allocated to hardware.
2. Design assurance level for each function, along with its associated requirements and failure conditions, if applicable.
3. Allocated probabilities and at risk exposure times for hardware functional failures.
4. Hardware/software interface description.
5. Requirements for safety strategies and design constraints, such as testability, design methods, and hardware architectures.
6. Requirements for system verification activities to be performed by hardware level verification.
7. Installation, ergonomic and environmental requirements allocated to hardware.
8. Integration problem reports that may have an impact on requirements. These may arise as a result of activities, such as system verification, generation of system requirements or SSA.

2.1.2 Information Flow from Hardware Design Life Cycle Process to System Development Process

This information flow may include:

1. Implementation of the requirements, such as mechanical drawings, schematics and parts lists.
2. Hardware derived requirements that may have an impact on any allocated requirement.
3. Implementation architecture, including fault containment boundaries.
4. Evidence of any required system verification and validation activities performed during the hardware design life cycle.
5. Product safety analysis data, such as:
   a. Probabilities and failure rates for designated hardware functional failures of concern to the SSA process.
   b. Common mode fault analysis.
   c. Isolation boundaries and generic fault mitigation strategies.
   d. Latency analysis data relevant to system requirements. Examples are hardware provisions for fault monitoring, fault detection intervals and undetectable faults.
6. Requirements for hardware verification activities to be performed by system level verification.
7. Assumptions and analysis methods regarding installation requirements and environmental conditions necessary for the analyses to be valid.
8. Problem or change reports that may have an impact on system, software or allocated hardware requirements.

2.1.3 Information Flow between Hardware Design Life Cycle Process and Software Life Cycle Process

This information flow may include:

1. Derived requirements needed for hardware/software integration, such as definition of protocols, timing constraints, and addressing schemes for the interface between hardware and software.
2. Instances where hardware and software verification activities require coordination.
3. Identified incompatibilities between the hardware and the software, which may be part of a reporting and corrective action system.
4. Safety assessment data that should also be made available to system processes.

2.2 SYSTEM SAFETY ASSESSMENT PROCESSES

There are three system safety assessment processes: functional hazard assessment (FHA), preliminary system safety assessment (PSSA) and SSA. These processes are used to establish the system safety objectives applicable to the system development assurance process, and to determine that the system functions achieve the safety objectives.

The SSA process should transform the safety objectives into system and equipment safety requirements. These requirements should embody the basic safety objectives and safety attributes for system and equipment functions and architecture. The SSA process and the system development process allocate these safety requirements to the hardware.

There are five system development assurance levels, Level A through Level E, corresponding to the five classes of failure conditions: catastrophic, hazardous/severe-major, major, minor and no effect. Table 2-1 correlates the hardware design assurance levels to the five classes of failure conditions and provides definitions of hardware failure conditions and their respective design assurance levels. Initially, the hardware design assurance level for each hardware function is determined by the SSA process using an FHA to identify potential hazards and then the PSSA process allocates the safety requirements and associated failure conditions to the function implemented in the hardware.

Throughout the hardware design life cycle, there may be iterative feedback between the safety, system and hardware processes to ensure that the hardware as designed and built will satisfy the system safety, functional and performance requirements allocated to the hardware.

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

TABLE 2-1: HARDWARE DESIGN ASSURANCE LEVEL DEFINITIONS AND THEIR RELATIONSHIPS TO SYSTEMS DEVELOPMENT ASSURANCE LEVEL

2.3 HARDWARE SAFETY ASSESSMENT

The hardware safety assessment is conducted in conjunction with and to support the SSA process. The intent of this safety process is to demonstrate that the applicable systems and equipment, including the hardware, have satisfied the safety requirements of applicable aircraft certification requirements.

Given the safety, functional and performance requirements allocated to the hardware by the system process, the hardware safety assessment determines the hardware design assurance level for each function and contributes to determining the appropriate design assurance strategies to be used.

2.3.1 Hardware Safety Assessment Considerations

The designer of a hardware item may show compliance with the safety requirements allocated to the hardware and with the hardware design assurance level by an appropriate design assurance strategy.

A single design assurance level and strategy may be applied to an entire hardware item or a hardware item may be evaluated as having separate functional failure paths (FFPs) in order to accommodate a mix of design assurance levels or design assurance strategies. A functional failure path analysis (FFPA) may be used to justify a lower design assurance level for a portion of the hardware item, or to accommodate different functions implemented with different technologies or product service histories.

NOTE: FFPA is described in Appendix B, Section 2. Although written to address the subject matter of Appendix B, this analysis method may be applied to any design assurance level.

If a hardware item contains functions that individually have different design assurance levels, such situations may be addressed by either of the following methods:

- The entire item may be assured at the highest design assurance level.
- The individual hardware functions may be assured separately at their respective hardware design assurance levels as defined by the hardware safety assessment, if their function, interfaces and shared resources can be protected from adverse effects of functions of lower design assurance levels. Design assurance of shared resources should be the design assurance level of the function with the highest level.

Guidance for hardware safety assessment includes:

1. Iterative hardware safety assessment and design should determine derived hardware safety requirements and ensure that system safety requirements allocated to the hardware are satisfied and ensure that derived requirements are satisfied.
2. These derived requirements should include safety requirements for hardware architecture, circuits and components, and protection against anomalous behaviors, including incorporating specific hardware architectural and functional safety attributes, such as:
    a. Circuit or component redundancy.
    b. Separation or electrical isolation between circuits or components.
    c. Dissimilarity between circuits or components.
    d. Monitoring of circuits or components.
    e. Protection or reconfiguration mechanisms.

f. Allowed failure rates and probabilities for circuit and component random failures and latent failures.

g. Limitations of usage or installation.

h. Prevention and management of upsets and upset recovery.

3. The hardware design assurance process and the hardware safety assessment should jointly determine the specific means of compliance and design assurance level for each function and should determine that an acceptable level of design assurance has been achieved.

NOTE: Anomalous behavior of the hardware may be caused by random faults or design errors in a hardware item, or by upsets to the hardware.

The hardware designer may choose a higher hardware design assurance level for a hardware item function. An example would be the anticipation of re-using a hardware item function in an installation requiring a higher level of design assurance.

The hardware safety assessment may use various qualitative and quantitative assessment methods. These may include fault tree analysis (FTA), common mode analysis, failure modes and effects analysis, and statistical reliability analysis methods for applicable quantitative assessment of random faults.

2.3.2 Quantitative Assessment of Random Hardware Faults

Statistical failure assessment and prediction methods, which are based on hardware failure rates, redundancy, separation and isolation, failure mode statistics, probability analysis, component de-rating, stress analysis, and manufacturing process control, have proven to be acceptable means of assessing quantitative risk factors for random failures of hardware.

2.3.3 Qualitative Assessment of Hardware Design Errors and Upsets

Unlike random failures of hardware, neither design errors nor some types of upsets are statistically predictable, and both may cross redundancy boundaries in the form of common mode faults. Redundancy management techniques and quantitative assessment methods to be used should be selected so that potential common mode faults and the effects of upsets are precluded or mitigated when necessary.

Although difficult to assess quantitatively, safety risk from design errors and upsets can be effectively assessed by a practical application of qualitative safety assessment methods. Analysis techniques, such as fault tree analysis, common mode analysis, and functional failure modes and effects analysis (F-FMEA), are fundamentally qualitative methods, and can be used to address hardware design errors and upsets. More specifically, these methods can determine the potential effects of design errors and upsets, and can help determine the means by which they are to be precluded or mitigated. Using these methods, the hardware safety assessment can contribute to determining the hardware design assurance strategies to be used and can be used iteratively throughout the hardware design process to qualitatively determine the assurance achieved by the selected strategies.

2.3.4 Design Assurance Considerations for Hardware Failure Condition Classification

As the severity of the system failure condition increases, the amount of hardware design assurance necessary to ensure that related failure conditions have been mitigated increases. For all design assurance levels, an approach or strategy should be developed to ensure an appropriate level of design assurance. Figure 2-3 outlines the decision-making process for developing an appropriate design assurance strategy.

Guidance includes:

1. For Level A or B functions implemented in hardware, the design assurance considerations should address potential anomalous behaviors and potential design errors of the hardware functions.
2. The decision making process outlined in Figure 2-3 should be used when developing design assurance strategies for each hardware function being implemented.
3. The strategies described in Appendix B should be applied for Level A and B functions in addition to the guidance provided in Section 3 through Section 11.
4. The design assurance strategy should be selected as a function of the hardware architecture and usage, and of the hardware implementation technology that has been chosen.

Different technologies, components selection, and components usage offer varying degrees of hardware design life cycle information and varying degrees of inherent protection against design errors and their effects. The most suitable design assurance method may vary for different functional paths within the same hardware item.

The numbers in the decision and activity blocks of Figure 2-3 refer to the numbered items following the figure that provide further clarification of the decision or activity.

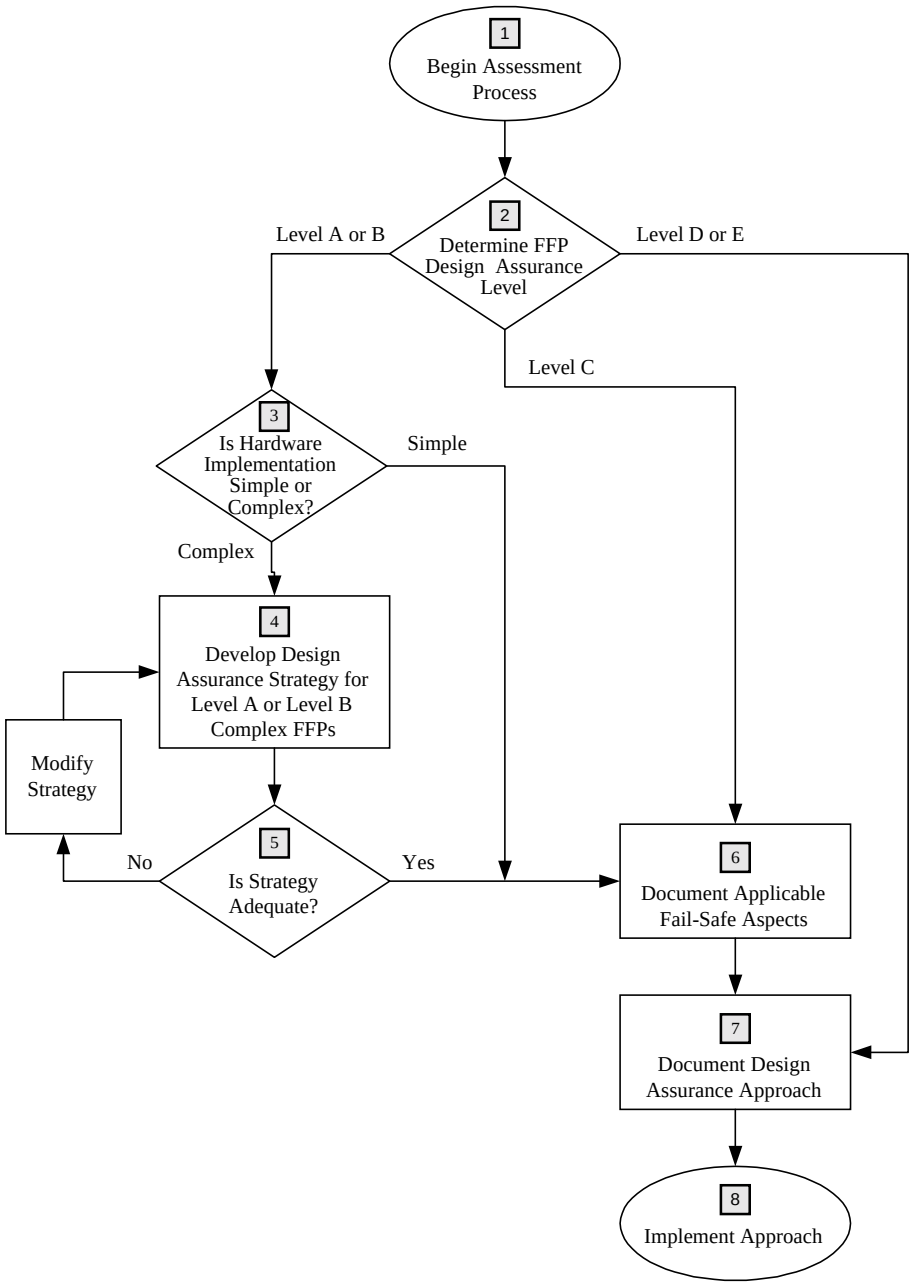


FIGURE 2-3: DECISION MAKING PROCESS FOR SELECTING THE HARDWARE DESIGN ASSURANCE STRATEGY

1. **Begin Assessment Process.** For all design assurance levels, an approach or strategy should be developed to ensure an appropriate level of design assurance.

2. **Determine FFP Design Assurance Level.** For each identified hardware item, determine and document the FFPs associated with the item and the design assurance level. Conventional safety assessment techniques should be used to determine which hardware circuits are and which are not in the identified Level A or B FFPs.

3. **Is the Hardware Implementation of the FFP Simple or Complex?** For hardware design assurance Level A or Level B FFPs, determine if the hardware is simple or complex as described in Section 1.6.

4. **Develop Design Assurance Strategy for Level A or Level B Complex FFPs.** If the FFP is complex and Level A or B, use the additional strategies described in Appendix B to determine the appropriate design assurance strategy, corresponding implementation concept and the error mitigation methods. For each Level A or B FFP, a design assurance strategy should be determined using advanced analysis, product service experience or architectural mitigation.

   Level A FFPs in an implementation may require more than one approach if the approach selected does not provide complete mitigation of potential failures and anomalous behaviors.

5. **Is the Strategy Adequate?** Determine if there are deficiencies in the design assurance strategies and, if deficiencies exist in the strategy or would exist in the data expected to be available, modify the strategy to correct the deficiencies by proposing additional design assurance, implementation or architectural strategies.

   When the design assurance strategy is acceptable, document the design assurance processes for each FFP. The strategy should also address certification authority participation aspects, such as schedule milestones, program reviews and oversight activities.

6. **Document the Applicable Fail-Safe Aspects.** Determine the appropriate fail-safe design architecture and features of the hardware item and perform an analysis to satisfy the availability and integrity requirements of the system. Document the fail-safe design aspects and the associated common mode analysis, probability analysis, architecture and other features.

7. **Document the Design Assurance Approach and Strategy.** Document and obtain certification authority approval of the applicable design assurance approach and strategy in the system certification plan or the Plan for Hardware Aspects of Certification (PHAC).

8. **Implement the Approach.** Implement the hardware design in compliance with the appropriate design assurance approach as defined in the approved plan and document evidence of compliance to approved plans and strategy.

CHAPTER 3

HARDWARE DESIGN LIFE CYCLE

This section outlines the hardware design life cycle discussed in Section 4 through Section 9. This document does not prescribe a preferred life cycle model, nor imply a structure for the performing organization. The hardware design life cycle is equally applicable to the development of new systems or equipment and modifications to existing systems or equipment. The life cycle for each project should be based on selection and arrangement of processes and activities determined by the attributes of the project, such as requirements stability, use of previously developed hardware and hardware design assurance levels. The hardware design life cycle processes may be iterative, that is, entered, re-entered and modified due to incremental development and feedback between the processes.

3.1 HARDWARE DESIGN LIFE CYCLE PROCESSES

The hardware design life cycle processes are:

The hardware planning process, described in Section 4, defines and coordinates the activities of the hardware design and supporting processes for a project.

The hardware design processes, described in Section 5, generate the design data and resultant hardware item. These processes are requirements capture, conceptual design, detailed design, implementation and production transition.

The supporting processes, described in Section 6 through Section 9, produce the hardware design life cycle data that assures correctness and control of the hardware design life cycle and its outputs, including planning, design, hardware safety assessment and supporting processes. These processes are typically performed concurrently with the planning and design processes. These processes are validation, verification, configuration management, process assurance and certification liaison.

3.2 TRANSITION CRITERIA

The challenges of developing a hardware item with different subitems at different stages of development require a means to provide a reasonable amount of control of the design process in order to manage the risk of starting the next process before all elements of the previous process are complete. Transition criteria, defined as the minimum data used to assess movement from one process to another, may be used at key process points. Analysis during the planning process should determine the use of transition criteria. It is not necessary to establish transition criteria between each pair of process steps defined in the plans. The selection of transition criteria should address the impact on safety. For example, before performing verification of a function for certification credit, the requirements for that function need to be documented and the implementation of that function needs to be under configuration management.

Transition criteria should be documented in the hardware plans. Use of transition criteria does not imply any particular life cycle model or prevent such development strategies as rapid prototyping and concurrent engineering.

CHAPTER 4

PLANNING PROCESS

This section describes the hardware planning process used to control the development of the hardware item. This process produces the hardware plans, which may be contained in one or more documents. If multiple documents are used, the main plan should contain appropriate references to the supporting documents. Standard documents covering specific hardware design life cycle processes, such as configuration management or process assurance, are acceptable provided they meet the planning objectives for the applicable process.

4.1 PLANNING PROCESS OBJECTIVES

The purpose of the hardware planning process is to define the means by which the functional and airworthiness requirements are converted into a hardware item with an acceptable amount of evidence of assurance that the item will safely perform its intended functions. The objectives of the hardware planning process are:

1. The hardware design life cycle processes are defined.

   NOTE: Activities, milestones, inputs, outputs and organizational responsibilities may be included in the plans.

2. Standards are selected and defined.

3. The hardware development and verification environments are selected or defined.

4. The means of compliance of the hardware design assurance objectives, including strategies identified using guidance in Section 2.3.4, are proposed to the certification authority.

   NOTE: New and evolving technologies, tools and processes may require details of the planning process to change. Therefore, flexibility is a key element of the planning process.

4.2 PLANNING PROCESS ACTIVITIES

Guidance for the planning process includes:

1. The hardware design life cycle process, including transition criteria, if applicable, and the inter-relationships between the individual processes, such as their sequencing and feedback mechanisms, should be defined.

2. The proposed design methods should be defined and explained. This includes consideration of the expected hardware design and the rationale of the proposed verification methods.

3. Hardware design standards, if any are to be used for the project, including acceptable deviations from the standards, should be identified. These may range from generic quality standards to company or program specific standards.

   NOTE: Standards help reduce the probability of undetected design errors by providing a compilation of proven engineering practices determined from past developments.

   The applicant and hardware developer should be aware when applying standards to new designs and new technologies, that the applicability may be invalid. Deviations from these standards may be necessary due to design constraints, conflicts with system requirements or incompatibility with new technologies. The planning process is an opportunity to review what deviations may be acceptable if standards are used.

4. The means of achieving coordination between the hardware design processes and the supporting processes, with particular attention to activities associated with systems, software and aircraft certification, should be determined.

   NOTE: Coordination may be in the form of a schedule showing milestones for events to accomplish the objectives of the processes described in this document.

5. The activities of each hardware design process and associated supporting processes should be defined. The definition should be at a level that enables the hardware design process and associated supporting processes to be controlled.

6. The design environment should be chosen, including the tools, procedures, software and hardware that are to be used to develop, verify and control the hardware item and the life cycle data.

   a. If certification credit is sought for use of tools in combination, the sequence of operation of the tools should be specified in the respective plan.

   b. The design environment can affect the design of a product. Section 11.4 provides guidance for the assessment of tools and determining when tool qualification may be necessary.

7. The process for deviating from the established plans, if deviations become necessary and affect certification, should be identified.

8. The policies, procedures, standards and methods to be used to identify, manage, and control the hardware, the associated baselines, and the hardware design life cycle data should be described.

9. Where the applicant intends to use subcontractors for all or part of the hardware design life cycle, the hardware plans should identify the method for ensuring that the design assurance objectives are met.

10. The policies and procedures for implementation of process assurance of the hardware design processes should be described.

11. Verification process independence, process assurance independence and associated organizational responsibilities should be described in the PHAC.

12. The means to satisfy the objectives of this guidance should be recorded and communicated to the certification authority early in the process. These means should be recorded in the PHAC.

    NOTE: Timely coordination of any changes to these means is encouraged to maximize acceptance of the resultant certification data as proper evidence of meeting the design assurance requirements.

CHAPTER 5

HARDWARE DESIGN PROCESSES

The hardware design processes produce a hardware item that fulfills the requirements allocated to hardware from the system requirements. This section describes five major processes as depicted in Figure 5-1. These are Requirements Capture, Conceptual Design, Detailed Design, Implementation and Production Transition. These design processes may be applied at any hierarchical level of the hardware item, such as LRUs, circuit board assemblies and ASICs/PLDs. The following sections describe each process, its objectives and the related activities that should be addressed to reduce the probability of design and implementation errors that affect safety. It is important that each of these processes is planned and the details recorded in a hardware design plan.

Each process, and interactions between the processes, can be iterative. For each iteration, the effect of the change on each of the processes should be addressed and evaluated for impact on the results of previous iterations.

NOTE 1: It is good engineering practice to document process artifacts, such as design notes, design review notes and problem reports, throughout the design process.

Current practices provide many different means, graphical, mathematical, database or text based, to represent requirements and design implementations. Examples of these representations are schematics, hardware description languages (HDL), state diagrams, Boolean representations and graphical methods.

NOTE 2: Some representations are adapted to a specific process or combination of processes, such as requirements capture, conceptual design or detailed design, and some are adapted to more efficiently implement a specific implementation technology. Evidence to support the design assurance level should be provided, regardless of the design representation used.

For each design representation used, the following should be considered:

1. The guidance of this document should be followed regardless of the representation, or combination of representations, used.
2. The design representation should allow the hardware item to be consistently replicated.
3. Small changes in design representation may have a large impact on the design implementation. The impact of these changes on design assurance should be addressed.
4. The design representation environment or method may change after the baseline of the design data has been established. If this occurs, the impact of the change on the replication of the design should be assessed.

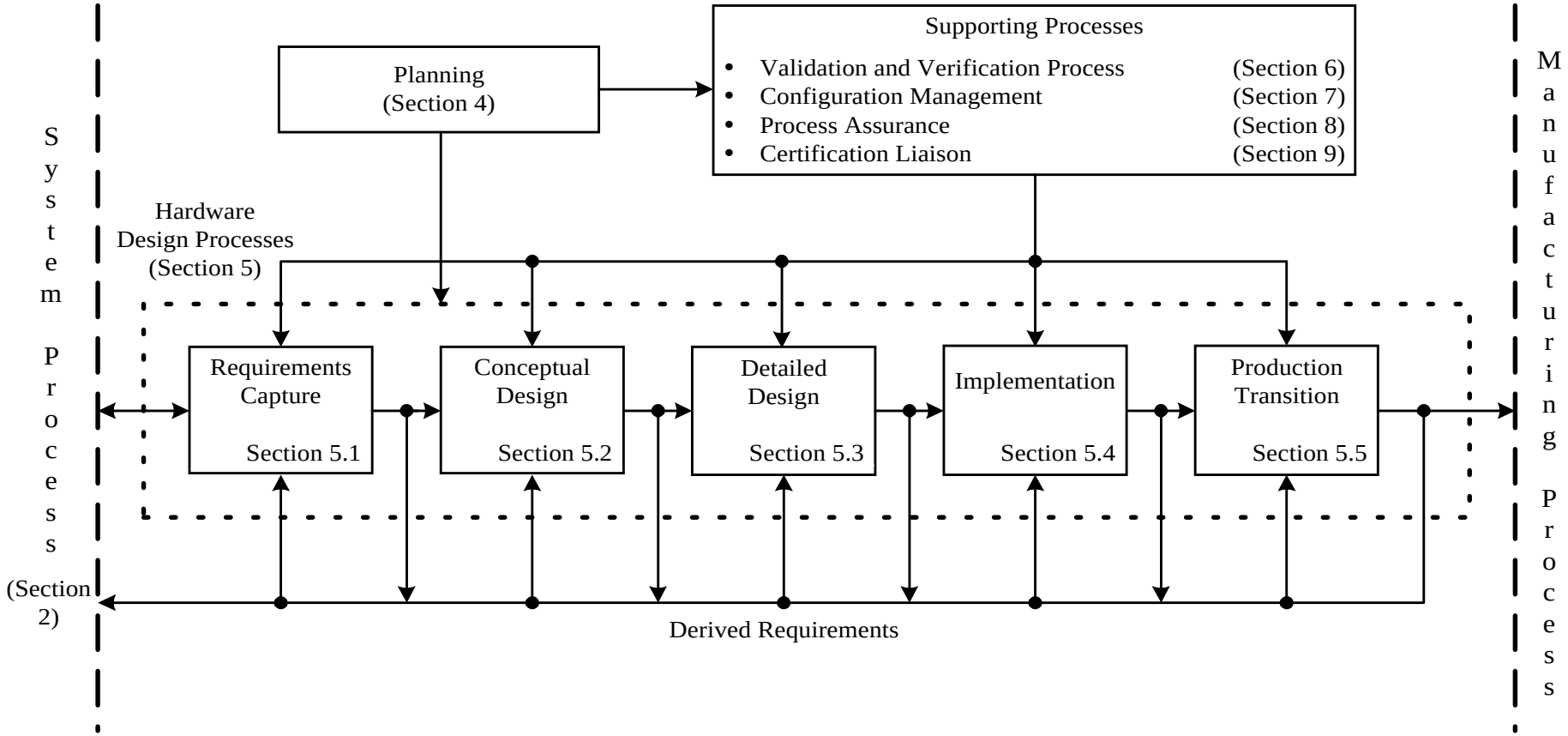


FIGURE 5-1: HARDWARE DESIGN LIFE CYCLE

HDL design representations use coded text based techniques that are similar in appearance to those used for software representations. This similarity in appearance can mislead one to attempt to use software verification methods directly on the design representation of HDL or other equivalent hardware specification languages. The guidance of this document is applicable for design assurance for designs using an HDL representation.

NOTE: The structured processes described throughout this document are applicable to complex hardware designs including ASICs and PLDs. As an example, the following table maps typical ASIC/PLD processes to the processes depicted in Figure 5-1 of this document.

Typical ASIC/PLD Process	Process
Part of higher level planning	Planning (Section 4)
ASIC/PLD Architectural Decisions	Safety Assessment (Section 2.3)
ASIC/PLD Requirements Capture	Requirements Capture (Section 5.1)
ASIC/PLD Preliminary Design including behavioral design	Conceptual Design (Section 5.2)
ASIC/PLD Detailed Design including synthesis, mask generation and fuse file generation	Detailed Design (Section 5.3)
ASIC/PLD Fabrication including external fabrication and test as well as programming programmable components	Implementation (Section 5.4)
ASIC/PLD Production Transition	Production Transition (Section 5.5)
ASIC/PLD Validation and Verification including timing analysis, behavioral simulation, gate level simulation and design reviews	Validation and Verification Process (Section 6)
ASIC/PLD Configuration Management including tools and part database	Configuration Management Process (Section 7)

TABLE 5-1: TYPICAL ASIC/PLD PROCESS MAPPING

5.1 REQUIREMENTS CAPTURE PROCESS

The requirements capture process identifies and records the hardware item requirements. This includes those derived requirements imposed by the proposed hardware item architecture, choice of technology, the basic and optional functionality, environmental, and performance requirements as well as the requirements imposed by the system safety assessment. This process may be iterative since additional requirements may become known during design.

5.1.1 Requirements Capture Objectives

The objectives for the requirements capture process are:

1. Requirements are identified, defined and documented. This includes allocated requirements from the PSSA and derived requirements from the hardware safety assessment.

NOTE: Traceability of verification results to the hardware requirements is addressed in Section 6. It is desirable to establish this method of traceability during the requirement capture process.

2. Derived requirements produced are fed back to the appropriate process.
3. Requirement omissions and errors are provided to the appropriate process for resolution.

5.1.2 Requirements Capture Activities

The requirements capture activities form an iterative process which helps assure consistency of the requirements with the design implementation, the system requirements and the software requirements.

Guidance for the requirements capture activities includes:

1. The system requirements allocated to the hardware item should be documented. These may include identifying requirements, such as functionality and performance, and architectural considerations, such as segregation, Built-In-Test, testability, external interfaces, environment, test and maintenance considerations, power, and physical characteristics.
2. The safety requirements from the PSSA related to the hardware item should be identified. These may include:
   a. Design assurance levels imposed on the functions to be implemented in the hardware.
   b. Probabilistic requirements for malfunctions or loss of function.
   c. Hardware architectural and functional safety attributes, such as those outlined in Section 2.3.1, selected to meet the functional allocation.
3. Design constraints due to production processes, standards, procedures, technology, design environment and design guidance should be identified.
4. Derived requirements necessary for implementation should be determined. Requirements derived from the hardware safety assessment that have safety implications should be uniquely identified.

   NOTE: Derived requirements may address conditions, such as:

   a. Specific constraints to ensure that functions of a higher design assurance level can withstand anomalies of functions of a lower design assurance level as seen at the interface of the function with the lower design assurance level.
   b. The range of data inputs considering typical and full-scale data values as well as the high and low states of bits in data words or control registers.
   c. Power-up reset or other reset states.
   d. Supply voltage and current demands.
   e. Performance of time-related functions, such as filters, integrators and delays.
   f. State machine transitions that are possible, whether they are anticipated or not.
   g. Signal timing relationships or electrical conditions under normal and worst-case conditions.
   h. Signal noise and cross-talk.
   i. Signal glitches in asynchronous logic circuits.
   j. Specific constraints to control unused functions.

5. Derived requirements should be fed back to the SSA process so that the effects on the system requirements can be assessed.

6. The requirement data should be documented in quantitative terms, with tolerances where applicable. This does not include the description of design or verification solutions.

7. Requirement omissions or errors discovered during this process should be provided to the system development process.

8. The requirements, including those generated to meet the PSSA requirements, should be traceable to the next higher hierarchical level of requirements. Derived requirements should be identified and traced as far as possible through the hierarchical levels.

   NOTE: System level validation of allocated hardware safety requirements may occur during the requirement capture process. Validation of derived hardware requirements is described in Section 6.1.

5.2 CONCEPTUAL DESIGN PROCESS

The conceptual design process produces a high-level design concept that may be assessed to determine the potential for the resulting design implementation to meet the requirements. This may be accomplished using such items as functional block diagrams, design and architecture descriptions, circuit card assembly outlines, and chassis sketches.

5.2.1 Conceptual Design Objectives

The conceptual design objectives are:

1. The hardware item conceptual design is developed consistent with its requirements.

2. Derived requirements produced are fed back to the requirements capture or other appropriate processes.

3. Requirement omissions and errors are provided to the appropriate processes for resolution.

5.2.2 Conceptual Design Activities

Guidance for the conceptual design activities includes:

1. A high-level description should be generated for the hardware item. This may include:

   a. Architectural constraints related to safety, including those necessary to address design errors and functional, component over-stress, reliability and robustness defects.

   b. Identification of any implementation constraints on software or other system components.

2. Major components should be identified. The way they contribute to the hardware safety requirements should be determined, including the impact of unused functions.

3. Derived requirements, including the interface definition, should be fed back to the requirements capture process.

4. Requirement omissions and errors should be fed back to the appropriate process for resolution.

5. The reliability, maintenance and test features to be provided should be identified.

NOTE: Consensus between the relevant parties that the conceptual design objectives have been met is recommended. Typically, a design review is used to accomplish this consensus.

5.3 DETAILED DESIGN PROCESS

The detailed design process produces detailed design data using the hardware item requirements and conceptual design data as the basis for the detailed design.

5.3.1 Detailed Design Objectives

The detailed design process objectives are:

1. The detailed design is developed from the hardware item requirements and conceptual design data.
2. Derived requirements are fed back to the conceptual design process or other appropriate processes.
3. Requirement omissions or errors are provided to the appropriate processes for resolution.

5.3.2 Detailed Design Process Activities

Guidance for the detailed design activities includes:

1. The detailed design data for the hardware item should be generated based on the requirements and conceptual design data. This may include assembly and interconnection data, component data, HDL, test methods and hardware-software interface data.

   NOTE: During the detailed design process, verification methods are used informally to facilitate the technical decisions made during this process. For example, analysis of design parameters, such as logic timing and parameter variations, can provide information on which to base design decisions.

2. Architectural design techniques should be implemented as necessary. These may include establishing safety monitors for proper functionality, dissimilarity between function and safety monitors, preclusion of a design error from impacting safety, and fault tolerant designs.
3. Test features should be designed in, where necessary, to allow verification of safety requirements.

   NOTE: It is important to develop the design in a way that certain safety features can be verified not only during the hardware design life cycle, but also as a part of an acceptance test and a field return to service test.

4. An assessment of unused functions should be performed to identify potential effects on safety. Adverse effects should be addressed.
5. Constraints on the design, installation or operation of the hardware item that, if not adhered to, could affect the safety of the item should be identified.
6. Derived requirements produced during the detailed design process should be fed back to the conceptual design or other appropriate processes.
7. Requirement omissions and errors discovered during the detailed design process should be provided to the appropriate process for resolution.

5.4 IMPLEMENTATION PROCESS

The implementation process uses the detailed design data to produce the hardware item that is an input to the testing activity.

5.4.1 Implementation Objectives

The objectives of the implementation process are:

1. A hardware item is produced which implements the hardware detailed design using representative manufacturing processes.
2. The hardware item implementation, assembly and installation data is complete.
3. Derived requirements are fed back to the detailed design process or other appropriate processes.
4. Requirement omissions and errors are provided to the appropriate processes for resolution.

5.4.2 Implementation Activities

Guidance for the implementation activities includes:

1. A hardware item should be produced using the design data and, where practical, the resources intended for the production product. This may include procurement, kitting, build, inspection and test.
2. Derived requirements generated by the implementation process should be fed back to the detailed design process or other appropriate processes.
3. Omissions and errors discovered during the implementation process should be provided to the appropriate process for resolution.

5.5 PRODUCTION TRANSITION PROCESS

In this process, manufacturing data, test facilities and general resources should be examined to ensure availability and suitability for production. The production transition process uses the outputs from the implementation and verification processes to move the product into production.

5.5.1 Production Transition Objectives

The objectives of this process are:

1. A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item.
2. Manufacturing requirements related to safety are identified and documented and manufacturing controls are established.
3. Derived requirements are fed back to the implementation process or other appropriate processes.
4. Errors and omissions are provided to the appropriate processes for resolution.

5.5.2 Production Transition Activities

Guidance for the production transition activities includes:

1. Manufacturing data should be prepared from configured design data.

2. Manufacturing data should be checked for completeness and consistency with the configured design data.

   NOTE: It is beyond the scope of this document to impose any conditions on the nature of the manufacturing build documentation.

3. Any changes or improvements that are incorporated during the production transition process should be evaluated to ensure they adhere to all product requirements, especially safety requirements. Any changes not compliant with customer or certification requirements should be approved by the relevant parties.

4. Manufacturing requirements pertaining to safety should be explicitly defined so they can be controlled during the production process.

5. Data required to develop acceptance test criteria should be determined.

6. Omissions or errors that are identified should be provided to the appropriate process for resolution.

5.6 ACCEPTANCE TEST

An acceptance test demonstrates that the manufactured, modified or repaired product performs in compliance with the key attributes of the unit on which certification is based. These key attributes are chosen using engineering judgement and are indicative that the product is capable of meeting the requirements to which the unit was developed.

NOTE 1: Configuration control of the "as built" product is not a function to be performed by the acceptance test activity. The configuration management plan, as described in Section 7 of this document, should describe how the applicant plans to perform this activity.

The scope of this document does include the determination of the acceptance test criteria, including pass/fail conditions. Production activities, including acceptance testing, are considered to be outside the scope of this document

NOTE 2: An acceptance test is not intended to verify all requirements on each production unit.

Subitem testing may be used as a part of the acceptance test.

Acceptance test criteria should ensure that:

1. Electrical tests are identified.

2. Environmental screening tests are identified when necessary.

3. The acceptance test provides coverage of those design aspects necessary to meet the safety requirements. Safety related item or subitems that are not covered by the test should be identified and other assurance means provided. These means may include analysis, design control, statistical process control or other means as appropriate.

5.7 SERIES PRODUCTION

This process is not within the scope of this document, but elements impacting design assurance are briefly described to complete the life cycle.

This process reproduces the hardware item on a routine basis that complies with the production data and requirements.

Considerations include:

1. Management of change of the production processes or the design provides assurance that change does not adversely impact existing safety or certification or compliance to the requirements.

   NOTE: In addition to the guidance proposed by the body of the document, Section 11.1.1 covers Modifications to Previously Developed Hardware. When addressing component obsolescence, refer to Section 11.2.

2. Updating of all documentation related to changes is performed in compliance with approved configuration management plans.

CHAPTER 6

VALIDATION AND VERIFICATION PROCESS

This section describes the validation process and the verification process. The validation process provides assurance that the hardware item derived requirements are correct and complete with respect to system requirements allocated to the hardware item. The verification process provides assurance that the hardware item implementation meets all of the hardware requirements, including derived requirements.

6.1 VALIDATION PROCESS

The validation process discussed here is intended to ensure that the derived requirements are correct and complete with respect to the system requirements allocated to the hardware item through the use of a combination of objective and subjective processes. Validation may be conducted before or after the hardware item is available, however, validation is typically conducted throughout the design life cycle.

NOTE 1: Experience indicates that attention to the development and validation of requirements can identify subtle errors or omissions early in the development cycle and reduce exposure to subsequent redesign or inadequate hardware performance.

The validation process discussed here is not intended to validate the requirements allocated from system requirements since validation of these requirements is assumed to occur as part of the system process. In addition, not all hardware item derived requirements need to be validated.

Design decisions that affect the system safety or functional requirements allocated to other portions of the system should be classified as derived requirements and should be validated. Additionally, design decisions and assumptions that constrain subsequent design tasks should be validated as derived requirements.

Derived requirements that need to be validated should be validated against the system requirements allocated to the hardware item. Derived requirements that are not traceable to a higher level requirement should be validated against the design decision from which they are derived.

NOTE 2: A design decision to include a separate power supply for circuitry performing a specific function could result in the derivation of requirements to guide the design of that power supply. These derived requirements could include safety requirements based on the failure condition that could result from the fault or failure of the function supported by the circuit that receives power from the power supply. These requirements should be validated.

Another example of a design decision that becomes a derived requirement is the memory address assignments for peripheral devices. There is often no requirements basis for the assignments, however, once made they constrain subsequent design tasks to comply with those assignments in order for the design to function correctly. This derived requirement may not need to be validated.

6.1.1 Validation Process Objectives

The objectives of the validation process for derived hardware requirements are:

1. Derived hardware requirements against which the hardware item is to be verified are correct and complete.

2. Derived requirements are evaluated for impact on safety.

3. Omissions and errors are fed back to the appropriate processes for resolution.

6.1.2 Validation Process Activities

The hardware validation objective may be satisfied through a combination of activities, such as reviews, simulation, prototyping, modeling, analysis, service experience, engineering assessment, or the development and execution of tests.

Guidance for validation process activities includes:

1. The derived hardware requirements that need to be validated should be identified.

2. For each requirement that was identified in item 1, the validation completion criteria should be identified and satisfied as shown below:

   a. Each requirement has been validated at some hierarchical level by review, analysis or test.

   b. The review, analysis or test of each requirement is appropriate for validating the requirement, especially with respect to safety.

   c. The review, analysis or test results associated with the validation of each requirement are correct and that discrepancies between actual and expected results are explained. When expected results are not pre-defined as may be the case for reviews and analyses, the results of the validation activity should be consistent with the requirement, especially with respect to safety requirements.

   NOTE: Validation completion criteria may be based on requirements, safety considerations, operational mode or implementation.

3. The derived requirements should be evaluated for their impact on safety.

4. The derived hardware requirements should be evaluated for completeness with respect to the system requirements allocated to the hardware item. For the purposes of this process, a set of requirements is complete when all the attributes that have been defined are necessary and all the necessary attributes have been defined.

5. The derived hardware requirements should be evaluated for correctness with respect to the system requirements allocated to the hardware item. For the purposes of this document, a requirement is correct when the requirement is defined without ambiguity and there are no errors in the defined attributes.

6. Traceability between the derived hardware requirements and the validation activities and results should be established.

7. Requirement omissions and errors should be fed back to the appropriate process for resolution.

6.2 VERIFICATION PROCESS

The verification process provides assurance that the hardware item implementation meets the requirements. Verification consists of reviews, analyses and tests applied as defined in the verification plan. The verification process should include an assessment of the results.

NOTE 1: Safety aspects of hardware design take the form of safety requirements to be met by the hardware implementation.

This section provides guidance for the verification process that should be applied to the hardware design. The verification process may be applied at any level of the design hierarchy as defined in the hardware verification plan. For safety requirements, it is advantageous to apply the verification process at various stages of the design process to increase the probability, to a high degree of confidence, that design errors have been eliminated. Some design assurance levels require that the objectives of the verification process be met with independence as addressed in Appendix A.

The software verification, software/hardware integration verification and systems integration verification processes are not addressed here. However, verification of hardware requirements during these processes is a valid method of hardware verification.

Changes to a verified configuration may be re-verified by similarity, analysis, newly designed tests or by repeating a portion of the original verification.

NOTE 2: Informal testing outside the documented verification process is recommended. The procedures and results, however, are not necessarily maintained under configuration management control but are highly effective in the detection and elimination of design errors early in the design process. Verification credit can be taken for this testing only if it is formalized.

6.2.1 Verification Process Objectives

The objectives of the verification process are:

1. Evidence is provided that the hardware implementation meets the requirements.
2. Traceability is established between hardware requirements, the implementation, and the verification procedures and results.
3. Acceptance test criteria are identified, can be implemented and are consistent with the hardware design assurance levels of the hardware functions.
4. Omissions and errors are fed back to the appropriate processes for resolution.

6.2.2 Verification Process Activities

Verification process objectives may be satisfied through a combination of methods, such as reviews, analyses, and the development and execution of tests. The verification plan documents the verification activities that should be employed to demonstrate compliance to the requirements.

Verification activities include:

1. Requirements that need a verification activity should be identified. It is not intended that requirements should be verified at every hierarchical level; requirements can be verified at a higher hierarchical level.
2. Verification methods, such as tests, simulation, prototyping, analyses and reviews, should be selected and performed.
3. Traceability between requirements, implementation, and the verification procedure and results should be established. Traceability should be consistent with the design assurance level of the function performed by the hardware. It is not intended to require traceability to detailed components, such as resistors, capacitors or gates, unless required for safety considerations.
4. Verification coverage analysis should be performed to determine that the verification process is complete, including:
    a. Each requirement has been verified at some hierarchical level by review, analysis or test.
    b. The review, analysis or test of each requirement is appropriate for verifying the requirement, especially with respect to safety requirements.

c. The review, analysis or test results associated with the verification of each requirement are correct and that discrepancies between actual and expected results are explained. When expected results are not pre-defined as may be the case for reviews and analyses, the results of the verification activity should be consistent with the requirement, especially with respect to safety requirements.

5. The results of the verification activities should be documented.

6. Omissions and errors should be fed back to the appropriate process for resolution.

6.3 VALIDATION AND VERIFICATION METHODS

This section describes some methods that may be applicable to both validation and verification.

6.3.1 Test

Test is a method that confirms that the hardware item correctly responds to a stimulus or series of stimuli. Examples of tests include functional test on the hardware item, system bench test, system validation facility test and aircraft test.

Tests may be conducted using manual, automated or specialized test equipment. Tests may also take advantage of internal hardware item test capabilities, such as Built-In-Test, in the verification process.

When it is not feasible to verify specific requirements by exercising the hardware item in its intended operational environment, other verification means should be provided, and justified.

Tests may be performed during various hardware design processes. Testing performed for certification credit requires a configured item. Systems integration or software/hardware integration test results may also be used for test credit.

Guidance for tests includes:

1. Each requirement to be validated or verified by test should be identified. Environmental qualification test requirements are part of these requirements.

2. The testing stimulus, sequence and test conditions, such as item ambient temperature and applied voltage, should be defined for each test.

3. Pass/fail criteria and a method for recording the results should be defined prior to test execution.

4. The complete identification of the test equipment and calibration date for each should be recorded.

5. The configuration identity of the hardware item being tested should be recorded.

6. Test results should be recorded and retained.

7. Test failures should be fed back to the appropriate process for resolution.

6.3.2 Analysis

Analysis is a detailed, repeatable, analytical method for evaluation of specific hardware item characteristics to demonstrate that a specific requirement is met. Examples of analyses are stress analysis, design margin analysis, common mode failure analysis, worst case analysis and test coverage analysis. Service experience may provide data for various analyses.

NOTE: As the complexity of the hardware design increases, it is advantageous to make use of computerized tools, such as simulation to verify requirements and implementation of the design.

Analyses may include a detailed examination of the functionality, performance, traceability and safety implications of a hardware item function and its relationship to other functions within the airborne system or equipment. Analysis alone or in combination with other verification methods provides evidence that a requirement is correctly implemented. Analysis should be based on data provided by the design process, service experience or other available databases.

Simulation is an important design analysis tool both for visualization of circuit operation and for higher level functional operation. Simulation can be used to analyze the impact of production variations in hardware parameters that would be difficult to do using other verification means and thus build confidence in reduction of design errors affecting safety due to these variations. Since the results depend on the models and scenarios employed, simulation results alone cannot be used for the purpose of certification credit without supporting evidence of their validity.

Examples of analysis include:

1. **Thermal Analysis.** Thermal analysis verifies that the design implementation meets the requirements when exposed to the operating thermal environment.
2. **Stress Analysis.** Stress analysis verifies that components meet de-rating criteria over the required operating range.
3. **Reliability Analysis.** Reliability analysis establishes whether the design implementation satisfies the reliability requirements of the product.
4. **Design Margin Analysis.** Design margin analysis verifies that the design implementation satisfies its functional requirements given the variability of components.
5. **Similarity Analysis.** Similarity analysis compares characteristics and usage to those of systems previously certified.
6. **Simulation Analysis.** A simulation analysis compares the simulation results and expected results.

6.3.3 Reviews

A review is a qualitative method for evaluation of the plans, requirements, design data, design concept or design implementation.

Reviews should be held throughout the hardware design life cycle as identified in the relevant plan. All reviews to be used for certification credit should be identified in the validation and verification plan.

Guidance for reviews may include:

1. Participants should have the knowledge necessary to perform the reviews.
2. Hardware review results may be used to permit or deny transitions between hardware design life cycle process activities.
3. Results of review should be documented, including decisions made and disposition of actions to be taken.

6.3.3.1 Requirements Review

The requirements review is a method to ensure the acceptability of requirements. A requirements review may address objectives from both the validation and the verification processes within the same review.

Requirement changes that occur after the initial requirements review should be subject to the same review process used initially or an equivalent review process. It is not the intent of this review to validate the system requirements allocated to the hardware item.

Guidance for requirements review includes:

1. Each requirement should be unambiguous, verifiable, and described in complete enough detail for its hierarchical level and should not conflict with other requirements.
2. Derived requirements should be consistent with the system requirements or requirements from which they are derived.
3. The requirements should be consistent with the SSA.
4. The derived safety requirements should be defined and fed back to the SSA.
5. The requirements should be compatible with relevant hardware design standards.
6. The requirements should be compatible with the capabilities and limitations of available technology.
7. The component's requirements, such as performance, temperature range, de-rating and screening, should be consistent with the safety and reliability requirements.
8. The ability to test, maintain and manufacture the hardware item should be addressed.
9. The software/hardware interface requirements should be defined.
10 The requirements should be traceable upward to the next hierarchical level according to the criteria defined in the plan.
11 The derived requirements should capture the implementation constraints that will not be verified at a higher hierarchical level.
12 Omissions and errors should be fed back to the appropriate process for resolution.

NOTE 1: The following questions may help assess completeness of requirements:

a. Are all upper level requirements considered?
b. Are applicable standards and guidance considered?
c. Are all hardware functions and interfaces covered?
d. Is the architecture covered completely?
e. Is all of the hardware implementation requiring verification adequately specified?
f. Are all prohibited behavior characteristics in the safety assessment covered?
g. Is the operating environment adequately specified?
h. Are assumptions and constraints considered?
i. Will this implementation avoid any known problems with existing or similar hardware?

NOTE 2: The following questions may help assess correctness of requirements:

a. Are the requirements in accordance with upper level requirements?
b. Are the requirements in accordance with the system requirements allocated to the hardware item?
c. Are the requirements stating "what" as opposed to "how"?
d. Are the requirements unambiguous?
e. Can the requirements be realized?
f. Can the requirements be verified?
g. Have the functioning modes been defined?

h. Are the requirements consistent with the safety assessment?

i. Are assumptions and constraints correctly identified as derived requirements?

6.3.3.2 Design Review

A design review is a method to determine that the design data and implementation satisfy the requirements. Design reviews should be performed as defined in the plan at multiple times during the hardware design life cycle. Examples are conceptual design, detail design and implementation reviews. For hierarchical designs that span several hardware item levels, such as ASICs and circuit card assemblies, design reviews should be considered where the potential is greatest for assuring a correct design.

Guidance for design reviews includes:

1. All requirements should be addressed and the derived requirements and the design data should be correctly defined.
2. Environmental requirements should be addressed.
3. Safety and reliability requirements should be addressed.
4. The safety aspects of the design data should be explicitly identified.
5. The design should be capable of being implemented, tested and maintained.
6. New manufacturing techniques should be evaluated.
7. The components selection criteria identified in the plans should be satisfied.
8. The design should be traceable to the requirements.
9. Omissions and errors should be fed back to the appropriate process for resolution.

CHAPTER 7

CONFIGURATION MANAGEMENT PROCESS

The configuration management process is intended to provide the ability to consistently replicate the configuration item, regenerate the information if necessary and modify the configuration item in a controlled fashion if modification is necessary. This section describes the objectives for hardware configuration management and activities that support those objectives.

7.1 CONFIGURATION MANAGEMENT OBJECTIVES

The objectives of the configuration management process are:

1. Configuration items are uniquely identified and documented.
2. Consistent and accurate replication of configuration items is ensured.
3. A controlled method of identifying and tracking modification to configuration items is provided.

7.2 CONFIGURATION MANAGEMENT ACTIVITIES

Guidance for the configuration management activities includes:

1. Configuration items should be uniquely identified, documented and controlled. This may include, but is not limited to, hardware, design representations of hardware, tools or other data items used for certification credit and baselines.
2. Baselines should be established.
3. Problems should be uniquely identified, tracked and reported.
4. Change control and traceability of changes should be maintained. This requires that life cycle data identified in the plans should be secure and retrievable.
5. Archiving, retrieval and release of configuration items should be controlled.

Various methods may be used to satisfy configuration management objectives and activities and the following paragraphs provide guidance on activities that may be used as an acceptable method.

7.2.1 Configuration Identification

The purpose of the configuration identification activity is to label unambiguously each configuration item so that a basis is established for the control and reference of configuration items.

Guidance includes:

1. Configuration identification should be established for data items.
2. Configuration identification should be established for each configuration item, for each separately controlled component of a configuration item and for combinations of configuration items that make up a product consistent with the plans agreed to by the certification authority.

   NOTE: The detail to which components, such as ASICs, configured PLDs, printed circuit boards and black boxes, are identified is determined by the Configuration Management Plan.

3. Configuration identification should be established for COTS components and previously developed hardware items before they are used in a baseline.

4. Configuration identification should be established for each configuration item before it is used in a new baseline, referenced by other data items or used for product manufacturing.

7.2.2 Baseline Establishment

The purpose of baseline establishment is to define a basis for further activities and allow reference to, control of and traceability between configuration items.

Guidance includes:

1. Baselines should be established for configuration items used for certification credit.

   NOTE: Intermediate baselines may be established to aid in controlling hardware activities.

2. Once a baseline is established it should be subject to change control procedures.

3. Change control guidance should be followed when developing a derivative baseline from an established baseline.

4. If in developing a new baseline, certification credit is sought for activities or data associated with design of a previous baseline, this new baseline should be traceable to the previous baseline from which it was derived.

   NOTE: The baseline may be a configuration item, a previously certified hardware item or a COTS component.

7.2.3 Problem Reporting, Tracking and Corrective Action

The purpose of problem reporting, tracking and corrective action is to record problems and ensure correct disposition and resolution. Problems may include non-compliance with plans and standards, deficiencies of life cycle process outputs, anomalous behavior of products, and inadequacy or deficiency of tools and technology processes. Problem reporting should be implemented no later than the establishment of the baseline from which certification credit is to be obtained.

Guidance includes:

1. Each reported problem should be covered by a problem report.

2. Problem reporting should identify the configuration of the affected configuration items.

3. Problem reports that require corrective action should invoke the change control activity.

4. All closed problem reports should include a description of action taken to close the problem report including the completion of data item changes that were needed to implement a corrective action.

5. Not all problem reports have to be closed in order to obtain certification, however, all problem reports should be evaluated and those that are determined to have safety or certification impact should be closed.

6. The problem reporting system should track the status of problem reports, including their approval and disposition.

7.2.4 Change Control

The purpose of the change control activity is to ensure the recording, evaluation, resolution and approval of changes. Change control should be implemented in compliance with the configuration management plan and should be started no later than the establishment of the baseline from which certification credit is to be obtained.

Guidance includes:

1. Change control should preserve the integrity of the configuration items by providing protection against unauthorized change.
2. Change control should ensure that a change is assessed to determine whether or not the configuration identity needs to be updated.
3. Changes to configuration items under change control should be recorded, approved, and tracked. Approval authority is defined in the configuration management plan.

   NOTE 1: Problem reporting is related to change control, since resolution of a reported problem may result in changes to configuration items.

   NOTE 2: It is generally recognized that early implementation of change control assists the control and management of process activities.

4. Change control should ensure traceability of changes to the reason for the change.
5. Change control should ensure that the impact of the change is assessed to determine the effect of the change on the outputs of the processes and that the output data is updated.

   NOTE 1: Some or all of the activities of the processes may need to be repeated from the point at which their outputs are affected.

   NOTE 2: It should be recognized that a change to the manufacturing tools, technology processes or external components may impact the design.

6. Change control should ensure that feedback is provided to affected processes.

7.2.5 Release, Archive and Retrieve

The purpose of the release activity is to place data items under configuration management control to ensure that only authorized data is used in other activities. The purpose of the archive and retrieve activity is to ensure that data items associated with the product can be retrieved in case of a need to duplicate, regenerate, re-test or modify the product.

Guidance includes:

1. Configuration items should be identified and released prior to use for manufacture and the authority for their release should be established.
2. Data items associated with the product should be retrievable from an approved source, such as the developing organization or company.

   NOTE: Change control data and problem report data are part of the data items.

3. Data retention procedures should be available to satisfy airworthiness requirements and enable modifications.
4. Procedures should be established to ensure the integrity of the stored data for as long as required by the certification authorities by:

   a. Ensuring that no unauthorized changes are made.

   b. Selecting storage media.

c. Maintaining availability of stored data. For example, by exercising or refreshing archived data at a frequency compatible with the storage life of the medium.

d. Ensuring that a single event that can cause irretrievable loss of archived data is unlikely. For example, by storing duplicate copies in physically separate archives.

7.3 DATA CONTROL CATEGORIES

Two categories associated with the configuration management of data items are defined: hardware control category 1 (HC1) and hardware control category 2 (HC2). Specifying two categories allows a less stringent configuration control for certain data items. HC1 requires all configuration management activities to be performed while HC2 is less restrictive. Data items classified as HC2 are not expected to change incrementally, but will be superceded by new data.

Table 7-1 defines the configuration management activities that are to be performed under HC1 and HC2. For example, Table 7-1 shows that data items identified in Appendix A, Table A-1 as HC2 need to be retrievable but do not need to be released. Additionally, Table 7-1 shows that any HC1 data item will have a baseline.

Appendix A identifies the control category for each data item as a function of hardware design assurance level. For example, in Table A-1, HC1 applies to hardware requirements for all assurance levels while HC2 applies to hardware review and analysis results for all assurance levels.

Reference	Configuration Management Activity	HC1	HC2
7.2.1	Configuration Identification	x	x
7.2.2 (1),(2),(3)	Baselines	x	
7.2.2 (4) ①	Baseline Traceability	x	x
7.2.3	Problem Reporting	x	
7.2.4 (1),(2)	Change Control - integrity and identification	x	x
7.2.4 (3),(4),(5),(6)	Change Control – records, approvals and traceability	x	
7.2.5 (1)	Release	x	
7.2.5 (2)	Retrieval	x	x
7.2.5 (3)	Data Retention	x	x
7.2.5 (4a)	Protection Against Unauthorized Changes	x	x
7.2.5 (4b),(4c),(4d)	Media Selection, Refreshing, Duplication	x	

TABLE 7-1: CONFIGURATION MANAGEMENT PROCESS ACTIVITIES ASSOCIATED WITH HC1 AND HC2

① Identification of HC2 data for use with the new baseline does not imply reclassification of the data to HC1.

CHAPTER 8

PROCESS ASSURANCE

Process assurance ensures that the life cycle process objectives are met and activities have been completed as outlined in plans or that deviations have been addressed. This section describes the objectives for process assurance and the activities that support those objectives. There is no intent to impose specific organizational structures.

Process assurance activities should be achieved with independence in order to objectively assess the life cycle process, identify deviations and ensure corrective action.

8.1 PROCESS ASSURANCE OBJECTIVES

The objectives of process assurance are to ensure that:

1. Life cycle processes comply with the approved plans.
2. Hardware design life cycle data produced complies with the approved plans.
3. The hardware item used for conformance assessment is built to comply with the associated life cycle data.

8.2 PROCESS ASSURANCE ACTIVITIES

Guidance for the process assurance activities includes:

1. Availability of hardware plans as specified in the planning process section of this document and as agreed to in the PHAC should be ensured.
2. Holding of reviews in compliance with the approved plans and tracking of resulting action items to closure should be ensured.
3. Detection, recording, evaluation, approval, tracking and resolution of deviations from the hardware plans and standards should be ensured.
4. Satisfaction of the transition criteria of the hardware life cycle processes in compliance with the approved plans should be ensured.

   NOTE: Audits are an effective method for performing activities in items 1 through 4 above.

5. An inspection should be performed to ensure that the hardware item is built in compliance with its design data.

   NOTE: An example of this activity is a First Article Inspection.

6. Records of the process assurance activities, including evidence of assessment of completion of design activities, should be produced.
7. Where applicable, the applicant should ensure that the processes used by subcontractors are consistent with the hardware plans.

CHAPTER 9

CERTIFICATION LIAISON PROCESS

The purpose of the certification liaison process is to establish communication and understanding between the applicant and the certification authority throughout the hardware design life cycle to assist in the certification process. The certification liaison process should be accomplished as described by the hardware planning process, Section 4, and the PHAC, Section 10.1.1. Table A-1 of Appendix A gives a summary of the outputs of this process. In addition, liaison activities may include design approach presentation for timely approval, negotiations concerning the means of compliance with the certification basis, approval of design approach, means of data approval, and any required certification authority reviews and witnessing of tests.

At completion of a project, a summary of the design processes followed, outputs produced and status of the hardware item should be described in the Hardware Accomplishment Summary, Section 10.9.

9.1 MEANS OF COMPLIANCE AND PLANNING

The applicant proposes a means of compliance for hardware. The PHAC defines the proposed means of compliance. Guidance includes:

1. The PHAC, hardware verification plan and other requested data should be submitted to the certification authority for review at a point in time when the effects of design changes on the program are minimal.
2. Issues identified by the certification authority concerning the planning for the hardware aspects of certification should be resolved.
3. Agreement on the PHAC should be obtained with the certification authority.
4. Liaison with the certification authority during the design and certification cycle as outlined in the plan should be continued and issues raised by the certification authority resolved in a timely manner.

In some programs, the certification liaison is not provided by the equipment manufacturer, but by the airframe or other customer with the equipment manufacturer in a supporting role. This relationship should be defined in the PHAC and contact with the certification authority should be through the applicant for certification. It is the responsibility of the applicant for certification to ensure that data is provided to the certification authority.

When some hardware items embedded in the equipment are procured from a subcontractor, the certification plan should identify which data are expected from the subcontractor and which are to be generated by the applicant.

It is acceptable for an applicant to include the PHAC and verification plan with other related plans within the top-level certification plan.

9.2 COMPLIANCE SUBSTANTIATION

The applicant provides evidence that the hardware design life cycle processes have satisfied the hardware plans. Certification authority reviews may take place at the applicant's facilities or applicant's supplier's facilities. The applicant arranges these reviews and makes hardware design life cycle data available as needed.

The applicant should:

1. Resolve issues raised by the certification authority as a result of its reviews.
2. Submit the Hardware Accomplishment Summary, Section 10.9 and Top Level Drawing, Section 10.3.2.2.1 to the certification authority.
3. Submit or make available other data or evidence of compliance requested by the certification authority.

CHAPTER 10

HARDWARE DESIGN LIFE CYCLE DATA

This section describes the hardware design life cycle data items that may be produced during the hardware design life cycle for providing evidence of design assurance and compliance with certification requirements. The scope, amount and detail of the life cycle data needed by the certification authorities as design assurance evidence will vary depending on a number of factors. These factors include the applicable certification authority requirements for the airborne system, the assigned design assurance levels, the complexity and the service experience of the hardware. Details of the design assurance evidence should be identified, recorded in the PHAC and agreed to with the certification authorities.

The additional considerations in Section 11 and the design assurance considerations for Level A and B functions in Appendix B may lead to the generation of additional life cycle data.

Appendix A indicates the hardware design life cycle data to be developed, the degree of verification independence, and the applicable data control category, as defined in Section 7, in terms of the hardware design assurance level.

1. The hardware design life cycle data characteristics should be:

   a. **Unambiguous.** Information/data is written in terms that allow only a single interpretation.

   b. **Complete.** Information/data includes necessary and relevant requirements and descriptive material, labeled figures, and defined terms and units of measure.

   c. **Verifiable.** Information/data can be checked for correctness by a person or a tool.

   d. **Consistent.** Information/data contains no conflicts.

   e. **Modifiable.** Information/data is structured and changes can be made completely, consistently and correctly while retaining the structure.

   f. **Traceable.** Information/data origin can be determined.

   The descriptions of this section are not intended to imply a particular data packaging method, form or organization of the hardware life cycle data within a package. For example, all plans, standards, and procedures may be described in a single document or multiple documents.

2. The data packaging method, form and organization should be proposed in the PHAC and agreement with the certification authority obtained early in the program.

3. Agreed-upon information and data should be retrievable and available throughout the service life of the airborne system or equipment.

10.1 HARDWARE PLANS

The hardware plans describe the processes, procedures, methods, and standards to be used for the hardware certification, design, validation, verification, process assurance and configuration control.

10.1.1 Plan for Hardware Aspects of Certification

The PHAC defines the processes, procedures, methods and standards to be used to achieve the objectives of this document and obtain certification authority approval for certification of the system containing hardware items. The PHAC, once approved, represents an agreement between the certification applicant and the certification authority on the processes and activities to be conducted and the resultant evidence to be produced to satisfy the hardware aspects of certification. The PHAC may be part of another plan, such as the airborne system certification plan.

The PHAC should include:

1. **System Overview.** This section provides an overview of the airborne system in which the hardware items are to be used, including a system functional description, system failure conditions, system architecture, a description of the allocation of the functions to hardware items and software, and references to existing system documentation.

2. **Hardware Overview.** This section describes the hardware functions, hardware items, architecture, new technologies to be used, and any fail-safe, fault tolerant, redundancy and partitioning techniques to be used.

3. **Certification Considerations.** This section describes the certification basis, proposed means of compliance and the hardware design assurance level of each function of the hardware item. It also provides the justification for the hardware design assurance level assignment based on a safety assessment of the hardware and its use within the airborne system, including a description of potential hardware failure conditions as discussed in Section 2.3.4. When applicable, either a summary of the FFPA or plan for performing an FFPA and applying the results should also be included.

4. **Hardware Design Life Cycle.** This section describes the procedures, methods and standards to be applied and processes and activities to be performed to meet the hardware design assurance objectives. It describes the activities, combinations and sequencing of activities, relationships between processes and activities, transition criteria, responsibilities, tool usage, and means for providing feedback and interaction among hardware processes and between hardware processes and the system and software processes. This section may reference applicable plans, policies, standards, procedures and deviations to those plans and standards for the program.

5. **Hardware Design Life Cycle Data.** This section describes or references the data to be developed and submitted or available as evidence of compliance to the objectives of this document and the plan.

6. **Additional Considerations.** This section describes the additional considerations. These include use of previously developed hardware, including references to applicable data to be reused, COTS usage, product service experience, and tool assessment and qualification as described in Section 11, or design assurance considerations for Level A or B functions as described in Appendix B.

7. **Alternative Methods**. This section describes any alternative methods proposed for the program which are either not described in this document or are to be applied in a manner other than as described in this document. Justification for why the alternative method is acceptable should be provided.

8. **Certification Schedule.** This section identifies the major program milestones and the dates when hardware design life cycle data will be submitted to the certification authority.

10.1.2 Hardware Design Plan

The hardware design plan describes the procedures, methods and standards to be applied and the processes and activities to be conducted for the design of the hardware item. This plan may be included in the PHAC and may reference design policies and standards to be applied.

The hardware design plan should include:

1. **Hardware Design Life Cycle.** References to design policies and standards to be applied and a description of the hardware design life cycle processes and activities that will be used to achieve the design objectives for the hardware design assurance level.
2. **Hardware Product Description.** Identification of the hardware specifications to be achieved, alternative uses, planned service life and upgrade considerations.
3. **Hardware Design Methods.** Description of the requirements capture and specification methods, conceptual design methods, detailed design methods, synthesis techniques, implementation methods, and production transition methods to be used for the hardware item. When architectural mitigation for Level A or B functions, as described in Appendix B, Section 3.1, has been considered but not finalized at the time this plan is written, state how the decision will be carried into the design process.
4. **Hardware Design Environment.** Description of the design tools to be used.
5. **Hardware Item Data.** Identification of hardware item design data to be produced or references to previously developed hardware item specifications, document and drawing numbers, and part numbers.
6. **Other Considerations.** Description of planned process technology options, use and assembly options, product packaging, and hardware mounting options.

10.1.3 Hardware Validation Plan

The validation plan describes the procedures, methods and standards to be applied and the processes and activities to be conducted for the validation of the hardware item derived requirements to achieve the validation objectives of this document. This plan may be included in the PHAC and may reference validation standards to be applied.

The validation plan should include:

1. **Validation Methods.** Description of and references to the validation procedures, standards and methods to be used. Methods may include analyses, reviews and testing.
2. **Validation Data.** Identification and description of the evidence to be produced as a result of the hardware validation process.
3. **Validation Environment.** Identification and description of analysis and test equipment and validation tools to be used to implement the validation process and activities.

10.1.4 Hardware Verification Plan

The verification plan describes the procedures, methods and standards to be applied and the processes and activities to be conducted for the verification of the hardware items to achieve the verification objectives of this document. This plan may be included in the PHAC and may reference verification policies and standards to be applied.

The verification plan should include:

1. **Verification Methods.** Description of and references to the verification policies, procedures, standards and methods to be used to provide objective evidence of the integrity of the hardware items, including COTS and unused functions. Methods may include analyses, reviews and testing. When the advanced analysis methods of Appendix B, Section 3.3 are employed, include a detailed description of the methods for the applicable FFPs and the applicable verification completion criteria.
2. **Verification Data.** Identification and description of the evidence to be produced as a result of the hardware verification process.
3. **Verification Independence.** Description of the means to be used to assure verification independence for those objectives requiring independence.
4. **Verification Environment.** Identification and description of analysis and test equipment and verification tools to be used to implement the verification process and activities.
5. **Organizational Responsibilities.** Identification of the organizations responsible for implementing the verification process.

10.1.5 Hardware Configuration Management Plan

The hardware configuration management plan describes the policies, procedures, standards and methods to be used to satisfy the configuration management objectives of this document.

The hardware configuration management plan should include:

1. **Hardware Configuration Management Methods.** Description of and reference to the policies, procedures, standards and methods to be used to identify, manage, and control the hardware and its life cycle data.
2. **Hardware Baselines.** Description of the methods and procedures used to establish design and product baselines and provide baseline traceability.
3. **Problem Reporting and Resolution.** Description of the methods and procedures to be used for recording, tracking and resolving problem reports.
4. **Change Control.** Description of the methods, procedures and processes for identifying, controlling, and tracking changes to controlled data items.
5. **Storage and Retrieval.** Description of the procedures for release, archival and retrieval of hardware design life cycle data. The description should include archive content, format, and medium standards, rules, methods and criteria.
6. **Environment Control.** Description of the procedures and method for identifying and controlling the tools used for developing and verifying the hardware.
7. **Configuration Management Tools.** Description of the tools and resources used for the configuration management process and activities.

10.1.6 Hardware Process Assurance Plan

The hardware process assurance plan describes the procedures, methods and standards to be applied and the processes and activities to be conducted for achieving the process assurance objectives of this document.

The hardware process assurance plan should include:

1. **Process Control.** Description of the policies and procedures for implementation of process assurance of the hardware design processes.

2. **Organizational Responsibilities.** Identification of the organizations responsible for implementing process assurance.
3. **Conformance.** Description of the policies, procedures and criteria for determining process and product conformance.
4. **Process Assurance Activities.** Description of the process assurance reviews and audits to be conducted to demonstrate compliance of the processes to plans and standards.
5. **Deviations.** Description of the methods for detecting, recording, evaluating, resolving and approving deviations from plans and standards.

10.2 HARDWARE DESIGN STANDARDS AND GUIDANCE

Hardware design standards and guidance may define the rules, procedures, methods, and criteria for hardware design, validation, verification, assurance and control processes and are used to assess the acceptability and quality of hardware design results. Standards may not be required, but, if the applicant invokes them for the project, they become part of the certification basis and plans for the project. As with the plans, such standards and guidance may be packaged as a single document or multiple documents. Tools may be used to enforce standards.

10.2.1 Requirements Standards

Requirements standards may be used during the requirements capture process to define the rules, procedures, methods, guidance and criteria for developing the requirements. Requirements standards may include methods and criteria for developing and specifying requirements, methods and criteria for validating the requirements, notations used to express the requirements, guidance on the use of requirements specification tools, and the means used to provide derived requirements to the system design process.

10.2.2 Hardware Design Standards

Hardware design standards may be used during the conceptual design process and detailed design process to define the rules, procedures, methods, guidance and criteria for developing and specifying the hardware design.

Hardware design standards may include:

1. Hardware design representation methods and notations.
2. Design specification and naming conventions.
3. Guidance on design methods.
4. Guidance on the use of hardware design tools.
5. Guidance for electronic component selection.
6. Guidance for assessing design alternatives.
7. Guidance for assessing the fail-safe and fault-tolerance design constructs.
8. Description of the means for providing feedback to the requirements process and for clarifying requirements.

10.2.3 Validation and Verification Standards

Hardware validation and verification standards may be used during the validation and verification processes to define the rules, procedures, methods, guidance and criteria for validating and verifying the hardware design and implementation.

10.2.4 Hardware Archive Standards

Hardware archive standards may be used to define the procedures, methods and criteria used to retain and archive product data and develop and maintain program and project archives. Hardware archive standards may include archive content, format, and medium standards, rules, methods and criteria.

10.3 HARDWARE DESIGN DATA

The hardware design data are the specifications, documents and drawings that define the hardware items.

10.3.1 Hardware Requirements

The requirements specify the functional, performance, safety, quality, maintainability, and reliability requirements for the hardware item being developed.

The requirements should include:

1. The system design and safety requirements allocated to the hardware.
2. Identification of applicable standards for the hardware.
3. Hardware functional and performance requirements, including derived requirements and stress limits for normal use.
4. Hardware reliability and quality requirements, including requirements related to failure rates, exposure times and design constraints.
5. Hardware maintenance and repair requirements throughout the hardware item service life.
6. Hardware manufacturability and assembly requirements.
7. Hardware testability requirements.
8. Hardware storage and handling requirements.
9. Installation requirements.

10.3.2 Hardware Design Representation Data

The hardware design representation data provides a definition of the hardware item and is comprised of the set of drawings, documents and specifications used to build the hardware item. The following paragraphs define some typical hardware design data and their content. The type of data, drawings and documents produced for a given hardware design will vary depending on the size, complexity and number of components the hardware item contains.

10.3.2.1 Conceptual Design Data

The conceptual design data is the data that describes the hardware item's architecture and functional design and may include:

1. A high-level description, such as a block diagram or HDL definition, which outlines the major functions and shows the flow of information between these functions.
2. The mechanical structure which describes the arrangement of the hardware item, such as drawings or sketches showing exterior package, printed circuit board arrangement, connector selection and location, and major interconnect wiring.
3. Other architectural features and partitioning that are important from an airworthiness point of view. This might include items such as EMI, lightning, shock or vibration protection, unused functions in major components as well as man-machine interfaces, such as ergonomic factors, lighting characteristics and display resolution.
4. Top-level hardware item functional description.
5. Hardware item functional architecture.
6. Preliminary hardware safety assessment data.

10.3.2.2 Detailed Design Data

The detailed design data describes the data necessary to implement the hardware item consistently with its requirements. Depending on the hierarchical level of the hardware item, this may include top-level drawing, assembly drawings, interconnection data, parts data, HDL hardware description, reliability data, test methodology data, list of unused functions in selected components and actions taken to assure they will not compromise the safety of the hardware item, installation control data, and hardware/software interface data. Some specific data are described below.

NOTE: In addition to the detailed design data required by other applicable certification requirements, such as Technical Standard Orders, the content and availability of other detailed design data items are proposed by the applicant to the certification authority in the PHAC.

10.3.2.2.1 Top-Level Drawing

The top-level drawing uniquely identifies the hardware item and identifies all assemblies, subassemblies, components and relevant documentation that define the hardware item.

10.3.2.2.2 Assembly Drawings

Assembly drawings include additional detailed information needed to assemble the hardware item, assembly, or subassembly.

An assembly drawing may include:

1. Location and orientation of the hardware items within a hardware assembly.
2. Identification of assembly instruction sequences or methods to ensure a correct and fault free assembly.
3. Locations for identifying marks, labels, vision references used in subsequent operations.

10.3.2.2.3 Installation Control Drawings

Installation control drawings ensure correct installation of a hardware item into a system or correct installation of a hardware item into another hardware item. For some lower level hardware item, assembly drawings for the next higher hardware item or assembly may act as the installation control drawing.

Installation control drawing may include:

1. Dimensions.
2. Clearance requirements.
3. Cooling and mounting information.
4. Information on weight, center of gravity, and other parameters necessary to ensure safe and proper installation.

10.3.2.2.4 Hardware/Software Interface Data

The performance of the hardware as determined by the requirements specification may depend upon the configuration of the hardware by the software, calibration of the hardware by the software or upon a necessary interaction between the hardware and software.

Data relating to the interface between the hardware and the software may include:

1. Memory addresses.
2. Allocation of memory address fields into which data can be loaded.
3. Timing and sequence information.
4. Other information necessary for the operation of the hardware/software interface.

10.4 VALIDATION AND VERIFICATION DATA

Validation and verification data is the evidence of the completeness and correctness of the hardware design results and of the hardware item itself. It provides assurance that the hardware has been developed to its requirements and design, correctly produced, and the design objectives achieved. Data includes procedures and results for hardware reviews, analyses and testing. Additional data items beyond that described in this section may be needed for Level A and B functions as described in Appendix B.

10.4.1 Traceability Data

Hardware traceability establishes a correlation between the requirements, detailed design, implementation and verification data that facilitates configuration control, modification and verification of the hardware item.

Hardware traceability data should include:

1. A correlation between the system requirements allocated to hardware and the requirements.
2. A correlation between the requirements and the hardware detailed design data.
3. A correlation between the hardware detailed design data and the as-built hardware item or assembly.
4. A correlation between the requirements, including derived hardware requirements, and detailed design data and the verification procedures and results.
5. The results of a traceability analysis.

10.4.2 Review and Analysis Procedures

Hardware review and analysis procedures define the process and criteria for conducting reviews and analyses.

Hardware review and analysis procedures should include:

1. Purpose of review or analysis.
2. Organizations to participate in the review.
3. Review or analysis criteria.
4. Detailed instructions for conducting the review or analysis.
5. Review or analysis acceptability and completion criteria.

10.4.3 Review and Analysis Results

Hardware review and analysis results are the evidence that the reviews and analyses have been completed to approved procedures and criteria.

Hardware review and analysis results should include:

1. Identification of review or analysis procedure.
2. Identification of data item reviewed or analyzed.
3. Personnel participating in the review or analysis.
4. Review or analysis results.
5. Corrective actions generated as a result of review or analysis, such as listing of problem reports or action items.
6. Review or analysis conclusion including, for reviews, a qualitative assessment of the item reviewed and, for analysis, a quantitative assessment of the item analyzed and the analysis data.

10.4.4 Test Procedures

Hardware test procedures define the methods, environment and instructions for conducting both functional and environmental qualification testing used for the verification of the hardware item.

Hardware test procedures should include:

1. Purpose of test.
2. Identification of the hardware test setups, software and test equipment setup instructions required for each hardware test.
3. Detailed instructions for conducting the test procedures.
4. Test input data.
5. Expected results, such as pass/fail criteria and requirements covered by the test.

10.4.5 Test Results

Hardware test results are the objective evidence that the tests have been completed to approved procedures in support of the verification of the hardware item.

Hardware test results should include:

1. Identification of the test procedure.
2. Identification of the item tested.
3. Actual results of conducting the test.
4. Identification of the personnel conducting and witnessing the tests, if applicable, and the date the tests were conducted.
5. Interpretation of results, either by analysis or review and actual test coverage achieved.

10.5 HARDWARE ACCEPTANCE TEST CRITERIA

This data provides the criteria and assessment data that the test and associated test results are capable of ensuring that an item is manufactured or repaired correctly.

The criteria should include:

1. Key attributes to be tested.
2. Pass/fail criteria for each key attribute.
3. Any test constraints.
4. Substantiation of the key attributes and pass/fail criteria.
5. Coverage of design aspects necessary to meet the safety requirements.
6. Assessment data that shows that the test criteria have been properly implemented based on the actual test procedures and associated test results.

10.6 PROBLEM REPORTS

Problem reports are a means to identify and record the resolution to hardware design problems, process non-compliance with hardware plans and standards, and deficiencies in hardware life cycle data.

Problem reports should include:

1. Identification of the configuration item and process activity in which the problem was observed.
2. Identification of the configuration items to be modified or a description of the process to be changed.
3. A problem description which enables the problem to be understood and resolved.
4. A description of the corrective action taken to resolve the reported problem.

10.7 HARDWARE CONFIGURATION MANAGEMENT RECORDS

The results of the configuration management process activities are recorded in configuration management records. These may include configuration identification lists, baseline or electronic records, change history reports, problem report summaries, tool identification data, archive records and release records.

10.8 HARDWARE PROCESS ASSURANCE RECORDS

The results of the process assurance process activities are recorded in process assurance records. These may include review or audit reports, meeting minutes, records of authorized process deviations, or conformity review records.

10.9 HARDWARE ACCOMPLISHMENT SUMMARY

The Hardware Accomplishment Summary is the primary data item for showing compliance to the PHAC and demonstrating to the certification authority that the objectives of this document have been achieved for the hardware items. This summary may be combined with the system accomplishment summary. The Hardware Accomplishment Summary should include the following information as documented in the PHAC:

1. System overview.
2. Hardware overview.
3. Certification considerations.
4. Hardware design life cycle description.
5. Hardware design life cycle data.
6. Previously developed hardware.
7. Additional considerations.
8. Alternative methods

Differences from the approved PHAC should be identified. In addition, the following four items should be addressed:

1. **Hardware Identification.** This section identifies the hardware configuration and hardware items by part number and version.
2. **Change History.** If applicable, this section includes a summary of hardware changes with attention to changes made due to failures affecting safety, and identifies changes from the hardware design life cycle processes since the previous certification.
3. **Hardware Status.** The section contains a summary of problem reports unresolved at the time of certification, including a statement of functional limitations.
4. **Compliance Statement.** This section includes a statement of compliance with this document and a summary of the methods used to demonstrate compliance with criteria specified in the hardware plans. This section also addresses additional rulings and deviations from the hardware plans, procedures, and this document.

   NOTE: The data included in the PHAC does not necessarily need to be repeated in the Hardware Accomplishment Summary, however doing so may expedite the certification process.

CHAPTER 11

ADDITIONAL CONSIDERATIONS

This section provides guidance on additional considerations of design assurance that are not covered in the previous sections. These additional considerations may be used at the applicant's discretion to satisfy some of the objectives of Section 2 through Section 9. Any use of additional considerations should be agreed with the certification authority.

11.1 USE OF PREVIOUSLY DEVELOPED HARDWARE

This section discusses the issues associated with the use of previously developed hardware. Guidance includes the assessment of modifications to the hardware, to the aircraft installation, to the application environment, or to the design environment and upgrading design baselines. Guidance for COTS component usage, a special case of previously developed hardware, is covered in Section 11.2. Configuration Management and Process Assurance considerations should also be addressed for each use of previously developed hardware.

The intention to use previously developed hardware should be stated in the PHAC.

11.1.1 Modifications to Previously Developed Hardware

This section discusses modifications to previously developed hardware. Modification may result from requirement changes, the detection of errors, hardware or technology enhancements, or procurement difficulties.

Analysis activities for proposed modifications include:

1. Review of the outputs of the system safety assessment process.
2. Application of the guidance of Section 11.1.4 if the hardware design assurance level is increased.
3. The impact of changes should be analyzed, including the consequences of changes that may result in a re-verification effort involving more than the area changed. This area may be determined by signal flow analysis, functional analysis, timing analysis, traceability analysis or other suitable means.

11.1.2 Change of Aircraft Installation

This section discusses the use in a new aircraft installation of hardware that has been previously certified at a certain hardware design assurance level and under a specific certification basis. When using previously developed hardware on new aircraft installations, the following guidance should be used:

1. The system safety assessment process assesses the new aircraft installation and determines the hardware design assurance level and the certification basis. No additional effort will be required if these are the same or less stringent for the new installation as they were in the previous installation.
2. If functional modifications are required for the new installation, the guidance of Section 11.1.1, Modifications to Previously Developed Hardware, should be satisfied.
3. If the previous design activity did not produce the outputs required to substantiate the safety objectives of the new installation, the guidance of Section 11.1.4, Upgrading A Design Baseline, should be satisfied.

11.1.3 Change of Application or Design Environment

Use of previously developed hardware may involve a new design environment, or integration with other software or hardware than that used for the original application.

New design environments may increase or reduce some activities within the hardware design life cycle processes. Guidance includes:

1. If a new design environment uses hardware design tools, the guidance of Section 11.4, Tool Assessment and Qualification, may be applicable.
2. Verification of hardware interfaces should be conducted where previously developed hardware is used with different interfacing hardware.
3. The need for re-verification of hardware/software interfaces should be addressed when previously developed hardware uses different software.

11.1.4 Upgrading a Design Baseline

The following guidance is for hardware items whose life cycle data from a previous application are determined to be deficient for the safety objectives associated with a new application. This guidance is intended to aid the applicant in obtaining agreement with the certification authority for hardware previously developed at a lower hardware design assurance level:

Guidance for upgrading a design baseline includes:

1. The objectives of this document should be satisfied, while taking advantage of life cycle data of the previous development.
2. Hardware aspects of certification should be based on the failure conditions and hardware design assurance levels as determined by the system safety assessment process. The impact of the changes to the previous application should be analyzed to determine areas of deficiency.
3. Life cycle data from a previous development should be evaluated to ensure that the verification process objectives are satisfied for the hardware that is planned for implementation of the upgraded function at the required hardware design assurance level.
4. Reverse engineering may be used to regenerate hardware life cycle data that is deficient or missing to satisfy the design assurance objectives of this document
5. If use of product service experience is planned to satisfy the design assurance objectives of this document in upgrading a design baseline, the guidance of Section 11.3, Product Service Experience, should be addressed.
6. The applicant should specify the strategy for accomplishing compliance with this document in the PHAC.

11.1.5 Additional Configuration Management Considerations

The configuration management process for the new application of previously developed hardware should include, in addition to the guidance of Section 7:

1. Traceability from the hardware product and life cycle data of the previous application to the new application.
2. Change control processes that can manage change requests from different applications of the common item.

11.2 COMMERCIAL-OFF-THE-SHELF (COTS) COMPONENTS USAGE

COTS components are used extensively in hardware designs and typically the COTS components design data is not available for review. The certification process does not specifically address individual components, modules, or subassemblies, as these are covered as part of the specific aircraft function being certified. As such, the use of COTS components will be verified through the overall design process, including the supporting processes, as defined in this document. The use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage.

11.2.1 Electronic Component Management for COTS Components

Electronic component management for COTS components is an important supporting process associated with the design and development of hardware. The processes of electronic component management apply to COTS electronic components. While there are both business and technical aspects of this process, this section only deals with the technical aspects as they impact certification.

Certification credit may be gained by establishing that:

1. The component manufacturer can demonstrate a track record for production of high quality components.
2. Quality control procedures are established at the component manufacturer.
3. There is service experience supporting the successful operation of the component.
4. The component has been qualified by the manufacturer or by means of additional testing, which establish the component reliability.
5. The component manufacturer has control of the component quality level or that this is assured by means of additional component testing.
6. The components have been selected on the basis of technical suitability of the intended application, such as component temperature range, power or voltage rating, or that additional testing or other means has been used to establish these.
7. The component performance and reliability are monitored on a continuous basis, with feedback to component manufacturers concerning areas that need improvement.

11.2.2 COTS Component Procurement

COTS component procurement guidance is not the intent of this document but feedback of procurement issues should be managed and resolved by the applicant when they have significant impacts on hardware design assurance.

Major concerns include:

1. Actual availability of COTS component design assurance data as required by this document.
2. Variations in component parameters that depend on production batches may not be identified, even by robustness tests.
3. Evolving aspects of electronic component technology.
4. COTS components which become non-procurable.

11.3 PRODUCT SERVICE EXPERIENCE

Service experience may be used to substantiate design assurance for previously developed hardware and for COTS components. Service experience relates to data collected from any previous or current usage of the component. Data from non-airborne applications is not excluded.

NOTE: Wide and successful use of an item in service may provide confidence that the item's design is mature and free of errors and that the manufacturing quality of the item is demonstrated.

11.3.1 Product Service Experience Data Acceptability Criteria

When service experience data is used for design assurance, the relevance and acceptability of the service experience data depends on one or more of the following:

1. Similarity of hardware item usage with respect to application, function, operating environment and design assurance level.
2. Extent to which the design assurance data is based on the proposed configuration of the hardware item.
3. Extent to which the design errors found during the service period being assessed have been eliminated, mitigated, or analyzed and determined to have no safety impact in the configuration to be used.
4. Actual failure rates in operation.

   NOTE: The PHAC should specifically address those aspects where the design assurance of parts of an application relies on service experience data.

11.3.2 Assessment of Product Service Experience Data

To satisfy the above criteria the applicant should:

1. Assess the relevance of previous applications, installations and environments to the target application, based upon engineering analysis.

   NOTE: Data used to determine appropriateness of use and usage limitations may be available in specifications, data sheets, application notes, service bulletins, user correspondence and errata notices. These sources of information may also describe the functions associated with the hardware item, so the airborne intended use can be correlated to previous uses.

2. Assess the intended usage for impacts on the safety assessment process, including possible mitigation of the effects of design errors identified by the data.
3. Assess any available statistics on design errors and their impact on the safety assessment process. A qualitative assessment can be used if statistics are not available.
4. Assess available problem reports. Problem reports may show that service experience has led to improvements now available in the current configuration. Problems identified but not fixed may still be mitigated by architectural means or by performing additional verification. Establish or assess the relationships between problem reports and hardware item or product requirement changes.

   NOTE: For electronic components, substantial service usage may increase the likelihood that errors have been detected and eliminated or that temporary "fixes" are available.

11.3.3 Product Service Experience Assessment Data

Service experience assessment data used to substantiate the design assurance for the proposed application should include:

1. Identification of the component and its intended function in the airborne system. Identify the design assurance level, or for components used in Level A and B functions, a description of additional means of assurance for the component, such as architectural means and additional or advanced verification strategies to be applied.
2. A description of the service experience data collection and assessment process, including criteria for determining the adequacy and validity of the data.
3. The service experience data, including the detailed service information being considered, change history, assumptions used to analyze the service experience data and a summary of the analysis results.
4. Justification for the adequacy of the service experience data relative to the intended use and required design assurance level.

11.4 TOOL ASSESSMENT AND QUALIFICATION

Tools, both hardware and software, will normally be used during hardware design and verification. When design tools are used to generate the hardware item or the hardware design, an error in the tool could introduce an error in the hardware item. When verification tools are used to verify the hardware item, an error in the tool may cause the tool to fail to detect an error in the hardware item or hardware design. Prior to the use of a tool, a tool assessment should be performed. The results of this assessment and, if necessary, tool qualification should be recorded and maintained.

The purpose of tool assessment and qualification is to ensure that the tool is capable of performing the particular design or verification activity to an acceptable level of confidence for which the tool will be used.

11.4.1 Tool Assessment and Qualification Process

Tool assessment assesses the role of the tool in a design life cycle process and may include qualification activities to be performed depending on the role of the tool and design assurance level of the hardware function. This assessment guidance is presented as a flowchart and applies to both design tools and verification tools when used to meet objectives or generate data items to satisfy those objectives. The flowchart will lead the applicant to limited appraisal of some categories of tools and to tool qualification of others.

The tool assessment and qualification process may be applied to either a single tool or a collection of tools. Tools often contain capabilities beyond those needed for a specific design or verification activity on any specific project. It is only necessary to assess those functions of the tool used for a specific hardware life cycle activity, not the entire tool.

It is recognized that tools are often integrated and shared during the various life-cycle phases. If the same tool is used during both the design and the verification phase, then the tool may need to be assessed as a design tool unless separation of and protection between the two functions can be established.

NOTE 1: If the assessment of a given tool indicates that some of its functions are used for design but other functions are used for verification, it may be worthwhile to address the functions separately and perform the assessment for each group of the tool's assessed functions.

NOTE 2: This assessment activity focuses as much or more on the application of the tool as the tool itself.

The flow chart of Figure 11-1 indicates the tool assessment considerations and activities and provides guidance for when tool qualification may be necessary. The numbers in the decision and activity blocks refer to the numbered items following the figure that provide further clarification of the decision or activity.

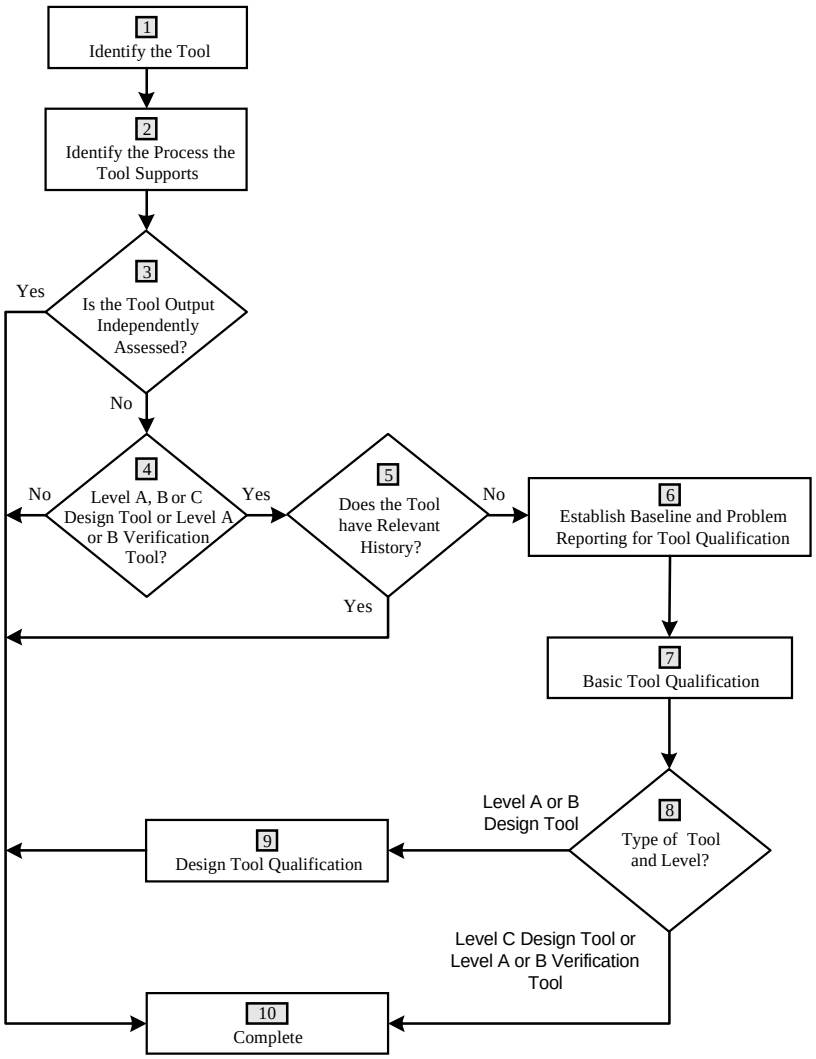


FIGURE 11-1: DESIGN AND VERIFICATION TOOL ASSESSMENT AND QUALIFICATION

1. **Identify the Tool**. Includes the name, source, version number and the host environment on which it is based. Tool updates should be documented and tracked.

   NOTE: *When updating a tool, assess the potential impacts of tool updates on existing results and on the remaining life cycle of the hardware.*

2. **Identify the Process the Tool Supports.** Identify the design or verification process that the tool supports, any relevant limitations of the tool and the outputs it produces for use in the hardware design life cycle. If certain problems are known to exist with the tool, provide a statement of acceptability for use of the tool with justification.

3. **Is the Tool Output Independently Assessed?** An independent assessment verifies the correctness of the tool output using an independent means. If the tool output is independently assessed, then no further assessment is necessary.

   NOTE: *Independent assessment of a design tool's output that is generated in whole or in part by the tool may be established by the verification activities performed on the item, such as component, netlist or assembly. In this case, the integrity of the end item does not depend upon the correctness of the design tool output alone.*

   Independent assessment of a verification tool's output may include a manual review of the tool outputs or may include a comparison against the outputs of a separate tool capable of performing the same verification activity as the tool being assessed.

   The applicant may propose other methods of independent assessment as well.

4. **Is the Tool a Level A, B or C Design Tool or a Level A or B Verification Tool?** If the tool is used for Level D functions, as a verification tool for Level C functions, or used to assess the completion of verification testing, such as in an elemental analysis as described in Appendix B, Section 3.3.1.1.2, no further assessment is necessary. If the tool is used as a design tool for hardware implementing a Level A, B or C function or is used as a verification tool for hardware implementing a Level A or B function, then further assessment is needed.

5. **Does the Tool have Relevant History?** When it is possible to show that the tool has been previously used and has been found to produce acceptable results, then no further assessment is necessary. A discussion of the relevance of the previous tool usage versus the proposed usage of the tool should be included in the justification.

   NOTE: *The history of the tool may be based on either an airborne or non-airborne application, provided that data is available to substantiate the relevance and credibility of the tool's history.*

6. **Establish Baseline and Problem Reporting for Tool Qualification.** Establish a baseline for tool configuration management and tool problem reporting to prepare for tool qualification.

7. **Basic Tool Qualification.** Establish and execute a plan to confirm that the tool produces correct outputs for its intended application using analysis or testing. The tool's user guide or other description of the tool's function and its use may be used to generate requirements.

8. **Type of Tool and Level?** Is the tool being considered a Level A or B hardware design tool or a Level C hardware design tool or a Level A or Level B hardware verification tool?

9. **Design Tool Qualification.** Qualify the Level A or B design tool using the strategies described in Appendix B of this document, the tool qualification guidance of RTCA DO-178B / EUROCAE ED-12B for software development tools or other means acceptable to the certification authority. Independence of this activity from the tool development should also be established.

   NOTE: Specific guidance for Level A and B design tool qualification is not provided here because of the variability of the circumstances of the tool usage, technology involved, visibility of the tool's implementation and life cycle data, and other factors. Using such a design tool without independent assessment of the tool's output or establishing relevant history is discouraged, as it may prove to be a task as challenging as the development of the hardware for which the tool is proposed to be used.

10. **Complete.** Document the tool assessment, justification for the assessment decisions, and if applicable, tool qualification data. Provide specific references to installation guides, user manuals and tool qualification data, as necessary to support the tool assignment and qualification.

11.4.2 Tool Assessment and Qualification Data

The tool assessment and qualification data should include:

1. Identify the tool, the process it supports and, when applicable, the following items:
   a. The rationale and results of the independent assessment per item 3 of Figure 11-1.
   b. The tool designation per item 4 of Figure 11-1.
   c. The tool's history when being used to satisfy item 5 of Figure 11-1. A discussion of the relevance of the previous tool usage versus the proposed usage of the tool should be included in the justification.
2. An unambiguous configuration definition to be used in tool qualification, in compliance with item 6 of Figure 11-1, and a justification for the applicability of the tested configuration if it differs from that actually used to design or verify the end hardware item.
3. Details of tool qualification, including the requirements used in testing, the test procedures, expected results, analysis procedures used to interpret and supplement the test results, and how independence is established.
4. The plan for qualifying a design tool, including the applicable procedures, and results for any activities identified in the plan.
5. The disposition of known tool errata, including workarounds, and, when applicable, problem reports generated as a result of tool qualification.

APPENDIX A

MODULATION OF HARDWARE LIFE CYCLE DATA BASED ON HARDWARE DESIGN ASSURANCE LEVEL

This appendix provides guidance for the modulation of the hardware design life cycle data based on the hardware design assurance level. It also provides guidance concerning the requirements for independence during the verification process.

Table A-1 identifies the data delivery classification and configuration management data control category for each data element. Refer to Table 7-1. There are two data delivery classification types defined:

1. **Submitted.** The data item should be submitted to the certification authority.
2. **Not Available.** The data item is not required.

All verification of Level A and B functions should be independent. Level C and lower functions do not require independent verification. Independence is needed only at the design hierarchy level at which the design is verified against the requirements. An equivalent means of independence, which addresses the issue of common mode failure, should be acceptable.

Independence is a means to address potential common mode errors that could occur when a designer verifies that the hardware item under development performs as designed, not as required. To address this concern, the responsibility for ensuring the verification process is consistent with demonstrating that the design requirements have been met should be performed with an individual, a process or a tool that is independent of the designer. There are many means of establishing independence and the verification plan should address the specific means to be used for a particular verification activity.

Some examples of acceptable means are:

1. Requirements or designs are reviewed by another individual.
2. Test cases or procedures are developed by another individual.
3. Test cases or procedures developed by the designer are reviewed by another individual.
4. An analysis performed by the designer is reviewed by another individual or a review team.
5. A different test is performed that confirms the results of testing by the designer, such as a test during flight test confirms a hardware item test or software verification tests, developed independently and performed on the target hardware item, confirm the results of testing by the designer.
6. Test or analysis results are verified by a tool.

NOTE 1: Often verification tests are automated and require only the "push of a key" to execute them. It is not the intent of independence to require someone other than the designer to execute the tests once they are evaluated or developed with independence. The results may still need to be reviewed independently to confirm proper procedures were followed and that the results verify that the requirements have been met.

NOTE 2: Organizational structure separation is not needed to achieve independence.

The circled numbers in Table A-1 refer to the notes following the table.

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

TABLE A-1: HARDWARE LIFE CYCLE DATA BY HARDWARE DESIGN ASSURANCE LEVEL AND HARDWARE CONTROL CATEGORY

① Data that should be submitted is indicated by an S in the Submit column. HC1 and HC2 data used for certification that need not be submitted should be available. Refer to Section 7.3.

② The objectives listed here are for reference only. Not all objectives may be applicable to all assurance levels.

③ If this data is used for certification, then its availability is shown in the table. This data is not always used for certification and may not be required.

④ This can be accomplished informally through the certification liaison process for Levels C and D. Documentation can be in the form of meeting minutes and or presentation material.

⑤ If the applicant references this data item in submitted data items, it should be available.

⑥ Only the traceability data from requirements to test is needed.

⑦ Test coverage of derived or lower hierarchical requirements is not needed.

APPENDIX B

DESIGN ASSURANCE CONSIDERATIONS FOR
LEVEL A AND B FUNCTIONS

1 INTRODUCTION

The designer of hardware implementing Level A and Level B functions makes design decisions that may impact safety. As the design assurance level increases, the approach needed to verify that a given design meets its safety requirements may need overlapping, layered combinations of design assurance methods. It is up to the applicant to select one or more of these methods or propose another method that would provide design assurance.

This appendix provides the designer with guidance on how to perform and use an FFPA to develop a design assurance strategy as well as guidance on some specific methods that may be used for design assurance.

2 FUNCTIONAL FAILURE PATH ANALYSIS

An FFPA is a structured, top-down, iterative analysis. It identifies the specific portions of the design which implement the function; that is, the assemblies, components and elements associated with each path; and the associated failure modes and effects to be analyzed to determine that the hardware architecture and implementation complies with the safety requirements. FFPA also identifies those assemblies, components and elements of the design that implement the Level A and B functions.

An FFPA begins with the PSSA, which is used to identify system level FFPs that may be decomposed into and allocated to hardware FFPs.

The goal of an FFPA is to identify individual FFPs so that:

Hardware implementing Levels A and B functions can be addressed by an appropriate design assurance method described in this appendix or another advanced method acceptable to the certification authority.

Considerations of this appendix are optional for hardware implementing level C or lower level functions, that is, those functions that will be assured using only the guidance of Section 3 through Section 11 of this document.

NOTE: Identification of separate FFPs for functions implemented in different technologies or offering different degrees of design visibility is often useful because the total hardware item's design assurance may be accomplished using multiple design assurance methods. The level of decomposition may vary for each FFP.

Decomposition is performed using conventional top-down safety assessment techniques, such as fault tree analysis. The decomposition may be complemented using F-FMEA, dependency diagrams and common mode analysis for each successive level of decomposition. The level of decomposition may vary for each system level FFP depending on the design assurance strategy, corresponding implementation concept and the error mitigation methods being proposed for the hardware being designed. Decomposition progresses from:

system level FFPs	into	hardware level FFPs;
hardware level FFPs	into	circuit level FFPs;
circuit level FFPs	into	component level FFPs; and
component level FFPs	into	elemental level FFPs.

2.1 Functional Failure Path Analysis Method

The FFPA should be performed as follows:

1. For each Level A and Level B function, identify the function and its design assurance level based on the hardware requirements and system FHA for that function. The function may be formed as a collection of subfunctions, each having a corresponding set of derived requirements and an associated design assurance level. These subfunctions may be decomposed further as necessary.
2. For each Level A and Level B function, determine the means of implementing the function or the subfunctions and analyze the design assurance options. The assurance data available or expected to be available for the implementation of the function or subfunction should be complete and acceptable for the design assurance strategy or strategies chosen. If the assurance data available or expected to be available is complete, correct and acceptable, then no further decomposition is necessary.
3. For FFPs that are not Levels A or B, their interrelationships with the Level A or B FFPs should be evaluated using an F-FMEA, common mode analysis or dependency diagram to ensure that the Level A and B FFPs cannot be adversely impacted by the FFPs which are not Level A or B.

This assessment process is iterative. If there is no acceptable method of design assurance for a FFP, the decomposition and evaluation process is repeated or the architecture or implementation of the hardware function changed until an acceptable method of design assurance has been determined and acceptable assurance data is provided or can be provided for each Level A and Level B FFP.

Results of the FFPA and selected methods used for design assurance for the hardware are communicated to the aircraft systems process as described in Section 2.1 of this document. These results are used to examine and validate that the aircraft level assumptions, especially those related to multiple cross system usage of similar hardware items, are still valid.

2.2 Functional Failure Path Analysis Data

The FFPA data should:

1. Identify the anomalous behaviors and functional failures that have been delegated to the hardware item from the system level.
2. Identify the FFPs, the effects of their anomalous behavior or functional failure, and decomposition level in the design hierarchy to which the analysis was performed and the type and location of the acceptable assurance data that should be available.
3. Describe the relationship between FFPs to determine their independence and inter-dependencies on other FFPs and components. Such relationships may be described using qualitative FTA or other top-down analysis, common mode analysis, F-FMEA or dependency diagrams. The relationship descriptions should identify those inter-related paths and components and the inter-dependencies.
4. Trace between the FFPs and the hardware requirements and derived requirements.

3 DESIGN ASSURANCE METHODS FOR LEVEL A AND B FUNCTIONS

It is not the intent of this appendix to restrict the implementation of design assurance through the use of any current or future method. Methods discussed in this appendix may be used in satisfying one or more of the objectives of the processes described in Section 4 through Section 6 of this document.

3.1 Architectural Mitigation

Architectural design features, such as dissimilar implementation, redundancy, monitors, isolation, partitioning and command/authority limits, can be specifically employed to mitigate or contain the adverse effects of hardware design and implementation errors. As part of the PSSA, activities such as qualitative fault tree analysis and common mode analysis can provide assurance for determining the scope of architectural attributes needed to mitigate or contain the effects of hardware faults, failures, and design and implementation errors. More specifically, this approach should be applied in conjunction with the FFPA approach for hardware as described in Appendix B, Section 2, and should use the common mode analysis process to determine the applicability of particular mitigation strategies for coverage of hardware design and implementation errors. For example, redundancy usually helps mainly in the area of random faults or upsets, but redundancy can also be used effectively to mitigate design and implementation errors if their common mode aspects have been addressed.

3.1.1 Architectural Mitigation Method

Architectural mitigation is performed by identifying FFPs associated with a proposed hardware implementation, and then analyzing design options to identify and propose design features and strategies that mitigate the effects of these FFPs. The overall effects of a proposed architecture in regards to mitigating all relevant effects of the FFPs should be evaluated and addressed. Introduction of an architectural mitigation strategy also introduces some derived requirements against which its implementation should be verified. Specifically, the architectural features should protect against some or all of the adverse effects of the identified FFPs and should be assessed for introduction of additional failure paths, which should then be addressed by further architectural mitigation, or by another of the design assurance strategies described in this appendix.

3.1.2 Architectural Mitigation Resolution

The safety assessment process determines the acceptability of the architectural mitigation. The FFPA should first identify all the Level A and B hardware FFPs where architectural mitigation is to be used for credit, and should identify the methods to be used, and should determine the rationale for that mitigation. Adequacy is determined by assessing each function supporting the mitigation in the context of the overall architecture approach that may involve a more or less complex aggregate of architectural mitigation strategies.

The common mode analysis should address the potential for common mode errors in requirements, implementation, manufacturing and maintenance that could defeat the mitigation. The designer should also consider potential random failures of the hardware forming the architectural mitigation functions that may cause the mitigation to become unavailable. The probabilistic availability of the functions supporting the mitigation should be commensurate with the consequences of the loss of mitigation, which may result in the reduction of safety margins.

The overall approach should ensure that correct operation and acceptable independence between the necessary functions are achieved and maintained. Any special safeguards needed to eliminate, isolate or bound residual common mode effects should be identified and incorporated either in the form of additional architectural mitigation or other design assurance strategies defined in this appendix.

When the architecture definition is complete, hardware functions in Level A and B FFPs which are determined to be unmitigated, or inadequately mitigated, should be re-addressed using another design assurance methods from this appendix. For example, partial architectural mitigation of individual circuits and components can be used in conjunction with the safety specific analysis method when that analysis is used to identify and provide verification coverage for the unmitigated portions of the applicable circuits and components.

3.1.3 Architectural Mitigation Data

Documentation of architectural mitigation means, applied to protect levels A and B FFPs in hardware, should be provided in the forms of safety assessment data, safety requirements data and traceability data. The safety assessment data should be based on the assessment of hardware FFPs and common mode failure analysis specifically addressing the architectural mitigation aspects of the hardware design.

Architectural mitigation data should include:

1. Identification of the Level A and B hardware FFPs that are to be protected by architectural means.
2. Description of the architectural approach and validation rationale about coverage provided by that approach.
3. Rationale for common mode boundaries and common mode design aspects applicable to that architecture.
4. Identification of unmitigated and inadequately mitigated Level A and B FFPs to be addressed by other design assurance methods.
5. Requirements about the functional operation and necessary design attributes of the architectural mitigation mechanisms.
6. Mitigation mechanisms used to meet safety requirements that include software, such as software partitioning, safety monitors and dissimilar software. These mechanisms and safety software requirements should be provided to the system process and the software development process.
7. Conventional failure rate data and latent fault exposure assessment data for any hardware that performs the applicable architectural mitigation.
8. Traceability data linking safety requirements to the applicable safety assessment data and to the applicable design verification data.

3.2 Product Service Experience

Section 11.3 provides basic guidance on how to assess product service experience data for applicability for use in airborne hardware. For Level A and B functions that use previously developed hardware as part of the design, additional design assurance is necessary. This assurance can be provided in the following manner.

3.2.1 Product Service Experience Method

After completion of the assessment of Section 11.3, the FFPs that are implemented by the hardware under consideration should be analyzed with respect to any applicable service experience. The applicant or designer should identify the service experience data and establish that the service experience data demonstrates that the reused functionality of the hardware was sufficiently exercised during previous uses of the hardware.

3.2.2 Product Service Experience Resolution

When the service experience data analysis is complete, hardware functions in Level A and B FFPs that are determined to be not exercised, inadequately exercised or for which no service experience is available by in-service operation, should be addressed using another design assurance method or by the identification of additional verification that can be applied to exercise the functions.

3.2.3 Product Service Experience Data

Data of product service experience applied to protect Level A and B FFPs in hardware, should include:

1. The product service experience assessment data of Section 11.3.2.
2. Identification of the FFPs for which design assurance is provided by service experience and justification for the sufficiency of the service experience data.
3. Identification of the FFPs for which service experience data is insufficient and identification of test environments, test procedures, analyses and results used to complete the design assurance for the FFPs.
4. Identification of FFPs and operational conditions not demonstrated by the service experience that will require additional architectural mitigation or advanced verification method.
5. Traceability data as described in Section 10.4.1 showing the explicit relationship of the service experience data and verification that provides design assurance coverage of each FFP.

3.3 Advanced Verification Methods

Additional design assurance confidence may be achieved and evidence provided by the application of advanced verification methods, such as Elemental Analysis, Formal Methods, Safety-Specific Verification Analysis, or other applicant-proposed and certification authority-accepted methods.

The advanced verification methods of design assurance both use and extend the scope of the FFPA method presented in Appendix B, Section 2. The FFPA method is applied progressively at equipment-level, circuit-level, and component-level to determine the hardware implementation of the Level A and B FFPs. Data from the FFPA is then used to determine the proposed means of design assurance applicable to the hardware circuits, components and elements contained in those Level A and B FFPs.

These three methods are summarized here and described in the following sections.

1. **Elemental Analysis.** Elemental analysis provides a measurement of the completeness of the hardware verification from a bottom-up perspective. Every functional element within the FFP is identified and verified using verification test cases that meet the verification objectives of Section 6.1. The analysis may also identify areas of concern that need to be addressed by other appropriate means.
2. **Safety-Specific Analysis.** This strategy focuses on exposing and correcting the design errors that could adversely affect the hardware outputs from a system-safety perspective. Applicable safety sensitive portions of the hardware input space and output space are analytically determined. The sensitive portions of the hardware input space are stimulated, and the output space is observed not only for the safety-sensitive intended-function requirements verification, but also for anomalous behaviors. The methods of output space observation are identified in advance, by analysis that is accomplished using traditional safety analysis techniques.
3. **Formal Methods.** Formal Methods employ techniques from formal logic and discrete mathematics for the specification, design and verification of computer systems. These techniques may be used to substantiate the reasoning employed in various processes of the hardware design life cycle.

Other advanced verification methods may be proposed by the applicant other than those described in this section.

3.3.1 Elemental Analysis

Elemental analysis may be used to show that FFPs are verified by associated verification test cases. Elemental analysis provides confidence and evidence that design errors are precluded by separating a complex implementation of the FFP into elements at the level that the designer generated it. This analysis method provides a measurement of the verification process to support the determination of verification coverage and completeness, and is most suited where the detailed design is visible and under configuration control. This would be the case in an ASIC or PLD, where the functions are addressed at the same design assurance level, or where functions of different design assurance levels are isolated or segregated. Every functional element of the applicable circuits or components is identified and verified for intended-function correctness using verification procedures that achieve the verification objectives of Section 6.1. Elemental analysis is generally applied to an entire component or an assembly without regard to the number of varied FFPs implemented in it, but may be applied to a portion of a component or assembly if a rationale can be provided for the isolation, independence or segregation of different FFPs.

NOTE: When an elemental analysis is performed on a function implemented in a PLD, the programmed contents and the application of the PLD's features should be included, and the unprogrammed component may be addressed using a separate method, such as prior service experience.

The analysis identifies areas of concern that need to be addressed by appropriate means. A verification process without such an analysis may leave some circuitry inadequately tested. Historically, such inadequacies have been due to shortcomings in requirements-based test procedures, unclear or incomplete hardware requirements, unused circuitry, initialization circuitry and library functions. This analysis examines verification of elements in the FFPs of concern and determines if the verification coverage related to each element is complete. Determination that verification coverage for elements is incomplete indicates a need for additional verification or appropriate activity.

The applicant should propose at what levels in the design hierarchy the elements are defined and how they are to be analyzed for verification coverage.

3.3.1.1 Elemental Analysis Method

The elemental analysis method begins by defining a set of criteria to be applied in the analysis in consideration of the hardware design assurance level, the hardware technology and visibility of the details of the implemented hardware.

The criteria should include:

1. Identification and a definition of the elements at an appropriate level of the hardware design.
2. The verification coverage to which each element should be verified.

These criteria are then applied to the analysis of verification activities to determine whether the verification coverage completion criteria will be achieved by the planned verification. If the criteria will not be achieved, then each element being examined should be exercised by an appropriate set of stimuli and cause appropriate observable effects on the signals being monitored in the test.

NOTE: As this process examines the tests against the hardware itself, it can detect deficiencies in the test procedures. Addressing the test deficiencies would then provide additional confidence and evidence that the testing is sufficient, and the execution of new or amended test cases can then uncover errors in the hardware.

3.3.1.1.1 Selecting Elemental Analysis Criteria

The elemental analysis criteria to be applied should be selected on a case-by-case basis depending on the hardware element type and complexity, and the identifiable functional operations of the element. The analysis may show either that all the low-level primitive blocks, such as counters, registers, multiplexers, adders, op amps and filters, have been adequately tested or that all groups of interconnected primitives have been adequately tested and achieve the verification coverage criteria. The analysis criteria of the test procedures should be derived based on an assessment of the functional operation of the element and its integration with other hardware elements in order to perform the next higher hierarchical level hardware function.

NOTE 1: *For example: if an element is a modulo-n counter used as a time delay, the test procedures may use appropriate equivalence-class selections of input data to verify that it counts when enabled, stops counting when disabled, counts at the correct rate, and reaches n and rolls-over at the specified time. It would not be necessary to show that the test procedures exercise the individual gates or flip-flops that collectively form the counter.*

As an example of using interconnected primitives as an element, an Arithmetic Logic Unit (ALU) may be constructed of primitives, such as registers, adders, and control logic. The ALU may be simulated to show that the primitives collectively form the ALU, but the verification procedures used in the elemental analysis should use appropriate equivalence-classes of input data to show that the ALU performs its functions.

The elements need not be defined at a level of the design below that specified by the designer of the hardware. Gate-level analysis may be appropriate only if the design is explicitly expressed as gates for combinatorial logic or state machine control.

NOTE 2: *Analyzing the implementation below the level of that specified by the designer, such as at the gate or transistor level, is not necessary as it would be analogous to analyzing software at the assembly language or binary pattern level. These lower abstraction levels are implicitly addressed by performing the elemental analysis on verification tests performed on the hardware, or on post-layout simulations successfully assessed, and if necessary, qualified as verification tools per Section 11.4.*

An ASIC or PLD may contain proprietary library functions that may not provide visibility of their internal design and therefore would not lend themselves to manual analysis. Library functions may be treated as COTS elements in the elemental analysis, with the COTS hardware aspects addressed as defined in Section 11.2 and Appendix B, Section 2.2. Verification of the application of the library function should show that it is consistent with its specification or description provided by the library manufacturer and the tests should be executed in an environment that allows the test results to be observed.

NOTE 3: *The intent is not to discourage the use of design libraries in favor of building new functions; the practical use of design libraries is encouraged to minimize further opportunities for introducing errors into the hardware.*

For ASICs or PLDs synthesized from a high level description in an HDL, the analysis criteria may be based on the high-level behavioral language code representing the hardware. However, since implementations synthesized from HDL representations may include parallel logic structures and non-sequential temporal aspects, the synthesized output should be included in the analysis completion determination. The synthesizer should be assessed as well.

3.3.1.1.2 Performing the Elemental Analysis

Elemental analysis should use the requirements-based verification tests performed in one or more of the following test environments:

1. Tests with the circuitry implementing the functional path installed in the target assembly.
2. Tests performed on a standalone prototype. Such tests are typical for an ASIC or PLD.
3. Manufacturing acceptance tests.

   NOTE: Since manufacturing tests often are not based on the requirements, manufacturing acceptance tests may be restricted in their application to elemental analysis.

4. A post-layout simulation, typically for an ASIC or PLD, that has been assessed and, if necessary, qualified for use as a verification tool as described in Section 11.4.

An elemental analysis itself may be performed using a simulation to measure the completeness achieved, provided that the test procedures to be analyzed can be related to the elemental analysis criteria being applied and are those used for hardware functional verification credit toward the objectives in Section 6. If the test procedures analyzed are derived from an in-circuit test of hardware or standalone prototype and are examined using a simulation, the test stimuli and expected results may be translated for the simulator provided that the translation process is checked for accuracy as a part of the elemental analysis. A simulator used to perform the elemental analysis should be shown to be able to correctly determine whether each type of element included in the implementation has met the analysis criteria.

3.3.1.2 Elemental Analysis Results Resolution

Elemental analysis may reveal hardware elements not verified, indicating either a need for additional verification process activities or perhaps a need to remove the untested element or mitigate any anomalous behavior that could result by architectural means. Untested hardware elements may be the result of:

1. **Shortcomings in verification test cases or procedures.** Shortcomings may arise if the test cases simply do not test the elements in the hardware item in compliance with the criteria in Appendix B, Section 3.3.1.1. They may also arise if there are “don’t cares” in the functional requirements but the hardware item was appropriately designed to produce repeatable responses. Under these circumstances, the test procedures and cases should be supplemented or changed. Furthermore, the assertion of the test’s ability to verify its respective requirements should be reviewed.
2. **Inadequacies in requirements.** The requirements should be modified or additional derived requirements identified. Additional verification tests should then be developed for the new or revised requirements, executed and analyzed.
3. **Unused functions.** The hardware item may contain functions that are not used in its target circuit application, such as unused subfunctions within a library function or test structures used only for component-level acceptance tests. Such functions should either be shown to be isolated from the other used functions or shown to present no potential anomalous behavior that could have an adverse effect on safety. This could possibly be achieved by showing that the unused elements are positively deactivated either within the hardware or when installed. If the unused functions are to be used in some future application, the elemental analysis deficiency may be revisited at that time provided that such functions are identified as not being fully verified.

4. **Element of no safety consequence.** The consequence of anomalous behavior of the element can be bound and shown by analysis to not cause an adverse safety effect to the airplane or its occupants. These items should be resolved by recording the analysis bounding the consequence of anomalous behavior of the element.

3.3.1.3 Elemental Analysis Life Cycle Data Output

The elemental analysis life cycle data output should:

1. Identify the FFPs to be addressed by elemental analysis, and propose at what levels in the design hierarchy the elements are defined and how they are to be analyzed for verification adequacy, this being part of the verification coverage completion criteria. This should be included in the PHAC or hardware verification plan.
2. Describe the methods and identify the FFPs addressed in the analysis and the levels in the design hierarchy at which the analysis was performed.
3. Ensure that the traceability data, as described in Section 10.4.1 shows the explicit relationship of the verification procedures to the elements in the elemental analysis.
4. Identify the verification test cases and requirements added or modified as a result of the elemental analysis.
5. State the level of the verification completeness achieved for the FFPs addressed by elemental analysis, including identification of the analysis discrepancies not resolved by modification to verification tests or requirements and the rationale for acceptability.

3.3.2 Safety-Specific Analysis

Where applied, the safety-specific analysis method extends the hardware FFPA concept by performing a more in-depth analysis of the selected circuits and components. The extended FFPA is used to both derive and validate safety-specific requirements about internal operations of those circuits and components. These derived safety requirements are then addressed by the verification tests as discussed below.

Safety-specific analysis is based on the concept that a potentially latent design error can affect a hardware item's output only when specific input stimuli expose it. Therefore, to properly stimulate and expose the safety errors of concern, the subset of input cases for which safe operation is necessary is identified and then appropriate equivalence classes from that subset are included in the verification tests. During execution of these test cases, the item's outputs are evaluated for absence of specific anomalous behaviors that could result in unsafe output conditions. The safety-specific analysis is used to bound the set of input conditions to be applied in the verification test cases so that a potentially infinite set of input test cases do not have to be addressed.

NOTE: The implementation may also bound the input set and conditions so that it is not possible or is adequately improbable that the implementation would allow an input outside the limits tested.

The safety-specific analysis method can also be used to determine the unmitigated aspects of circuit and component functions in which partial architectural mitigation is applicable. In this case, the additional safety-specific analysis can be a useful and effective method to determine what additional design assurance is needed to complete the safety coverage.

The safety–specific analysis method is equally applicable to either COTS hardware or custom circuits and components because it is able to use user guide data about those circuit and components instead of detailed internal design data. By combining the user guide data with this more detailed application of the FFPA method, the safety-specific analysis is able to successfully determine the safety-sensitive aspects of circuit and component usage and the associated internal FFPs where design error removal emphasis is needed. This information can then be used to successfully derive circuit and component verification tests which, when completed, maximize the likelihood that the verification process has exposed and corrected, mitigated, or provided work-arounds for those circuit and component design errors which could adversely affect the hardware from a system-safety perspective.

3.3.2.1 Safety-Specific Analysis Method

Once the circuits and components which are to be addressed using the safety-specific analysis method of design assurance are selected, then an additional FFPA is performed to examine them in greater detail. This analysis determines more specifically which circuit and component functions contribute to the already identified Level A and B functions that use those circuits and components. This is accomplished by examining each applicable circuit and component, case-by-case, at its functional boundaries, considering the actual functional usage of that circuit or component to perform the higher level hardware functions contained in the identified Level A and B FFPs.

NOTE: Sufficient information may be available in circuit and component user's guide data that a user can successfully use the functions of that circuit or component to perform higher level hardware functions. If sufficient information is available about the circuit's or component's internal functioning, it should also be adequate to make this assessment. If sufficient information is not available, this assessment cannot be done, and another method should be used instead or in conjunction with this method.

After the relevant safety-sensitive functions of the circuits and components have been identified based on the actual usage of those circuits and components, the next step is an even more detailed functional analysis. This analysis should determine the specific safety-sensitive and unmitigated attributes of those circuit and component functions that are to be addressed in more detail by the safety-specific verification conditions. These verification conditions should be derived and validated by using F-FMEA techniques to determine the specific functional attributes that are safety-sensitive and further to determine any specific anomalous behavior of those functions that would constitute a Level A and B FFP within the circuit or component.

Derived verification conditions obtained via the above safety-specific analysis activities are then used in conjunction with the following guidance to complete the safety-specific analysis criteria for verification of circuit and components contained in Level A and B FFPs. Guidance includes:

1. Identify the relevant input space of the functions. Determine the associated output space pass/fail criteria, based on the identified safety-sensitive functional attributes and anomalous behaviors, and develop the equivalence-classes that will provide the necessary coverage of the relevant input space.

2. Identify relevant observable detection means, and input space stimulation means for each considered function.

   NOTE: Special tools and implementation features may be used to ensure observe-ability and testability.

3. Specify the test environments that address verification of potential error sources and interdependencies.

   NOTE: Component-level functions should be tested at the highest integration level feasible. Testing at higher levels of integration usually provides the best coverage of error-sources, such as upset, interdependencies and potential cross-functional interactions.

Tests should be developed using equivalence-classes. Testing should address key logic decisions, arithmetic, timing, state transitions and real-time attributes.

3.3.2.2 Safety-Specific Analysis Resolution

The safety-specific verification completion criteria should be established by completion of the safety-specific analysis for all the applicable circuits and components. Any deficiencies found by that analysis or by the verification itself should be resolved by one of the following methods:

1. Change the design to correct the error.
2. Add architectural mitigation, which resolves the error by removing it from the relevant FFP.
3. Add appropriate tests.

3.3.2.3 Safety-Specific Analysis Data

Documentation of safety-specific analysis, when applied to circuits and components in Level A and B FFPs, should be provided in the form of safety assessment data, safety requirements data, verification procedures and results, and traceability data. The verification procedures should be traceable to the safety requirements, and to the safety-specific analysis. Safety-specific analysis data should include:

1. Identification of the circuit and components which are to be addressed by the safety-specific analysis method.
2. Identification of the Level A and B FFPs in which each of those circuits and components reside.
3. Identification of partial architectural mitigation applicable to circuits and components where design assurance completion is to be provided by the safety-specific analysis method.
4. For each applicable circuit and component, identification of safety sensitive functions.
5. For each identified safety-sensitive function, identification of safety-sensitive attributes and anomalous behaviors of concern.
6. Verification conditions addressing the applicable circuits, components, internal functions, functional attributes and anomalous behaviors.
7. Verification conditions addressing input dependencies and output space behaviors to be verified.
8. Verification procedures and results.
9. Traceability data linking verification procedures and hardware safety verification conditions to safety-specific hardware analysis data.

3.3.3 Formal Methods

The term formal methods refers to the use of techniques from logic and discrete mathematics in the specification, design and construction of computer systems.

NOTE: The material in this section is derived from "Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems, Volume II: A Practitioner's Companion," May 1997, NASA-GB-001-97. A more detailed presentation of the application of formal methods, illustrated with a worked example, can be found there.

Applications of formal methods fall into two broad categories, descriptive and deductive. Descriptive methods employ formal specification languages, which provide for clear, unambiguous descriptions of requirements and other design artifacts. Deductive methods rely on a discipline that requires the explicit enumeration of all assumptions and reasoning steps. In addition, each reasoning step must be an instance of a small number of allowed rules of inference. The most rigorous formal methods apply these techniques to substantiate the reasoning used to justify the requirements, or other aspects of the design or implementation of a complex or critical system. The purpose of formal methods is to reduce reliance on human intuition and judgment in evaluating arguments. That is, deductive formal methods reduce the acceptability of an argument to a *calculation* that can, in principle, be checked by a tool, thereby replacing the inherent subjectivity of the review process with a repeatable exercise.

There are several areas where application of formal methods provides additional assurance in the design process. Although formal methods are applicable throughout the design process, increases in design assurance may be obtained by targeted application. The following list highlights some of the possibilities:

1. Formal methods may be applied at different stages of the development life cycle. Generally, applications of formal methods are most effective at the early stages of the life cycle, specifically during requirements capture and high-level design.

2. Formal methods may be applied to the entire design or they may be targeted to specific components. The FFPA is used to determine which FFPs to analyze with formal methods. Protocols dealing with complex concurrent communication and hardware implementing fault-tolerant functions may be effectively analyzed with formal methods.

3. Formal methods may be applied to verify system functionality or they may be used to establish specific properties. Although formal methods have traditionally been associated with "proof-of-correctness," that is, ensuring that a component meets its functional specification, they can also be applied to only the most important properties. Often, it is more important to confirm that a design does not exhibit certain undesirable properties, rather than to prove that it has full functionality.

Practical application of formal methods typically requires tool support. Tools used should be assessed and, if necessary, qualified as described in Section 11.4.

3.3.3.1 The Methodology of Formal Methods

The application of formal methods begins by expressing the requirements using a formal language. The requirement specification serves an important descriptive function. It provides a basis for documenting, communicating and prototyping the behavior and properties of a system using an unambiguous notation. In addition, the requirements specification serves as a basis for calculating or formally predicting system behavior. A formal model of the component to be analyzed is constructed using a formal language. The model is analyzed with respect to the formal statement of requirements using the rules of the selected formal logic. The characteristics of the model are determined by the style of formal analysis to be performed.

The level of detail in the component model is determined by the goal of the chosen formal analysis technique. Some approaches are tailored to finding design errors that may have eluded testing, while other approaches seek to guarantee the absence of certain classes of design errors.

1. **Error-Detection.** The most common formal technique for error detection is called model checking. Here the requirements are expressed as formula in a decidable temporal logic. The model of the component is an abstract state machine designed so that the property to be tested is preserved. The proof procedure is automatic. A failed proof attempt indicates a design error in the modeled component. The result of failed proof is a sequence of input stimuli that demonstrate specifically how the component does not satisfy the stated requirement.

2. **Error Preclusion.** Formal methods targeted to prevention of errors are generally based upon an expressive specification language with a supporting proof theory. With the increased expressiveness, more complicated requirements may be stated and more detailed models of the component may be constructed. However, the proof procedure may only be partially automated. An appropriate level of detail for the component model may be a synthesizable HDL description. In some cases, the same model may be used both for simulation and formal analysis. A completed proof is evidence that the component is logically correct with respect to the stated requirements for the analyzed input space.

3.3.3.2 Formal Methods Resolution

There are three possible outcomes of a deductive formal analysis:

1. If the proof attempt is successful, the verification activity is complete. The level of design assurance depends upon the fidelity of the models employed. For example, if the model of the hardware item corresponds to a detailed design, the proof provides assurance of functional correctness equivalent to that of exhaustive testing.

2. In some cases, a failed proof results in an explicit counter-example; that is, it identifies a test scenario to illustrate specifically how the design does not meet the stated requirements. This may indicate either a deficiency in the design or a deficiency in the requirements. Such deficiencies may be resolved by correcting the design, revising the requirements, shown to not be a physically realizable condition or using another method. All counter-examples should be identified so that they can be resolved. Changes to the design or requirements need to be reflected back to the appropriate process.

    a. After a design or requirement has been modified to address a deficiency identified by a failed proof attempt, the proof should be attempted again to confirm that the modification has successfully addressed the identified problems. This cycle is repeated until a successful proof is achieved.

    b. In cases where a counter-example is considered resolved without requirement or design changes but the tool identifies only one counter-example, that is, the resolved counter-example, the process should be modified so that it can identify all other counter-examples.

3. The most difficult case to resolve is when a proof cannot be produced and a counter-example cannot be identified. One possible option is to revise the design in order to simplify the verification effort. Alternatively, the verification activity may be decomposed with a clear delineation between the cases addressed by proof and those cases where the requirement needs to be addressed by some other means. Changes to the design and derived requirements should be reflected back to the FFPA.

3.3.3.3 Formal Methods Data

The data developed during the application of formal methods includes:

1. Description of the specific formal methods approach to be used and the components or FFPs to which formal methods will be applied.
2. Formal statement of requirements.
3. Formal models of the component.
4. Proof, or sufficiently detailed script to generate proof, relating the models of the component to the formal statement of requirements and including correlation in the traceability data.
5. Identification of tools employed and tool assessment results.
6. Identification of the verification test cases and requirements added or modified as a result of the analysis.
7. Statement of the level of the verification completeness achieved for the FFPs addressed by analysis. Include a list of the analysis discrepancies not resolved by modification to verification test cases or requirements and their rationale for acceptability of the discrepancies.

APPENDIX C

GLOSSARY OF TERMS

These definitions are provided for the terms as used in this document. If a term is not defined in this appendix, it may be defined in the associated body of text.

Acceptance - Acknowledgment by the certification authority that a submittal of data, argument or claim of equivalence satisfies applicable requirements.

Airworthiness - The condition of an item, which can be an aircraft, aircraft system or component, in which that item operates in a safe manner to accomplish its intended function.

Analysis - A process of mathematical or other logical reasoning that leads from stated premises to the conclusion concerning specific capabilities of equipment or hardware item and its adequacy for a particular application.

Anomalous Behavior - Behavior that is inconsistent with specified requirements.

Applicant - A person or organization seeking approval from the certification authority.

Application Specific Integrated Circuit (ASIC) - Integrated Circuits which are developed to implement a function, including, but not limited to: gate arrays, standard cell and full custom components encompassing linear, digital and mixed mode technologies.

Approval - The act or instance of expressing a favorable opinion or giving formal or official sanction.

Assembly - A number of components or any combination thereof, joined together to perform a specific function.

Assessment - An evaluation based upon engineering judgment.

Assumptions - Statements or principles offered without proof.

Assurance - The result of planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements.

Availability - Probability that an item or function is in an operable state.

Baseline - An identified and approved configuration that thereafter serves as the basis for further design, and that is changed only through change control procedures.

Certification - Legal recognition by the certification authority that a product, service, organization or person complies with the 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 documents as are 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 issuance of a certificate required by national laws to declare that compliance or conformity has been found with standards in accordance with the above two items.

Certification Authority - The organization or person responsible within the state or country concerned with the certification of compliance with the requirements.

NOTE: A matter concerned with aircraft, engine or propeller type certification or with equipment approval would usually be addressed by the certification authority; matters concerned with continuing airworthiness might be addressed by what would be referred to as the airworthiness authority.

Certification Basis - Defined by the Certification Authority in consultation with the Applicant, as the particular certification requirements, together with any special conditions which may supplement the published regulations, that become the basis for certification of the aircraft, engine, or propeller.

Certification Credit - Acceptance by the Certification Authority that a process, product or demonstration satisfies a certification requirement.

Change Control - (1) The process of recording, evaluating, approving or disapproving, and coordinating changes to configuration items after formal establishment of their configuration identity, or to a baseline after its establishment. (2) The systematic evaluation, coordination, approval or disapproval and implementation of approved changes in a configuration of a configuration item after formal establishment of its configuration identity or to baseline after its establishment.

Commercial Off-The-Shelf (COTS) Component - Component, integrated circuit or subsystem developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification.

NOTE: Examples of COTS components may include resistors, capacitors, microprocessors, unprogrammed Field Programmable Gate Array and Erasable Programmable Logic Devices, other integrated circuit types and their implementable models, printed wiring assemblies and complete LRUs which are typically available from a supplier as a catalog item.

Common Mode - Event which causes anomalous behavior of two or more items, subitems or functions.

Complex Hardware Item - All items that are not simple are considered to be 'complex'. See definition of Simple Hardware Item.

Compliance - Successful performance of all mandatory activities, agreement between the expected or specified result, and the actual result.

Component - A self-contained part, combination of parts, subassembly or unit that performs a distinct function of a system.

Component De-rating - This is a design method which increases the operational margins of components by imposing modified component usage limitations which are more restrictive than the usual or manufacturer's component operational ratings.

Concurrent Engineering - A process whereby multiple disciplines participate in the hardware design process in order to ensure that the unique requirements of each discipline are considered.

Configuration - A list of Configuration Items that completely defines an implementation of a function.

Configuration Identification -The process of defining and designating a Configuration Item.

Configuration Identity - The unique name given to a configuration item or to a configuration as the result of Configuration Identification.

Configuration Item - One or more components, tools or data items treated as a unit for configuration management purposes.

Configuration Management - (1) The process of Configuration Identification, and the control of issues and changes of Configuration Identities. (2) A discipline applying technical and administrative direction and surveillance to identify and record the functional and physical characteristics of a configuration item, control changes to those characteristics, and record and report change control processing and implementation status.

Conformance - Established as correct with reference to a standard, specification or drawing.

Conformity - Agreement of physical realization of the hardware item with the defining documents.

Coverage Analysis - The process of determining the degree to which a proposed hardware verification process activity satisfies its objective.

Defect - Any non-conformance of a characteristic with specified requirements.

Derived Requirement - Additional requirement resulting from the hardware design processes, which may not be directly traceable to higher level requirements.

Design Assurance – All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the hardware satisfies the application certification basis.

Design Margin Analysis - The process of determining that the sum effect of various hardware component design margins provides a product which meets or exceeds its performance requirements as well as requirements for producibility and service.

Design Process - The process of creating a hardware item from a set of requirements using the following set of processes: requirements capture, conceptual design, detailed design, implementation and production transition.

Design Tools - Tools whose output is part of hardware design and thus can introduce errors. For example, an ASIC router or a tool that creates a board or chip layout based on a schematic or other detailed requirement.

Equivalence Class – The partitions of the input space of a function such that a test of a representative value of the class is equivalent to a test of other values of the class.

Error - A mistake in requirements, design or implementation.

Exposure Time - The period of time between when a hardware item was last known to be operating properly and when it will be known to be operating properly again.

Failure - The inability of a system or system component to perform a required function within specified limits. A failure may be produced when a fault is encountered.

Failure Condition - The effect on the aircraft and its occupants both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operational and environmental conditions.

Failure Effect - (1) A description of the operation of an item as the result of a failure; (2) the consequences a failure mode has on the operation, function, or status of a system or an item.

Failure Mode - The way in which the failure of an item occurs.

Failure Rate - The total number of failures within an item population, divided by the total number of item power-on hours under stated conditions.

Fault - (1) A manifestation of a flaw in hardware due to an error or random event. A fault, if it occurs, may cause a failure. (2) An undesired anomaly in an item.

First Article - A unit submitted for inspection to verify the production drawings, tools and procedures.

First Article Inspection - A Process Assurance inspection that verifies that the hardware "as-built" conforms to the manufacturing process documentation. Performed on production hardware items representing first-off-the-line configuration as a precondition for production approval.

Functional Defects - Defects which cause hardware functions to operate incorrectly, even though a hardware physical failure has not occurred. Resultant incorrect hardware operation in turn may cause dependent software functions to operate incorrectly.

Functional Failure Path - The specific set of interdependent circuits that could cause a particular anomalous behavior in the hardware that implements the function or in the hardware that is dependent upon the function.

Functional Path - The specific set of interdependent circuits that implement a function.

Glitch – An input transition or voltage spike that occurs in a time period that is shorter than the delay through the affected logic that can propagate to the output.

Guidance - Advice or counseling for complying with certification requirements.

Hardware Design Life Cycle Process - One of the set of design or supporting processes determined by an organization to be sufficient for the design of a hardware item.

Hardware Description Language - HDL is used in this document to represent all of the Hardware Description Languages, including "Verilog HDL", Very High Speed Integrated Circuit Hardware Description Language and Analog Hardware Description Language.

Hardware Item - An item that has physical being. This generally refers to LRUs, circuit board assemblies, power supplies and components.

Hardware Partitioning - A method for enhancing reliability and safety by physical separation and isolation of the hardware that is implementing the functions, including redundancy, to prevent failure effects due to common faults.

Hardware/Software Integration - The joining of hardware and software to implement an application or function.

Independence - Separation of responsibilities which ensures the accomplishment of objective evaluation. Refers to intellectual independence, such as another individual, and not departmental or company independence.

1. For verification, independence is achieved by evaluation of the technical correctness of the data by means, either someone or something, other than those used to produce the data.
2. For process assurance, independence is achieved by evaluation of process compliance by means, either someone or something, other than those used to perform the process.

Implementation - The act of generating a physical reality from a specification.

Inspection - The examination and testing of supplies and services, including when appropriate, raw materials, components, intermediate assemblies and services, to determine whether they conform to specified requirements.

Integrated Circuit - A circuit consisting of elements inseparably associated and formed in-situ on or within a single substrate to perform an electronic circuit function.

Integrity - Attribute of an item indicating that it can be relied upon to perform the intended function.

Item -A general term used to refer to a subject hardware component, system or software.

Life Cycle - the period of time between starting the design or modification of a hardware item and completing the design or modification up as far as transition to production.

NOTE: In this document, unless defined otherwise in the text, this means "Hardware Design Life cycle"

Maintainability - A characteristic of design and installation which is expressed as the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Malfunction -The occurrence of a condition whereby the operation is outside specified limits.

Manufacturability - Product design features which facilitate economic mass production by optimizing materials and manufacturing tools and by employing design techniques which minimize the impact of component variations on functionality.

Means of Compliance - The methods to be used by the applicant to satisfy the requirements stated in the certification basis for an aircraft or engine. Examples include statements, drawings, analyses, calculations, testing, simulation, inspection and environmental qualification. Advisory material issued by the certification authority is used if appropriate.

Monitoring - (1) **Safety.** Functionality within a system that is designed to detect anomalous behavior of that system. (2) **Process Assurance.** The act of witnessing or inspecting selected instances of test, inspection, or other activity, or records of those activities, to assure that the activity is under control and that the reported results are representative of the expected results. Monitoring is usually associated with activities done over an extended period of time where 100% witnessing is impractical or unnecessary. Monitoring permits authentication that the claimed activity was performed as planned.

Over-stress defects - Defects which either cause a component to exceed rated design limits or result from over-stress encountered during the hardware design life cycle.

Part Number - A set of numbers, letters or other characters used to identify a configuration item, a configuration identity.

Planning Process – A process to define and coordinate the activities of the hardware design and support processes.

Preliminary System Safety Assessment – A systematic evaluation of a proposed system architecture and its implementation, based on the functional hazard assessment and failure condition classification, to determine safety requirements for all items in the architecture.

NOTE: A Preliminary Systems Safety Assessment applies to the system under development. It is used to direct further safety analysis activity required to complete the final system safety assessment.

Process - A set of interrelated activities performed to produce a prescribed output or product.

Process Assurance – The objective of process assurance is to ensure that plans are followed, hardware design life cycle process objectives are met and activities have been completed.

Product - Hardware, software, item or system generated in response to a defined set of requirements.

Product Service Experience - A period of time during which the hardware is operated within a known environment and during which successive failures are recorded.

Production -Manufacture of product by a documented and controlled sequence of processes.

Programmable Logic Device (PLD) - A component that is purchased as an electronic component and altered to perform an application specific function. PLDs include, but are not limited to, Programmable Array Logic components, Programmable Logic Array components, General Array Logic components, Field Programmable Gate Array components and Erasable Programmable Logic Devices.

Prototype - A pre-production hardware item that is fully representative of the final product using approved components and suitable for complete evaluation of form, design and performance.

Release – The act of formally placing the data of a hardware item under configuration control.

Reliability - The probability that an item will perform its intended function for a specified interval under stated conditions.

Reliability Defects - Defects that cause hardware to fail at an excessive rate when subjected to stress conditions not exceeding rated design limits. Both over-stress defects and reliability defects may be manifested as excessive random failure rate, excessive infant mortality or excessive wear-out rate.

Requirement - An identifiable element of a specification that is verifiable.

Reverse Engineering - Re-implementation of a hardware item by study of its construction, function and performance within a particular environment.

Review - Qualitative evaluation to assess the plans, requirements, design data, design concept or design implementation to demonstrate to a high degree of confidence that the requirements have been or will be met.

Risk - The combination of the frequency and the consequence of a specified hazardous state.

Robustness Defects - Defects that cause hardware to fail or operate incorrectly when subjected to stress conditions and service life not exceeding design limits. Results of these defects may include susceptibility to environmental stress and instability over service life.

Safety - The state in which risk is lower than the boundary risk. The boundary risk is the upper limit of the acceptable risk. It is specific for a technical process or state. The risk is defined by the rate or probability of occurrence and the expected damage or injury.

Similarity - Applicable to systems comparable in characteristics and usage to systems used on an airplane previously certificated by the applicant. It is further assumed that there are no parts of the subject system are more at risk due to environment or installation and that operational stresses are no more severe than on the analogous system.

Simple Hardware Item - A hardware item is considered simple if a comprehensive combination of deterministic tests and analyses can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior.

Simulator - A device, computer program or system used during hardware verification, that accepts the same inputs and produces the same output as a given system.

Software - Computer programs and, possibly associated documentation and data pertaining to the operation of a computer system.

Specification - A collection of requirements that, when taken together, constitute the criteria which define the functions and attributes of an item.

Standard - A rule or basis of comparison used to provide both guidance in and assessment of a given activity or the content of a specified data item.

Structure - A specified arrangement or interrelation of parts to form a whole.

Supporting Process – A process used to support the design process consisting of one of the following set of processes: validation, verification, configuration management, process assurance and certification liaison.

System Architecture - The structure of the hardware and the software selected to implement the system requirements.

System - A collection of hardware and software components organized to accomplish a specific function or set of functions.

System Safety Assessment (SSA) - An ongoing, systematic, comprehensive evaluation of the proposed system to show that relevant safety requirements are satisfied.

Test - A quantitative procedure to prove performance using stated objective criteria with pass/fail results.

- Hardware Item. To determine its performance characteristics while functioning under controlled conditions.
- Electronic digital computation. To ascertain the state or condition of an element, component, program, etc.
- Sometimes used as a general term to include both check and diagnostic procedures.
- Loosely, same as check.
- Is an element of inspection and generally denotes the determination by technical means of the properties of elements of supplies, or comments thereof, including functional operation, and involves the application of established scientific principles and procedures.

Testability - (1) The ability to test a hardware item sufficiently to guarantee that all possible states of the hardware item performs to its specification. (2) The ease with which a hardware item can be tested to provide evidence of compliance with its requirements.

Testing - The process of verifying the performance of a hardware item.

Test Procedure - Detailed instructions for controlling the conditions for executing a given set of tests.

Tool Assessment - A set of activities to assess the tools used in the design and verification of the hardware item to provide confidence that the tool is capable of performing its functions correctly consistent with the design assurance level of the functions to be performed by the hardware item.

Tool Qualification - The process necessary to obtain certification credit for a tool within the context of a specific airborne system.

Traceability - An identifiable association between hardware items or processes, such as between a requirement and the source of the requirement or between a verification method and its base requirement.

Upset - Interference caused by external events, such as lightning or other environmental events.

Validation - The process of determining that the requirements are the correct requirements and that they are complete.

Verification - The evaluation of an implementation of requirements to determine that they have been met.

Verification Tool - Tools used to ensure performance against predetermined standards or requirements. These tools do not introduce errors, but may fail to detect them. For example, an analog or digital circuit simulator or an automated test that measures actual circuit performance.

APPENDIX D

ACRONYMS

ALU	Arithmetic Logic Unit
ARP	Aerospace Recommended Practice
ASIC	Application Specific Integrated Circuit
HC1	Hardware Control Category 1
HC2	Hardware Control Category 2
COTS	Commercial-Off-The-Shelf
EUROCAE	European Organization for Civil Aviation Equipment
FAR	Federal Aviation Regulations
FFP	Functional Failure Path
FFPA	Functional Failure Path Analysis
FHA	Functional Hazard Assessment
F-FMEA	Functional Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HDL	Hardware Description Language
JAR	Joint Aviation Requirements
LRU	Line Replaceable Unit
PHAC	Plan for Hardware Aspects of Certification
PLD	Programmable Logic Device
PSSA	Preliminary System Safety Assessment
RTCA	RTCA, Inc.
SAE	Society of Automotive Engineers
SC	Special Committee
SSA	System Safety Assessment
WG	Working Group

MEMBERSHIP

EUROCAE WG-46/RTCA SC-180

Chairmen:

EUROCAE WG-46	Arnaud Demichelis	DGA/SPAe (FR)
RTCA SC-180	Robert Clark	Honeywell, Inc.
RTCA SC-180	Lee Johnson	Rockwell Collins, Inc.

Secretaries:

EUROCAE WG-46	William Betts	Lucas Electronics (UK)
EUROCAE WG-46	Cleland Newton	DERA (UK)
RTCA SC-180	Connie Beane	Federal Aviation Administration

EUROCAE Representative:	**RTCA Representative:**
Francis Grimal	Jack Cattilini
Geoffrey Hunt	Jerry Bryant
	Rudy Ruana

Joint Team 1 Co-Chairs:

Jacques Azum	Aerospatiale
Denis Mayfield	Boeing Commercial Airplane Group

Joint Team 2 Co-Chairs:

Ken Hunt	British Aerospace Airbus
Ted Parker	Honeywell, Inc.

Joint Team 3 Co-Chairs:

Brian Davis	Smiths Industries
David Richter	Rockwell Collins, Inc.

Joint Team 4 Co-Chairs:

David Austin	AlliedSignal
Francis Capecchi	Aerospatiale

Editorial Team:

Connie Beane	Federal Aviation Administration
Steven Beland	Boeing Commercial Airplane Group
Thierry Bickard	SNECMA
Francis Capecchi	Aerospatiale
Arnaud Demichelis	DGA/SPAe (FR)
Ken Hunt	British Aerospace Airbus
Lee Johnson	Rockwell Collins, Inc.
Thomas Neveling	Daimler Chrysler Aerospace Airbus
Cleland Newton	DERA (UK)
Ted Parker	Honeywell, Inc.
Dave Richter	Rockwell Collins, Inc.
William Struck	Federal Aviation Administration
Chris Wilkinson	Smiths Industries
Timothy Zimmerman	Cessna

MEMBERS

Ian Alderton	Ultra Electronics, Ltd.
Jozef van Baal	RLD
Barry Beaman	Woodward Governor Co.
Denys Bernard	Aerospatiale
Barbara BonJour	Boeing - Commercial Avionics Systems
Carmine Cifaldi	RAI
Christophe Conge	Dassault Aviation
Joe Costello	Rockwell Collins, Inc.
Rich Cuplin	Woodward Governor Co.
Dale Davidson	Honeywell, Inc.
Mike DeWalt	Certification Services, Inc.
William Donoghue	Pratt & Whitney
Cheryl Dorsey	Digital Flight
Joseph Eller	Liebherr-Aerospace
Brian Estep	Interstate Electronics Corp.
Bob Friday	AlliedSignal
Francois Gaffard	Intertechnique
Antoine Gautier	Dassault Aviation
John Glass	Smiths Industries
Bernard Gonzales	Bombardier Aerospace – Learjet, Inc.
Nathalie Goubert	STTE
Bill Greenleaf	Rockwell Collins, Inc.
Olivier Humez	Sextant Avionique
David Kirkland	Boeing Commercial Airplane Group
Tony Lambregts	Federal Aviation Administration
Dave Larkman	Boeing - Commercial Avionics Systems
Douglas Lee	Transport Canada
Michel Le Pimpec	Intertechnique
Brian Lucas	Proteus Corporation
Robert Maitan	Proteus Corporation
Joseph McHugh	ILC Data Device Corp.
Michael Miller	Honeywell, Inc.
Paul Miner	NASA, Langley Research
Ian Newton	GEC-Marconi Avionica
Jean Ofanowski	Dassault Aviation
Tom Olson	Rockwell Collins, Inc.
Steven Paasch	Certification Services, Inc.
Pascal Pampagnin	Aerospatiale
Chandrakant Patel	Litton Aero Products

Gerald Pilj	Bombardier Aerospace – Learjet, Inc.
Christian Pitot	Sextant Avionique
Benard Pro	AlliedSignal EAS
Misha Radich	Woodward Governor Co.
Leanna Rierson	Federal Aviation Administration
David Sandefur	Cessna
Paul Sapp	Universal Avionics Systems
Pete Saraceni	Federal Aviation Administration
Dennis Schmidt	Bombardier Aerospace – Learjet, Inc.
Kenneth Schmidt	Westinghouse ESG
Brian Shumaker	Proteus Corporation
Bruce Smith	Rockwell Collins, Inc.
Larry Smith	Honeywell, Inc.
Michael C. Smith	Ametek Aerospace
Pascal Thibault	Intertechnique
Laurie Thompson	Honeywell, Inc.
Jack Thornton	Rockwell Collins, Inc.
James Treacy	Federal Aviation Administration
Bertrand Voisin	Dassault Aviation
Kirk Walworth	Hamilton Sundstrand
Carl Ward	Lockheed Martin Aeronautical Systems
Brian Watkins	Bombardier Aerospace – Learjet, Inc.
Larry Yount	Honeywell, Inc.

The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Equipement de l'Aviation Civile

RECOMMANDATIONS POUR L'ASSURANCE CONCEPTION DE MATERIEL ELECTRONIQUE DE BORD

ED-80

Avril 2000

102 rue Etienne Dolet
92240 Malakoff, France
Web Site: www.eurocae.net

Tel: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net

RECOMMANDATIONS POUR L'ASSURANCE CONCEPTION DE MATERIEL ELECTRONIQUE DE BORD

ED-80

Avril 2000

PREFACE

1. Le présent document préparé par le Groupe de Travail 46 d'EUROCAE a été approuvé par le Comité de Direction en avril 2000.

2. EUROCAE est une organisation internationale à but non lucratif. Peuvent en être membres les utilisateurs et les fabricants en Europe d'équipements destinés à l'aéronautique, les associations professionnelles, les administrations d'aviation civile, et, sous certaines conditions, des membres non européens. Son programme de travail est principalement orienté vers l'élaboration des spécifications de performance et des directives relatives aux équipements de l'aviation civile pour leur adoption et leur emploi aux niveaux européen et mondial.

3. Les décisions d'EUROCAE sont prises après discussion entre ses membres et en collaboration avec RTCA Inc., Washington D.C, USA et/ou SAE (Society of Automotive Engineers), Warrendale, PA, USA, par l'intermédiaire de leurs comités appropriés.

4. Ce document a été élaboré conjointement avec RTCA SC-180 et est identique au RTCA DO-254.

5. Les spécifications de performances d'EUROCAE ne constituent que des recommandations. EUROCAE n'est pas un organisme officiel des gouvernements européens; ses recommandations, par conséquent, ne sont validées en tant que positions officielles que lorsqu'elles sont adoptées par un gouvernement particulier ou par une conférence de gouvernements.

6. Des exemplaires de ce document peuvent être obtenus sur demande à:

EUROCAE
102 rue Etienne Dolet
92240 Malakoff
France

Tel: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
E-mail: eurocae@eurocae.net
Web site: www.eurocae.net

RESUME

Le développement et l'utilisation de matériel électronique complexe par l'industrie aéronautique a amené de nouveaux problèmes en terme de sûreté et de certification. Pour y répondre les groupes de travail EUROCAE WG-46 et RTCA SC-180 ont été constitués. Ils se sont ensuite associés dans un même Comité dès le début de l'élaboration du document. Ce Comité commun a été mandaté pour élaborer des recommandations claires et cohérentes pour la conception de matériel électronique de bord, afin qu'il effectue de manière sûre les fonctions attendues.

L'expression "matériel électronique de bord" concerne les unités remplaçables en ligne, les assemblages sur cartes, les circuits intégrés spécifiques à une application, les composants logiques programmables, etc. Ces recommandations sont applicables aux technologies existantes, nouvelles, et à venir.

Les recommandations de ce document sont destinées aux fabricants d'aéronef et aux fournisseurs d'articles matériels électroniques à utiliser dans les systèmes d'aéronefs. Les processus du cycle de vie de la conception du matériel sont identifiés. Les objectifs et les activités de chaque processus sont décrits. Les recommandations sont applicables à tous les niveaux d'assurance conception, tels que définis par l'évaluation de la sûreté du système.

Lors de l'élaboration de ce document le Comité a pris en compte d'autres documents propres à l'industrie, notamment les documents EUROCAE ED-79 (ARP 4754) « Considérations sur la Certification des Systèmes de Bord à Haute Intégration ou Complexes, « SAE ARP 4761 » » Guide et Méthodes pour la Conduite du Processus d'Evaluation de la Sécurité des Systèmes et Equipements de Bord Civils, et EUROCAE ED-12/RTCA DO-178, « Considérations sur le Logiciel en vue de la Certification des Systèmes et Equipements de Bord ».

TABLE DES MATIERES

CHAPITRE 1

INTRODUCTION

L'utilisation de matériel électronique toujours plus complexe pour un plus grand nombre de fonctions critiques d'un aéronef au plan de la sécurité, crée de nouveaux défis en ce qui concerne la sûreté et la certification. Ces défis résultent de la vulnérabilité croissante des fonctions de l'aéronef vis à vis des effets dangereux des erreurs de conception, celles-ci pouvant être de plus en plus difficiles à gérer en raison de la complexité croissante du matériel. Pour contrebalancer l'augmentation perçue du risque, il est devenu nécessaire de garantir que l'éventualité des erreurs de conception du matériel soit prise en compte de manière plus cohérente et vérifiable au cours des processus de conception et de certification.

Ce document sera révisé et revu en accord avec les procédures EUROCAE/RTCA, au fur et à mesure de l'expérience acquise par son application de l'évolution de la technologie et de la complexité du matériel électronique de bord.

1.1 BUT

Ce document a été préparé pour aider les organisations en leur fournissant des recommandations pour l'assurance conception du matériel électronique de bord, de telle sorte que celui-ci exécute de manière sûre les fonctions attendues, dans les environnements spécifiés. Ces recommandations devraient être applicables aux technologies existantes, nouvelles et à venir. Les buts de ce document sont de:

1. Définir les objectifs de l'assurance conception.
2. Décrire les fondements de ces objectifs pour aider à garantir une interprétation correcte des recommandations.
3. Donner des descriptions de ces objectifs pour permettre le développement de moyens de mise en conformité à partir de ces recommandations ou d'autres recommandations.
4. Donner des recommandations propres aux activités d'assurance conception, pour satisfaire aux objectifs d'assurance conception.
5. Autoriser la flexibilité dans le choix des processus nécessaires pour satisfaire aux objectifs de ce document, y compris à leurs améliorations, avec l'arrivée des nouvelles technologies.

Ce document recommande des activités qui seraient susceptibles de satisfaire aux objectifs d'assurance conception, au lieu de détailler la façon dont la conception devrait être implémentée.

Ce document de directives utilise une approche descendante s'appuyant sur les fonctions système implémentées par le matériel électronique, et non une approche montante, ou encore s'appuyant uniquement sur les composants matériels spécifiques utilisés pour implémenter la fonction. Une approche descendante est plus efficace pour traiter les erreurs de conception impactant la sécurité, en facilitant des décisions avisées pour la conception du système et du matériel, ainsi que la pertinence et l'efficacité du processus de vérification. Par exemple, la vérification devrait être réalisée au niveau hiérarchique le plus élevé du système, de l'ensemble et du sous-ensemble, du composant, ou de l'article matériel, auquel la conformité de l'article matériel à ses exigences peut être obtenue et les objectifs de la vérification satisfaits.

1.2 DOMAINE D'APPLICATION

Ce document donne des recommandations pour l'assurance conception du matériel électronique de bord depuis la conception jusqu'à la certification initiale, ainsi que sur les améliorations post-certification, pour garantir le maintien de la navigabilité. Il a été élaboré en s'appuyant sur la démonstration de conformité aux exigences de certification des aéronefs et équipements dans la catégorie transport. Néanmoins des parties de ce document peuvent être appliquées à d'autres équipements.

La relation entre le cycle de vie du système et celui de la conception du matériel est décrite pour aider à la compréhension des interdépendances des processus d'assurance conception du système et du matériel. Il n'est pas prévu de faire une description détaillée du cycle de vie du système comprenant l'évaluation (SSA) et la validation de la sécurité du système, ni du processus de certification de l'aéronef.

Les problèmes de la certification ne sont abordés que par leurs relations avec le cycle de vie de la conception du matériel. Les aspects concernant l'aptitude à produire, tester et maintenir l'article matériel ne sont uniquement traités que dans la mesure ou ils sont liés à la navigabilité de la conception du matériel.

Les recommandations sont applicables, mais non limitées, aux:

1. Unités Remplaçables en Ligne (LRU).
2. Assemblages sur cartes.
3. Composants microcodés personnalisés tels que les Circuits Intégrés pour Applications Spécifiques (ASICs), les Composants Logiques Programmables (PLDs), y compris toutes les macrofonctions associées.
4. Composants à technologie intégrée tels que les circuits hybrides et les modules multipuces.
5. Composants du Commerce sur Etagère (COTS).

Des considérations complémentaires concernant spécifiquement les COTS sont données au Chapitre 11, car les fournisseurs de ces composants ne suivent pas nécessairement les processus de conception décrits dans ce document ou ne fournissent pas les données du cycle de vie demandées.

Ce document ne se propose pas de définir le "firmware". Le "firmware" devrait être classé comme du matériel ou du logiciel et traité par les processus qui lui sont applicables. Ce document suppose que lors de la définition du système, les fonctions ont été attribuées soit au matériel soit au logiciel. Le document EUROCAE ED-12 donne des recommandations pour les fonctions allouées à une implémentation logicielle. Ce document donne des recommandations pour l'implémentation de fonctions allouées au matériel.

NOTA : Ceci permet de déterminer une méthode efficace d'implémentation et d'assurance conception, lorsque le système est spécifié et que les fonctions lui sont allouées. Tous les intervenants devraient avoir accepté les décisions prises au niveau du système lorsque cette allocation est faite.

L'évaluation et la qualification des outils utilisés pour la conception et la vérification d'un article matériel sont traitées au Chapitre 11.4.

Ce document ne fournit pas de recommandations ni en ce qui concerne les structures organisationnelles ni sur la façon dont les responsabilités sont réparties dans ces structures.

Les critères de qualification environnementale sont également hors du domaine couvert par ce document.

1.3 RELATION AVEC LES AUTRES DOCUMENTS

En plus des exigences de navigabilité, il existe différents standards nationaux et internationaux pour le matériel. Dans certains cas la conformité à ces standards peut être demandée. Cependant, le but de ce document n'est pas de faire référence à des standards nationaux ou internationaux spécifiques, ou de proposer les moyens par lesquels ces standards pourraient être utilisés en tant qu'alternative ou complément.

Lorsque ce document utilise le terme règle, cela doit être interprété comme signifiant l'utilisation de règles spécifiques au projet telles que celles utilisées par les constructeurs de systèmes de bord, d'équipements de bord, de moteurs, ou d'aéronefs. De telles règles peuvent être déduites de règles générales produites ou adoptées par le constructeur. Des recommandations relatives aux règles sont données au Paragraphe 10.2.

1.4 DOCUMENTS APPARENTES

EUROCAE ED-79/SAE ARP 4754, Considérations sur la Certification des Systèmes de Bord à Haute Intégration ou Complexes, document de recommandations propres au développement de systèmes d'aéronefs complexes ou hautement intégrés.

SAE ARP 4761, Guide et Méthodes pour la Conduite du Processus d'Evaluation de la Sécurité des Systèmes et des Equipements de Bord Civils, méthodes d'évaluation de la sécurité à utiliser pour le processus d'assurance conception du matériel.

EUROCAE ED-12/RTCA DO-178, Considérations sur le Logiciel en Vue de la Certification de Systèmes et Equipements de Bord, document complémentaire pour l'assurance développement du logiciel.

EUROCAE ED-14/RTCA DO-160, Conditions d'Environnemental et Procédures d'Essais pour les Equipements de Bord, document pouvant être utilisé par les concepteurs d'équipement comme norme primaire de test environnemental pour la qualification d'un article matériel.

1.5 COMMENT UTILISER CE DOCUMENT

Ce document est destiné à une utilisation par la communauté aéronautique internationale. Dans ce but les références à des procédures et règlements nationaux spécifiques sont minimisées et, des termes génériques sont utilisés. Par exemple, la terminologie Autorité de Certification est utilisée dans le sens d'organisation ou de personne qui approuve au nom des responsables nationaux de la certification. Lorsque un second pays ou groupe de pays valide ou participe à cette certification, ce document peut être utilisé, avec la reconnaissance dûment attribuée aux accords bilatéraux ou protocole d'accord entre les pays concernés.

Les recommandations de ce document constituent un consensus de la communauté aéronautique et un recueil des meilleures pratiques de l'industrie pour l'assurance conception du matériel électronique de bord. Pour la prise en compte du processus qui est développé, la ligne directrice a été de produire des recommandations qui devraient être appliquées à des développements entièrement nouveaux ainsi qu'à leurs modifications ultérieures. Les recommandations relatives aux matériels développés auparavant conformément à d'autres processus sont traitées au Paragraphe 11.1. Il est entendu que des moyens autres que ceux décrits ici peuvent être disponibles et être utilisés par le postulant.

Lorsque des exemples sont utilisés pour soutenir une recommandation soit au moyen de schémas, soit de descriptions, ces exemples ne doivent pas être compris comme étant la méthode préférentielle.

Le Chapitre 11 propose des considérations complémentaires pour des situations spécifiques connues, lorsque certains objectifs des Chapitres 2 à 9 ne peuvent pas être satisfaits. Elles consistent en des recommandations sur l'utilisation des matériels développés auparavant et des composants COTS, sur l'expérience en exploitation des produits, et sur l'évaluation et la qualification des outils.

L'Annexe A fournit des recommandations sur les données du cycle de vie de la conception à produire en fonction du niveau d'assurance conception du matériel qui est recherché.

L'annexe B contient des recommandations sur les techniques d'assurance conception à appliquer en complément des recommandations des Chapitres 2 à 11 lorsque l'on implémente des fonctions de niveau A et B. L'Annexe B peut être utilisée pour des matériels de niveau d'assurance conception C et D à la convenance du postulant.

Le Glossaire des Termes utilisés dans ce document se trouve en Annexe C. L'Annexe D contient une liste des acronymes utilisés et la désignation complète de leur dénomination.

Une liste ne signifie pas que tous ses éléments sont complets dans tous les cas, ou que tous ses éléments sont pertinents pour n'importe quel produit spécifique.

Les notes sont utilisées dans ce document afin de fournir le matériau explicatif, de développer un point, ou d'attirer l'attention sur des sujets apparentés qui ne sont pas totalement dans le contexte. Les notes ne contiennent pas de recommandations.

Le texte anglais utilise l'auxiliaire "Should" dans l'intention de fournir des recommandations, "May" est utilisé dans les textes proposant des options.

Ce document utilise le terme "article matériel" pour décrire le matériel électronique objet de ce document;

Le qualificatif "matériel" est supposé s'appliquer à tout le document, sauf spécification contraire. Lorsque le terme "exigences" est utilisé, il est supposé signifier "exigences du matériel". Le qualificatif système ou logiciel sera toujours exprimé explicitement, par exemple "exigence du système".

NOTA : Les différents documents d'information de l'industrie et les documents d'exigences aéronautiques n'utilisent pas toujours une terminologie harmonisée. Par exemple, la Réglementation de l'Aviation Fédérale (FAR) 21 et les exigences de l'Aviation Européenne (JAR) 21 utilisent le terme "produit" pour désigner un aéronef, un moteur d'aéronef, ou une hélice. Le document EUROCAE ED-79/SAE ARP4754 utilise le terme "produit" afin de désigner le matériel, le logiciel, l'article ou le système créé en réponse à un ensemble d'exigences défini. Il est demandé au lecteur d'être averti de ces différences ainsi que de toutes les autres dans l'utilisation de la terminologie. Ce document utilise les définitions du glossaire.

1.6 CONSIDERATIONS SUR LA COMPLEXITE

Bien que différents niveaux classifications du terme complexité soient utilisés pour décrire des systèmes électroniques, tels que simple, complexe et hautement complexe, la différentiation n'est pas rigoureusement définie. La définition de différents niveaux de complexité est basée ici sur la faisabilité et sur le niveau de difficulté pour obtenir une vérification acceptable par des moyens déterministes.

Le matériel devrait être examiné hiérarchiquement au niveau des circuits intégrés, des cartes et des LRU, en ce qui concerne la complexité y compris la prise en compte de fonctions qui peuvent ne pas être testables, tels que les modes non activés pour les dispositifs à utilisations multiples et les états potentiellement cachés des machines séquentielles.

Un article matériel est dit simple uniquement lorsqu'une combinaison de cas tests détaillés et d'analyses déterministes appropriés au niveau d'assurance conception est capable de garantir des performances fonctionnelles correctes, et sans comportements anormaux dans toutes les conditions opérationnelles prévisibles.

Lorsqu'un article matériel ne peut pas être classé simple il doit être classé complexe. Un article entièrement construit à partir d'articles simples peut être lui-même complexe. Les articles qui contiennent un dispositif tel qu'un ASIC ou un PLD, peuvent être considérés comme simple s'ils satisfont aux critères de simplicité décrits dans ce paragraphe.

Pour les articles complexes, les moyens proposés pour l'obtention de l'assurance conception devraient être acceptés par l' autorité de certification au début du cycle de vie du matériel, afin de réduire les risques inhérents au programme.

Les processus transverses de vérification et de gestion de la configuration doivent être réalisés et documentés pour des articles matériels simples, mais une documentation détaillée n'est pas nécessaire. Par conséquent, pour la conception d'un article matériel simple, il est demandé peu de documentation générique pour satisfaire à ce document. Ce document vise essentiellement à la conception d'articles matériels complexes.

1.7 METHODES OU PROCESSUS ALTERNATIFS

Des méthodes et des processus autres que ceux décrits dans ce document peuvent être utilisés afin de pourvoir à l'assurance conception du matériel. Ces processus et méthodes devraient être évaluées en fonction de leur capacité à satisfaire les règlements applicables. Les méthodes ou les processus alternatifs devraient être approuvés par l'autorité de certification préalablement à leur mise en œuvre. En lieu et place d'une comparaison directe avec les règlements applicables, le postulant pourrait utiliser les recommandations qui suivent afin de réduire les risques pour le programme quand il évalue les méthodes ou processus alternatifs par comparaison avec ce document.

Les considérations pour l'évaluation des méthodes ou des processus alternatifs peuvent inclure:

1. La démonstration d'un niveau d'assurance comparable lorsque les processus utilisés à la place de ceux décrits par ce document satisfont à un ou plusieurs objectifs des Chapitres 2 à 9.
2. L'évaluation de l'effet des méthodes ou processus alternatifs proposés, vis à vis de la satisfaction des objectifs de l'assurance conception du matériel.
3. L'évaluation de l'effet des méthodes et processus alternatifs proposés sur les données du cycle de vie.
4. Le raisonnement sur lequel s'appuie l'utilisation des méthodes ou processus alternatifs pour apporter la preuve que ces méthodes ou processus produiront les résultats escomptés.

1.8 VUE D'ENSEMBLE DU DOCUMENT

La Figure 1.1 est une représentation illustrée des chapitres de ce document, de certaines relations entre les chapitres et vers des processus apparentés. Il ne fait pas partie du propos de montrer le flux des données, mais plutôt de montrer quels sont les chapitres et les processus externes qui sont liés.

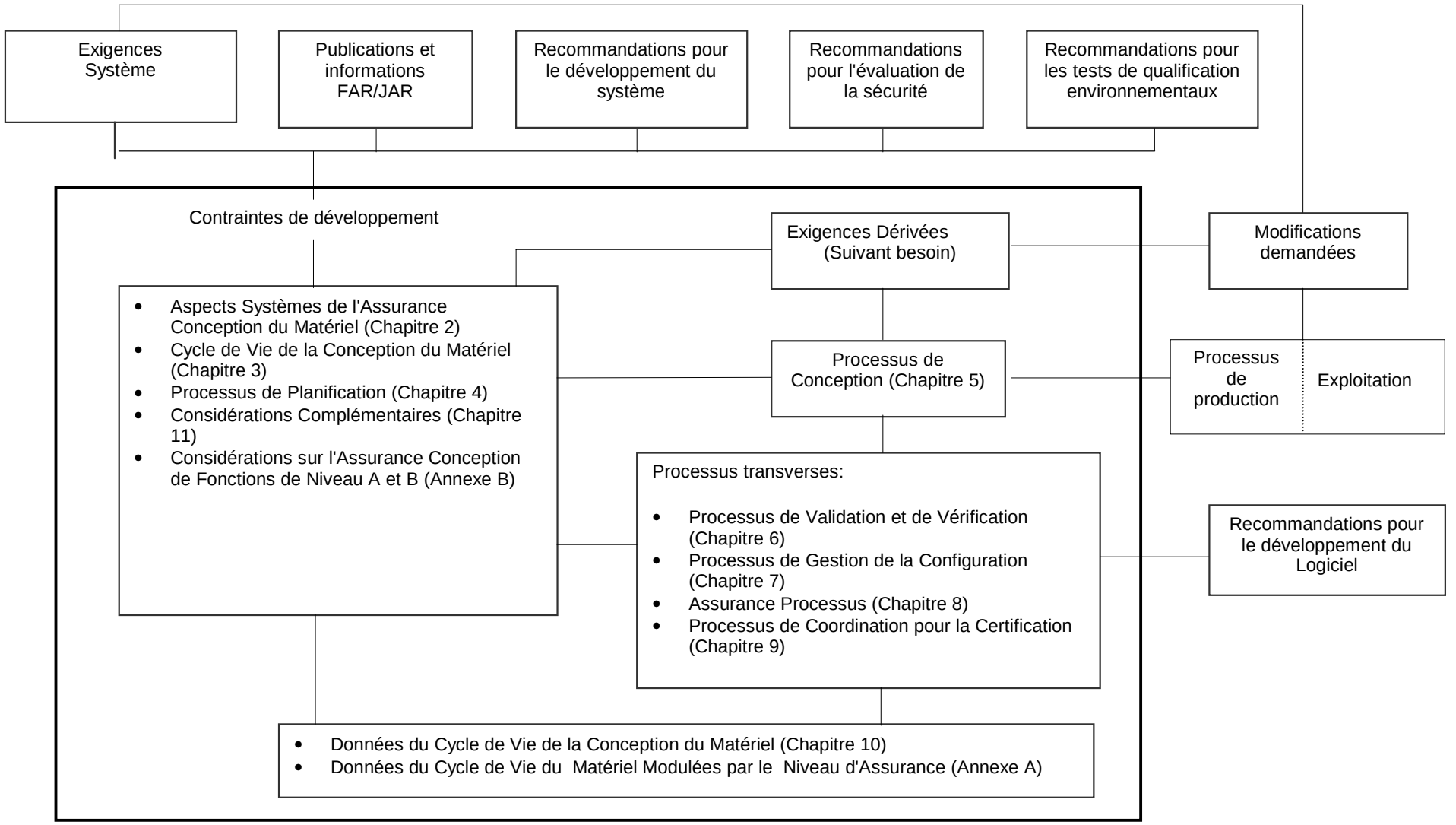


FIGURE 1-1 : VUE GENERALE DU DOCUMENT

CHAPITRE 2

ASPECTS SYSTEME DE L'ASSURANCE CONCEPTION DU MATERIEL

L'assurance conception du matériel commence au niveau du système par l'attribution au matériel des fonctions et par l'affectation du niveau d'assurance développement correspondant du système.

Une fonction donnée du système peut être affectée à un article matériel, à un composant du logiciel ou à une combinaison de matériel et de logiciel. Les exigences de sécurité associées à la fonction sont abordées dans une optique système, une optique logiciel et une optique matériel, afin de déterminer les niveaux de fiabilité et d'assurance nécessaires pour satisfaire à ces exigences.

La Figure 2-1 montre les relations du processus de développement du système pour les systèmes et équipements de bord avec les évaluations de la sécurité, et les processus de développement du matériel et du logiciel.

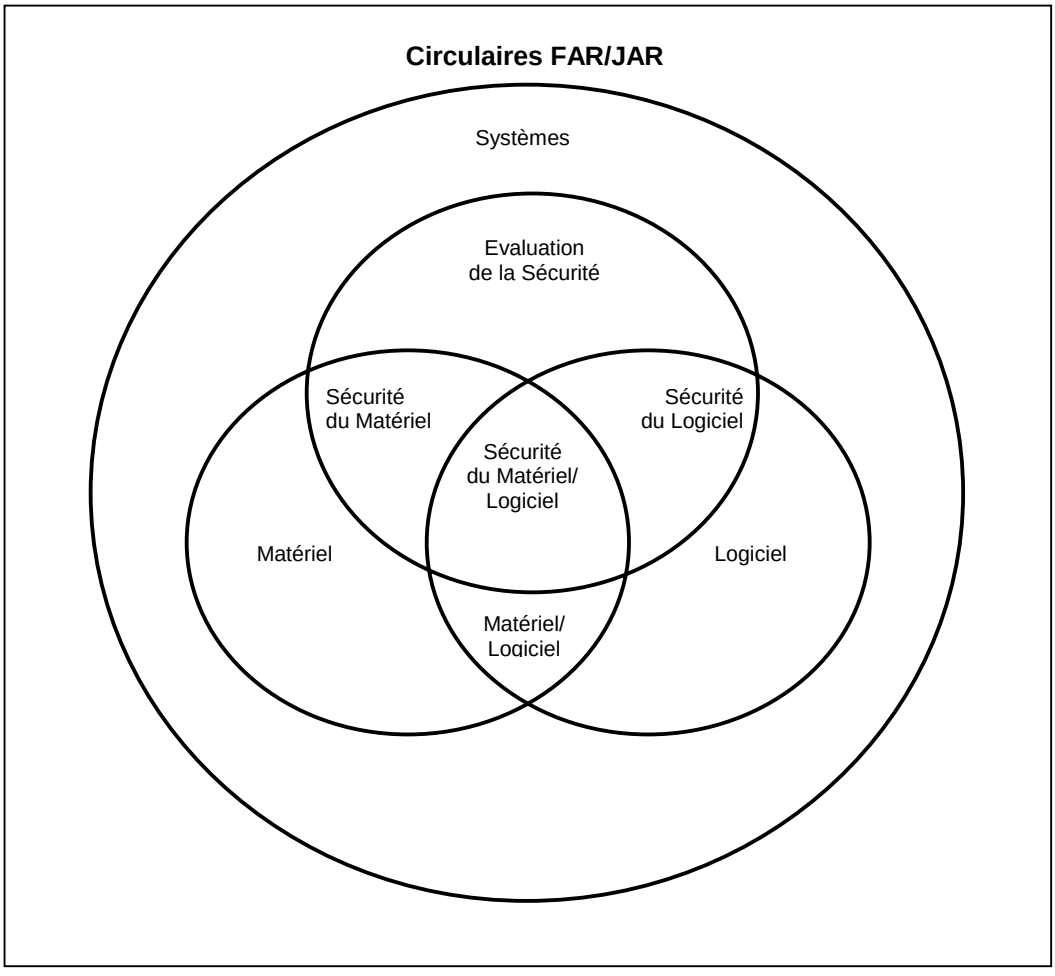


FIGURE 2-1 : RELATIONS ENTRE LES PROCESSUS DES SYSTEMES DE BORD, D'EVALUATION DE LA SECURITE, DU MATERIEL ET DU LOGICIEL

La figure comporte quatre zones de superposition, Sécurité du Matériel, Sécurité du Logiciel, Matériel/Logiciel et Sécurité du Matériel/Logiciel. Ces superpositions illustrent les relations et les interactions entre ces processus, lorsqu'une exigence du système peut être traduite en exigences dans ce domaine et en recommandations d'assurance conception concernant les processus multiples. Par exemple, une fonction du matériel qui comporterait des exigences de sécurité impliquerait à la fois les processus d'évaluation de la sécurité et du cycle de vie de la conception du matériel.

Ces superpositions illustrent le besoin d'une coordination interactive entre les processus afin de garantir que les exigences d'assurance de la fonction du système sont satisfaites. Les considérations sur l'assurance processus du système ou du logiciel sont en dehors du cadre de ce document. Cependant par la coordination des actions d'assurance conception d'une fonction du matériel, le postulant peut prétendre au bénéfice de l'assurance obtenue par les activités liées aux processus du système et du logiciel.

Ces relations et interdépendances sont décrites aux Paragraphes 2.1.1 à 2.1.3.

2.1 FLUX D'INFORMATION

Le flux d'information entre les processus du cycle de vie est montré à la Figure 2.2. Les paragraphes suivants décrivent le flux d'information des processus de développement du système vers les processus du cycle de vie de conception du matériel, des processus du cycle de vie du matériel vers ceux du développement du système et entre les processus du cycle de vie du matériel et les processus du cycle de vie du logiciel.

NOTA : Il est admis que ce sont des processus itératifs et que des modifications interviendront tout au long du cycle de vie du matériel.

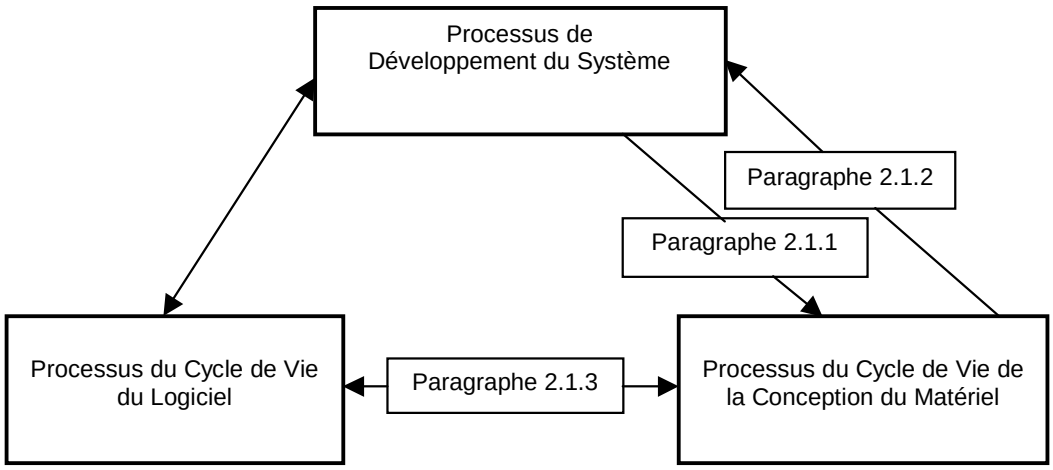


FIGURE 2-2 : PROCESSUS DE DEVELOPPEMENT DU SYSTEME

2.1.1 Flux d'information entre processus de développement du système et processus du cycle de vie de la conception du matériel

Ce flux d'information peut contenir:

1. Les exigences de conception et de sécurité allouées au matériel.
2. Le niveau d'assurance conception de chacune des fonctions, les exigences et les cas de défaillances associées, s'il y a lieu.
3. Les probabilités et les temps de risque allouées aux défaillances fonctionnelles du matériel.
4. La description des interfaces matériel/logiciel.
5. Les exigences liées aux stratégies de sécurité et les contraintes de conception, telles que la testabilité, les méthodes de conception et l'architecture du matériel.
6. Les exigences relatives aux activités de vérification du système à réaliser par une vérification au niveau du matériel.
7. Les exigences d'installation, d'ergonomie et d'environnement allouées au matériel.
8. Les constats d'anomalies d'intégration susceptibles d'avoir un impact sur les exigences. Ceux-ci peuvent résulter d'activités telles que la vérification du système, l'élaboration d'exigences propres au système ou la SSA.

2.1.2 Flux d'information entre cycle de vie de la conception du matériel et processus de développement du système

Ce flux d'information peut inclure:

1. La matérialisation des exigences telle que les dessins de la mécanique, les schémas et les listes de composants.
2. Les exigences dérivées du matériel susceptibles d'avoir un impact sur toute exigence allouée.
3. La matérialisation de l'architecture y compris les frontières de confinement de fautes.
4. Les éléments de preuve liés aux activités de validation et de vérification effectuées pendant le cycle de vie de conception du matériel.
5. Les données des analyses de sécurité telles que:
   a. Les probabilités et les taux de défaillances du matériel pour les défaillances fonctionnelles redoutées connues vers le processus SSA.
   b. L'analyse des fautes de mode commun.
   c. Les frontières de confinement et les stratégies de passivation des fautes génériques.
   d. Les données d'analyses de temps de latence en rapport avec les exigences du système. Par exemple, les provisions du matériel pour la surveillance des fautes, l'intervalle de détection de faute et les fautes non détectables.
6. Les exigences propres à des activités de vérification du matériel à effectuer lors des vérifications au niveau du système.
7. Les hypothèses et les méthodes d'analyses relatives aux exigences d'installations et les conditions d'environnement nécessaires à la validité des analyses.
8. Les constats d'anomalies ou les rapports de modifications susceptibles d'avoir un impact sur le système, le logiciel ou les exigences allouées au matériel

2.1.3 Flux d'information entre processus du cycle de vie de la conception du matériel et processus du cycle de vie du logiciel

Ce flux d'information peut inclure:

1. Les exigences dérivées nécessaires à l'intégration du matériel et du logiciel, telles que la définition des protocoles, les contraintes de temps, les plans d'adressage pour l'interface entre le matériel et le logiciel
2. Les cas pour lesquels les activités de vérification du matériel et du logiciel nécessitent une coordination.
3. Les incompatibilités identifiées du matériel et du logiciel qui peuvent être des éléments du système de constats et d'actions correctives.
4. Les données d'évaluation de la sécurité qui doivent être disponibles pour les processus système.

2.2 PROCESSUS D'EVALUATION DE LA SECURITE DU SYSTEME

Il y a trois processus d'évaluation de la sécurité du système: l'évaluation des risques fonctionnels (FHA), l'évaluation préliminaire de la sécurité du système (PSSA) et la démonstration de la tenue des objectifs (SSA). Ces processus sont utilisés pour élaborer les objectifs de sécurité du système applicables au processus d'assurance développement du système, et pour déterminer si les fonctions du système satisfont aux objectifs de sécurité.

Le processus PSSA doit transformer les objectifs de sécurité en exigences de sécurité du système et des équipements. Ces exigences doivent inclure les objectifs de sécurité de base, les attributs de sécurité pour les fonctions du système et des équipements et pour l'architecture. Le processus PSSA et les processus de développement du système allouent les exigences de sécurité au matériel.

Il y a cinq niveaux d'assurance développement pour les systèmes, du niveau A au niveau E, correspondant aux cinq classes de cas de défaillance: catastrophique, dangereuse/sévère majeure, majeure, mineure et sans effet. Le Tableau 2.1 donne la corrélation entre les niveaux d'assurance conception du matériel et les cinq classes de cas de défaillance, il donne aussi les définitions des cas de défaillances du matériel et leur niveau respectif d'assurance conception. Initialement le niveau d'assurance conception, de chacune des fonctions du matériel, est déterminé par le processus d'évaluation de la sécurité (SSA) en utilisant la FHA pour identifier les risques potentiels, le processus PSSA alloue ensuite les exigences de sécurité et les cas de défaillance associées aux fonctions implémentées par le matériel.

Tout au long du cycle de vie de la conception du matériel, il peut y avoir un retour itératif entre les processus de sécurité, du système et du matériel pour garantir que le matériel tel qu'il a été conçu et construit satisfait à la sécurité du système, aux exigences fonctionnelles et aux performances allouées au matériel.

Niveau d'Assurance Développement du Système	**Classification du cas de défaillance**	**Descriptions du cas de défaillance**	**Définition du Niveau d'Assurance Conception du Matériel**
Niveau A:	Catastrophique	Cas de défaillance qui pourrait empêcher la poursuite du vol ou de l'atterrissage dans des conditions sûres.	A: Fonctions du matériel dont la défaillance ou le comportement anormal, tel que montré par l'évaluation de la sécurité du matériel, pourrait produire une défaillance de la fonction du système se traduisant par un cas de défaillance catastrophique pour l'aéronef.
Niveau B:	Dangereux/ Sévère -Majeur	Cas de défaillance qui pourrait réduire la capacité de l'aéronef ou l'aptitude de l'équipage à faire face à des conditions opérationnelles défavorables pouvant aller jusqu'à: une réduction importante des marges de sécurité ou des capacités fonctionnelles, des douleurs physiques ou un accroissement de charge de travail telle que l'on ne puisse pas compter sur l'équipage pour l'exécution précise et complète de ses tâches, ou des conséquences dangereuses sur les occupants y compris des blessures graves ou mortelles pour un petit nombre d'entre eux.	B: Fonctions du matériel dont la défaillance ou le comportement anormal, tel que montré par l'évaluation de la sécurité du matériel, pourrait produire une défaillance de la fonction du système se traduisant par un cas de défaillance Dangereux/ Sévère-Majeur pour l'aéronef.
Niveau C:	Majeur	Cas de défaillance qui pourrait réduire la capacité de l'aéronef ou l'aptitude de l'équipage à faire face à des conditions opérationnelles défavorables pouvant aller jusqu'à: une réduction significative des marges de sécurité ou des capacités fonctionnelles, un accroissement significatif de la charge de travail ou des conditions diminuant l'efficacité de l'équipage, ou des malaises des occupants y compris d'éventuelles blessures.	C: Fonctions du matériel dont la défaillance ou le comportement anormal, tel que montré par l'évaluation de la sécurité du matériel, pourrait produire une défaillance de la fonction du système se traduisant par un cas de défaillance Majeur pour l'aéronef.
Niveau D:	Mineur	Cas de défaillance qui ne réduirait pas, de façon significative la sûreté de l'aéronef, et qui pourrait nécessiter des actions de l'équipage qui sont parfaitement dans ses possibilités. Les cas de défaillance mineurs peuvent consister en: une légère réduction des marges de sécurité ou des capacités fonctionnelles, une légère augmentation de la charge de travail de l'équipage, telle que les modification du plan de vol courant, ou quelques désagréments pour les passagers.	D: Fonctions du matériel dont la défaillance ou le comportement anormal, tel que montré par l'évaluation de la sécurité du matériel, pourrait produire une défaillance de la fonction du système se traduisant par un cas de défaillance Mineur pour l'aéronef.
Niveau E:	Sans Effet	Cas de défaillance qui n'affecte pas la capacité opérationnelle de l'aéronef ou n'augmentant pas la charge de travail de l'équipage.	E: Fonctions du matériel dont la défaillance ou le comportement anormal, tel que montré par l'évaluation de la sécurité du matériel, pourrait produire une défaillance de la fonction du système, "Sans Effet" sur la capacité opérationnelle de l'aéronef ou sur la charge de travail de l'équipage. Pour une fonction à laquelle est affecté le niveau E, il n'est pas nécessaire d'utiliser les recommandations proposées par le document, celles-ci peuvent néanmoins être utilisées comme référence.

TABLEAU 2-1 : DEFINITIONS DES NIVEAUX D'ASSURANCE CONCEPTION DU MATERIEL ET LEURS RELATIONS AVEC LES NIVEAUX D'ASSURANCE DEVELOPPEMENT DES SYSTEMES

2.3 EVALUATION DE LA SECURITE DU MATERIEL

L'évaluation de la sécurité du matériel est effectuée conjointement avec la SSA pour la supporter. Le but du processus d'évaluation de la sécurité est de démontrer que les systèmes et équipements auxquels il est appliqué, y compris le matériel, ont satisfait aux exigences de sécurité des règlements de certification des aéronefs.

En prenant en compte les exigences de la sécurité, fonctionnelles et de performances allouées au matériel par le processus système, le processus d'évaluation de la sécurité du matériel détermine le niveau d'assurance conception du matériel pour chaque fonction et contribue à la détermination de la stratégie d'assurance conception appropriée.

2.3.1 Considérations sur l'évaluation de la sécurité du matériel

Le concepteur d'un article matériel peut montrer la conformité aux exigences de sécurité allouées au matériel ainsi qu'au niveau d'assurance conception du matériel par une stratégie d'assurance conception appropriée.

Un niveau d'assurance conception unique et une même stratégie peuvent être appliqués à la totalité d'un article matériel, ou on peut également évaluer un article matériel en considérant les différents chemins de propagation des défaillances (FFPs) afin d'imaginer une combinaison de différents niveaux d'assurance conception ou de différentes stratégies d'assurance conception. Une analyse des chemins de propagation des défaillances (FFPA) peut être utilisée pour justifier un niveau inférieur d'assurance conception pour une partie de l'article matériel, ou pour combiner différentes fonctions implémentées avec des technologies ou des historiques d'exploitation de produits différents.

NOTA : La FFPA est décrite au Paragraphe 2 de l'Annexe B. Bien qu'elle ait été écrite pour prendre en compte le contenu objet de l'Annexe B, cette méthode d'analyse peut être utilisée pour n'importe quel niveau d'Assurance conception.

Si l'article matériel contient des fonctions qui ont des niveaux d'assurance conception différents, ce cas peut être traité par l'une des méthodes ci-dessous:

La totalité de l'article peut être assurée au niveau d'assurance conception le plus élevé.

Chacune des fonctions du matériel peut être assurée séparément à son niveau d'assurance conception tel que défini par l'évaluation de la sécurité du matériel si les fonctions, les interfaces et les ressources partagées peuvent être protégées des effets dangereux des fonctions de niveaux d'assurance conception inférieurs. L'assurance conception des ressources partagées doit être celle affectée à la fonction de niveau d'assurance le plus élevé.

Les recommandations pour l'évaluation de la sécurité consistent en:

1. L'évaluation itérative de la sécurité du matériel et de la conception qui doivent déterminer les exigences de sécurité dérivées du matériel et garantir que les exigences de sécurité du système allouées au matériel ainsi que les exigences dérivées sont satisfaites.
2. L'introduction dans les exigences dérivées d'exigences de sécurité concernant l'architecture du matériel, les circuits et les composants, les protections vis à vis des comportements anormaux, y compris l'incorporation d'attributs spécifiques à la sécurité de l'architecture et de la fonction du matériel, tels que:
   a) Les redondances de circuits ou de composants.
   b) La ségrégation ou l'isolement électrique entre les circuits ou les composants.
   c) La dissymétrie entre les circuits ou les composants.
   d) La surveillance des circuits ou des composants.
   e) Les mécanismes de protection ou de reconfiguration.

f) Les taux de défaillances et les probabilités des pannes aléatoires et des pannes latentes alloués aux circuits et composants.

g) Les limitations d'usage ou d'installation.

h) La prévention, la gestion des "upsets" et leur recouvrement.

3. La détermination conjointe par les processus d'assurance conception et d'évaluation de la sécurité du matériel, des moyens de démonstration de conformité spécifiques au niveau d'assurance conception pour chacune des fonctions et d'obtention d'un niveau acceptable d'assurance conception.

NOTA : les comportements anormaux du matériel peuvent résulter de fautes aléatoires, ou d'erreurs de conception de l'article ou "d'upsets" du matériel.

Le concepteur de matériel peut choisir un niveau d'assurance conception supérieur pour une fonction de l'article matériel. Un exemple pourrait être celui de l'anticipation de la réutilisation d'une fonction d'un matériel dans une installation pour laquelle un niveau d'assurance supérieur sera nécessaire.

L'évaluation de la sécurité du matériel peut faire appel à différentes méthodes d'évaluation qualitatives et quantitatives. Celles-ci peuvent comprendre des analyses d'arbres de fautes (FTA), des analyses des modes communs, des analyses des modes de défaillances et de leurs effets, des méthodes statistiques d'analyses de fiabilité pour les évaluations quantitatives de fautes aléatoires.

2.3.2 Evaluation quantitatives des fautes aléatoires du matériel

Les méthodes statistiques d'évaluation et de prédiction des défaillances qui sont basées sur le taux de défaillance du matériel, les redondances, les ségrégations et isolements, les statistiques des modes de défaillances, les analyses probabilistes, les détarages de composants, les analyses de contraintes et la maîtrise des processus de fabrication, ont prouvé qu'elles étaient des moyens acceptables d'évaluation quantitative des facteurs de risques liés aux défaillances aléatoires du matériel.

2.3.3 Evaluations qualitatives des erreurs de conception du matériel et des "upsets"

Contrairement aux défaillances aléatoires du matériel, ni les erreurs de conception, ni certains types "d'upsets" ne sont statistiquement prévisibles, tous deux peuvent franchir les frontières des redondances sous la forme de fautes de mode commun. Les techniques de gestion des redondances et les méthodes d'évaluation quantitatives à utiliser, devraient être choisies de façon à éliminer ou passiver lorsque cela est nécessaire les fautes potentielles de mode commun et les effets des "upsets".

Bien qu'ils soient difficiles à évaluer quantitativement, les risques vis à vis de la sécurité résultant d'erreurs de conception et "d'upsets" peuvent être effectivement évalués par une application pratique de méthodes d'évaluations qualitatives. Les techniques d'analyses, telles que celles d'analyse d'arbres de fautes, de mode commun, les analyses fonctionnelles de mode de défaillances et de leurs effets (AMDE_F), sont fondamentalement des méthodes qualitatives, et elles peuvent être utilisées pour traiter les erreurs de conception du matériel et les "upsets". De façon plus précise, ces méthodes sont capables de déterminer les effets potentiels d'erreurs de conception et des "upsets", et peuvent aider à la détermination des moyens par lesquels ils sont éliminés ou passivés. En utilisant ces méthodes, l'évaluation de la sécurité du matériel peut contribuer à la détermination des stratégies d'assurance conception du matériel et elles peuvent être employées itérativement tout au long du processus de conception du matériel pour déterminer qualitativement l'assurance obtenue par les stratégies retenues.

2.3.4 Considérations sur l'assurance conception pour la classification des cas de défaillance

Lorsque la sévérité des cas de défaillance augmente, le niveau d'assurance conception du matériel nécessaire pour garantir un accroissement de la passivation des cas de défaillance associés augmente. Pour tous les niveaux d'assurance conception une approche ou une stratégie doit être développée pour garantir un niveau approprié d'assurance conception. La Figure 2-3 montre le processus de prise de décision pour le développement d'une stratégie d'assurance conception appropriée.

Les recommandations concernent:

1. Les considérations d'assurance conception pour le traitement des comportements anormaux potentiels et des erreurs de conception des fonctions de niveaux A et B implémentées par le matériel.
2. L'utilisation du processus de décision donné par la Figure 2.3, lorsque l'on développe des stratégies d'assurance conception pour chacune des fonctions du matériel à implémenter.
3. L'application pour les fonctions de niveaux A et B en sus des recommandations données par les Chapitre 3 à 11, des stratégies décrites par l'Annexe B.
4. Le choix de la stratégie d'assurance conception en fonction de l'architecture du matériel et de son utilisation ainsi que de la technologie d'implémentation retenue.

Les différentes technologies, la sélection de composants et l'utilisation de composants offrent des degrés variables d'information sur le cycle de vie de la conception du matériel et sur les protections inhérentes vis à vis des erreurs de conception et de leurs effets. La méthode d'assurance conception la mieux indiquée peut varier pour les différents chemins fonctionnels de propagation à l'intérieur d'un même article matériel.

Les nombres dans les blocs d'activités et de décision de la Figure 2-3 renvoient au numéro de paragraphe au dessous de la figure, ils donnent des clarifications complémentaires pour la décision ou l'activité.

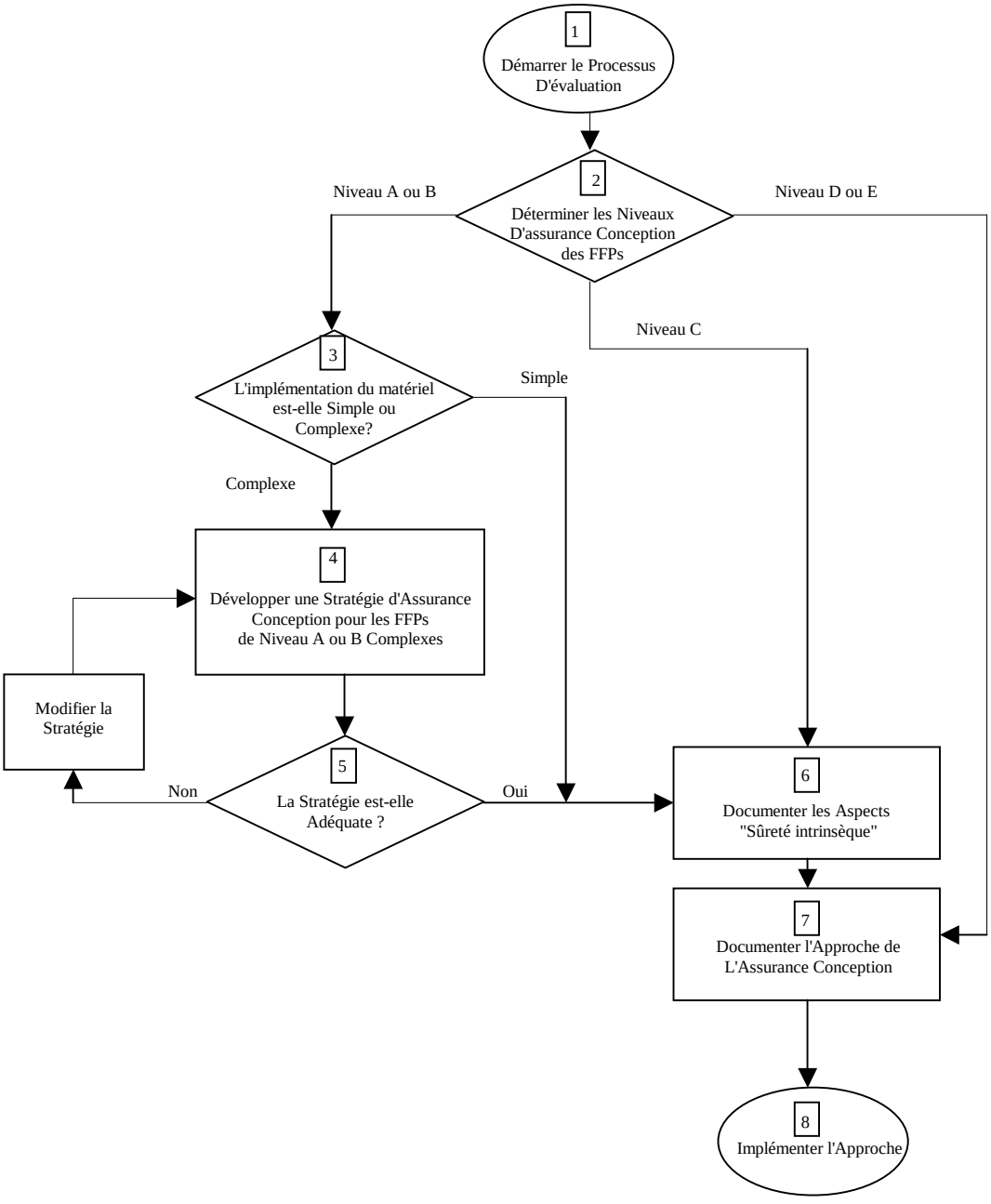


FIGURE 2-3 : PROCESSUS DE PRISE DE DECISION POUR LA SELECTION DE LA STRATEGIE D'ASSURANCE CONCEPTION DU MATERIEL

1 **Démarrer le Processus d'Evaluation.** Pour tous les niveaux d'assurance conception, une démarche ou une stratégie doit être développée afin de garantir un niveau d'assurance conception approprié

2 **Déterminer les Niveaux d'Assurance Conception des FFPs.** Pour chaque article identifié du matériel, déterminer et documenter les FFPs associés à l'article, et le niveau d'assurance conception. Les techniques conventionnelles d'évaluation de la sécurité doivent être utilisées pour déterminer quels sont les constituants du matériel qui se trouvent ou non dans des FFPs de niveaux A ou B.

3 **L'implémentation matérielle du FFP est-elle Simple ou Complexe ?** Pour les FFPs de niveau d'assurance conception A ou B déterminer si leurs constituants sont simples ou complexes tel que décrit par le Paragraphe 1.6.

4 **Développer une Stratégie d'Assurance Conception pour les FFP de Niveau A ou B Complexes.** Si le FFP est complexe et de niveau A ou B, alors utiliser les stratégies complémentaires décrites par l'Annexe B pour déterminer la stratégie d'assurance conception appropriée, les concepts d'implémentation et les méthodes de passivation des erreurs correspondantes. Pour chaque FFP de niveau A ou B, une stratégie d'assurance conception doit être déterminée en utilisant les analyses avancées, l'expérience en exploitation du produit ou les passivations par l'architecture.

Les FFPs de niveau A d'une implémentation peuvent nécessiter l'utilisation de plusieurs techniques si celle qui a été retenue ne fournit pas une passivation complète des défaillances potentielles et des comportements anormaux.

5 **La Stratégie est-elle Adéquate ?** Déterminer s'il existe des insuffisances dans la stratégie d'assurance conception, si des insuffisances existent ou pourraient exister dans les données dont on pense disposer alors modifier la stratégie afin de corriger ces insuffisances en proposant des stratégies d'assurance conception, d'implémentation ou d'architecture complémentaires.

Lorsque la stratégie d'assurance conception est acceptable, documenter les processus d'assurance conception pour chacun des FFPs. La stratégie doit également prendre en compte les aspects qui concernent la participation de l'autorité de certification tels que les évènements programmés, les revues et les activités de surveillance.

6 **Documenter les Aspects de Sûreté Intrinsèque.** Déterminer l'architecture à sûreté intrinsèque appropriée, les caractéristiques de l'article matériel et effectuer une analyse pour satisfaire aux exigences de disponibilité et d'intégrité du système. Documenter les aspects relatifs à la conception à sûreté intrinsèque, aux analyses de mode commun associées, aux analyses de probabilité, à l'architecture et aux autres caractéristiques.

7 **Documenter l'Approche et la Stratégie de l'Assurance Conception.** Documenter l'approche et la stratégie d'assurance conception applicables dans le plan de certification du système ou le Plan des Aspects Matériels de la Certification (PHAC) et obtenir l'approbation de l'autorité de certification.

8 **Appliquer l'Approche.** Implémenter la conception du matériel conformément à l'approche d'assurance conception appropriée telle que définie dans les plans approuvés et documenter la preuve de conformité aux plans et à la stratégie.

CHAPITRE 3

CYCLE DE VIE DE LA CONCEPTION DU MATERIEL

Ce chapitre décrit le cycle de vie du matériel explicité dans les Chapitres 4 à 9. Ce document ne préconise pas de modèle de cycle de vie préférentiel, il n'implique pas non plus de structure pour l'organisation qui l'applique. Le cycle de vie de la conception du matériel est applicable de la même manière au développement de systèmes ou d'équipements nouveaux, et aux modifications des systèmes et des équipements existants. Pour chaque projet le cycle de vie devrait être élaboré par une sélection et une combinaison de processus et d'activités déterminées à partir des attributs du projet tels que la stabilité des exigences, l'utilisation de matériel développé auparavant et le niveau d'assurance conception du matériel. Les processus du cycle de vie de conception du matériel peuvent être itératifs c'est à dire entrants, réentrants et modifiés en raison de l'aspect incrémental du développement et des rétroactions entre les processus.

3.1 PROCESSUS DU CYCLE DE VIE DE LA CONCEPTION DU MATERIEL

Les processus du cycle de vie du matériel sont:

Le processus de planification du développement du matériel, décrit au Chapitre 4, qui définit et coordonne pour un projet les activités de conception du matériel ainsi que les processus transverses.

Les processus de conception du matériel, décrits au Chapitre 5, qui créent les données de conception et l'article matériel qui en résulte. Ces processus sont le recueil des exigences, la conception générale, la conception détaillée, l'implémentation et la transition vers la production.

Les processus transverses, décrits par les Chapitres 6 à 9, qui produisent les données du cycle de vie assurant l'exactitude et la maîtrise du cycle de vie de la conception du matériel et de ses produits, y compris la planification, la conception, l'évaluation de la sécurité du matériel et les processus transverses. Ces processus se déroulent en général de manière concurrentes avec les processus de planification et de conception. Ce sont les processus de validation, de vérification, de gestion de configuration, d'assurance processus et de coordination pour la certification.

3.2 CRITERES DE TRANSITION

Les difficultés liées au développement d'un article matériel constitué de plusieurs sous-ensembles à des étapes différentes du développement imposent un niveau raisonnable de maîtrise du processus de conception; ce moyen doit permettre de gérer le risque lié au démarrage du processus suivant avant que tous les résultats de la phase précédente n'aient été obtenus. Les critères de transition sont définis comme les données minimales utilisées afin d'évaluer le passage d'un processus à un autre, et peuvent être utilisés à des points clefs des processus. L'analyse doit déterminer au cours du processus de planification la façon d'utiliser les critères de transition. Il n'est pas nécessaire de définir des critères de transition entre chaque couple de phases dans un processus défini par les plans. Le choix des critères de transition doit prendre en compte les impacts sur la sécurité. Par exemple, avant d'effectuer la vérification d'une fonction pour l'obtention d'un crédit de certification, les exigences de cette fonction doivent être documentées et l'implémentation de cette fonction doit être gérée en configuration.

Les critères de transition devraient être documentés dans les plans du matériel. L'utilisation de critères de transition n'implique pas de modèle particulier du cycle de vie et n'interdit pas les stratégies de développement telles que le prototypage rapide ou l'ingénierie concurrente.

CHAPITRE 4

PROCESSUS DE PLANIFICATION

Ce chapitre décrit le processus de planification utilisé pour maîtriser le développement d'un article matériel. Ce processus élabore les plans qui peuvent faire l'objet d'un ou de plusieurs documents. Lorsque des plans multiples sont utilisés, le plan principal doit contenir les références correspondantes des documents sur lesquels il s'appuie. Les règles couvrant des points particuliers du cycle de vie de la conception du matériel, tels que gestion de la configuration ou assurance processus sont acceptables, sous réserve qu'elles satisfassent aux objectifs de la planification pour le processus considéré.

4.1 OBJECTIFS DU PROCESSUS DE PLANIFICATION

Le but du processus de planification du matériel est de définir les moyens par lesquels les exigences fonctionnelles et de navigabilité sont transformées en un article matériel, qui réalise avec une assurance démontrée et de manière sûre les fonctions attendues. Les objectifs du processus de planification du développement matériel sont:

1. Définir les processus du cycle de vie de la conception du matériel.

   NOTA : Les activités, les jalons, les données, les produits et les responsabilités dans l'organisation peuvent être intégrés aux plans.

2. Choisir et définir les règles.
3. Choisir et définir les environnements de développement et de vérification du matériel.
4. Proposer à l'autorité de certification les moyens d'obtention de la conformité aux objectifs d'assurance conception du matériel, y compris les stratégies identifiées en utilisant les recommandations du Paragraphe 2.3.4.

   NOTA : Le caractère novateur et évolutif des technologies, des outils et des processus peuvent nécessiter des modifications du processus de planification. Par voie de conséquence, la flexibilité est un élément clef du processus de planification.

4.2 ACTIVITES DU PROCESSUS DE PLANIFICATION

Recommandations pour les activités du processus de planification:

1. Définition du cycle de vie de la conception du matériel y compris les critères de transition s'il y a lieu, ainsi que des interdépendances entre chaque processus tels que leurs enchaînements, et les mécanismes de rétroaction.
2. Définition et justification des méthodes de conception proposées. Ceci comprend les procédures de conception du matériel prévues ainsi que la justification des méthodes de vérification proposées.
3. Identification des règles de conception du matériel si certaines d'entre elles doivent être utilisées pour le projet, y compris les dérogations acceptables à ces règles. Cela peut aller de règles de qualité génériques à des règles internes à l'entreprise ou propres au programme.

   NOTA : Les règles de conception aident à réduire la probabilité de non détection d'erreurs de conception, en procurant une compilation de pratiques d'ingénierie éprouvées élaborées au cours des développements précédents.

   Le postulant et le développeur de matériel devraient être conscients, lorsqu'ils comptent appliquer des règles existantes à de nouveaux développements ou de nouvelles technologies, de leur éventuelle non validité. Des dérogations à ces règles peuvent se révéler nécessaires en raison de contraintes de conception, de conflits avec les exigences du système ou d'incompatibilités avec de nouvelles technologies. Le processus de planification offre l'opportunité de faire la revue des dérogations acceptables lorsque des règles sont utilisées.

4. Détermination des moyens pour assurer la coordination entre les processus de conception du matériel et les processus transverses, avec une attention particulière pour les activités liées à la certification des systèmes, du logiciel, et de l'aéronef.

   NOTA : *La coordination peut prendre la forme d'un calendrier donnant le jalonnement des évènements permettant d'atteindre les objectifs des processus décrits dans ce document.*

5. Définition de chaque activité du processus de conception du matériel ainsi que des processus transverses associés. La définition doit se situer à un niveau permettant de maîtriser les processus de conception du matériel et les processus transverses associés.

6. Choix de l'environnement de conception y compris les outils, les procédures, le logiciel et le matériel utilisés pour développer, vérifier ,contrôler l'article matériel et les données du cycle de vie.

   a. Lorsqu'un crédit de certification est recherché par l'utilisation combinée d'outils la séquence de mise en œuvre des outils doit être spécifiée dans les plans respectifs.

   b. L'environnement de conception peut affecter la conception d'un produit. Le Paragraphe 11.4 donne des recommandations en ce qui concerne l'évaluation des outils et la détermination du besoin de qualification des outils.

7. Identification du processus de dérogation aux plans établis lorsque les dérogations deviennent nécessaires et affectent la certification.

8. Description de la politique, des procédures, des règles et des méthodes à utiliser pour identifier, gérer et contrôler le matériel, les référentiels associés et les données du cycle de vie de la conception du matériel.

9. Identification par les plans du matériel de la méthode garantissant que les objectifs d'assurance conception sont satisfaits lorsque le postulant a l'intention d'utiliser des sous-contractants pour tout ou partie du cycle de vie de la conception du matériel.

10. Description de la politique et des procédures de mise en place de l'assurance processus pour la conception du matériel.

11. Description dans le PHAC de l'indépendance du processus de vérification, d'assurance processus et des responsabilités organisationnelles associées.

12. Enregistrement et communication à l'autorités de certification, au début du processus, des moyens pour satisfaire aux objectifs ci-dessus. Ces moyens doivent être enregistrés dans le PHAC.

    NOTA : *Afin d'augmenter les chances d'acceptation des données de certification, en tant que preuve recevable de la satisfaction des exigences d'assurance conception, une incitation est faite pour la coordination en temps opportun de toute les modification des moyens.*

CHAPITRE 5

PROCESSUS DE CONCEPTION DU MATERIEL

Les processus de conception produisent un article matériel qui satisfait aux exigences qui lui sont allouées à partir des exigences du système. Ce chapitre détaille les cinq processus majeurs décrits par la Figure 5-1. Ce sont le Recueil des Exigences, la Conception Générale, la Conception Détaillée, l'Implémentation et la Transition vers la Production. Ces processus de conception peuvent être appliqués à tous les niveaux hiérarchiques de l'article matériel, tels que LRUs, cartes et ASICs/PLDs. Les paragraphes ci-dessous décrivent chaque processus, leurs objectifs et les activités associées que l'on devrait accomplir afin de réduire la probabilité de présence d'erreurs de conception et d'implémentation ayant une incidence sur la sécurité. Pour cela il est fondamental que chaque processus soit planifié et que sa description détaillée soit consignée dans le plan de conception du matériel.

Chaque processus, ainsi que les interactions entre les processus, peuvent être itératifs. Lors de chaque itération, les effets des modifications apportées à chacun des processus doivent être pris en compte et évalués vis à vis de leurs impacts sur les résultats des itérations précédentes.

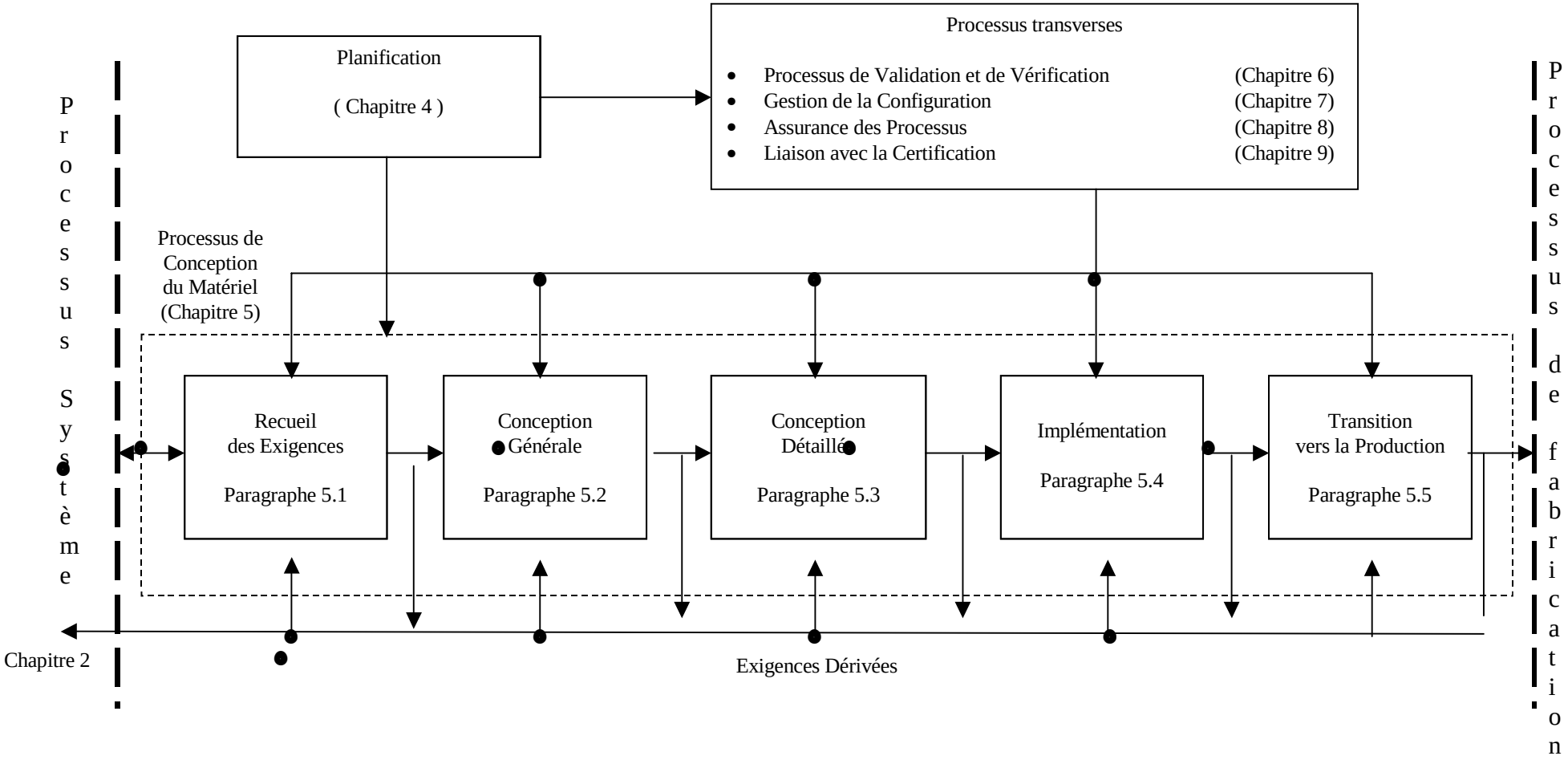
NOTA 1 : *Une pratique d'ingénierie reconnue consiste à documenter les résultats du processus, par des notes de conception, des notes de revues de la conception et des constats d'anomalies, tout au long du processus de conception.*

Les pratiques usuelles offrent des moyens nombreux et différents de représentation des exigences et des implémentations de la conception, graphiques, formulations mathématiques, bases de données ou textes . Les schémas, les langages de description du matériel (HDL), les machines d'état, les représentations booléennes et les méthodes graphiques sont des exemples de ces représentations.

NOTA 2 : *Certaines représentations sont adaptées à un processus particulier ou à une association de processus, tel que le recueil des exigences, la conception générale ou détaillée, alors que d'autres sont mieux adaptées à la représentation d'une technologie particulière d'implémentation. Les preuves à apporter, vis à vis du niveau d'assurance conception, doivent être fournies indépendamment de la représentation de la conception utilisée.*

Pour chaque représentation de la conception utilisée, les points ci-dessous devraient être pris en compte:

1. Suivre les recommandations de ce document, indépendamment des représentations utilisées ou de leurs combinaisons.
2. Permettre une reproduction uniforme de l'article matériel à partir de la représentation de sa conception.
3. Evaluer l'effet des modifications mineures de la représentation sur l'assurance conception. Ces modifications peuvent avoir un effet très significatif sur l'implémentation de la conception.
4. Evaluer l'incidence d'une modification de la représentation sur la reproduction de la conception, car l'environnement de la représentation ou les méthodes de conception peuvent évoluer après que le référentiel des données de la conception ait été élaboré.



- Processus de Validation et de Vérification (Chapitre 6)
- Gestion de la Configuration (Chapitre 7)
- Assurance des Processus (Chapitre 8)
- Liaison avec la Certification (Chapitre 9)

FIGURE 5-1 : CYCLE DE VIE DE LA CONCEPTION DU MATERIEL

Les représentations HDL de la conception utilisent des techniques basées sur des textes codés qui ont une apparence similaire à celles utilisées pour les représentations du logiciel. Cette similitude d'apparence peut tromper ceux qui essayeraient d'utiliser directement les méthodes de vérification du logiciel sur des représentations HDL de la conception, ou sur tout autre langage de spécification du matériel équivalent. Les recommandations de ce document sont applicables à l'assurance conception de développements utilisant une représentation HDL.

NOTA : Les processus structurés décrits tout au long de ce document sont applicables aux conceptions de matériels complexes qui comportent des ASICs et des PLDs. A titre d'exemple, la tableau ci-dessous donne une cartographie des processus types pour les ASIC/PLD et les relie aux processus décrits en Figure 5-1.

Processus ASIC/PLD Types	**Processus Génériques**
Elément de planification des niveaux hiérarchiques supérieurs	Planification (Chapitre 4)
Choix de l'Architecture de l'ASIC/PLD	Evaluation de la Sécurité (Paragraphe 2.3)
Recueil des Exigences de l'ASIC/PLD	Recueil des Exigences (Paragraphe 5.1)
Conception Préliminaire de l'ASIC/PLD comprenant la conception comportementale	Conception Générale (Paragraphe 5.2)
Conception Détaillée de l'ASIC/PLD comprenant la synthèse, la création des masques et la génération des fichiers de fusibles	Conception Détaillée (Paragraphe 5.3)
Fabrication de l'ASIC/PLD comprenant l'externalisation du processus de la fabrication et des tests, ainsi que la programmation des composants programmables	Implémentation (Paragraphe 5.4)
Transition vers la Production de l'ASIC/PLD	Transition vers la Production (Paragraphe 5.5)
Validation et Vérification de l'ASIC/PLD comprenant l'analyse temporelle, la simulation comportementale, la simulation au niveau des portes et les revues de conception	Processus de Validation et Vérification (Chapitre 6)
Gestion de la Configuration de l'ASIC/PLD, y compris pour les outils et pour la bibliothèque de données composants	Processus de Gestion de la Configuration (Chapitre 7)

TABLEAU 5-1 : CARTOGRAPHIE DES PROCESSUS ASIC/PLD

5.1 PROCESSUS DE RECUEIL DES EXIGENCES

Le processus de recueil des exigences identifie et enregistre les exigences de l'article matériel. Celles-ci comprennent les exigences dérivées qui résultent de l'architecture proposée pour le matériel, des choix technologiques, des fonctionnalités de base et optionnelles, de l'environnement opérationnel, des exigences de performance ainsi que des exigences de sécurité imposées par l'évaluation de la sécurité du système. Ce processus peut être itératif car des exigences complémentaires peuvent apparaître lors de la conception.

5.1.1 Objectifs du recueil des exigences

Les objectifs du recueil des exigences sont :

1. Identifier, définir et documenter les exigences. Celles-ci comprennent, les exigences allouées à partir de la PSSA, ainsi que les exigences dérivées issues de l'évaluation de la sécurité du matériel.

NOTA : La traçabilité des résultats de la vérification par rapport aux exigences du matériel est traitée au Chapitre 6. Il est souhaitable d'élaborer la méthode de traçabilité au cours du processus de recueil des exigences.

2. Re-introduire les exigences dérivées produites dans les processus concernés.
3. Réaffecter les problèmes d'omission et d'erreurs d'exigences aux processus concernés pour qu'ils soient résolus.

5.1.2 Recueil des exigences

Le recueil des exigences constituent un processus itératif qui aide à garantir leur cohérence avec l'implémentation de la conception, les exigences du système et celles du logiciel.

Recommandations pour le recueil des exigences :

1. Documentation des exigences du système allouées à l'article matériel. Ceci peut consister en l'identification d'exigences telles que les fonctionnalités, les performances et les contraintes d'architecture comme les ségrégations, les tests intégrés, la testabilité, les interfaces avec l'extérieur, l'environnement opérationnel, les considérations sur le test et la maintenance, la puissance et les caractéristiques physiques.
2. Identification des exigences de sécurité issues de la PSSA propres à l'article matériel. Ceci peut inclure :
   a. Le niveau d'assurance conception imposé aux fonctions à implémenter dans le matériel.
   b. Les exigences, en termes probabilistes, associées aux dysfonctionnements ou aux pertes de fonctions.
   c. Les attributs propres à l'architecture et à la sécurité fonctionnelle du matériel, tels que ceux décrits au Paragraphe 2.3.1, choisis pour satisfaire à l'allocation fonctionnelle.
3. Identification des contraintes de la conception liées au processus de la production, aux règles, aux procédures, à la technologie, à l'environnement de conception et aux recommandations pour la conception.
4. Détermination des exigences dérivées nécessaires à l'implémentation. Identification de manière unique des exigences dérivées issues de l'évaluation de la sécurité du matériel qui ont un impact sur la sécurité.

   NOTA : Les exigences dérivées peuvent prendre en compte des aspects tels que :

   a. Les contraintes spécifiques qui garantissent que les fonctions de plus haut niveau d'assurance conception peuvent résister aux anomalies des fonctions de niveau d'assurance conception inférieur, telles qu'elles sont vues aux interfaces de la fonction qui a le niveau d'assurance conception inférieur.

   b. La dynamique des entrées prenant en compte les valeurs typiques et extrêmes ainsi que les états bas ou haut des bits des mots de données ou des registres de commandes.

   c. Les états lors des mises sous tension ou lors de réinitialisations.

   d. Les caractéristiques attendues en tension et en courant des alimentations.

   e. Les performances de fonctions dépendantes du temps telles que les filtres, les intégrateurs et les retards.

   f. Les transitions possibles des machines d'états, qu'elles soient prévisibles ou non.

   g. Les relations temporelles entre les signaux ou les conditions électriques dans les cas normaux et dans les pires cas.

   h. Les bruits des signaux et les diaphonies.

   i. Les "glitches" des signaux dans les circuits logiques asynchrones.

   j. Les contraintes spécifiques afin de maîtriser les fonctions non utilisées.

5. La réintroduction dans la SSA des exigences dérivées, de telle sorte que leurs effets sur les exigences système puissent être évalués.
6. La documentation des exigences en termes quantitatifs ainsi que des tolérances lorsque cela est possible. Elle ne comprend pas la description des solutions relatives à la conception ou à la vérification.
7. La réaffectation aux processus de développement du système des exigences erronées ou oubliées découvertes au cours du processus de recueil.
8. La traçabilité entre les exigences, y compris entre celles destinées à satisfaire aux exigences de la PSSA, et les exigences du niveau hiérarchique immédiatement supérieur. Les exigences dérivées doivent être identifiées et tracées autant que possible aux niveaux hiérarchiques concernés.

   NOTA : La validation au niveau du système des exigences de sécurité allouées au matériel peut avoir lieu lors du processus de recueil des exigences. La validation des exigences dérivées du matériel est décrite au Paragraphe 6.1.

5.2 PROCESSUS DE CONCEPTION GENERALE

Le processus de conception générale élabore une conception de haut niveau qui peut être évaluée afin de déterminer son aptitude à satisfaire aux exigences. Ceci peut être accompli par l'utilisation de représentations telles que les blocs diagrammes fonctionnels, les descriptions de conception et d'architecture, les pré-implantations de cartes équipées et les croquis de la mécanique.

5.2.1 Objectifs de conception générale

Les objectifs de conception générale sont :

1. Développer la conception générale de l'article matériel en cohérence avec ses exigences.
2. Réaffecter les exigences dérivées produites au processus de recueil des exigences ou à tout autre processus approprié.
3. Réintroduire les exigences omises et les erreurs dans les processus appropriés afin de leur donner une solution.

5.2.2 Activités de conception générale

Recommandations pour les activités de conception générale :

1. Elaboration d'une description de haut niveau de l'article matériel. Celle-ci peut inclure:
   a. Les contraintes d'architecture liées à la sécurité, y compris celles nécessaires pour prendre en compte les erreurs de conception et les erreurs fonctionnelles, les contraintes excessives sur les composants, les défauts de fiabilité et de robustesse.
   b. L'identification de toute contrainte d'implémentation pour le logiciel ou pour d'autre composants du système.
2. Identification des composants majeurs. Détermination de leur contribution aux exigences de sécurité du matériel, y compris de l'impact des fonctions non utilisées.
3. Réintroduction des exigences dérivées y compris de la définition de l'interface dans le processus de recueil des exigences.
4. Réintroduction dans les processus appropriés des exigences omises et erronées afin de leur donner une solution.

5. Identification des caractéristiques de fiabilité, de maintenance et des tests à fournir.

NOTA : L'obtention d'un consensus, entre les parties concernées, sur la satisfaction des objectifs de conception générale est recommandé. Une revue de conception est en général utilisée pour l'obtention de ce consensus.

5.3 PROCESSUS DE CONCEPTION DETAILLEE

Le processus de conception détaillée élabore les données de cette conception à partir des exigences de l'article matériel et des données de conception générale.

5.3.1 Objectifs de conception détaillée

Les objectifs de conception détaillée sont :

1. Développer une conception détaillée à partir des exigences de l'article matériel et des données de conception générale.
2. Réintroduire les exigences dérivées dans le processus de conception générale ou dans les processus appropriés.
3. Réintroduire les exigences omises ou erronées dans les processus appropriés afin de leur donner une solution.

5.3.2 Activités de conception détaillée

Recommandations pour les activités de conception détaillée :

1. Elaboration des données de conception détaillée de l'article matériel à partir des exigences et des données de conception générale. Celles-ci peuvent comporter des données d'assemblage et d'interconnexion, des données propres aux composants, du code HDL, des méthodes de test ainsi que des données propres à l'interface matériel/logiciel.

   NOTA : Au cours du processus de conception détaillée des techniques de vérification sont utilisées de manière informelle afin de faciliter les choix techniques effectués lors de ce processus. Par exemple, l'analyse de paramètres de conception, tels que les caractéristiques temporelles de la logique et les variations des paramètres, peut fournir des informations sur lesquelles s'appuient les choix de conception.

2. Mise en œuvre, en fonction du besoin, des techniques architecturales de conception. Celles-ci peuvent comprendre la mise en place de dispositifs de surveillance de la sécurité pour un fonctionnement acceptable, des dissemblances entre les fonctions et les dispositifs de surveillance de la sécurité, des techniques d'élimination des effets des erreurs de conception sur la sécurité ainsi que des conceptions tolérantes aux fautes.
3. Intégration à la conception de dispositifs de tests, lorsque cela est nécessaire, afin de permettre la vérification des exigences de sécurité.

   NOTA : Il est important de développer la conception de manière à ce que certaines caractéristiques de la sécurité puissent être vérifiées, non seulement au cours du cycle de vie de la conception du matériel, mais également lors des tests d'acceptation et des tests de retour en service.

4. Evaluation des fonctions non utilisées afin d'identifier leur effet potentiel sur la sécurité. Les effets dangereux doivent être traités.
5. Identification des contraintes sur la conception, l'installation ou l'exploitation de l'article pouvant avoir un effet sur la sûreté si elles ne sont pas satisfaites.
6. Réintroduction des exigences dérivées produites au cours de conception détaillée dans le processus de conception générale ou tout autre processus approprié.
7. Réaffectation des exigences oubliées et erronées découvertes au cours du processus de conception détaillée aux processus concernés afin de leur donner une solution.

5.4 PROCESSUS D'IMPLEMENTATION

Le processus d'implémentation utilise les données de conception détaillée pour élaborer un article matériel qui soit une entrée des activités de test.

5.4.1 Objectifs de l'implémentation

Les objectifs du processus d'implémentation sont de :

1. Produire un article matériel qui concrétise la conception détaillée en appliquant un processus de production représentatif des pratiques industrielles du postulant.
2. Terminer l'élaboration des données d'implémentation, d'assemblage et d'installation.
3. Réintroduire les exigences dérivées dans le processus de conception détaillée ou dans tout autre processus approprié.
4. Réaffecter les exigences omises et erronées aux processus appropriés afin de leur donner une solution.

5.4.2 Les activités d'implémentation

Recommandations pour les activités d'implémentation :

1. Production d'un article matériel utilisant les données de la conception, et lorsque cela est faisable les ressources que l'on compte mettre en œuvre pour la production de l'article. Ceci peut concerner les achats, la préparation des composants et des matériaux, le conditionnement des composants, la fabrication, les inspections et les tests.
2. Réintroduction des exigences dérivées générées par le processus d'implémentation dans le processus de conception détaillée ou dans tout autre processus approprié.
3. Réaffectation des omissions et des erreurs découvertes au cours du processus d'implémentation aux processus concernés afin de leur donner une solution.

5.5 PROCESSUS DE TRANSITION VERS LA PRODUCTION

Dans ce processus, les données de la production, les moyens de test ainsi que les ressources principales devraient être examinés afin de garantir leur disponibilité et leur adaptation à la production. Le processus de transition vers la production utilise les produits du processus d'implémentation et de vérification pour mettre le produit en phase de production.

5.5.1 Objectifs de la transition vers la production

Les objectifs de ce processus sont :

1. Elaborer un référentiel qui comporte toutes les données de conception et de production nécessaires à une reproduction conforme de l'article matériel.
2. Identifier et documenter les exigences de production liées à la sécurité, établir les points de contrôle de la production.
3. Réintroduire les exigences dérivées dans le processus d'implémentation ou dans tout autre processus approprié.
4. Réintroduire les erreurs et omissions dans les processus appropriés afin de leur donner une solution.

5.5.2 Activités de la transition vers la production

Recommandations pour les activités de transition vers la production :

1. Elaboration des données pour la production à partir des données de conception gérées en configuration.

2. Vérification de la complétude et de la cohérence des données de production par rapport aux données gérées en configuration.

   NOTA : *L'Imposition de contraintes sur la nature des dossiers de fabrication à produire ne fait pas partie des intentions de ce document.*

3. Evaluation de toutes les modifications et améliorations qui sont introduites au cours du processus de transition vers la production, afin de garantir qu'elles satisfont à toutes les exigences du produit, tout particulièrement aux exigences de sécurité. Toutes les modifications non conformes aux exigences du client ou de la certification doivent être approuvées par les parties compétentes.
4. Définition explicite des exigences de production qui contribuent à la sécurité, pour qu'elles puissent être contrôlées au cours du processus de production.
5. Détermination des données nécessaires au développement des critères pour les tests d'acceptation.
6. Réaffectation des omissions ou des erreurs identifiées aux processus appropriés afin de leur apporter une solution.

5.6 TESTS D'ACCEPTATION

Les tests d'acceptation démontrent que le produit fabriqué, modifié ou réparé fonctionne conformément aux attributs essentiels de l'entité sur laquelle la certification a été établie. Les attributs essentiels sont choisis en s'appuyant sur le savoir faire en ingénierie, ils démontrent l'aptitude du produit à satisfaire aux exigences à partir desquelles l'entité a été développée.

NOTA 1 : *Le contrôle de la configuration du produit qui a été fabriqué n'est pas une activité qui fait partie des tests d'acceptation. Le plan de gestion de configuration, tel que décrit au Chapitre 7 de ce document, devrait décrire la façon dont le postulant compte effectuer cette activité.*

Le domaine couvert par ce document comprend la détermination des critères des tests d'acceptation, y compris les conditions de succès et d'échec. Les activités de production, y compris l'application des tests d'acceptation, ne font pas partie du domaine couvert par ce document.

NOTA 2 : *Les tests d'acceptation ne sont pas destinés à vérifier l'ensemble des exigences sur chaque entité produite.*

Le test des sous-articles peut faire partie des tests d'acceptation.

Les critères des tests d'acceptation doivent garantir que:

1. Les tests électriques ont été identifiés.
2. Les tests environnementaux de déverminage ont été identifiés lorsque cela est nécessaire.
3. Les tests d'acceptation apportent une couverture des aspects de la conception nécessaires à la satisfaction des exigences de sécurité. Les articles ou sous-articles relatifs à la sécurité qui ne font pas l'objet de tests devraient être identifiés et d'autres moyens d'assurance proposés. Ces moyens peuvent inclure des analyses, du contrôle de conception, du contrôle statistique des processus ou d'autres moyens appropriés.

5.7 PRODUCTION EN SERIE

Ce processus ne fait pas partie du domaine couvert par ce document, cependant, les points ayant un impact sur l'assurance conception sont décrits sommairement afin de compléter le cycle de vie.

Ce processus reproduit les articles matériels de manière répétitive en conformité avec les données et les exigences de la production.

Les points essentiels consistent en :

1. La gestion des modifications des processus de production ou de conception qui apporte l'assurance qu'aucune des modifications n'a d'impact négatif sur le niveau de sûreté acquis, sur la certification ou la conformité aux exigences.

   NOTA : En plus des recommandations proposées par le corps de ce document, le Paragraphe 11.1.1 traite des "Modifications de Matériels Développés Auparavant". Pour le traitement des obsolescences de composants voir le Paragraphe 11.2.

2. La mise à jour des documents liés aux modifications effectuée en conformité avec les plans de gestion de configurations approuvés.

CHAPITRE 6

PROCESSUS DE VALIDATION ET DE VERIFICATION

Ce chapitre décrit les processus de validation et de vérification. Le processus de validation donne l'assurance que les exigences dérivées de l'article matériel sont exactes et complètes par rapport aux exigences du système. Il assure que l'implémentation matérielle satisfait à toutes les exigences, y compris aux exigences dérivées.

6.1 PROCESSUS DE VALIDATION

Le processus de validation décrit ici a pour but de garantir que les exigences dérivées sont exactes et complètes, par rapport aux exigences du système allouées à l'article matériel, par l'utilisation de processus objectifs et subjectifs. La validation peut être effectuée avant ou après que l'article matériel soit disponible; cependant la validation est en général effectuée tout au long du cycle de vie de la conception.

NOTA 1 : L'expérience montre que l'attention apportée au développement et à la validation des exigences permet de détecter des erreurs subtiles ou des omissions tôt lors du cycle de développement, et de réduire l'exposition à des reprises de développements ou à des performances du matériel inadéquates.

Le processus de validation décrit ici n'a pas pour but de valider les exigences qui lui sont allouées à partir du système car leur validation est supposée appartenir au processus système. De plus, toutes les exigences dérivées du matériel ne doivent pas être nécessairement validées.

Les décisions de conception qui ont une incidence sur la sécurité du système ou sur les exigences fonctionnelles allouées à d'autre parties du système doivent être classées en exigences dérivées et doivent être validées. Par ailleurs, les décisions et les hypothèses de conception qui induisent des contraintes sur les tâches de conception qui en découlent doivent être validées en tant qu'exigences dérivées.

Les exigences dérivées à valider doivent l'être par rapport aux exigences du système allouées à l'article matériel. Les exigences dérivées qui ne sont pas traçables vers des exigences de haut niveau doivent être validées par rapport à la décision de conception dont elles ont été dérivée.

NOTA 2 : La décision de conception d'incorporation d'une alimentation séparée pour des composants assurant une fonction particulière, peut entraîner des dérivations d'exigences pour guider la conception de cette alimentation. Ces exigences dérivées peuvent comporter des exigences de sécurité issues de cas de défaillance de la fonction implantée dans le circuit et qui reçoit l'énergie de cette alimentation. Ces exigences doivent être validées.

Un autre exemple de décision de conception, qui devient une exigence dérivée, est celui de l'affectation d'une adresse mémoire à un dispositif périphérique. Il n'y a pas en général d'exigence de base pour ces affectations, cependant, dès lors que cette contrainte est établie, toutes les tâches de conception qui en découlent doivent la satisfaire pour que la conception soit fonctionnellement correcte. Cette exigence dérivée peut ne pas être validée.

6.1.1 Objectifs du processus de validation

Les objectifs du processus de validation des exigences dérivées du matériel, sont de:

1. Démontrer l'exactitude et la complétude des exigences dérivées, par rapport auxquelles l'article matériel doit être vérifié.

2. Evaluer les exigences dérivées vis à vis de leur impact sur la sécurité.
3. Réintroduire les omissions et les erreurs dans les processus appropriés, afin de leur apporter une solution.

6.1.2 Activités du processus de validation

Les objectifs de la validation du matériel peuvent être satisfaits par des combinaisons d'activités telles que les revues, la simulation, le prototypage, la modélisation, l'analyse, l'expérience en exploitation, les jugements d'ingénierie, ou le développement et l'exécution de tests.

Recommandations pour les activités du processus de validation :

1. Identification des exigences dérivées à valider.
2. Identification et satisfaction du critère de complétude de la validation pour chacune des exigences identifiées au point 1, comme indiqué ci-dessous:
   a. Chacune des exigences a été validée, à un certain niveau hiérarchique par une revue, une analyse ou un test.
   b. La revue, l'analyse ou le test de chaque exigence est approprié à la validation de l'exigence, en particulier vis à vis de la sécurité.
   c. Les résultats de la revue, de l'analyse ou du test associés à la validation de chaque exigence sont exacts, et tous les écarts entre les résultats réels et les résultats attendus sont expliqués. Lorsque les résultats attendus ne sont pas pré-établis, comme ce peut être le cas pour les revues et les analyses, les produits des activités de la validation doivent être cohérents avec les exigences, en particulier vis à vis des exigences de sécurité.

   NOTA : Les critères de complétude de la validation peuvent être établis à partir des exigences, des considérations de sécurité, du mode opérationnel ou de l'implémentation.

3. Evaluation des exigences dérivées vis à vis de leur incidence sur la sécurité.
4. Evaluation de la complétude des exigences dérivées vis à vis des exigences du système allouées à l'article matériel. Pour les finalités de ce processus, un ensemble d'exigences est complet lorsque tous les attributs que l'on a défini sont nécessaires et que tous les attributs nécessaires ont été définis.
5. Evaluation de l'exactitude des exigences dérivées du matériel, vis à vis des exigences du système allouées à l'article matériel. Pour les finalités de ce processus, une exigence est exacte lorsqu'elle est définie sans ambiguïté et qu'il n'y a pas d'erreurs dans les attributs définis.
6. Mise en place des liens de traçabilité entre les exigences dérivées, les activités de validation et les résultats.
7. Réintroduction des omissions et des erreurs d'exigences dans les processus appropriés afin de leur apporter une solution.

6.2 PROCESSUS DE VERIFICATION

Le processus de vérification donne l'assurance que l'article matériel réalisé satisfait les exigences. La vérification consiste en des revues, des analyses et des tests appliqués comme défini par le plan de vérification. Le processus de vérification devrait comporter une évaluation des résultats.

NOTA 1 : Les aspects sécurité de la conception du matériel prennent la forme d'exigences de sécurité à satisfaire par l'implémentation du matériel.

Ce chapitre donne des recommandations pour le processus de vérification à appliquer à la conception du matériel. Le processus de vérification peut être appliqué à tous les niveaux hiérarchiques de la conception, tel que défini par le plan de vérification. En ce qui concerne les exigences de sécurité, il est avantageux d'appliquer le processus de vérification aux différentes étapes du processus de conception, afin d'augmenter la probabilité d'élimination des erreurs de conception pour l'obtention d'un niveau de confiance élevé. Pour certains niveaux d'assurance, la satisfaction des objectifs de vérification doit être obtenue avec indépendance comme décrit par l'Annexe A.

Les processus de vérification du logiciel, d'intégration du matériel et du logiciel, et d'intégration du système, ne sont pas traités ici. Néanmoins, la vérification des exigences du matériel au cours de ces processus est une méthode recevable pour la vérification du matériel.

Les modifications d'une configuration précédemment vérifiée peuvent être re-vérifiées par similitude, par analyse, par de nouveaux jeux de tests, ou en reconduisant une partie de la vérification antérieure.

NOTA 2 : L'exécution de tests informels, hors du processus de vérification documenté, est recommandée. Les procédures de test et les résultats ne sont pas maintenus sous contrôle de la gestion de la configuration, mais ils sont très efficaces pour la détection et l'élimination des erreurs de conception au début du processus de conception. Un crédit de vérification ne peut être obtenu pour ces tests que s'ils sont formalisés.

6.2.1 Objectifs du processus de vérification

Les objectifs du processus de vérification sont de :

1. Fournir la preuve de la satisfaction des exigences par l'implémentation matérielle.
2. Etablir la traçabilité entre les exigences du matériel, l'implémentation, les procédures et les résultats de la vérification.
3. Identifier des critères les tests d'acceptation, s'assurer qu'ils sont réalisables et cohérents avec le niveau d'assurance conception des fonctions du matériel.
4. Réintroduire les omissions et les erreurs dans les processus appropriés afin de leur apporter une solution.

6.2.2 Activités du processus de vérification

Les objectifs du processus de vérification peuvent être satisfaits par une combinaison de méthodes telles que les revues, les analyses, le développement et l'exécution de tests. Les plans de vérification doivent décrire les activités à exercer afin de démontrer la conformité aux exigences.

Recommandations pour les activités de vérification :

1. Identification des exigences qui nécessitent une activité de vérification. Il n'est pas demandé de vérifier les exigences à tous les niveaux hiérarchiques: elles peuvent être vérifiées à un niveau plus élevé.
2. Choix et exécution de méthodes de vérification telles que les tests, la simulation, le prototypage, les analyses et les revues.
3. Mise en place des éléments de traçabilité entre les exigences, l'implémentation, les procédures et les résultats de la vérification. La traçabilité doit être cohérente avec le niveau d'assurance conception de la fonction que réalise le matériel. Il n'est pas demandé d'établir la traçabilité jusqu'aux composants élémentaires tels que les résistances, les capacités ou les portes logiques, à moins que ce ne soit nécessaire du point de vue de la sécurité.
4. Réalisation d'une analyse de la couverture de la vérification afin d'évaluer la complétude du processus de vérification, celle-ci concerne :
    a. La vérification de chacune des exigences à un niveau hiérarchique donné, par une revue, une analyse ou un test.
    b. La pertinence de la revue, de l'analyse ou du test, de chacune des exigences afin de la vérifier en particulier vis à vis des exigences de sécurité.

c. L'exactitude des résultats de la revue, de l'analyse ou du test associés à la vérification de chacune des exigences, et l'explication des écarts entre les résultats réels et attendus. Lorsque les résultats attendus ne sont pas préétablis, ce qui peut être le cas pour les revues et les analyses, les résultats de l'activité de vérification doivent être cohérents avec l'exigence, en particulier vis à vis des exigences de sécurité.

5. Documentation des résultats des activités de vérification.
6. Réintroduction des omissions et des erreurs dans les processus appropriés afin de leur apporter une solution.

6.3 METHODES DE VALIDATION ET DE VERIFICATION

Ce paragraphe décrit des méthodes qui peuvent être utilisées à la fois pour la validation et pour la vérification.

6.3.1 Le test

Le test est une méthode de confirmation de l'exactitude des réponses à un stimulus ou à une série de stimuli. Exemples: les tests fonctionnels de l'article matériel, les tests sur banc système, les tests sur les installations de validation du système et les tests sur l'aéronef.

Les tests peuvent être effectués sur des équipements de tests manuels, automatisés ou spécialisés. Les tests peuvent également tirer partie des dispositifs internes au matériel, tels que les éléments propres aux tests intégrés, au cours du processus de vérification.

Lorsqu'il est impossible de vérifier une exigence particulière en excitant l'article matériel dans l'environnement opérationnel souhaité, d'autres moyens de vérification doivent être fournis et justifiés.

Les tests peuvent être effectués au cours des différents processus de conception du matériel. Pour obtenir un crédit de certification, à partir de tests, il faut un article géré en configuration. Les résultats des tests d'intégration du système ou d'intégration du matériel et du logiciel, peuvent aussi être utilisés pour l'obtention de crédits de tests.

Recommandations pour les tests :

1. Identification de chaque exigence à valider ou vérifier. Les exigences de test environnementaux font partie de ces exigences.
2. Définition pour chacun des cas de test, des stimuli, de la séquence et des conditions de test telles que la température ambiante et la tension appliquée.
3. Définition des critères de succès et d'échec et de la méthode d'enregistrement des résultats avant exécution des tests.
4. Enregistrement de l'identification et des dates d'étalonnage de chaque équipement de test.
5. Enregistrement de l'identité de configuration de l'article matériel soumis au test.
6. Enregistrement et conservation des résultats des tests.
7. Réintroduction des défaillances détectées par le test au niveau approprié des processus afin de leur apporter une solution.

6.3.2 L' analyse

L'analyse est une méthode détaillée, et reproductible d'évaluation des caractéristiques d'un article matériel donné qui permet de démontrer qu'une exigence spécifique est satisfaite. Les analyses, de contraintes, de marges de mode commun, de pires cas et de la couverture des tests sont des exemples. L'expérience en exploitation peut fournir des données pour différentes analyses.

NOTA : Lorsque la complexité de la conception du matériel augmente, il est bénéfique d'utiliser des outils informatiques tels que les simulateurs, afin de vérifier les exigences et l'implémentation de la conception.

Les analyses peuvent consister en un examen détaillé de la fonctionnalité, des performances, de la traçabilité, et des implications de la sécurité d'une fonction de l'article matériel et de ses interdépendances avec d'autres fonctions à l'intérieur d'un système ou d'un équipement de bord. L'analyse effectuée individuellement, ou en combinaison avec d'autres méthodes de vérification, fournit la preuve qu'une exigence a été correctement implémentée. L'analyse doit s'appuyer sur les données fournies par le processus de conception, l'expérience en exploitation ou sur d'autres bases de données disponibles.

La simulation est un outil de conception important à la fois pour la visualisation du fonctionnement des circuits, et pour les fonctionnements à des niveaux supérieurs. La simulation peut être utilisée pour l'analyse d'impact des dispersions des paramètres du matériel en production, ce qui est difficile à réaliser en utilisant d'autres moyens de vérification, et par conséquent donner confiance en l'élimination des erreurs de conception liées à cette dispersion ayant une incidence sur la sécurité. Les résultats dépendent des modèles et des scénarios mis en œuvre, par conséquent ceux-ci ne peuvent pas être utilisés seuls pour l'obtention d'un crédit de certification sans apporter la preuve de leur validité.

Exemples d'analyses :

1. **Analyse Thermique.** L'analyse thermique vérifie que la réalisation de la conception satisfait aux exigences lorsqu'elle est soumise à l'environnement thermique opérationnel.
2. **Analyse de Contraintes.** L'analyse de contrainte vérifie que les composants satisfont aux critères de détarage sur la totalité de la gamme opérationnelle.
3. **Analyse de Fiabilité.** L'analyse de fiabilité démontre que l'implémentation de la conception satisfait aux exigences de fiabilité du produit.
4. **Analyse de Marge de Conception.** L'analyse de marge de conception vérifie que l'implémentation de la conception satisfait aux exigences fonctionnelles compte tenu de la dispersion des composants.
5. **Analyse de Similitude.** L'analyse de similitude compare les caractéristiques et l'utilisation à celles de systèmes certifiés auparavant.
6. **Analyse de Simulation.** L'analyse de simulation compare les résultats de celle-ci aux résultats attendus.

6.3.3 Les revues

La revue est une méthode qualitative d'évaluation des plans, des exigences, des données de conception, du concept ou de l'implémentation de la conception.

Les revues doivent être effectuées tout au long du cycle de vie du matériel comme indiqué dans le plan approprié. Toute les revues utilisées pour l'obtention d'un crédit de certification doivent être identifiées par les plans de validation et de vérification.

Recommandations pour les revues :

1. Connaissance nécessaire du sujet par les participants pour réaliser les revues.
2. Utilisation des résultats des revues pour autoriser ou interdire le passage entre les activités des processus du cycle de vie de la conception.
3. Documentation des résultats des revues, y compris des décisions prises et du traitement des actions à effectuer

6.3.3.1 Revue des exigences

La revue des exigences est une méthode qui peut garantir l'acceptabilité des exigences. Une seule et même revue des exigences peut répondre à la fois aux objectifs des processus de validation et de vérification.

Les modifications d'exigences qui apparaissent après la revue initiale des exigences devraient être soumises au même processus de revue que celui utilisé initialement, ou à un processus de revue équivalent. La validation des exigences du système allouées à l'article matériel ne font pas partie des buts de cette revue.

Recommandations pour la revue des exigences :

1. Non ambiguïté, vérifiabilité, complétude de la description détaillée de chaque exigence pour le niveau hiérarchique considéré et absence de conflits avec les autres exigences.
2. Cohérence des exigences dérivées et les exigences système ou les exigences dont elles sont dérivées.
3. Cohérence des exigences avec la SSA.
4. Définition et réintroduction dans la SSA des exigences dérivées de sécurité.
5. Compatibilité des exigences avec les règles de conception du matériel applicables.
6. Compatibilité des exigences avec les possibilités et les limitations des technologies disponibles.
7. Cohérence des caractéristiques des composants telles que les performances, les gammes de températures, le détarage et le déverminage avec les exigences de sécurité et de fiabilité.
8. Prise en compte de l'aptitude de l'article matériel à être testé, maintenu et fabriqué.
9. Définition des exigences d'interface entre le matériel et le logiciel.
10. Traçabilité ascendante vers le niveau hiérarchique précédent, conformément au critère défini par le plan.
11. Recueil des exigences dérivées résultant de contraintes d'implémentation qui ne sont pas vérifiées à un niveau hiérarchique supérieur.
12. Réintroduction des omissions et des erreurs dans les processus appropriés afin de leur apporter une solution.

NOTA 1 : Les questions ci-dessous peuvent aider à évaluer la complétude des exigences :

- *a. Les exigences de niveau supérieur ont-elles été toutes prises en considération ?*
- *b. Les règles et les recommandations applicables ont-elles été prises en considération ?*
- *c. Les fonctions et les interfaces du matériel sont elles toutes couvertes ?*
- *d. L'architecture est-elle entièrement couverte ?*
- *e. L'implémentation du matériel qui doit être vérifiée est-elle spécifiée de manière adéquate ?*
- *f. Les caractéristiques de comportements interdits sont-elles couvertes par l'évaluation de sécurité ?*
- *g. L'environnement opérationnel est-il suffisamment spécifié ?*
- *h. Les hypothèses et les contraintes sont-elles prises en compte ?*
- *i. Est-ce que cette implémentation résout les problèmes connus sur des matériels existants ou similaires ?*

NOTA 2 : Les questions ci-dessous peuvent aider à évaluer l'exactitude des exigences :

- *a. Les exigences sont-elles en accord avec les exigences de niveau supérieur ?*
- *b. Les exigences sont-elles en accord avec les exigences du système allouées à l'article matériel ?*
- *c. Les exigences expriment-elles des "QUOI" à la place de "COMMENT"?*
- *d. Les exigences sont-elles non ambiguës ?*
- *e. Peut-on implémenter les exigences ?*
- *f. Peut-on vérifier les exigences ?*
- *g. Les modes de fonctionnement ont-ils été définis ?*

h. Les exigences sont-elles cohérentes avec les évaluations de la sécurité ?

i. Les hypothèses et les contraintes sont-elles correctement identifiées en tant qu'exigences dérivées ?

6.3.3.2 Revue de conception

La revue de conception est une méthode pour déterminer si les données de conception et l'implémentation satisfont aux exigences. Les revues de conception doivent être effectuées, telles que définies par les plans, à différentes étapes tout au long du cycle de vie de la conception du matériel. Exemples: revues de conception générale, de conception détaillée et d'implémentation. Pour les conceptions réparties sur plusieurs niveaux hiérarchiques de l'article matériel, telles que les ASICs et les cartes, les revues de conception doivent être placées aux endroits où le potentiel de garantie d'exactitude de la conception est le plus grand.

Recommandations pour la revue de la conception :

1. Prise en compte de l'ensemble des exigences, évaluation de la pertinence de la définition des exigences dérivées et des données de la conception.
2. Prise en compte des exigences d'environnement.
3. Prise en compte des exigences de sécurité et de fiabilité.
4. Identification explicite des points de la conception touchant la sécurité.
5. Capacité de la conception à être implémentée, testée et maintenue.
6. Evaluation des nouvelles techniques de fabrication.
7. Satisfaction des critères de sélection des composants identifiés dans les plans.
8. Traçabilité de la conception vis à vis des exigences.
9. Réintroduction des omissions et des erreurs dans les processus appropriés afin de leur apporter une solution.

CHAPITRE 7

PROCESSUS DE GESTION DE LA CONFIGURATION

Le processus de gestion de la configuration a pour but de permettre de reproduire de manière conforme l'article de configuration, de régénérer les informations et de modifier l'article de configuration de manière maîtrisée, si nécessaire. Ce chapitre décrit les objectifs de gestion de la configuration du matériel ainsi que les activités qui supportent ces objectifs.

7.1 OBJECTIFS DE GESTION DE LA CONFIGURATION

Les objectifs du processus de gestion de la configuration sont :

1. Identifier et documenter les articles de configuration de manière unique.
2. Garantir la duplication conforme et exacte de l'article de configuration.
3. Fournir une méthode de maîtrise de l'identification et de la traçabilité des modifications des articles de configuration.

7.2 ACTIVITES DE GESTION DE LA CONFIGURATION

Recommandations pour les activités de gestion de la configuration :

1. Identification de manière unique de l'article de configuration, documentation et contrôle de celui-ci. Ceci peut être appliqué sans que ce soit exhaustif, au matériel, aux représentations de la conception du matériel, aux outils ou aux autres éléments de données utilisés pour les crédits de certification et par les référentiels.
2. Elaboration des référentiels.
3. Identification de manière unique, traçage et élaboration des constats de problèmes.
4. Maintenance de la gestion et de la traçabilité des modifications. Ceci implique que les données du cycle de vie identifiées par les plans soient mises en lieu sûr et puissent être restaurées.
5. Maîtrise de l'archivage, de la restauration et de la mise à disposition des articles de configuration.

Des méthodes différentes peuvent être utilisées pour satisfaire aux objectifs de gestion de la configuration, les paragraphes ci-dessous donnent des recommandations pour les activités qui peuvent être effectuées en tant que méthodes acceptables.

7.2.1 Identification de la configuration

Le but de l'activité d'identification de la configuration est d'étiqueter de manière non ambiguë chaque article de configuration de telle sorte qu'une base soit établie pour le contrôle et la mise en référence des articles de configuration.

Recommandations pour l'identification de la configuration :

1. Création des identifications de la configuration pour les éléments de données.
2. Création d'une identification de la configuration pour chaque article de configuration, pour chaque élément de l'article de configuration contrôlé individuellement et pour les combinaisons d'articles de configuration qui constituent un produit conforme aux plans acceptés par l'autorité de certification.

   NOTA : Le niveau de détail avec lequel sont identifiés les composants, tels que les ASICs, les PLDs programmés, les cartes équipées et les boites noires est défini par le Plan de Gestion de la Configuration.

3. Création d'une identification de la configuration pour les composants COTS et les articles matériels précédemment développés, avant leur intégration dans le référentiel.
4. Création d'une identification de la configuration pour chaque article de configuration appelé par d'autres items de données ou utilisé pour la fabrication du produit, avant son intégration dans un nouveau référentiel.

7.2.2 Elaboration du référentiel

L'élaboration du référentiel a pour but de définir une base pour des activités ultérieures et de permettre de faire référence aux articles de configuration, de les gérer et d'assurer la traçabilité entre les articles.

Recommandations pour l'élaboration du référentiel :

1. Elaboration d'un référentiel pour les articles de configuration utilisés pour l'obtention de crédits de certification.

   NOTA : *Des référentiels intermédiaires peuvent être élaborés pour aider à maîtriser les activités liées au matériel.*

2. Application des procédures de gestion des modifications dès lors qu'un référentiel a été élaboré.
3. Application des recommandations pour la gestion des modifications lors du développement d'un référentiel dérivé d'un référentiel existant.
4. Elaboration des éléments de traçabilité avec un référentiel antérieur, lorsque pour le développement d'un nouveau référentiel, un crédit de certification est recherché pour des activités ou des données associées au référentiel dont il est dérivé.

   NOTA : *Le référentiel peut-être celui d'un article de configuration, d'un article matériel précédemment certifié ou d'un composant COTS.*

7.2.3. Constat d'anomalies et suivi des actions correctives

Le but du constat d'anomalies et du suivi et des actions correctives est d'enregistrer les problèmes et de garantir la pertinence de leur classement et leur solution. Les anomalies peuvent concerner la non conformité aux plans et aux règles, les insuffisances des produits des processus du cycle de vie, les comportements anormaux du produit, les inadaptations ou les carences des outils et des processus technologiques. Le constat des anomalies devraient être mis en place au plus tard lors de l'élaboration du référentiel pour lequel un crédit de certification est recherché.

Recommandations pour le constat d'anomalies et le suivi des actions correctives :

1. Couverture par un constat de chaque anomalie mise en évidence.
2. Identification de la configuration des articles de configuration affectés dans un constat d'anomalies.
3. Invocation des activités de gestion des modifications pour les constats d'anomalies qui impliquent des actions correctives.
4. Description des actions qui ont été faites pour clore le constat d'anomalies, y compris la réalisation complète des modifications des éléments de données nécessaires à l'application de l'action corrective.
5. Non obligation de clore tous les constats d'anomalies pour obtenir la certification, cependant toutes les anomalies doivent être évaluées et celles qui sont reconnues avoir des incidences sur la sécurité ou sur la certification doivent être closes.
6. Suivi de la situation du constat d'anomalies par le système de gestion des constats, y compris leur approbation et leur classement.

7.2.4 Gestion des modifications

Le but de l'activité de gestion des modifications est de garantir l'enregistrement, l'évaluation, et l'approbation des modifications. La gestion des modifications doit être effectuée conformément au plan et commencer au plus tard lors de l'élaboration du référentiel à partir duquel la certification est recherchée.

Recommandations pour la gestion des modifications.

1. Conservation par la gestion des modifications de l'intégrité des articles de configuration en apportant des protections contre les modifications non autorisées.
2. Garantie par la gestion des modifications, de l'évaluation des modifications afin de déterminer si l'identification de configuration doit ou non être mise à jour.
3. Enregistrement, approbation et suivi des modifications des articles soumis à la gestion des modifications. L'autorité chargée de l'approbation est définie dans le plan de gestion de configuration.

   NOTA 1 : Le constat des anomalies est lié à la gestion des modifications, car le traitement des anomalies constatées peut entraîner des modifications des articles de configuration.

   NOTA 2 : D'une manière générale, il est admis qu'une mise en place précoce de la gestion des modifications aide à la maîtrise et à la gestion des activités des processus.
4. Assurance par la gestion des modifications de la traçabilité de la modifications vers la cause de celle-ci.
5. Assurance par la gestion des modifications de l'évaluation de l'impact de la modification afin de déterminer l'effet de celle-ci sur les produits des processus et sur la mise à jour des données.

   NOTA 1 : Certaines ou toutes les activités des processus peuvent nécessiter une reprise à partir du point où leurs produits sont affectés.

   NOTA 2 : Il est admis que les modifications des outils de fabrication, des processus technologiques ou des éléments venant de l'extérieur peuvent avoir une incidence sur la conception.
6. Assurance par la gestion des modifications de rétroactions vers les processus concernés.

7.2.5 Mise à disposition, archivage et restauration

Le but de l'activité de mise à disposition est de placer les données sous le contrôle de la gestion de la configuration afin de garantir que seules les données autorisées soient utilisées par les autres activités. Le but des activités d'archivage et de restauration est de garantir que les données associées au produit peuvent être restaurées en cas de besoin pour la duplication, la régénération, la répétition de tests ou pour la modification du produit.

Recommandations pour la mise à disposition, l'archivage et la restauration:

1. Identification et mise à disposition des articles de configuration avant leur utilisation par la fabrication et définition de la responsabilité de leur mise à disposition.
2. Restauration des données associées au produit à partir d'une source approuvée, telle que l'organisation ou la société chargée du développement.

   NOTA : Les données de gestion des modifications et les constats d'anomalies font partie des items de données.
3. Disponibilité des procédures de conservation des données, afin de répondre aux exigences de navigabilité, et de permettre les modifications.
4. Elaboration des procédures qui garantissent l'intégrité des données stockées aussi longtemps qu'exigé par l'autorité de certification, en:
   a. Garantie d'absence de modifications non autorisées.
   b. Sélection les supports de stockage.

c. Maintien de la disponibilité des données stockées. Par exemple, par l'activation ou le rafraîchissement des données archivées à une fréquence compatible avec la durée de vie du stockage préconisée pour le support.

d. Garantie qu'un événement unique pouvant provoquer la perte irrémédiable des données archivées est improbable. Par exemple, en stockant des copies dupliquées dans des sites d'archives physiquement séparés.

7.3 CATEGORIES DE CONTROLE DES DONNEES

Deux catégories sont définies pour le contrôle des données de gestion de la configuration : la catégorie de contrôle 1 du matériel (HC1) et la catégorie 2 (HC2). Elles permettent un contrôle moins contraignant pour certains types de données. La catégorie HC1 implique la réalisation de toutes les activités de gestion de la configuration, alors que la catégorie HC2 est moins restrictive. Les données classées HC2 ne doivent pas être modifiées de façon incrémentale mais doivent être remplacées par de nouvelles données.

Le Tableau 7-1 identifie les activités de gestion de la configuration qui doivent être réalisées en fonction des catégories HC1 et HC2. Par exemple, le Tableau 7-1 montre que les données identifiées au Tableau A-1 de l'Annexe A en catégorie HC2, doivent être restaurées mais ne doivent pas être mises à disposition. En plus, le Tableau 7-1 montre que les données de la catégorie HC1 doivent avoir un référentiel.

L'Annexe A identifie la catégorie de contrôle pour chaque item de données en fonction du niveau d'assurance conception du matériel. Par exemple, dans le Tableau A-1, la catégorie HC1 est applicable aux exigences du matériel pour tous les niveaux d'assurance, tandis que la catégorie HC2 n'est applicable qu'aux revues et aux résultats d'analyses du matériel pour tous les niveaux d'assurance.

Tableau 7-1 Activités du processus de gestion de configuration associées aux catégories HC1 et HC2

Référence	Activités de Gestion de la configuration	HC1	HC2
7.2.1	Identification de la configuration	X	X
7.2.2 (1),(2),(3)	Référentiels	X	
7.2.2 (4) ①	Traçabilité du référentiel	X	X
7.2.3	Constats d'anomalies	X	
7.2.4 (1),(2)	Gestion des modifications - intégrité et identification	X	X
7.2.4 (3),(4),(5),(6)	Gestion des modifications - enregistrements, Approbation et traçabilité	X	
7.2.5 (1)	Mise à disposition	X	
7.2.5 (2)	Restauration	X	X
7.2.5 (3)	Conservation des données	X	X
7.2.5 (4a)	Protection vis à vis des modifications non autorisées	X	X
7.2.5 (4b),(4c),(4d)	Choix du support, rafraîchissement, duplication	X	

① L'identification des données catégorie HC2 à utiliser pour un nouveau référentiel n'implique pas de re-classification des données en HC1.

CHAPITRE 8

ASSURANCE PROCESSUS

L'assurance processus garantit que les objectifs des processus du cycle de vie ont été satisfaits et que les actions ont été accomplies conformément aux plans ou que les dérogations ont été traitées. Ce chapitre décrit les objectifs de l'assurance processus ainsi que les actions qui supportent ces objectifs. Il n'y a pas ici de volonté d'imposer une structure d'organisation particulière.

Les actions de l'assurance processus devraient être accomplies avec indépendance, dans le but d'évaluer objectivement les processus du cycle de vie, d'identifier les écarts et de garantir les actions correctives.

8.1 OBJECTIFS DE L'ASSURANCE PROCESSUS

Les objectifs de l'assurance processus sont de :

1. Garantir que les processus du cycle de vie sont conformes aux plans approuvés.
2. Garantir que les données du cycle de vie produites sont conformes aux plans approuvés.
3. Garantir que l'article matériel utilisé pour l'évaluation de la conformité est élaboré pour satisfaire aux données du cycle de vie associé.

8.2 ACTIVITES DE L'ASSURANCE PROCESSUS

Recommandations pour les activités de l'assurance processus :

1. Garantie de la disponibilité des plans du matériel, comme spécifié par la section processus de planification de ce document et comme convenu dans le PHAC.
2. Garantie de la tenue des revues conformément aux plans approuvés, du suivi et de la réalisation des actions induites jusqu'à leur clôture.
3. Garantie de détection, d'enregistrement, d'évaluation, d'approbation, de suivi et de résolution des écarts par rapport aux plans et aux règles du matériel.
4. Garantie de satisfaction des critères de transition des processus du cycle de vie du matériel en accord avec les plans approuvés.

   NOTA : L'audit est une méthode efficace pour réaliser les actions des points 1 à 4 ci-dessus.

5. Réalisation d'une inspection, pour garantir que l'article matériel est construit en conformité avec ses données de conception.

   NOTA : L'Inspection du Premier Article est un exemple de cette action.

6. Production des enregistrements des actions d'assurance processus, y compris des preuves d'évaluation de l'achèvement des actions de conception.
7. Garantie, le cas échéant, de la conformité des processus utilisés par les sous-contractants vis à vis des plans du matériel.

CHAPITRE 9

PROCESSUS DE COORDINATION POUR LA CERTIFICATION

Le but du processus de coordination pour la certification est de mettre en place les moyens de communication et de compréhension entre le postulant et l'autorité de certification au cours du cycle de vie de la conception du matériel, pour aider au processus de certification. Le processus de coordination pour la certification doit se dérouler tel que décrit au processus de planification du matériel du Chapitre 4, et au PHAC du Paragraphe 10.1.1. Un résumé des produits de ce processus est fourni par le Tableau A-1 de L'Annexe A. De plus, les actions de coordination peuvent inclure la présentation de l'approche de la conception en vue de l'approbation de sa pertinence, les négociations relatives aux moyens de mise en conformité à la base de certification, l'approbation de démarche de conception, les moyens d'approbation des données, ainsi que toutes les demandes de présence aux revues et aux essais exprimées par l'autorité de certification.

A la fin du projet, un résumé du processus de conception suivi, les données produites et un état de l'article matériel devraient être décrits dans le Résumé des Travaux Réalisés, Paragraphe 10.9.

9.1 MOYENS DE DEMONSTRATION DE LA CONFORMITE ET PLANIFICATION

Le postulant propose les moyens de démonstration de la conformité du matériel. Le PHAC définit les moyens de démonstration de la conformité proposés.

Recommandations pour la démonstration de la conformité :

1. Soumission pour revue par l'autorité de certification du PHAC, du plan de vérification du matériel et des autres documents requis, à un moment où l'effet des modifications sur le programme est minimal.
2. Résolution des problèmes identifiés par l'autorité de certification relatifs à la planification des aspects matériels de la certification.
3. Obtention d'un accord sur le PHAC de la part de l'autorité de certification.
4. Coordination permanente avec l'autorité de certification pendant le cycle de développement et de certification comme indiqué par le plan, et résolution appropriée des problèmes soulevés.

Pour certains programmes, la coordination pour la certification n'est pas assurée par le constructeur de l'équipement, mais par l'avionneur ou par un autre client qui bénéficie du support du constructeur de l'équipement. Cette relation doit être définie dans le PHAC et les contacts avec l'autorité de certification doivent passer par le postulant. Il est de la responsabilité du postulant de garantir que les données sont fournies à l'autorité de certification.

Lorsque certains articles matériel intégrés à l'équipement, sont achetés à un sous-contractant, le plan de certification doit identifier les données attendues de celui-ci et celles produites par le postulant.

Il est acceptable qu'un postulant intègre le PHAC et le plan de vérification ainsi que d'autres plans afférents dans le plan de certification de plus haut niveau.

9.2 JUSTIFICATION DE LA CONFORMITE

Le postulant apporte la preuve que les processus du cycle de vie de la conception du matériel sont conformes aux plans du matériel. Les revues par les autorités de certification peuvent avoir lieu dans les locaux du postulant ou dans ceux des fournisseurs du postulant. Le postulant organise ces revues et met à disposition, suivant le besoin, les données du cycle de vie de conception du matériel.

Le postulant doit :

1. Résoudre les problèmes soulevés par l'autorité de certification qui résultent de ces revues.
2. Soumettre à l'autorité de certification le Résumé des Travaux Réalisés (Paragraphe 10.9) et le Dossier de l'Ensemble Supérieur (10.3.2.2.1)
3. Soumettre ou rendre disponible toute autre donnée ou preuve de conformité requise par l'autorité de certification.

CHAPITRE 10

DONNEES DU CYCLE DE VIE DE LA CONCEPTION DU MATERIEL

Ce chapitre décrit les données du cycle de vie de la conception du matériel qui peuvent être produites, pour apporter la preuve de l'assurance conception et de la conformité aux exigences de certification. L'étendue, la quantité et le niveau de détail des données du cycle de vie nécessaires à l'autorité de certification, comme preuves de l'assurance conception, dépendront de plusieurs facteurs. Ces facteurs concernent les exigences de l'autorité de certification pour les systèmes de bord, les niveaux d'assurance conception alloués, la complexité et l'expérience en exploitation du matériel. Les détails de la preuve d'assurance conception devraient être identifiés, enregistrés dans le PHAC et acceptés par l'autorité de certification.

Les considérations complémentaires du Chapitre 11, et les considérations d'assurance conception propres aux fonctions de niveau A et B données en Annexe B, peuvent conduire à produire des données supplémentaires du cycle de vie.

L' Annexe A, décrit les données du cycle de vie de la conception à produire, le degré d'indépendance de la vérification, et la catégorie de contrôle des données définie par le Chapitre 7, pour chacun des niveaux d'assurance conception du matériel.

1. Les données du cycle de vie de la conception du matériel devraient être :
   a. **Non Ambiguës.** Les informations et les données sont exprimées en des termes qui ne permettent qu'une seule interprétation.
   b. **Complètes.** Les informations et les données contiennent les exigences nécessaires et pertinentes ainsi que les supports descriptifs, l'identification des schémas, les définitions des termes, et les unités de mesure.
   c. **Vérifiables.** L'exactitude des informations et des données peut être contrôlée par une personne ou un outil.
   d. **Cohérentes.** Les informations et les données sont cohérentes lorsqu'elles ne contiennent pas de contradiction.
   e. **Modifiables.** Les informations et les données sont structurées et permettent de faire des modifications de manière complète, cohérente et correcte tout en conservant la structure.
   f. **Traçables.** L'origine des informations et des données peut être établie.

Les descriptions de ce chapitre n'ont pas pour but de recommander une méthode particulière de mise en forme des données, de présentation ou d'organisation des données du cycle de vie du matériel dans un dossier. Par exemple, tous les plans, les règles et les procédures peuvent être décrits dans un ou plusieurs documents.

2. La méthode de constitution des dossiers de données, leur forme et leur organisation doivent être proposées dans le PHAC et un accord avec l'autorité de certification doit être obtenu au début du programme.
3. Les informations ayant fait l'objet d'un accord doivent pouvoir être restaurées et mises à disposition tout au long de la vie en exploitation du système ou de l'équipement de bord.

10.1 PLANS DU MATERIEL

Les plans du matériel décrivent les processus, les procédures, les méthodes et les règles à utiliser pour la certification , la conception, la validation, la vérification, l'assurance processus et la gestion de la configuration du matériel.

10.1.1 Plan des aspects matériels de la certification

Le PHAC définit les processus, les procédures, les méthodes et les règles à utiliser pour satisfaire aux objectifs d'après ce document et obtenir l'approbation de l'autorité de certification pour le système qui contient les articles matériels. Dès lors qu'il a été approuvé, le PHAC constitue l'accord entre le postulant à l'approbation et l'autorité de certification, pour les processus et les activités à conduire et les preuves à produire qui en découlent afin de satisfaire les aspects matériels de la certification. Le PHAC peut faire partie d'un autre plan, par exemple le plan de certification du système de bord.

Le PHAC devrait inclure :

1. **Une Vue d'Ensemble du Système.** Ce chapitre donne une vue générale du système de bord dans lequel les articles matériels seront utilisés y compris une description des fonctions du système, des cas de défaillance, de son architecture, des allocations de fonctions aux articles matériels et logiciels et les références aux documentations du système existantes.
2. **Une Vue d'Ensemble du Matériel.** Ce chapitre décrit les fonctions du matériel, les articles matériels, l'architecture, les nouvelles technologies qui seront utilisées, toutes les techniques de sûreté intrinsèque, de tolérance aux fautes, de redondance et de partitionnement à utiliser.
3. **Les Procédures de Certification.** Ce chapitre décrit la base de certification, les moyens d'obtention de la conformité proposés et le niveau d'assurance conception pour chacune des fonctions de l'article matériel. Il donne aussi les justifications concernant l'allocation du niveau d'assurance conception du matériel en se référant à l'évaluation de la sécurité du matériel et à son utilisation dans le système de bord, y compris une description des cas de défaillance du matériel explicitées au Paragraphe 2.3.4 . S'il y a lieu, il doit également inclure soit un résumé de la FFPA, soit un plan de réalisation de la FFPA et d'utilisation des résultats.
4. **Le Cycle de Vie de la Conception du Matériel.** Ce chapitre décrit les procédures, les méthodes et les règles à appliquer, ainsi que les processus et les activités à effectuer afin de satisfaire aux objectifs d'assurance conception du matériel. Il décrit les activités, leurs combinaisons et leurs séquences, les relations entre processus et activités, les critères de transition, les responsabilités, les utilisations d'outils, et les canaux de communication pour les rétroactions et les interactions entre les processus du matériel, ainsi qu'entre les processus du matériel et les processus du système et du logiciel. Ce chapitre peut faire référence aux plans, aux politiques, aux règles, aux procédures et aux dérogations par rapport aux plans et règles applicables au programme.
5. **Les Données du Cycle de Vie de la conception du Matériel.** Ce chapitre décrit ou donne les références des données à produire et à soumettre ou à mettre à disposition comme preuve de conformité aux objectifs décrits par ce document et aux plans.
6. **Les Considérations Complémentaires.** Ce chapitre décrit les considérations complémentaires. Celles-ci concernent l'utilisation de matériels développés auparavant, y compris les références aux données réutilisées, l'utilisation de COTS, l'expérience en exploitation du produit, l'évaluation et la qualification des outils décrites au Chapitre 11 ou les procédures d'assurance conception pour les fonctions de niveau A et B décrites par l'Annexe B.
7. **Les Méthodes Alternatives.** Ce chapitre décrit toutes les méthodes alternatives proposées pour le programme qui soit ne sont pas décrites dans ce document, soit sont appliquées d'une manière différente de celle décrite dans celui-ci. Les justifications expliquant pourquoi ces méthodes sont acceptables doivent être données.
8. **Le Calendrier de la certification.** Ce chapitre identifie les principaux jalons du programme et les dates auxquelles les données du cycle de vie de la conception du matériel seront soumises à l'autorité de certification.

10.1.2 Plan de la conception du matériel

Le plan de la conception du matériel décrit les procédures, les méthodes et les règles de conception à appliquer ainsi que les processus et les activités à accomplir pour concevoir l'article matériel. Ce plan peut être inclus dans le PHAC et donner les références des politiques et des règles de conception à appliquer.

Le plan de la conception du matériel devrait inclure :

1. **Le Cycle de Vie de la Conception du Matériel.** Il donne les référence des politiques et des règles de conception à appliquer et décrit les processus et les activités du cycle de vie de la conception du matériel qui seront utilisés pour atteindre les objectifs de la conception associés au niveau d'assurance du matériel.
2. **La Description du Produit Matériel.** Elle identifie les spécifications du matériel à satisfaire, les utilisations d'alternatives, la durée de vie en opération et les procédures de mise à jour.
3. **Les Méthodes de Conception du Matériel.** Description des méthodes, de recueil des exigences et de spécification, de conception générale et détaillée, et les techniques de synthèse, d'implémentation et de transition vers la production à utiliser pour l'article matériel. Lorsque des techniques de passivation des erreurs pour des fonctions de niveau A et B, décrites par l'Annexe B Paragraphe 3.1, sont envisagées sans être parachevées au moment de la rédaction du plan, décrire comment seront prises les décisions au cours du processus de conception.
4. **L'Environnement de Conception du Matériel.** Description des outils de développement à utiliser.
5. **La Documentation de l'Article Matériel.** Identification des données de la conception du matériel à produire ou des références aux spécifications, des documentations, des numéros de dessin et des numéros de type de l'article matériel développé auparavant.
6. **Autres Considérations.** Description des options technologiques et d'assemblage, de conditionnement et de montage du matériel prévues.

10.1.3 Plan de validation du matériel

Le plan de validation du matériel décrit les procédures, les méthodes et les règles à appliquer ainsi que les processus et les activités à accomplir pour la validation des exigences dérivées de l'article matériel, afin de satisfaire aux objectifs de la validation définis par ce document. Ce plan peut être inclus dans le PHAC et peut faire référence aux règles de validation à appliquer.

Le plan de validation du matériel devrait inclure :

1. **Les Méthodes de Validation.** Description et références des procédures, des règles et des méthodes de validation à utiliser. Les méthodes peuvent comporter des descriptions, des analyses, des revues et des tests.
2. **Les Données de Validation.** Identification et description des preuves à produire en tant que résultats du processus de validation du matériel.
3. **L'Environnement de Validation.** Identification et description des équipements d'analyse et de test à utiliser pour l'accomplissement du processus et des activités de validation.

10.1.4 Plan de vérification du matériel

Le plan de vérification du matériel décrit les procédures, les méthodes et les règles à appliquer, ainsi que les méthodes et les activités de vérification de l'article matériel pour satisfaire aux objectifs de la vérification définis par ce document. Ce plan peut être inclus dans le PHAC et peut faire référence aux politiques et aux règles de vérification à appliquer.

Le plan de vérification du matériel devrait inclure :

1. **Les Méthodes de Vérification.** Description et références aux politiques, aux procédures, aux règles et aux méthodes de vérification à utiliser pour apporter des preuves objectives de l'intégrité des articles matériels, y compris des COTS et des fonctions non utilisées. Ces méthodes peuvent comporter des analyses, des revues et des tests. Lorsque les méthodes d'analyses avancées décrites par l'Annexe B Paragraphe 3.3 sont utilisées, y inclure une description détaillée des méthodes concernant les FFPs et les critères d'achèvement de la vérification applicables.
2. **Les Données de Vérification.** Identification et description des preuves à produire en tant que résultats du processus de vérification du matériel.
3. **L'Indépendance de la Vérification.** Description des moyens à utiliser afin de garantir l'indépendance de la vérification pour les objectifs qui requièrent une indépendance.
4. **Responsabilités Organisationnelles.** Identification des responsables de l'organisation chargée de réaliser le processus de vérification.

10.1.5 Plan de gestion de la configuration du matériel

Le plan de gestion de la configuration du matériel décrit les politiques, les procédures, les règles et les méthodes à utiliser pour satisfaire aux objectifs de gestion de la configuration d'après ce document.

Le plan de gestion de la configuration du matériel devrait inclure :

1. **Les Méthodes de Gestion de la Configuration du matériel.** Description et références des politiques, des procédures, des règles et des méthodes à utiliser pour identifier, gérer et contrôler le matériel et les données du cycle de vie.
2. **Les Référentiels du Matériel.** Description des méthodes, des procédures à utiliser pour construire les référentiels de la conception et du produit et établir la traçabilité des ces référentiels.
3. **Le Constat et la Résolution des Anomalies.** Description des méthodes et des procédures à utiliser pour enregistrer, faire le suivi et résoudre les constats d'anomalies.
4. **La Gestion des Modifications.** Description des méthodes, des procédures à utiliser pour identifier, contrôler et suivre les modifications des données des articles gérés en configuration.
5. **L'Archivage et la Restauration.** Description des procédures de mise à disposition, d'archivage et de restauration des données du cycle de vie de la conception du matériel. Cette description doit inclure le contenu des archives, les formats, les types de supports, les règles de gestion, les méthodes et les critères.
6. **La Maîtrise de l'Environnement.** Description des procédures et des méthodes d'identification et de contrôle des outils utilisés pour le développement et la vérification du matériel.
7. **Les Outils de Gestion de Configuration.** Description des outils et des ressources utilisés par le processus et les activités de gestion de la configuration.

10.1.6 Plan d'assurance processus du matériel

Le plan d'assurance processus du matériel décrit les procédures, les méthodes et les règles à appliquer ainsi que les processus et les activités à accomplir pour satisfaire aux objectifs d'assurance processus de ce document.

Le plan de l'assurance processus du matériel devrait inclure :

1. **Le contrôle des processus.** Description des politiques et des procédures pour la mise en place de l'assurance processus de la conception du matériel.

2. **Les responsabilités organisationnelles.** Identification des organisations chargées de la mise en œuvre de l'assurance processus.
3. **La conformité.** Description des politiques, des procédures et des critères de détermination de la conformité des processus et des produits.
4. **Les activités de l'assurance processus.** Description des revues et des audits de l'assurance processus à accomplir pour démontrer la conformité des processus aux plans et aux règles.
5. **Les dérogations.** Description des méthodes de détection, d'enregistrement, d'évaluation, de résolution et d'approbation des dérogations aux plans et aux règles.

10.2 RECOMMANDATIONS ET REGLES DE CONCEPTION DU MATERIEL

Les recommandations et les règles de conception peuvent définir les consignes, les procédures, les méthodes et les critères qui concernent la conception, la validation, la vérification, l'assurance et la maîtrise des processus que l'on utilise pour évaluer l'acceptabilité et la qualité des résultats. Les règles de conception peuvent ne pas être nécessaires, mais lorsque le postulant y fait référence pour le projet, elles font partie de la base de certification et des plans du projet. Comme pour les plans, ces règles et recommandations peuvent être regroupées dans un ou plusieurs documents. Des outils peuvent être nécessaires pour mettre en application les règles.

10.2.1 Règles d'exigences

Des règles d'exigences peuvent être utilisées pour le processus de recueil des exigences afin de définir les consignes, les procédures, les méthodes, les recommandations et les critères pour le développement des exigences. Les règles d'exigences peuvent comporter des méthodes et des critères pour le développement et la spécification des exigences, des méthodes et des critères pour la validation des exigences, un langage pour exprimer les exigences, des recommandations sur l'utilisation des outils de spécification, ainsi que les moyens utilisés pour transmettre les exigences dérivées aux processus de conception du système.

10.2.2 Règles de conception du matériel

Des règles de conception du matériel peuvent être utilisées au cours des processus de conception générale et détaillée afin de définir les consignes, les procédures, les méthodes, les recommandations et les critères pour la spécification et le développement du matériel à concevoir.

Les règles de conception du matériel peuvent inclure :

1. Les langages et les méthodes de représentation.
2. Les spécifications de conception et les conventions de dénomination.
3. Des recommandations sur les méthodes de conception.
4. Des recommandations sur l'utilisation des outils de conception du matériel.
5. Des recommandations sur la sélection des composants électroniques.
6. Des recommandations sur l'évaluation des conceptions alternatives.
7. Des recommandations sur l'évaluation de structures de conception à sûreté intrinsèque et tolérantes aux fautes.
8. Une description des moyens de transmission et de rétroactions vers le processus de recueil des exigences pour la clarification de celles-ci.

10.2.3 Règles de validation et de vérification

Des règles de validation et de vérification peuvent être utilisées par les processus de validation et de vérification afin de définir les réglementations, les procédures, les méthodes, les recommandations et les critères pour valider, vérifier la conception et l'implémentation du matériel.

10.2.4 Règles d'archivage du matériel

Des règles d'archivage peuvent être utilisées pour définir les procédures, les méthodes et les critères utilisés pour conserver et archiver les données du produit, développer et maintenir les archives du programme et du projet. Les règles d'archivage du matériel peuvent porter sur le contenu des archives, leur format, les types de support, les réglementations, les méthodes et les critères.

10.3 DONNEES DE CONCEPTION DU MATERIEL

Les données de conception du matériel sont constituées par les spécifications, les documents et les dessins qui définissent les articles matériels.

10.3.1 Exigences du matériel

Les exigences spécifient les fonctions, les performances et les objectifs de sécurité, de qualité, de maintenabilité et de fiabilité de l'article matériel à développer.

Les exigences du matériel devraient inclure :

1. Les exigences de conception et de sécurité du système allouées au matériel.
2. L'identification des règles de conception applicables au matériel.
3. Les exigences fonctionnelles et de performances du matériel, y compris les exigences dérivées et les limites des contraintes autorisées pour une utilisation normale.
4. Les exigences de fiabilité et de qualité du matériel, y compris celles relatives aux taux de pannes, aux temps d'exposition et aux contraintes de conception.
5. Les exigences de maintenance et de réparation pendant la vie en exploitation du matériel.
6. Les exigences concernant l'aptitude du matériel à être fabriqué et assemblé.
7. Les exigences de testabilité du matériel.
8. Les exigences de stockage et de manutention du matériel.
9. Les exigences d'installation.

10.3.2 Données de représentation de la conception du matériel

Les données de représentation de la conception du matériel définissent l'article matériel, elles sont constituées de l'ensemble des dessins, des documents et des spécifications qui sont utilisés pour construire l'article matériel. Les paragraphes ci-dessous définissent des données types de la conception du matériel ainsi que leur contenu. Les types de données, les dossiers et les documents produits pour une conception donnée varient en fonction de la taille, de la complexité et du nombre de composants contenus dans l'article matériel.

10.3.2.1 Données de conception générale

Les données de conception générale décrivent l'architecture et la conception fonctionnelle de l'article matériel; elles peuvent inclure :

1. Une description de haut niveau telle que des blocs-diagrammes ou des descriptions HDL qui mettent en évidence les fonctions principales et montrent les flux d'informations entre ces fonctions.
2. La structure de l'implantation mécanique qui donne l'organisation de l'article matériel sous la forme de dessins ou d'esquisses montrant le boîtier vu de l'extérieur, l'organisation des cartes, le choix et l'emplacement des connecteurs ainsi que les principaux faisceaux d'interconnexions.
3. Les caractéristiques de l'architecture et de partitionnement importantes du point de vue de la navigabilité. Cela peut inclure des points tels que les EMI, le foudroiement, les protections vis à vis des chocs ou des vibrations, les fonctions non utilisées dans les principaux composants, ainsi que les interfaces homme/machine tels que les facteurs ergonomiques, les caractéristiques de l'éclairage et la résolution des afficheurs.
4. La description fonctionnelle de l'article matériel au niveau le plus haut.
5. L'architecture fonctionnelle de l'article matériel.
6. Les données préliminaires d'évaluation de la sécurité du matériel.

10.3.2.2 Données de conception détaillée

Les données de conception détaillée constituent les données nécessaires pour implémenter l'article matériel conformément à ses exigences. Les données peuvent comporter en fonction du niveau hiérarchique de l'article matériel, les dossiers de l'ensemble supérieur, les dossiers des assemblages, les définitions des interconnections, les fiches des caractéristiques des composants, la description HDL du matériel, les éléments de fiabilité, la méthodologie de test, la liste des fonctions non utilisées dans les composants choisis, ainsi que les actions mises en place pour garantir qu'elles ne compromettent pas la sécurité de l'article matériel, les éléments de contrôle de l'installation et les interfaces matériel/logiciel. Certaines données spécifiques sont décrites ci-dessous :

NOTA : En sus des données de conception détaillée nécessaires pour satisfaire aux exigences de certification applicables autres, telles que les "Technical Standard Orders", le contenu et la disponibilité des éléments de données de conception détaillée supplémentaires seront proposés par le postulant à l'autorité de certification dans le PHAC.

10.3.2.2.1 Dossier de l'ensemble supérieur

Le dossier de l'ensemble supérieur identifie de manière unique l'article matériel, les ensembles supérieurs, les sous-ensembles, les constituants ainsi que les documents associés qui définissent l'article matériel.

10.3.2.2.2 Dossier d'assemblage

Le dossier d'assemblage comporte des informations détaillées complémentaires nécessaires pour assembler l'article matériel ou ses sous-ensembles.

Un dossier d'assemblage peut inclure :

1. L'emplacement et l'orientation des articles matériels dans l'ensemble matériel.
2. L'identification des séquences d'instructions ou des méthodes d'assemblage qui garantissent un assemblage correct et exempt de défaut.
3. L'emplacement des marquages d'identification, des étiquettes, des repères visuels utilisés dans les opérations d'assemblage ultérieures.

10.3.2.2.3 Dossier de contrôle de l'installation

Le dossier de contrôle de l'installation garantit que l'installation de l'article matériel dans un système ou dans un autre article matériel est correcte. Pour certains articles de bas niveau, les dessins d'assemblage de l'article ou d'assemblage du niveau supérieur peuvent jouer le rôle de dossier de contrôle de l'installation.

Le dossier de contrôle de l'installation peut inclure :

1. Les dimensions.
2. Les exigences de dégagement.
3. Les informations concernant le refroidissement et le montage.
4. Les informations concernant le poids, le centre de gravité, et autre paramètres nécessaires pour garantir une installation sûre et adéquate.

10.3.2.2.4 Données d'interface matériel/logiciel

Les performances du matériel obtenues à partir de la spécification des exigences peuvent dépendre de la configuration du matériel par le logiciel, du calibrage du matériel par le logiciel, ou des interactions nécessaires entre le matériel et le logiciel.

Les données en rapport avec les interfaces du matériel et du logiciel peuvent inclure :

1. Les adresses mémoires.
2. Les allocations de champs d'adresses mémoires dans lesquels les données peuvent être chargées.
3. Les informations de temps et d'enchaînement.
4. Toute autre information nécessaire au fonctionnement de l'interface du matériel et du logiciel.

10.4 DONNEES DE VALIDATION ET DE VERIFICATION

Elles constituent la preuve de l'exactitude et de la complétude des exigences et de la conformité aux exigences des résultats de la conception de l'article matériel. Elles donnent l'assurance que le matériel a été développé conformément à ses exigences et à sa conception, correctement fabriqué, et que les objectifs de la conception sont atteints. Ces données comprennent les procédures et les résultats des revues, des analyses et des tests du matériel. Des données complémentaires en plus de celles décrites dans ce paragraphe peuvent être nécessaires pour des fonctions de niveau A et B, comme décrit par l'Annexe B.

10.4.1 Données de traçabilité

Elles établissent une corrélation entre les exigences, la conception détaillée, l'implémentation et la vérification ce qui facilite la maîtrise de la configuration, les modifications et la vérification de l'article matériel.

Les données de traçabilité du matériel devraient inclure :

1. La corrélation entre les exigences du système allouées au matériel et les exigences du matériel.
2. La corrélation entre les exigences et les données de conception détaillée du matériel.
3. La corrélation entre des données de conception détaillée du matériel et l'article matériel tel que réalisé ou de son assemblage.
4. La corrélation entre les exigences, y compris les exigences dérivées du matériel et les données de conception détaillées ainsi que les procédures et les résultats de la vérification.
5. Les résultats de l'analyse de traçabilité.

10.4.2 Procédures pour les revues et les analyses

Elles définissent les processus et les critères de conduite des revues et des analyses.

Les procédures spécifiques aux revues et aux analyses du matériel devraient inclure :

1. Le but de la revue ou de l'analyse.
2. Les organisations qui participent aux revues.
3. Les critères applicables aux revues et aux analyses.
4. Les instructions détaillées pour la conduite des revues et des analyses.
5. Les critères d'acceptabilité et d' achèvement des revues et des analyses.

10.4.3 Résultats des revues et des analyses

Ils apportent la preuve que celles-ci ont été effectuées en suivant les procédures et les critères approuvés.

Les résultats des revues et des analyses du matériel devraient inclure :

1. L'identification des procédures pour les revues et les analyses.
2. L'identification des éléments de données soumis aux revues et aux analyses.
3. Les personnes participant aux revues et aux analyses.
4. Les résultats des revues et des analyses.
5. Les actions correctives résultant des revues ou des analyses telles que des listes de constats d'anomalies ou d'actions.
6. Les conclusions des revues ou analyses, y compris pour les revues une évaluation qualitative de l'élément soumis à la revue, pour les analyses une évaluation quantitative de l'élément analysé ainsi que les données de l'analyse.

10.4.4 Procédures de tests

Les procédures de test définissent les méthodes, l'environnement et les instructions pour la conduite à la fois des essais fonctionnels et des essais de qualification dans l'environnement effectués pour la vérification de l'article matériel.

Les procédures de test du matériel devraient inclure :

1. Le but du test.
2. L'identification des consignes de mise en œuvre du matériel, du logiciel et des équipements de test nécessaires à chacun des tests du matériel.
3. Les instructions nécessaires à la conduite des procédures de test.
4. Les cas de test.
5. Les résultats attendus tels que les critères de succès et d'échec et les exigences couvertes par les tests.

10.4.5 Résultats des tests

Les résultats des tests du matériel apportent la preuve objective de l'accomplissement de ces tests, conformément aux procédures approuvées supportant la vérification de l'article matériel.

Ils devraient inclure :

1. L'identification de la procédure de test.
2. L'identification de l'article testé.
3. Les résultats réels des tests réalisés.
4. L'identification des personnels chargés de réaliser et d'attester les tests s'il y a lieu et la date à laquelle les tests ont été effectués.
5. L'interprétation des résultats soit par l'analyse, soit par les revues ainsi que le taux de couverture réel obtenu par ces tests.

10.5 CRITERES DES TESTS D'ACCEPTATION DU MATERIEL

Ces données fournissent les critères et les éléments d'évaluation qui prouveront que les tests et les résultats associés garantiront que l'article a été fabriqué ou réparé correctement.

Ces critères devraient inclure :

1. Les principaux attributs du matériel à tester.
2. Les critères de succès ou d'échec pour chaque attribut principal.
3. Les contraintes des tests.
4. Les justifications des attributs principaux et des critères de succès ou d'échec.
5. La couverture des points de conception nécessaires pour satisfaire aux exigences de sécurité.
6. L'évaluation des données qui montrera que les critères de test ont été appliqués de manière adéquate, en s'appuyant sur des les procédures de test et les résultats des tests réels associés.

10.6 CONSTATS DES ANOMALIES

Les constats des anomalies sont le moyen d'identifier et d'enregistrer la solution des problèmes de conception du matériel, la non conformité des processus avec les plans et les règles, et les insuffisances des données du cycle de vie du matériel.

Les constats des anomalies devraient inclure :

1. L'identification de la configuration de l'article et de l'activité du processus dans laquelle l'anomalie a été observée.
2. L'identification de la configuration de l'article à modifier ou une description du processus à corriger.
3. Une description de l'anomalie qui permettra de comprendre et de résoudre le problème.
4. Une description des actions correctives à entreprendre pour traiter l'anomalie constatée.

10.7 ENREGISTREMENTS DE GESTION DE LA CONFIGURATION DU MATERIEL

Les résultats des activités du processus de gestion de la configuration sont enregistrés dans les rapports de gestion de la configuration. Ceux-ci peuvent comporter les listes d'identification de la configuration, les enregistrements les référentiels ou les enregistrements électroniques, les historiques des rapports de modifications, les résumés des rapports d'anomalies, les données d'identification des outils, les rapports d'archivage et de mise à disposition.

10.8 ENREGISTREMENTS DE L'ASSURANCE PROCESSUS DU MATERIEL

Les résultats des activités d'assurance processus sont enregistrés dans les rapports d'assurance processus. Ceux-ci peuvent être des comptes-rendus d'audit ou de revue, des minutes de réunion, des rapports de dérogations accordées pour les processus, ou des comptes-rendus de revues de conformité.

10.9 RESUME DES TRAVAUX REALISES POUR LE MATERIEL

Le Résumé des Travaux Réalisés pour le Matériel est le document principal qui montre la conformité au PHAC, et démontre à l'autorité de certification que les objectifs du présent document ont été atteints pour les articles matériels. Ce résumé peut-être combiné avec celui réalisé pour le système. Le Résumé des Travaux Réalisés pour le Matériel devrait comporter les informations ci-dessous, telles que décrites par le PHAC :

1. La vue d'ensemble du système.
2. La vue d'ensemble du matériel.
3. Les procédures de certification.
4. La description du cycle de vie de la conception du matériel.
5. Les données du cycle de vie de la conception du matériel.
6. Le matériel développé auparavant.
7. Les considérations complémentaires.
8. Les méthodes alternatives.

Les écarts par rapport au PHAC approuvé doivent être identifiés. De plus les quatre points ci-dessous doivent être pris en compte :

1. **Identification du matériel.** Ce chapitre identifie la configuration du matériel et des articles matériels par leur numéro de type et leur numéro de version.
2. **Historique des Modifications.** S'il y a lieu, ce chapitre contient le résumé des modifications du matériel avec une mention particulière pour les modifications qui résultent de défaillances affectant la sécurité, ainsi qu'une identification des modifications du cycle de vie de conception du matériel depuis la certification précédente.
3. **Situation du Matériel.** Ce chapitre contient un résumé des constats d'anomalies non résolues au moment de la certification, y compris une déclaration des limitations fonctionnelles.
4. **Déclaration de conformité.** Ce chapitre comporte une déclaration de conformité à ce document, ainsi qu'un résumé des méthodes de démonstration de conformité utilisées pour satisfaire aux critères spécifiés par les plans du matériel. Ce chapitre traite également les directives complémentaires et les écarts par rapport aux plans et aux procédures du matériel ainsi qu'au présent document.

   NOTA : Les informations que contient le PHAC ne doivent pas nécessairement être reprises par le Résumé des Travaux Réalisés pour le Matériel, cependant lorsqu'elles sont reprises le processus de certification doit s'en trouver accéléré.

CHAPITRE 11

CONSIDERATIONS COMPLEMENTAIRES

Ce chapitre fournit des recommandations sur des considérations complémentaires d'assurance conception qui n'ont pas été abordées dans les paragraphes précédents. Ces considérations complémentaires peuvent être utilisées à la discrétion du postulant pour satisfaire à certains objectifs des Chapitres 2 à 9. Toute utilisation de ces considérations complémentaires devrait être acceptée par l'autorité de certification.

11.1 UTILISATION DE MATERIEL DEVELOPPE AUPARAVANT

Ce paragraphe examine les problèmes associés à l'utilisation de matériel développé auparavant. Ces recommandations recouvrent, l'évaluation des modifications du matériel, l'installation dans l'aéronef, l'environnement de l'application, ou l'environnement de développement de l'application et la mise à jour des référentiels. Les recommandations sur l'utilisation des composants COTS, qui sont un cas particulier de matériel développé auparavant, sont proposées par le Paragraphe 11.2. La Gestion de la Configuration et l'Assurance Processus devraient aussi être prises en compte pour chaque utilisation de matériel développé auparavant.

L'intention d'utiliser du matériel développé auparavant devrait être exprimée dans le PHAC.

11.1.1 Modification de matériel développé auparavant

Ce paragraphe examine les modifications de matériel développé auparavant. La modification peut être le résultat du changement des exigences, de la détection d'erreurs, d'améliorations du matériel ou de la technologie ou de difficultés d'approvisionnement.

Les activités d'analyses pour les modifications proposées consistent en :

La revue des données résultant du processus d'évaluation de la sécurité du système.

L'application des recommandations du Paragraphe 11.1.4 lorsque le niveau d'assurance conception du matériel a été augmenté.

L'analyse d'impact de la modification, y compris les conséquences des modifications qui peuvent se traduire par un effort de re-vérification concernant une zone plus étendue que celle qui a été modifiée. Cette zone peut être délimitée par les analyse, de flux des signaux, fonctionnelle, temporelle, de traçabilité ou par d'autres moyens appropriés.

11.1.2 Modification de l'installation dans l'aéronef

Ce paragraphe examine l'utilisation par une nouvelle installation dans l'aéronef d'un matériel qui a été certifié auparavant à un certain niveau d'assurance conception dans le cadre d'une base de certification donnée. Lorsque l'on utilise du matériel développé auparavant dans une nouvelle installation, les recommandations suivantes devraient être suivies :

1. Evaluation de la nouvelle installation dans l'aéronef et détermination du niveau d'assurance conception matériel ainsi que de la base de certification par le processus d'évaluation de la sécurité du système. Il n'est pas demandé d'effort supplémentaire si ceux-ci sont identiques ou moins contraignants dans la nouvelle installation que ce qu'ils étaient dans la précédente.
2. Prise en compte des recommandations du paragraphe 11.1 modification de matériel développé auparavant, si des modifications fonctionnelles sont demandées dans la nouvelle installation.
3. Prise en compte des recommandations du paragraphe 11.1.4, augmentation du niveau d'un référentiel de conception, si les activités de conception précédentes n'ont pas produit les éléments nécessaires pour justifier que les objectifs de sécurité dans la nouvelle installation sont satisfaits.

11.1.3 Modification de l'application ou de l'environnement de conception

La réutilisation d'un matériel développé auparavant peut demander de recourir à un nouvel environnement de conception, ou de procéder à l'intégration du matériel avec d'autres logiciels ou matériels que ceux utilisés par l'application initiale.

Le nouvel environnement de conception peut augmenter ou réduire certaines activités des processus du cycle de vie de la conception du matériel. Les recommandations concernent :

1. La prise en compte des conseils du Paragraphe 11.4, Evaluation et qualification des outils, si le nouvel environnement de conception utilise des outils de conception du matériel.
2. La vérification des interfaces du matériel quand le matériel développé auparavant est utilisé avec un interface différent dans le nouveau matériel.
3. La prise en compte du besoin de re-vérification des interfaces matériel/logiciel, lorsque le matériel développé auparavant utilise un logiciel différent.

11.1.4 Mise à jour du référentiel de la conception

Les recommandations ci-dessous concernent les articles du matériel dont les données du cycle de vie sont produites pour une application antérieure et estimées insuffisantes vis à vis des objectifs de sécurité de la nouvelle application. Ces recommandations ont pour but d'aider le postulant à obtenir l'agrément de l'autorité de certification pour du matériel développé auparavant à un niveau d'assurance conception inférieur:

Recommandations concernant la mise à jour du référentiel de la conception :

1. Satisfaction des objectifs décrits par ce document en mettant à profit des données du cycle de vie du développement antérieur.
2. Elaboration des éléments de la certification du matériel à partir des cas de défaillance et des niveaux d'assurance conception déterminés par le processus d'évaluation de la sécurité du système. L'impact des modifications de l'application antérieure devrait être analysé afin de déterminer les zones d'insuffisances.
3. Evaluation des données du cycle de vie du développement antérieur afin de garantir que les objectifs du processus de vérification du matériel sont satisfaits par la fonction mise à jour, au niveau d'assurance conception requis pour le matériel.
4. Utilisation de la ré-ingénierie pour reconstituer les données du cycle de vie du matériel qui se révéleraient insuffisantes ou manquantes afin de satisfaire les objectifs d'assurance conception de ce document.
5. Lorsque l'utilisation de l'expérience en exploitation du produit est prévue pour satisfaire les objectifs d'assurance conception de ce document, lors d'une mise à jour du référentiel de conception, les recommandations du Paragraphe 11.3, Expérience en exploitation du produit devraient être prises en compte.
6. Description explicite dans le PHAC de la stratégie que va appliquer le postulant pour obtenir la conformité à ce document.

11.1.5 Procédures complémentaires pour la gestion de la configuration

Pour une utilisation nouvelle de matériel développé auparavant, en sus des recommandations du Chapitre 7, le processus de gestion de la configuration devrait inclure :

1. La traçabilité des données du cycle de vie et du produit matériel entre l'application antérieure et la nouvelle application.
2. Le processus de gestion des modifications capable de gérer les demandes de modifications pour des utilisations différentes d'un article commun.

11.2 UTILISATION DE COMPOSANTS DU COMMERCE SUR ETAGERE (COTS)

Les composants COTS sont utilisés très largement dans les conceptions du matériel alors que dans la plupart des cas leurs données de conception ne sont pas disponibles pour être examinées. Le processus de certification ne prend pas expressément en compte les composants, les modules et les sous-ensembles de manière individuelle car ceux-ci sont couverts en tant que parties de la fonction aéronef spécifique qui est l'objet de la certification. A ce titre, l'utilisation de composants COTS sera vérifiée au travers de l'ensemble du processus de conception, y compris par les processus transverses définis dans ce document. L'utilisation d'un processus de gestion des composants électroniques, conjointement aux processus de conception, fournit les bases pour l'utilisation des composants COTS.

11.2.1 Gestion de composants électroniques COTS

La gestion de composants électroniques COTS est un processus transverse important associé à la conception et au développement du matériel. Les processus de gestion des composants s'appliquent aux composants électroniques COTS. Bien qu'il y ait à la fois des aspects techniques et commerciaux dans ce processus, ce paragraphe ne traite que des aspects techniques lorsqu'ils ont un impact sur la certification.

Un crédit de certification peut être obtenu en établissant que :

1. Le fabricant du composant peut justifier par des enregistrements du suivi d'une production de composants de grande qualité.
2. Des procédures de maîtrise de la qualité existent chez le fabricant du composant.
3. Il y a une expérience en exploitation qui atteste du fonctionnement satisfaisant du composant.
4. Le composant a été qualifié par le fabricant ou au moyen de tests complémentaires qui établissent la fiabilité du composant.
5. Le fabricant du composant maîtrise le niveau de qualité du composant, ou bien celle-ci est garantie par le biais de tests complémentaires.
6. Les composants ont été choisis sur la base de leur adéquation technique à l'utilisation visée telle que la gamme de température, les limitations de puissance ou de tension, ou bien des tests complémentaires ou d’autres moyens ont été utilisés pour établir celle-ci.
7. La performance et la fiabilité du composant sont surveillées de manière continue, avec des retours vers les fabricants pour les points qui doivent être améliorés.

11.2.2 Achat des composants COTS

Les recommandations pour l'achat des composants COTS ne font pas partie des finalités de ce document, mais les rétroactions relatives à des problèmes d'achat devraient être gérées et résolues par le postulant, lorsqu'elles ont des impacts significatifs sur l'assurance conception du matériel.

Les principaux sujets sensibles concernent :

1. La disponibilité effective des données d'assurance conception des composants COTS demandée par ce document.
2. Les dispersions des paramètres des composants qui dépendent des lots de production qui peuvent ne pas avoir été identifiées, y compris par des tests de robustesse.
3. Le caractère évolutif de la technologie des composants électroniques.
4. L'obsolescence des composants COTS.

11.3 EXPERIENCE EN EXPLOITATION DU PRODUIT

L'expérience en exploitation peut être utilisée pour justifier l'assurance conception de matériels développés auparavant ainsi que celle des composants COTS. L'expérience en exploitation est liée aux données recueillies au cours de toute utilisation antérieure ou présente du composant. Les données des applications non embarquées ne sont pas exclues.

NOTA : L' utilisation opérationnelle, large et satisfaisante, d'un article peut donner confiance en la maturité de sa conception et en l'absence d'erreur et ainsi démontrer la qualité de sa production.

11.3.1 Critères d'acceptabilité des données d'expérience en exploitation d'un produit

Lorsque des données d'expérience en exploitation sont utilisées pour l'assurance conception, la pertinence et l'acceptabilité de ces données dépend d'un ou de plusieurs des points suivants :

1. Similitude de l'utilisation de l'article matériel par rapport à l'application, à la fonction, à l'environnement opérationnel et au niveau d'assurance conception.
2. Degré de pertinence des données d'assurance conception vis à vis de la configuration de l'article matériel proposé.
3. Degré de complétude avec lequel les erreurs de conception découvertes au cours de la période d'exploitation évaluée ont été éliminées, passivées ou analysées et considérées comme n'ayant pas d'impact sur la sécurité dans la configuration à utiliser.
4. Taux de défaillance réel observé en exploitation.

   NOTA : Le PHAC devrait expressément aborder ces aspects lorsque l'assurance conception des éléments s'appuie sur les données de l'expérience en exploitation.

11.3.2 Evaluation des données d'expérience en exploitation du produit

Pour satisfaire aux critères ci-dessus le postulant devrait procéder à l'évaluation de :

1. La pertinence des applications, des installations et des environnements antérieurs par rapport à l'application cible en s'appuyant sur des analyses d'ingénierie.

   NOTA : Les données utilisées afin de déterminer la justesse de l'emploi et les limites d'utilisation peuvent être fournies par les spécifications, les feuilles de caractéristiques, les notes d'applications, les rapports d'exploitation, les correspondances avec les utilisateurs et les notes d'errata. Ces sources d'informations peuvent aussi décrire les fonctions associées à l'article matériel, de sorte que l'utilisation embarquée projetée puisse être corrélée aux utilisations antérieures.
2. L'utilisation projetée quant à ses impacts sur le processus d'évaluation de la sécurité, y compris l'éventuelle passivation des effets des erreurs de conception identifiée par les données.
3. Des statistiques sur les erreurs de conception disponibles et leur impact sur le processus d'évaluation de la sécurité. Des évaluations qualitatives peuvent être utilisées lorsque les statistiques ne sont pas disponibles.
4. Des constats d'anomalies disponibles. Ceux-ci peuvent montrer que l'expérience en exploitation a induit des améliorations actuellement disponibles dans la configuration courante. Les problèmes identifiés qui n'ont pas été résolus peuvent toujours être passivés au moyen de l'architecture ou en effectuant des vérifications complémentaires. Etablir ou évaluer les relations entre les constats d'anomalies et les articles matériels ou les exigences de modification du produit.

   NOTA : Pour les composants électroniques une utilisation en exploitation significative peut accroître la probabilité de détection et d'élimination des erreurs, ou la disponibilité de réparations provisoires.

11.3.3 Données d'évaluation d'expérience en exploitation du produit

L'évaluation des données d'expérience en exploitation utilisées pour justifier l'assurance conception pour l'application proposée devrait comprendre :

1. L'identification du composant et des fonctions que l'on en attend dans le système de bord. L'identification du niveau d'assurance conception, ou pour les composants utilisés pour des fonctions de niveau A et B la description des moyens d'assurance supplémentaires pour ceux-ci, tels que les moyens architecturaux et les stratégies de vérifications complémentaires ou avancées à appliquer.
2. Une description des données d'expérience en exploitation recueillies et du processus d'évaluation, y compris les critères de détermination de l'adéquation et de la validité des données.
3. Les données d'expérience en exploitation, y compris le détail des informations d'exploitation prises en compte, l'historique des modifications, les hypothèses utilisées pour analyser ces données, ainsi qu'un résumé des résultats d'analyse.
4. La justification de l'adéquation des données d'expérience en exploitation vis à vis de l'utilisation souhaitée au niveau d'assurance conception requis.

11.4 EVALUATION ET QUALIFICATION DES OUTILS

Des outils logiciels et matériels sont en général utilisés lors de la conception et de la vérification du matériel. Lorsque des outils de conception sont utilisés pour créer l'article matériel ou concevoir le matériel, une erreur de l'outil est susceptible d'introduire une erreur dans l'article matériel. Lorsque des outils de vérifications sont utilisés afin de vérifier un article matériel, une erreur propre à l'outil peut produire une incapacité à détecter une erreur dans l'article matériel ou dans sa conception. Avant toute utilisation d'un outil, une évaluation de l'outil devrait être effectuée. Les résultats de cette évaluation ,et si nécessaire de la qualification de l'outil, devraient être enregistrés et maintenus.

Le but de l'évaluation et de la qualification de l'outil est de garantir qu'il est capable de réaliser l'activité de conception ou de vérification spécifique, avec un niveau de confiance convenable pour l'utilisation qui en sera faite.

11.4.1 Processus d'évaluation et de qualification d'un outil

L'évaluation d'un outil consiste en l'estimation du rôle de l'outil dans les processus du cycle de vie de la conception, elle peut inclure les activités de qualifications à réaliser en fonction du rôle de l'outil et du niveau d'assurance conception de la fonction du matériel. Cette recommandation pour l'évaluation des outils est présentée sous la forme d'un organigramme, et s'applique à la fois aux outils de conception et aux outils de vérification lorsqu'ils sont utilisés pour atteindre des objectifs ou générer des données pour les satisfaire. L'organigramme conduira le postulant à des évaluations limitées pour certaines catégories d'outils et à des qualifications pour d'autres.

Le processus d'évaluation et de qualification des outils peut être appliqué soit à un outil seul, soit à un ensemble d'outils. Les outils ont souvent des capacités qui vont au-delà de celles qui sont nécessaires à une activité particulière de conception ou de vérification pour un projet donné. Il est nécessaire de n'évaluer que les fonctions de l'outil utilisées pour une activité spécifique du cycle de vie du matériel et non la totalité de l'outil.

Il est admis que les outils sont souvent intégrés et partagés au cours des différentes phases du cycle de vie. Lorsqu'un outil est utilisé à la fois lors de phases de conception et de vérification, l'évaluation en tant qu'outil de conception peut-être nécessaire, à moins que la ségrégation et la séparation entre ses deux fonctions soient démontrées.

NOTA 1 : Si l'évaluation d'un outil donné montre que certaines de ses fonctions sont utilisées pour la conception et d'autres fonctions pour la vérification, il peut être judicieux de traiter les fonctions séparément et de réaliser l'évaluation de chacun des groupes de fonctions de l'outil.

NOTA 2 : Cette activité d' évaluation se concentre d'avantage sur l'utilisation de l'outil que sur l'outil lui même.

Le diagramme de la Figure 11-1 propose une procédure d'évaluation de l'outil et des activités, il donne des recommandations dans le cas où une qualification d'outil s'avère nécessaire. Les nombres qui figurent dans les blocs de décision et d'activités se réfèrent aux numéros qui suivent la figure, ils donnent des explications plus détaillées sur la décision ou sur l'activité.

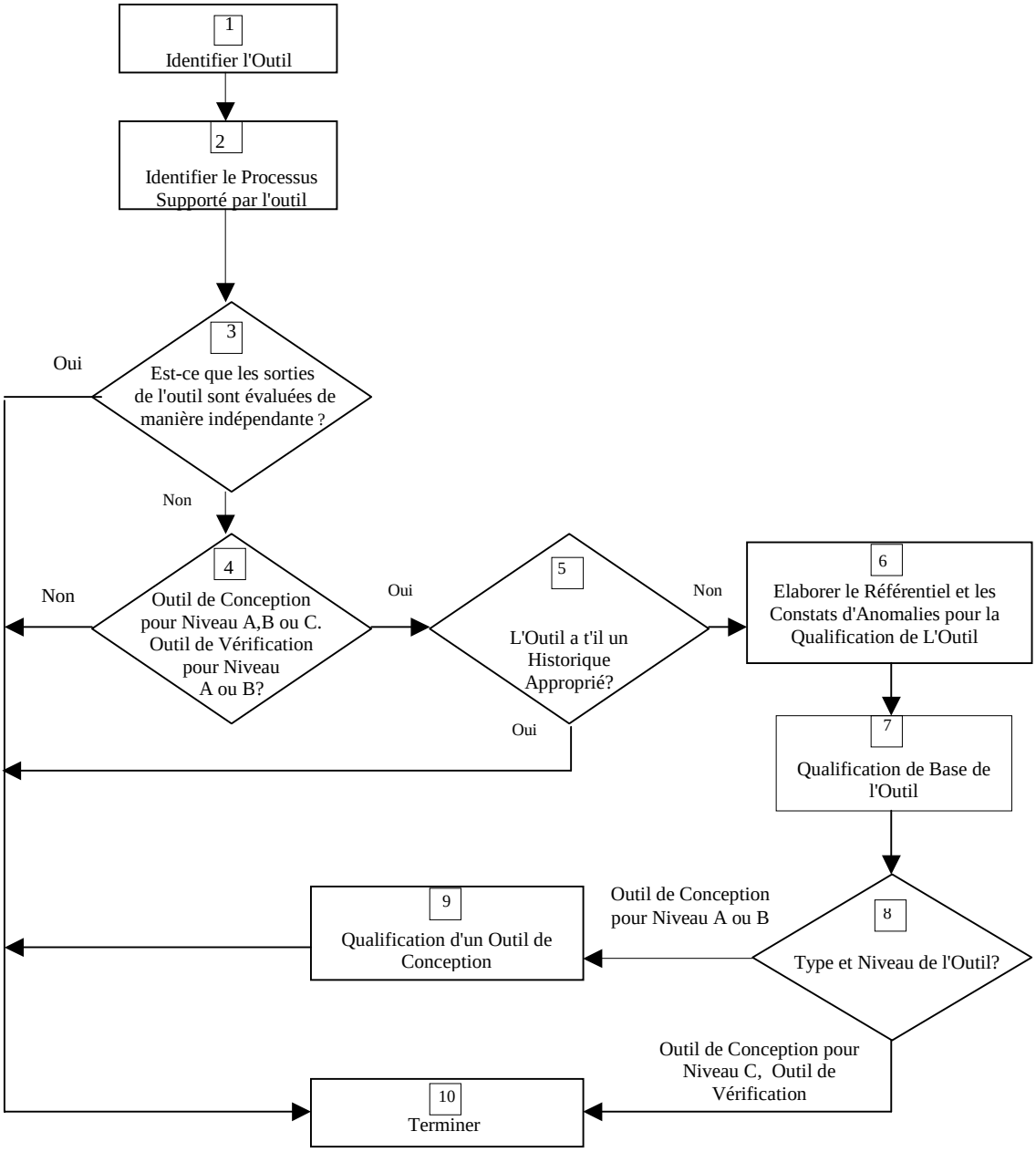


FIGURE 11-1 : EVALUATION ET QUALIFICATION DES OUTILS DE CONCEPTION ET DE VERIFICATION

1. **Identifier l'Outil.** Comprend le nom, l'origine, le numéro de version et l'environnement hôte dans lequel il fonctionne. Les mises à jour de l'outil devraient être documentées et suivies.

   NOTA : *Lorsqu'un outil est amélioré, évaluer les impacts potentiels des mises à jour sur les résultats existants ainsi que sur la suite du cycle de vie du matériel.*

2. **Identifier le Processus Supporté par l'Outil.** Identifier le processus de conception ou de vérification qui est supporté par l'outil, toute limitation propre à l'outil, ainsi que les sorties produites et utilisées dans le cycle de vie de conception du matériel. Si certains problèmes existent dans l'outil, fournir une déclaration d'acceptabilité et une justification pour l'utilisation de l'outil.

3. **Est-ce que les Sorties de l'Outil Sont Evaluées de Manière Indépendante ?** Une évaluation indépendante vérifie l'exactitude des sorties de l'outil en utilisant des moyens indépendants. Si les sorties de l'outil sont évaluées indépendamment alors il n'est pas nécessaire de poursuivre l'évaluation.

   NOTA : *L'évaluation indépendante des sorties qui sont produites en totalité ou en partie par un outil de conception peut être effectuée à partir des activités de vérification faites sur un article tel qu'un composant, sur une liste de câblage ou sur un assemblage. Dans ce cas, l'intégrité de l'article final ne dépend plus uniquement de l'exactitude des sorties de l'outil de conception.*

   L'évaluation indépendante des sorties d'un outil de vérification peut consister en une revue manuelle des sorties de l'outil, ou peut inclure une comparaison avec les sorties d'un outil différent capable de réaliser les mêmes activités de vérification que l'outil objet de l'évaluation.

   Le postulant peut également proposer d'autres méthodes d'évaluation indépendantes.

4. **Outil de Conception pour Niveau A, B ou C, Outil de Conception ou de Vérification pour Niveau A ou B ?** Si l'outil est utilisé pour des fonctions de niveau D, comme un outil de vérification de niveau C, ou utilisé pour évaluer la complétude d'un test de vérification telle que l'analyse d'élément comme décrit par l'Annexe B, Paragraphe 3.3.1.1.2, il n'est pas nécessaire de l'évaluer plus en détail. Si l'outil est utilisé comme outil de conception pour du matériel implémentant des fonctions de niveaux A,B, ou C ou s'il est utilisé comme outil de vérification pour des fonctions de niveaux A ou B, alors des évaluations plus poussées sont nécessaires.

5. **L'Outil a t'il un Historique Approprié ?** Lorsqu'il est possible de montrer que l'outil a été utilisé auparavant et que l'on considère qu'il a donné des résultats acceptables, il n'est pas nécessaire de faire une évaluation plus détaillée. Un examen de la pertinence de l'utilisation antérieure par rapport à l'utilisation proposée devrait faire partie de la justification.

   NOTA : *L'historique de l'outil peut s'appuyer sur des applications soit embarquées, soit non embarquées sous réserve que les données qui justifient la pertinence et la crédibilité de l'historique de l'outil soient disponibles.*

6. **Elaborer le Référentiel et les Constats d'Anomalies pour la Qualification de l'Outil.** Elaborer un référentiel pour la gestion de la configuration et une procédure de constat d'anomalies afin de préparer la qualification de l'outil.

7. **Qualification de Base de l'Outil.** Elaborer et exécuter un plan pour confirmer, en utilisant l'analyse et le test, que l'outil produit des sorties correctes vis à vis de l'application visée. Le manuel d'utilisation de l'outil ou toute autre description de ses fonctions et de son utilisation peut servir à élaborer les exigences.

8. **Type et Niveau de l'Outil ?** Est-il envisagé d'utiliser l'outil comme outil de conception du matériel de niveau A,B ou C, ou comme outil de vérification du matériel de niveau A ou B ?

9. **Qualification d'un Outil de Conception.** Qualifier un outil de conception de niveau A ou B en utilisant les stratégies décrites par l'Annexe B de ce document, les recommandations de l'ED-12B pour les outils de développement de logiciels, ou d'autres moyens acceptables par l'autorité de certification. L'indépendance de cette activité vis à vis du développement de l'outil doit également être établie.

NOTA : Les recommandations spécifiques à la qualification des outils de conception de niveau A et B ne sont pas données ici compte tenu de la variabilité des conditions d'utilisation de l'outil, de la technologie appliquée, de la visibilité sur l'implémentation de l'outil, des données du cycle de vie et autres facteurs. L'utilisation d'outils de conception sans l'évaluation de l'indépendance des sorties ou l'élaboration d'un historique approprié n'est pas recommandée car elle peut s'avérer être une tâche aussi ardue que le développement du matériel pour lequel on se propose de l'utiliser.

10. **Terminer.** Document l'évaluation de l'outil, les justifications des décisions d'évaluation et si applicable, les données de la qualification de l'outil. Donner les références spécifiques des guides d'installation, des manuels d'utilisation, des données de qualification de l'outil, qui sont nécessaires à sa mission et à sa qualification.

11.4.2 Données d'évaluation et de qualification d'un outil

Les données d'évaluation et de qualification d'un outil devraient inclure:

1. L'identification de l'outil, du processus qu'il supporte et, si applicable, les points suivants :
   a. La logique d'élaboration et les résultats de l'évaluation indépendante en suivant le point 3 de la Figure 11.1.
   b. La désignation de l'outil en suivant le point 4 de la Figure 11.1.
   c. L'historique de l'outil lorsqu'il est utilisé pour satisfaire le point 5 de la Figure 11.1. Un argumentaire sur la pertinence de l'utilisation antérieure de l'outil vis à vis de l'utilisation envisagée doit être compris dans la justification.
2. Une définition non ambiguë de la configuration à utiliser lors de la qualification de l'outil, conformément au point 6 de la Figure 11.1, ainsi qu'une justification de l'applicabilité de la configuration testée lorsqu'elle diffère de celle réellement utilisée pour concevoir et vérifier l'article matériel final.
3. Les détails de la qualification de l'outil y compris les exigences utilisées lors des tests, les procédures de test, les résultats attendus, les procédures d'analyses utilisées pour interpréter et compléter les résultats de tests, et la manière dont l'indépendance a été établie.
4. Le plan de qualification de l'outil de conception, y compris les procédures applicables, et les résultats de toutes les activités identifiées dans le plan.
5. Le traitement de tous les errata de l'outil connus y compris les moyens mis en œuvre pour contourner les erreurs identifiées, et s'il y a lieu les constats d'anomalies résultant de la qualification de l'outil.

ANNEXE A

MODULATION DES DONNEES DU CYCLE DE VIE DU MATERIEL EN FONCTION DU NIVEAU D'ASSURANCE CONCEPTION DU MATERIEL

Cette annexe recommande la modulation des données du cycle de vie de conception du matériel en fonction de son niveau d'assurance conception. Elle fait également des recommandations concernant les exigences d'indépendance au cours du processus de vérification.

La Tableau A-1 identifie les types de données à livrer ainsi que les catégories de contrôle de gestion de la configuration pour chaque type de donnée. Voir Tableau 7-1. Deux types de données livrables sont définis :

1. **A Soumettre.** L'élément de donnée doit être soumis à l'autorité de certification.
2. **Non Soumis.** L'élément de donnée n'est pas exigé.

Toute vérification de fonctions de niveaux A et B doit être indépendante. Les fonctions de niveau C ou inférieur ne nécessitent pas une vérification indépendante. L'indépendance n'est demandée qu'au niveau hiérarchique de la conception pour lequel la vérification par rapport aux exigences est faite. Un moyen indépendant équivalent qui prend en compte le problème de défaillance de mode commun est acceptable.

L'indépendance est un moyen de prendre en compte les erreurs potentielles de mode commun qui pourraient apparaître lorsque le concepteur vérifie l'article matériel en développement par rapport à sa conception et non par rapport à ses exigences. Pour prendre en compte ce problème, la responsabilité de la cohérence du processus de vérification en démontrant que les exigences de la conception sont satisfaites, doit être assurée par un individu, un processus ou un outil indépendant du concepteur. Il y a de nombreux moyens de d'assurer l'indépendance, le plan de vérification doit proposer les moyens spécifiques à utiliser pour une activité particulière de vérification.

Les exemples ci-dessous sont acceptables :

1. Les exigences ou les conceptions sont examinés par une personne différente.
2. Les tests ou les procédures sont développés par une personne différente.
3. Les tests ou les procédures développés par le concepteur sont examinés par une autre personne.
4. L'analyse effectuée par le concepteur est examinée par une autre personne ou une équipe.
5. Un test différent est réalisé pour confirmer les résultats des tests effectués. A titre d'exemples : un test effectué au cours d'essais en vol confirme les tests d'un article matériel, et un test de vérification du logiciel développé indépendamment et effectué sur l'article matériel cible confirme les résultats des tests effectués par le concepteur.
6. Les résultats de tests ou d'analyse sont vérifiés par un outil.

NOTA 1 : Les tests de vérification sont souvent automatisés et n'exige que "d'appuyer sur un bouton". Il n'est pas nécessaire d'exiger qu'une personne différente du concepteur réalise ces tests, dès lors qu'ils ont été évalués ou développés indépendamment. Il peut être cependant nécessaire d'examiner les résultats de manière indépendante, afin de confirmer que les procédures appropriées ont été suivies et que ces résultats montrent que les exigences sont satisfaites.

NOTA 2 : La séparation des structures de l'organisation n'est pas une exigence implicite d'indépendance.

Les chiffres cerclés du Tableau A-1 renvoient aux notes qui suivent le tableau.

Paragraphe Données	Données du Cycle de Vie du matériel ①	Objectifs ②	A Soumettre	Niveau A	Niveau B	Niveau C	Niveau D
10.1	Plans du Matériel						
10.1.1	Plan des Aspects Matériel de la Certification	4.1(1,2,3,4)	S	HC1	HC1	HC1	HC1
10.1.2	Plan de la Conception du Matériel	4.1(1,2,3,4)		HC2	HC2	HC2	ND
10.1.3	Plan de la Validation du Matériel ⑦④	4.1(1,2,3,4); 6.1.1(1)		HC2	HC2	HC2	ND
10.1.4	Plan de la Vérification du Matériel	4.1(1,2,3,4); 6.2.1(1)	S	HC2	HC2	HC2	HC2
10.1.5	Plan de Gestion de la Configuration du Matériel	4.1(1,2,3,4); 7.1(3)		HC1	HC1	HC2	HC2
10.1.6	Plan d'Assurance Processus du Matériel	4.1(1,2,4); 8.1(1,2,3)		HC2	HC2	NS	NS
10.2	Règles pour la Conception du Matériel						
10.2.1	Règles d'Exigences ③	4.1.(2)		HC2	HC2	NS	NS
10.2.2	Règles de conception du Matériel ③	4.1(2)		HC2	HC2	NS	NS
10.2.3	Règles de Validation et de Vérification ③	4.1(2)		HC2	HC2	NS	NS
10.2.4	Règles d'Archivage du Matériel ③	4.1(2); 5.5.1(1); 7.1(1,2)		HC2	HC2	NS	NS
10.3	Données de Conception du Matériel						
10.3.1	Exigences du Matériel	5.1.1(1,2); 5.2.1(2); 5.3.1(2); 5.4.1(3); 5.5.1(1,2,3); 6.1.1(1,2); 6.2.1(1)		HC1	HC1	HC1	HC1
10.3.2	Données de la Représentation de la Conception du Matériel.						
10.3.2.1	Données de Conception Générale ③	5.2.1.(1)		HC2	HC2	NS	NS
10.3.2.2	Données de Conception Détaillée	5.3.1(1); 5.4.1(2)		⑤	⑤	⑤	⑤
10.3.2.2.1	Dossier de l'Ensemble Supérieur	5.3.1(1); 5.4.1(2); 5.5.1.(1)	S	HC1	HC1	HC1	HC1
10.3.2.2..2	Dossier d'Assemblage	5.3.1(1); 5.4.1(2); 5.5.1.(1)		HC1	HC1	HC1	HC1
10.3.2.2..3	Dossier de Contrôle de l'Installation	5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2..4	Données d'interface Matériel/Logiciel ③	5.3.1(1); 5.5.1(1)		HC1	HC1	HC1	HC1
10.4	Données de Validation et de Vérification						
10.4.1	Données de Traçabilité	6.1.1(1); 6.2.1(1,2)		HC2	HC2	HC2 ⑥	HC2 ⑥
10.4.2	Procédures Pour les Revues et les Analyses ③	6.1.1(1,2); 6.2.1(1)		HC1	HC1	NS	NS
10.4.3	Résultats des Revues et des Analyses ③	6.1.1 (1,2); 6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	Procédures de tests ③	6.1.1 (1,2); 6.2.1(1)		HC1	HC1	HC2	HC2⑦
10.4.5	Résultats des Tests ③	6.1.1 (1,2); 6.2.1(1)		HC2	HC2	HC2	HC2⑦
10.5	Critères d'Acceptation des tests du Matériel	5.5.1(3); 6.2.1(3)		HC2	HC2	HC2	HC2
10.6	Constats d'Anomalies	5.1.1(3); 5.2.1(3); 5.3.1(3); 5.4.1(4); 5.5.1(4);6.1.1(3); 6.2.1(4); 7.1(3)		HC2	HC2	HC2	HC2
10.7	Enregistrements de Gestion de la Configuration du Matériel	5.5.1(1); 7.1(1,2,3)		HC2	HC2	HC2	HC2
10.8	Enregistrements de l'Assurance Processus du Matériel	7.1(2); 8.1(1,2,3)		HC2	HC2	HC2	NS
10.9	Résumé des Travaux Réalisés pour le Matériel	8.1(1,2,3)	S	HC1	HC1	HC1	HC1

TABLEAU A-1 : DONNEES DU CYCLE DE VIE EN FONCTION DU NIVEAU D'ASSURANCE DE LA CONCEPTION DU MATERIEL ET DE LA CATEGORIE DE CONTROLE

① Les données sont indiquées par un S dans la colonne Soumettre. Les données HC1 et HC2 utilisées pour la certification qui ne doivent pas être soumises doivent être disponibles. Voir Paragraphe 7.3.

② Les objectifs qui sont donnés ici ne le sont qu'à titre de référence. Tous ces objectifs ne sont pas applicables pour tous les niveaux d'assurance.

③ Si ces données sont utilisées pour la certification, leur disponibilité est indiquée par la tableau. Ces données ne sont pas toujours utilisées pour la certification et peuvent ne pas être requises.

④ Pour les niveaux C et D, ceci peut être obtenu de manière informelle au travers du processus de liaison. La documentation peut être sous la forme de compte rendus de réunion et ou de support de présentation.

⑤ Lorsque le postulant fait référence à ces éléments de données dans les éléments requis, ceux-ci doivent être disponibles.

⑥ Seules les données de traçabilité des exigences vers les tests sont nécessaires.

⑦ L'analyse de la couverture par le test des exigences dérivées ou des exigences des niveaux hiérarchiques inférieurs n'est pas demandée.

ANNEXE B

CONSIDERATIONS RELATIVES A L'ASSURANCE CONCEPTION
DE FONCTIONS DE NIVEAUX A ET B

1 INTRODUCTION

Le concepteur de matériel réalisant des fonctions de niveaux A ou B fait des choix qui peuvent avoir une incidence sur la sécurité. Avec l'augmentation du niveau d'assurance conception, l'approche nécessaire pour vérifier qu'une conception donnée satisfait à ses exigences de sécurité peut demander l'association de méthodes se recouvrant partiellement. Le choix d'une ou de plusieurs méthodes, ou la proposition d'autres méthodes qui fourniraient l'assurance conception, est laissé au concepteur.

Cette annexe fait des recommandations sur la manière de réaliser et d'utiliser une FFPA pour développer une stratégie d'assurance conception, ainsi que des recommandations relatives à quelques méthodes spécifiques utilisables pour l'assurance conception.

2 ANALYSE DES CHEMINS DE PROPAGATION DES DEFAILLANCES FONCTIONNELLES

La FFPA est une analyse itérative structurée descendante. Elle identifie les parties spécifiques de la conception qui implémentent la fonction, c'est à dire les ensembles, les composants et éléments associés à chaque chemin, ainsi que les modes de défaillance associés et leurs effets qu'il faut analyser afin de déterminer si l'architecture et l'implémentation du matériel satisfont aux objectifs de la sécurité. La FFPA identifie aussi les ensembles, composants et éléments de la conception qui implémentent les fonctions de niveaux A et B.

La FFPA démarre avec la PSSA, qui est utilisée pour identifier les FFPs au niveau du système pouvant être déclinés et alloués aux FFPs du matériel.

Le but d'une FFPA est d'identifier les FFPs particuliers de telle sorte que :

Le matériel réalisant des fonctions de niveau A ou B soit traité par une méthode d'assurance conception décrite dans cette annexe ou par une autre méthode avancée acceptable par l'autorité de certification.

Les considérations de cette annexe sont optionnelles pour du matériel implémentant une fonction de niveau C ou inférieur, c'est à dire pour les fonctions dont l'assurance est établie en utilisant seulement les recommandations des Sections 3 à 11 de ce document.

NOTA : L'identification de FFPs séparés pour des fonctions implémentées par des technologies différentes, ou offrant des degrés de visibilité différents sur la conception, est souvent utile car l'assurance conception de l'article complet peut être obtenue par l'utilisation des méthodes d'assurance multiples. Le niveau de déclinaison peut varier pour chaque FFP.

La décomposition est réalisée en utilisant les techniques descendantes conventionnelles d'évaluation de la sécurité telles que les analyses d'arbres de fautes (FTA). La décomposition peut être complétée par l'utilisation de AMDE_F, de diagrammes de dépendance, et d'analyses de mode commun pour chaque niveau successif de la déclinaison. Le niveau de décomposition peut varier pour chaque FFP du système en fonction de la stratégie d'assurance conception, des concepts d'implémentation correspondants, et des méthodes de passivation des erreurs proposées pour le matériel objet de la conception. La décomposition progresse :

des FFPs au niveau du système	vers	les FFPs au niveau du matériel;
des FFPs au niveau du matériel	vers	les FFPs au niveau des circuits;
des FFPS au niveau des circuits	vers	les FFPs au niveau des composants; et
des FFPs au niveau des composants	vers	les FFPs au niveau des éléments.

2.1 Méthode d'analyse du chemin de propagation des défaillances fonctionnelles

La FFPA devrait être réalisée comme suit :

1. Pour chaque fonction de niveaux A et B, identifier la fonction et son niveau d'assurance conception à partir des exigences du matériel et de la FHA du système pour cette fonction. La fonction peut être constituée d'un ensemble de sous-fonctions, chacune ayant une série d'exigences dérivées et un niveau d'assurance conception associé. Ces sous-fonctions peuvent être déclinées plus en détail si nécessaire.
2. Pour chaque fonction de niveaux A et B, déterminer les ressources nécessaires à l'implémentation de la fonction ou des sous-fonctions et analyser les options d'assurance conception. Les données d'assurance disponibles, ou dont on espère disposer pour la fonction ou pour la sous-fonction doivent, être complètes et acceptables pour la stratégie d'assurance conception ou les stratégies choisies. Si les données d'assurance disponibles ou que l'on espère être disponibles sont complètes, correctes et acceptables, alors une décomposition plus détaillée n'est pas nécessaire.
3. Pour les FFPs qui ne sont pas de niveau A ou B, leurs interdépendances avec les FFPs de niveau A ou B doivent être évaluées en utilisant une AMDE_F, une analyse de mode commun ou un diagramme de dépendance, afin de fournir l'assurance que les FFPs de niveau A ou B ne sont pas impactées de manière dangereuse par des FFPs qui ne sont pas de niveau A ou B.

Ce processus d'évaluation est itératif. S'il n'y a pas de méthode d'assurance conception acceptable pour un FFP, le processus d'évaluation et de décomposition est répété, l'architecture ou l'implémentation du matériel sont modifiées jusqu'à ce qu'une méthode d'assurance conception acceptable ait été établie et que des données d'assurance acceptables soient ou puissent être disponibles pour chaque FFP de niveau A ou B.

Les résultats de la FFPA et des méthodes choisies utilisées pour l'assurance conception du matériel doivent être communiqués aux processus systèmes de l'aéronef comme décrit par le Paragraphe 2.1 de ce document. Ces résultats sont utilisés pour l'examen et la confirmation de la validité des hypothèses au niveau de l'aéronef, particulièrement de celles reliées aux utilisations croisées et multiples de systèmes constitués d'articles ayant du matériel similaire.

2.2 DONNEES DES ANALYSES DES CHEMINS DE PROPAGATION DES DEFAILLANCES

Les données des FFPA devraient :

1. Identifier les comportements anormaux et les défaillances fonctionnelles qui ont été allouées à l'article matériel à partir du système.
2. Identifier les FFPs, les effets de leurs comportements anormaux ou de leurs défaillances fonctionnelles, et le niveau de décomposition dans la hiérarchie de conception auquel l'analyse a été réalisée, ainsi que le type et la localisation des données d'assurance acceptables qui sont disponibles.
3. Décrire les relations entre les FFPs afin de déterminer leur indépendance et leurs interdépendances avec les autres FFPs et leurs composants. De telles liaisons peuvent être décrites par l'utilisation des FTA qualitatives ou d'une autre analyse descendante, l'analyse des modes communs, les AMDE_F ou les diagrammes de dépendances. La description des liaisons doit identifier les chemins connexes, les composants et les interdépendances.
4. Etablir les liens entre les FFPs, les exigences du matériel et les exigences dérivées.

3 METHODES D'ASSURANCE CONCEPTION POUR LES FONCTIONS DE NIVEAUX A ET B

Il n'est pas dans l'intention de cette annexe de restreindre la mise en place de l'assurance conception à l'utilisation d'une quelconque méthode existante ou à venir. Les méthodes présentées dans cette annexe peuvent être utilisées pour satisfaire un ou plusieurs des objectifs des processus décrits par les Chapitres 4 à 6 de ce document.

3.1 Méthodes de passivation par l'architecture

Les particularités de l'architecture telles que l'implémentation dissimilaire, la redondance, les surveillances, la ségrégation, le partitionnement et les limitations d'autorité des commandes, peuvent être tout particulièrement utilisées pour passiver ou confiner les effets dangereux des erreurs de conception et d'implémentation du matériel. En tant que composantes de la PSSA, les activités telles que les analyses qualitatives des arbres de fautes et les analyses de mode commun peuvent assurer la détermination du domaine des attributs de l'architecture nécessaires à la passivation ou au confinement des effets des fautes du matériel, des défaillances, des erreurs de conception et d'implémentation. Plus spécifiquement cette approche devrait être appliquée conjointement à l'approche FFPA du matériel décrite par l'Annexe B Paragraphe 2, et devrait utiliser le processus d'analyse de mode commun pour déterminer l'applicabilité des stratégies de passivation particulières pour la couverture des erreurs de conception et d'implémentation du matériel. Par exemple, la redondance apporte une contribution principalement dans le domaine des fautes aléatoires et des "upsets", mais elle peut aussi être efficacement utilisée pour la passivation des erreurs de conception et d'implémentation si les aspects liés aux modes communs ont été pris en compte.

3.1.1 Méthode de passivation par l'architecture

La passivation par l'architecture est réalisée en identifiant les FFPs associés à l'implémentation proposée du matériel, et en analysant les options de conception pour identifier et proposer les particularités de conception et les stratégies de passivation des effets de ces FFPs. Les propriétés génériques d'une architecture proposée pour la passivation des effets en rapport avec les FFPs devraient être évalués et traités. L'adoption d'une stratégie architecturale de passivation introduit des exigences dérivées dont l'implémentation doit être vérifiée. En particulier, les caractéristiques de l'architecture devraient protéger contre certains ou tous les effets dangereux des FFPs identifiés, et devraient être évaluées en ce qui concerne l'introduction de chemins de défaillances supplémentaires qui devraient alors être pris en compte par des protections architecturales supplémentaires, ou par l'une des stratégies d'assurance conception décrites dans cette annexe.

3.1.2 Solution pour la passivation par l'architecture

Le processus d'évaluation de la sécurité décide si la passivation par l'architecture est acceptable. La FFPA devrait tout d'abord identifier tous les FFPs matériels de niveau A et B pour lesquels la passivation par l'architecture va être utilisée pour obtenir des crédits, puis identifier les méthodes à utiliser et déterminer la logique de cette passivation. L'adéquation est établie en évaluant chaque fonction objet de la passivation dans le contexte d'une approche architecturale globale qui peut induire un ensemble plus ou moins complexe de stratégies de passivation par l'architecture.

L'analyse des modes communs devrait prendre en compte l'éventualité d'erreurs dans les exigences, l'implémentation, la fabrication et la maintenance pouvant mettre en échec la passivation. Le concepteur devrait aussi envisager les défaillances aléatoires potentielles du matériel qui réalise les fonctions de passivation architecturale susceptibles de rendre la passivation inopérante. La probabilité de la disponibilité des fonctions qui assurent la passivation devrait être proportionnée aux conséquences de la perte de la passivation pouvant conduire à une réduction des marges de sécurité.

L'approche globale devrait garantir qu'un fonctionnement correct et qu'une indépendance acceptable entre les fonctions nécessaires soit obtenue et maintenue. Toutes les protections particulières nécessaires pour éliminer, isoler ou limiter les effets de mode commun résiduel devraient être identifiées et incorporées sous la forme soit d'une passivation supplémentaire par l'architecture, soit d'autres stratégies d'assurance conception définies dans cette annexe.

Quand la définition de l'architecture est terminée, les fonctions du matériel dans les FFPs de niveaux A et B qui sont estimées ne pas être passivées, ou incorrectement passivées, devraient à nouveau être prises en compte en utilisant une autre méthode d'assurance conception de cette annexe. Par exemple une passivation partielle par l'architecture, de circuits ou de composants individuels, peut être utilisée conjointement à une méthode spécifique d'analyse lorsque cette analyse est utilisée pour identifier et établir la couverture de la vérification pour les parties non passivées des circuits et composants concernés.

3.1.3 Données de passivation par l'architecture

La documentation des moyens de passivation par l'architecture utilisée pour durcir les FFPs du matériel de niveaux A et B devrait être fournie sous la forme de données d'évaluation de la sécurité, de données d'exigences de la sécurité et de données de traçabilité. Les données d'évaluation de la sécurité devraient s'appuyer sur l'évaluation des FFPs du matériel et sur les analyses des défaillances de mode commun qui prennent en compte en particulier les aspects de la passivation par l'architecture.

Les données de passivation par l'architecture devraient inclure :

1. L'identification des FFPs du matériel de niveaux A et B qui doivent être protégés au moyen de l'architecture.
2. La description de l'approche architecturale et du mécanisme de validation de la couverture obtenue par cette approche.
3. Les mécanismes, vus sous l'angle des frontières des modes communs et des particularités des modes communs de la conception de cette architecture.
4. L'identification des FFPs de niveau A et B non passivés ou passivés de manière insuffisante à traiter par d'autres méthodes d'assurance conception.
5. Les exigences concernant l'utilisation fonctionnelle et les attributs de la conception nécessaires aux dispositifs de passivation par l'architecture.
6. Les dispositifs de passivation réalisés par du logiciel, utilisés pour satisfaire les exigences de sécurité tels que le partitionnement, les surveillances de la sécurité, et les dissemblances. Ces dispositifs et les exigences de sécurité concernant le logiciel doivent être mis à la disposition du processus système et du processus de développement du logiciel.
7. Les données de taux de défaillance et d'exposition aux fautes latentes pour tout le matériel qui réalise la passivation par l'architecture mise en œuvre.
8. Les données de traçabilité liant les exigences de sécurité aux données d'évaluation de la sécurité et aux données de vérification de la conception auxquelles elles sont liées.

3.2 EXPERIENCE EN EXPLOITATION DU PRODUIT

Le Paragraphe 11.3 fait des recommandations de base sur la manière d'évaluer si des données d'expérience en exploitation peuvent être applicables et utilisées pour du matériel de bord. Pour les fonctions de niveau A et B qui utilisent du matériel développé auparavant pour une partie de la conception, une assurance conception complémentaire est nécessaire. Cette assurance peut être fournie de la manière suivante.

3.2.1 Méthodes basées sur l'expérience en exploitation du produit

Lorsque l'évaluation décrite au Paragraphe 11.3 est terminée, les FFPs implémentés par le matériel considéré devraient être analysés en se référant à toute expérience en exploitation applicable. Le postulant ou le concepteur devraient identifier les données d'expérience en exploitation et démontrer que ces données apportent la preuve que la fonctionnalité du matériel réutilisée a été suffisamment éprouvée lors des utilisations précédentes.

3.2.2 Solution pour l'expérience en exploitation du Produit

Lorsque l'analyse des données de l'expérience en exploitation est terminée, les fonctions du matériel dans les FFPs de niveaux A et B que l'on estime ne pas avoir été éprouvées, insuffisamment éprouvées ou pour lesquelles l'on ne dispose pas d'expérience en exploitation au cours d'utilisations opérationnelles, devraient être traitées par une autre méthode d'assurance conception ou par l'identification des vérifications complémentaires que l'on peut réaliser pour éprouver les fonctions.

3.2.3 Données de l'expérience en exploitation du produit

Les données d'expérience en exploitation de produits, mises en œuvre pour la protection des FFPs du matériel de niveaux A et B, devraient inclure :

1. Les données d'évaluation de l'expérience en exploitation du produit, voir Paragraphe 11.3.2.
2. L'identification des FPPs pour lesquels l'assurance conception est fournie par l'expérience en exploitation, ainsi que les justifications montrant que les données de l'expérience en exploitation sont suffisantes.
3. L'identification des FFPs pour lesquels les données de l'expérience en exploitation sont insuffisantes, ainsi que l'identification des tests d'environnement, des procédures de tests, des analyses et des résultats utilisés pour compléter l'assurance conception de ces FFPs.
4. L'identification des FFPs et des conditions opérationnelles pour lesquelles il n'y a pas de démonstration basée sur l'expérience en service, qui nécessitent des passivations par l'architecture ou des méthodes de vérification avancées complémentaires.
5. Les données de traçabilité, décrites au Paragraphe 10.4.1, montrant les relations explicites des données d'expérience en exploitation et de vérification qui contribuent à la couverture de l'assurance conception de chaque FFP.

3.3 METHODES DE VERIFICATION AVANCEES

Un niveau supplémentaire de confiance dans l'assurance conception peut-être obtenu par l'utilisation des méthodes de vérification avancées telles que l'analyse des éléments, les méthodes formelles, les analyses de vérification spécifiques de sécurité ou toutes autres méthodes proposées par le postulant et acceptées par l'autorité de certification.

Les méthodes de vérification avancées de l'assurance conception utilisent et étendent à la fois le domaine d'application de la méthode de la FFPA présentée en Annexe B Paragraphe 2. La méthode de la FFPA est appliquée progressivement au niveau de l'équipement, au niveau des circuits, et au niveau des composants, afin de délimiter l'implémentation matérielle des FFPs de niveaux A et B. Les données de la FFPA sont alors utilisées pour définir les moyens d'assurance conception applicables aux circuits, aux composants et aux éléments du matériel contenus dans ces FFPs de niveaux A et B.

Ces trois méthodes sont résumées ci-dessous puis décrites dans les paragraphes suivants.

1. **L'Analyse des Eléments** - L'analyse des éléments fournit une mesure de la complétude de la vérification du matériel d'un point de vue ascendant. Chaque élément fonctionnel à l'intérieur d'un FFP est identifié et vérifié en utilisant des cas de test qui satisfont aux objectifs de vérification du Paragraphe 6.1 L'analyse peut également identifier les points sensibles qui devront être traités par d'autres moyens appropriés.
2. **Les Analyses Spécifiques de Sécurité -** Cette stratégie est centrée sur la mise en évidence et la correction des erreurs de conception susceptibles d'affecter de manière dangereuse les sorties du matériel au plan de la sécurité du système. Les parties de l'espace des entrées et de l'espace des sorties sensibles d'un point de vue sécurité sont déterminés analytiquement. Les parties sensibles de l'espace des entrées du matériel sont stimulées et l'espace des sorties est observé, non seulement pour la vérification des exigences sensibles du point de vue de la sécurité des fonctions souhaitées, mais également vis à vis des comportements anormaux. Les méthodes d'observation de l'espace des sorties sont identifiées en amont par une analyse effectuée en utilisant les techniques traditionnelles d'analyses de la sécurité.
3. **Les Méthodes Formelles** - Les méthodes formelles utilisent des techniques de logique formelle et de mathématiques des discrets pour la spécification, la conception, et la vérification des systèmes informatiques. Ces techniques peuvent être employées pour justifier la démonstration utilisée pour les différents processus du cycle de vie de la conception du matériel.

Des méthodes de vérification avancées autres que celles présentées dans ce paragraphe peuvent être proposées par le postulant.

3.3.1 Analyse des éléments

L'analyse des éléments peut être utilisée pour montrer que les FFPs sont vérifiés par les cas de test associés. L'analyse des éléments donne confiance et prouve que les erreurs de conception sont éliminées en découpant une réalisation complexe de FFP en éléments à un niveau défini par le concepteur. Cette méthode d'analyse fournit un indicateur du processus de vérification qui aide à la détermination de la couverture de la vérification et de sa complétude, elle est la mieux adaptée lorsque la conception détaillée est "visible" et gérée en configuration. Ceci pourrait être le cas d'un ASIC ou d'un PLD lorsque leurs fonctions sont traitées au même niveau d'assurance conception, ou lorsque les fonctions de différents niveaux d'assurance sont isolées ou ségréguées. Chaque élément fonctionnel du circuit ou composant auquel elle s'applique est identifié et vérifié vis à vis de l'exactitude des fonctions attendues, par l'utilisation des procédures de vérification qui satisfont aux objectifs de vérification du Paragraphe 6.1. L'analyse par éléments s'applique en général à un composant complet ou un ensemble de composants sans prendre en considération le nombre de FFPs différents qu'ils implémentent, mais elle peut être aussi appliquée à une partie d'un composant ou à un ensemble de composants lorsqu'une démonstration de l'isolement, de l'indépendance ou de la ségrégation des différents FFPs peut être fournie.

NOTA : *Lorsqu'une analyse d'élément est réalisée sur une fonction implémentée dans un PLD, le contenu programmé et les caractéristiques d'utilisation du PLD doivent être inclus dans l'analyse, le composant non programmé peut être traité en utilisant une méthode différente telle que l'expérience en exploitation.*

L'analyse identifie les points sensibles qui doivent être traités par des moyens appropriés. Un processus de vérification sans une telle analyse peut oublier certains circuits testés de manière inappropriée. Par le passé, de telles inadéquations ont été dues à des insuffisances des procédures de test basées sur les exigences, à des exigences du matériel peu claires ou incomplètes, à des circuits non utilisés, à des circuits d'initialisation et à des fonctions en bibliothèque. Cette analyse examine la vérification des éléments des FFPs sensibles et détermine si la couverture de la vérification associée à chaque élément est complète. L'identification d'éléments dont la couverture de vérification est incomplète dénote un besoin complémentaire de vérification ou d'activités appropriées.

Le postulant doit proposer les niveaux de la hiérarchie de conception auquel les éléments sont définis et comment ils doivent être analysés pour obtenir la couverture de la vérification.

3.3.1.1 Méthodes d'analyse des éléments

La méthode d'analyse des éléments démarre par la définition d'une série de critères à appliquer qui prennent en compte le niveau d'assurance conception et la technologie du matériel ainsi que la visibilité sur les constituants de son implémentation.

Ces critères devraient inclure :

1. L'identification et une définition des l'éléments de la conception du matériel à un niveau approprié.
2. La couverture de la vérification à atteindre pour chaque élément.

Ces critères sont ensuite appliqués à l'analyse des activités de vérification afin de déterminer s'ils seront satisfaits par la vérification proposée. Lorsqu'un critère ne sera pas satisfait, chaque élément examiné devra être excité par des stimuli judicieux qui provoqueront des effets observables appropriés sur les signaux surveillés au cours du test.

NOTA : *Comme ce processus examine les tests par rapport au matériel qui est conçu, il peut détecter les insuffisances des procédures de test. Le traitement de ces lacunes doit donner une confiance supplémentaire et prouver que le test est suffisant; l'exécution de nouveaux cas de test ou de cas de test amendés peut mettre en évidence des erreurs non couvertes du matériel.*

3.3.1.1.1 Sélection des critères d'analyse des éléments

Les critères d'analyse des éléments à appliquer devraient être choisis au cas par cas, en fonction du type et de la complexité de l'élément matériel, ainsi que des fonctions opérationnelles identifiables de l'élément. L'analyse peut montrer, soit que tous les blocs de primitives de bas niveau tels que les compteurs, les registres, les multiplexeurs, les additionneurs, les amplificateurs opérationnels et les filtres ont été testés convenablement, ou que tous les groupes de primitives interconnectées ont été testés convenablement, et qu'ils satisfont aux critères de couverture de la vérification. Les critères d'analyse des procédures de test doivent être déduits d'une évaluation de l'utilisation fonctionnelle de l'élément et de son intégration à d'autres éléments matériels pour réaliser la fonction du matériel de niveau hiérarchique immédiatement supérieur.

NOTA 1 : Par exemple, si l'élément est un compteur modulo N utilisé comme temporisateur, la procédure de test peut s'appuyer sur des sélections de classes d'équivalences des données d'entrée afin de vérifier qu'il compte quand il est activé, s'arrête de compter quand il est désactivé, compte à la bonne fréquence, atteint la valeur N et se réinitialise à l'instant spécifié. Il n'est pas nécessaire d'exciter individuellement les portes et les bascules qui constituent le compteur par leur association.

Exemple d'utilisation de primitives interconnectées dans un même élément: une unité arithmétique et logique (ALU) peut être construite à partir de primitives telles que les registres, les additionneurs et les logiques de contrôle. L'ALU peut être simulée afin de montrer que l'ensemble des primitives constituent par leur association une ALU, mais les procédures de vérification utilisées pour l'analyse des éléments doivent s'appuyer sur des classes d'équivalence des données d'entrée appropriée, pour montrer que l'ALU réalise bien ses fonctions.

Il n'est pas nécessaire de définir les éléments à un niveau de conception inférieur à celui spécifié par le concepteur du matériel. L'analyse au niveau des portes n'est approprié que si la conception est explicitement représentée par des portes pour des logiques combinatoires ou pour des contrôles de machines d'état.

NOTA 2 : L'analyse d'une implémentation en dessous du niveau spécifié par le concepteur, par exemple au niveau des portes ou des transistors, n'est pas nécessaire car ce serait analogue au test du logiciel au niveau de l'assembleur ou de sa représentation binaire. Ces niveaux d'abstraction inférieurs sont implicitement traités lorsque l'on effectue l'analyse des éléments sur les tests de vérification appliqués au matériel ou sur des simulations après routage jugées satisfaisantes; et si nécessaire le simulateur est qualifié comme outil de vérification selon le Paragraphe 11.4.

Un ASIC ou un PLD peut contenir des bibliothèques de fonctions propriétaires qui ne permettent pas l'observation de leur conception interne et par conséquent ne se prêtent pas à des analyses manuelles. Les fonctions en bibliothèques peuvent être traitées comme des éléments COTS par l'analyse des éléments à partir des aspects matériel des COTS traités par le Paragraphe 11.2 et par l'Annexe B Paragraphe 2.2. La vérification de l'utilisation de la fonction en bibliothèque doit montrer que la fonction est cohérente avec sa spécification ou avec la description fournie par le fabricant, et les tests doivent être réalisés dans un environnement qui permette l'observation des résultats.

NOTA 3: Le but n'est pas de décourager l'utilisation de fonctions en bibliothèque en faveur du développement de nouvelles fonctions; l'utilisation en pratique de fonctions en bibliothèque est encouragée afin de minimiser les occasions d'introduire d'erreurs supplémentaires dans le matériel.

Pour les ASICs ou PLDs synthétisés à partir d'une description de haut niveau dans un HDL, les critères d'analyse peuvent porter sur le code du langage comportemental de haut niveau représentant le matériel. Cependant, puisque la matérialisation synthétisée à partir des représentations HDL peut contenir des structures logiques parallèles ainsi que des aspects temporels non séquentiels, les produits issus de la synthèse doivent être pris en compte dans la détermination de la complétude de l'analyse. Le synthétiseur doit également être évalué.

3.3.1.1.2 Exécution de l'analyse des éléments

Les analyses des éléments doivent utiliser les tests de vérification basés sur les exigences, dans un ou plusieurs des environnements de test suivants :

1. Tests avec les constituants implémentant le chemin fonctionnel dans l'ensemble cible.
2. Tests effectués sur un prototype isolé. De tels tests sont typiques pour un ASIC ou un PLD.
3. Tests d'acceptation en production.

   NOTA : Les tests en production n'étant pas en général basés sur les exigences leur utilisation peut être limitée dans les analyses des éléments.

4. Simulation après routage, en particulier d'un ASIC ou d'un PLD par un simulateur qui a été évalué, et si nécessaire qualifié pour l'utilisation en tant qu'outil de vérification décrit par le Paragraphe 11.4.

L'analyse d'un élément peut être réalisée en utilisant une simulation pour mesurer la complétude obtenue, sous réserve que la procédure de test à analyser puisse être reliée aux critères d'analyse appliqués à l'élément et soit celle utilisée pour l'obtention de crédits de vérification dans le sens des objectifs du Chapitre 6. Si les procédures de test sont déduites d'un test "in situ" du matériel ou d'un prototype isolé et sont évaluées en utilisant une simulation, les stimuli de test et les résultats attendus peuvent être adaptés au simulateur sous réserve que le processus de traduction soit vérifié en terme de fidélité et considéré comme une composante de l'analyse de l'élément. On doit montrer que le simulateur utilisé pour réaliser cette analyse est en mesure de déterminer correctement si chaque type d'élément inclus dans l'implémentation a satisfait aux critères d'analyse.

3.3.1.2 Solutions pour les résultats de l'analyse des éléments

L'analyse peut faire apparaître des éléments du matériel qui ne sont pas vérifiés, indiquant soit le besoin d'activités complémentaires du processus de vérification, soit peut-être le besoin de supprimer les éléments non testés ou de passiver par des moyens architecturaux tout comportement anormal qui pourrait en résulter. Les éléments du matériel qui n'ont pas été testés peuvent être le résultat :

1. **De défauts des cas de test ou des procédures.** Des défauts des cas de test ou des procédures peuvent apparaître tout simplement si les cas de test ne vérifient pas les éléments de l'article matériel conformément aux critères de l'Annexe B Paragraphe 3.3.1.1. Ils peuvent apparaître lorsqu'il y a des attributs à ne pas prendre en compte dans les exigences fonctionnelles, bien que le matériel ait été conçu de manière appropriée pour produire des réponses reproductibles. Dans ces situations les cas et les procédures de test doivent être complétés ou modifiés. Par ailleurs l'affirmation de l'aptitude du test à vérifier ses propres exigences doit être révisée.
2. **De la non adéquation des exigences.** Les exigences doivent être modifiées ou bien des exigences dérivées complémentaires identifiées. Des tests de vérification complémentaires doivent alors être développés pour les exigences nouvelles ou révisées, exécutés et analysés.
3. **De fonctions non utilisées.** L'article matériel peut contenir des fonctions qui ne sont pas utilisées par les circuits de l'application cible, telles que les sous-fonctions d'une fonction en bibliothèque ou des structures de test qui ne sont utilisées qu'au niveau composant pour les tests de recette. On doit montrer que de telles fonctions sont soit isolées des autres fonctions utilisées, soit qu'elles ne présentent pas de comportements potentiels anormaux qui puissent avoir des effets dangereux sur la sécurité. Ceci pourrait être obtenu en montrant que les éléments non utilisés sont indéniablement désactivés dans le matériel ou lorsque le matériel est installé. Si les fonctions non utilisées doivent l'être dans des applications à venir, la carence de l'analyse de l'élément devra être réexaminée là si de telles fonctions sont identifiées comme n'ayant pas été totalement vérifiées.

4. **D'éléments sans effets sur la sécurité.** Par l'analyse, on peut montrer que les conséquences du comportement anormal de l'élément peuvent être limitées et n'ont pas d'effet dangereux sur la sécurité de l'aéronef ou de ses occupants. Ces cas doivent être traités par l'enregistrement de l'analyse qui limite les conséquences des comportements anormaux de l'élément.

3.3.1.3 Données du cycle de vie produites par l'analyse des éléments

Les données du cycle de vie produites par l'analyse des éléments devraient :

1. Identifier les FFPs à traiter par l'analyse et proposer le niveau hiérarchique de la conception auquel les éléments sont définis et comment ils doivent être analysés pour l'adéquation de la vérification, celle-ci faisant partie des critères de complétude de la couverture de vérification. Ceci doit être intégré au PHAC ou au plan de vérification du matériel.
2. Décrire les méthodes et identifier les FFPs traités par l'analyse, ainsi que les niveaux hiérarchiques de conception auxquels l'analyse a été réalisée.
3. Donner l'assurance que les données de traçabilité décrites au Paragraphe 10.4.1 montrent les relations explicites entre les procédures de vérification et les éléments dans l'analyse des éléments.
4. Identifier les cas de test de la vérification et les exigences ajoutés ou modifiés résultant de l'analyse des éléments.
5. Donner le niveau atteint par la complétude de la vérification pour les FFPs traités par l'analyse des éléments; identifier les divergences de l'analyse non résolues par la modification des tests de vérification ou des exigences et la démonstration montrant qu'elles sont acceptables.

3.3.2 Analyse spécifique de sécurité

Là où elle est appliquée, la méthode d'analyse spécifique de sécurité étend le concept de FFPA du matériel en réalisant une analyse plus en profondeur des circuits et composants sélectionnés. La FFPA étendue est utilisée à la fois pour proposer et valider les exigences spécifiques à la sécurité qui concernent le fonctionnement interne de ces circuits ou composants. Les exigences de sécurité dérivées sont ensuite traitées par des tests de vérification comme décrit ci-dessous.

L'analyse spécifique de sécurité est basée sur le concept suivant: une erreur de conception potentiellement latente ne peut affecter les sorties d'un article que lorsque des stimuli spécifiques l'y exposent. Par conséquent pour stimuler et mettre en évidence les erreurs de conception, le sous ensemble de cas pour lesquels un fonctionnement sûr est nécessaire est identifié, et les classes d'équivalences appropriées de ce sous-ensemble sont ensuite ajoutées aux tests de vérification. Lors de l'exécution de ces cas de test, les sorties de l'article sont évaluées par rapport à l'absence de comportements anormaux spécifiques qui pourraient se traduire par des conditions de sorties dangereuses. L'analyse spécifique de sécurité est utilisée pour borner l'ensemble des conditions d'entrée à appliquer dans les cas de test, de sorte qu'un ensemble potentiellement infini de cas de test ne doive pas être pris en compte.

NOTA : L'implémentation peut aussi borner les jeux et les conditions d'entrées de telle sorte qu'il ne soit pas possible, ou qu'il soit fortement improbable, que l'implémentation puisse accepter une entrée en dehors des limites du test.

La méthode d'analyse spécifique de sécurité peut aussi être utilisée afin de déterminer les aspects non passivés des fonctions de circuit et de composant dans lesquels une passivation partielle par l'architecture existe. Dans ce cas l'analyse spécifique de sécurité complémentaire peut être une méthode utile et efficace pour déterminer quel est le complément d'assurance conception nécessaire pour obtenir la couverture de la sécurité.

Les analyses spécifiques de sécurité sont également applicables soit aux matériels COTS, soit aux circuits à la demande et aux composants, car il est possible d'utiliser les données du manuel utilisateur de ces circuits et composants au lieu des données détaillées de la. conception interne. En combinant les données du manuel utilisateur avec l'application détaillée de la méthode FFPA, l'analyse spécifique de la sécurité est en mesure d'identifier avec succès les aspects sensibles à la sécurité liés à l'utilisation des circuits et composants, ainsi que les FFPs internes associés pour lesquels un effort plus grand est nécessaire pour éliminer les erreurs de conception. Cette information peut alors être utilisée avec succès pour en déduire les tests de vérification des circuits et composants qui, lorsqu'ils sont terminés, maximalisent la probabilité d'avoir par le processus de vérification mis en évidence, corrigé, passivé, ou fourni des contournements pour les erreurs de conception des circuits et composants qui pourraient affecter de manière dangereuse le matériel du point de vue de la sécurité du système.

3.3.2.1 Méthode d'analyse spécifique de la sécurité

Lorsque les circuits et composants que l'on doit traiter en utilisant la méthode d'analyse spécifique de la sécurité pour l'assurance conception sont sélectionnés, une FFPA complémentaire est réalisée pour les examiner plus en détail. Cette analyse détermine plus précisément quelles sont les fonctions des composants et des circuits qui contribuent aux fonctions de niveaux A et B déjà identifiées. Ceci est réalisé, au cas par cas, par l'examen de chaque circuit et composant auxquels elle s'applique, à leurs frontières fonctionnelles en prenant en compte l'utilisation fonctionnelle réelle de ces circuits ou composants pour réaliser les fonctions de niveau supérieur du matériel contenues dans les FFPs identifiés en niveau A et B.

NOTA : *Des informations suffisantes peuvent être disponibles dans le manuel utilisateur du circuit et du composant pour qu'un concepteur puisse utiliser avec succès leurs fonctions pour implémenter des fonctions du matériel au niveau supérieur. Si des informations suffisantes concernant le fonctionnement interne du circuit ou du composant sont disponibles, elles devraient également convenir pour effectuer cette évaluation. S'il n'y a pas suffisamment d'informations disponibles cette évaluation ne peut pas être réalisée, et une autre méthode doit être utilisée à la place ou en association avec celle-ci.*

Lorsque les fonctions sensibles vis à vis de la sécurité des circuits et composants ont été identifiées en s'appuyant sur leur utilisation réelle, l'étape suivante consiste en une analyse fonctionnelle encore plus détaillée. Cette analyse doit déterminer les attributs spécifiques non passivés, sensibles vis à vis de la sécurité des fonctions des circuits et des composants, à traiter plus en détails par les conditions de vérification spécifiques à la sécurité. Ces conditions de vérification doivent être dérivées et validées par l'utilisation des techniques de l'AMDE_F pour déterminer les attributs fonctionnels qui sont sensibles vis à vis de la sécurité, et par ailleurs pour, déterminer tout comportement anormal de ces fonctions qui pourrait contribuer à des FFPs de niveaux A et B à l'intérieur de ces circuits ou composants.

Les conditions de vérifications dérivées obtenues grâce aux analyses spécifiques de sécurité ci-dessus, sont alors utilisées en association avec les recommandations suivantes pour compléter les critères d'analyse concernant la vérification de composants et circuits appartenant à des FFPs de niveaux A et B. Les recommandations consistent en :

1. L'identification de l'espace des entrées de ces fonctions. La détermination des critères de succès et d'échec associés à l'espace des sorties en s'appuyant sur les attributs fonctionnels sensibles et sur les comportements anormaux identifiés, le développement des classes d'équivalence qui fourniront la couverture nécessaire de l'espace des entrées.
2. L'identification des moyens de détection observables et pertinents et des moyens de stimulation de l'espace des entrées pour chacune des fonctions considérées.

   NOTA : *Les caractéristiques spécifiques des outils et de l'implémentation peuvent être utilisées afin d'assurer l'observabilité et la testabilité.*

3 La spécification des environnements de test qui concernent la vérification des sources d'erreurs potentielles et des interdépendances.

NOTA : Les fonctions du composant devraient être traitées au niveau d'intégration le plus élevé possible. Le test au niveau d'intégration le plus élevé fournit en général la meilleure couverture des sources d'erreurs telles que les "upsets", les interdépendances et les interactions fonctionnelles potentielles.

Les cas de test doivent être développés en utilisant les classes d'équivalences. Les tests concernent les attributs clés des décisions logiques, l'arithmétique, la chronologie, les transitions d'états et les aspects temps réel.

3.3.2.2 Solution pour les analyses spécifiques de sécurité

Le constat d'achèvement de la vérification spécifique de sécurité doit être établi à la fin de ces analyses pour tous les circuits et composants auxquels elle est applicable. Toute carence trouvée par cette analyse ou par la vérification elle même doit être résolue par l'une des méthodes ci-dessous :

1. Modification de la conception pour corriger les erreurs.
2. Ajout d'une passivation par l'architecture qui résout le problème en l'éliminant du FFP auquel il est rattaché.
3. Ajout de tests appropriés.

3.3.2.3 Données d'analyses spécifiques de sécurité

La documentation des analyses spécifiques de sécurité, lorsqu'elles sont appliquées à des circuits et composants dans des FFPs de niveaux A et B, doivent être fournies sous la forme de données d'évaluation de sécurité, d'exigences de sécurité, de procédures et de résultats de vérification, et de données de traçabilité. Les procédures de vérification doivent être traçables vers les exigences de sécurité et vers les analyses spécifiques de sécurité. Les analyses spécifiques doivent inclure :

1. L'identification des circuits et des composants à traiter par le biais des méthodes d'analyses spécifiques de sécurité.
2. L'identification de FFPs de niveaux A et B dans lesquels se trouvent chacun de ces circuits et composants.
3. L'identification de la passivation partielle par l'architecture applicable aux circuits et aux composants pour lesquels une assurance conception complémentaire doit être obtenue par des méthodes d'analyses spécifiques de sécurité.
4. Pour chacun des circuits et composants concernés, l'identification des fonctions sensibles vis à vis de la sécurité.
5. Pour chaque fonction concernée, l'identification des attributs sensibles vis à vis de la sécurité et des comportements anormaux redoutés.
6. Les conditions de vérification concernant les circuits, les composants, les fonctions internes, les attributs fonctionnels et les comportements anormaux.
7. Les conditions de vérification traitant les dépendances des entrées et les comportements de l'espace des sorties à vérifier.
8. Les procédures de vérification et les résultats.
9. Les données de traçabilité reliant les procédures de vérification et les conditions de vérification de la sécurité aux données d'analyse spécifique à la sécurité du matériel.

3.3.3 Méthodes formelles

L'appellation méthode formelle renvoie à l'utilisation de techniques mathématiques de la logique et des discrets pour la spécification, la conception et la construction des systèmes informatiques.

NOTA : Ce paragraphe provient du "Formal Methods Specification and Analysis Guidebook for the verification of Software and Computer Systems, Volume II: A Practionner's Companion" May 1997, NASA-GB-001-97". Une présentation plus détaillée de l'utilisation des méthodes formelles, illustrée d'un exemple pratique, est donnée ci-dessous.

Les applications des méthodes formelles appartiennent à deux grandes catégories, les descriptives et les déductives. Les méthodes descriptives utilisent un langage de spécification formel qui permet des descriptions claires, non ambiguës des exigences et des autres objets de la conception. Les méthodes déductives s'appuient sur une discipline qui demande une énumération explicite de toutes les hypothèses et les étapes du raisonnement. De plus chaque étape du raisonnement doit être l'instanciation d'un nombre réduit de règles d'inférences autorisées. Les méthodes formelles les plus rigoureuses appliquent ces techniques afin d'argumenter le raisonnement utilisé pour justifier les exigences, ou les autres aspects de la conception ou de l'implémentation de systèmes complexes ou critiques. L'objectif des méthodes formelles est de réduire le rôle de l'intuition et du jugement humain lors de l'évaluation des arguments. Ainsi, les méthodes formelles réduisent l'acceptabilité d'un argument à un calcul qui peut en principe être vérifié par un outil, se substituant de ce fait à la subjectivité inhérente au processus de revue, avec une reproductibilité de l'opération.

Il y a plusieurs domaines dans lesquels l'application des méthodes formelles apportent une assurance complémentaire au processus de conception. Bien que les méthodes formelles soient utilisables tout au long du processus de conception, une augmentation de l'assurance conception peut être obtenue en ciblant leur utilisation. Ce qui suit met en évidence certaines des possibilités :

1. Les méthodes formelles peuvent être appliquées à plusieurs étapes du cycle de vie du développement. En général, les utilisations de méthodes formelles sont plus efficaces au cours des premières étapes du cycle de vie, plus particulièrement lors du recueil des exigences et de la conception de haut niveau.
2. Les méthodes formelles peuvent être appliquées à la totalité de la conception ou êtres ciblées sur des composants spécifiques. La FFPA est utilisée pour la détermination des FFPs à analyser par les méthodes formelles. Les protocoles qui font appel à des communications concurrentes complexes, et le matériel implémentant des fonctions tolérantes aux fautes, peuvent être efficacement analysés par des méthodes formelles.
3. Les méthodes formelles peuvent être utilisées pour vérifier la fonctionnalité des systèmes ou encore pour élaborer des propriétés particulières. Bien que les méthodes formelles aient été traditionnellement associées aux preuves d'exactitude, c'est à dire à l'assurance qu'un composant satisfait à ses spécifications fonctionnelles, elles peuvent aussi n'être appliquées qu'aux propriétés les plus importantes. Souvent, il est plus important de montrer qu'une conception ne présente pas de propriétés indésirables, que de montrer qu'elle a toutes les fonctionnalités.

En pratique l'utilisation des méthodes formelles exige habituellement l'assistance d'outils. Les outils utilisés doivent être évalués et si nécessaire qualifiés comme décrit au Paragraphe 11.4.

3.3.3.1 Méthodologie des méthodes formelles

L'application des méthodes formelles commence par l'expression des exigences dans un langage formel. Les spécifications d'exigences contribuent à une activité de la description importante. Elles fournissent les bases pour documenter, communiquer et prototyper le comportement et les propriétés d'un système par l'utilisation de formulations non ambiguës. De plus, les spécifications d'exigences fournissent les bases du calcul ou de prédiction formelle du comportement du système. Le modèle formel du composant à analyser est construit en utilisant un langage formel. Il est analysé par rapport aux expressions formelles des exigences, en utilisant les règles de la logique formelle sélectionnée. Les caractéristiques du modèle sont déterminées par le style d'analyse formelle à réaliser.

Le niveau de détail du modèle du composant est déterminé par le but à atteindre par la technique d'analyse formelle. Certaines techniques sont adaptées à la recherche d'erreurs de conception qui peuvent avoir échappé aux tests, alors que d'autres cherchent à garantir l'absence de certaines classes d'erreurs de conception.

1. **Détection des erreurs.** La technique formelle la plus répandue pour la détection des erreurs est appelée contrôle du modèle. Dans ce cas, les exigences sont exprimées par des formules dans une logique de décision temporelle. Le modèle du composant est une machine d'état abstrait conçue de telle sorte que la propriété à tester soit conservée. La procédure de preuve est automatique. Une tentative de preuve infructueuse indique une erreur de conception dans le composant modélisé. Le résultat d'une preuve infructueuse est une séquence de stimuli d'entrée qui démontre explicitement en quoi le composant ne satisfait pas l'exigence donnée.
2. **Elimination des erreurs.** Les méthodes formelles ciblées sur la prévention des erreurs sont en général, basées sur un langage de spécification formelle s'appuyant sur la théorie des preuves. Avec l'accroissement de l'expressivité, des exigences plus complexes peuvent être exprimées et des modèles plus détaillés de composants peuvent être construits. Cependant, la procédure de preuve ne peut être automatisée que partiellement. Un niveau de détail approprié pour le modèle du composant peut être une description HDL synthétisable. Dans certains cas, le même modèle peut être utilisé à la fois pour la simulation et pour l'analyse formelle. Une preuve menée à bien prouve l'exactitude, du point de vue de la logique, du modèle du composant vis à vis des exigences exprimées pour l'espace d'entrée analysé.

3.3.3.2 Solution pour les méthodes formelles

Il y a trois issues possibles à une analyse formelle déductive :

1. Si la tentative de preuve a abouti, la vérification est terminée. Le niveau d'assurance conception dépend de la fidélité du modèle utilisé. Par exemple, si le modèle de l'article matériel correspond à la conception détaillée, la preuve fournit autant d'assurance que le test exhaustif vis à vis de l'exactitude fonctionnelle.
2. Dans certains cas, la défaillance de la preuve aboutit à un scénario de contre-exemple explicite; à savoir qu'il identifie un scénario de test qui illustre explicitement en quoi la conception ne satisfait pas les exigences exprimées. Ceci peut indiquer soit une déficience de la conception, soit une déficience des exigences. De telles déficiences peuvent être résolues en corrigeant la conception, en révisant les exigences mises en évidence telles que des conditions non réalisables physiquement, ou en utilisant d'autres méthodes. Tous les scénarios de contre-exemple doivent être identifiés de manière à être résolus. Les modifications de la conception ou des exigences doivent être répercutées vers le processus approprié.
    a. Après qu'une conception ou qu'une exigence ait été modifiée pour traiter une déficience identifiée par un échec de preuve, un nouvel essai de preuve doit être tenté pour s'assurer que la modification a résorbé totalement le problème identifié. Ce cycle est reconduit jusqu'à ce qu'une preuve satisfaisante ait été obtenue.
    b. Lorsqu'un scénario de contre-exemple est considéré comme étant résolu sans modification des exigences ou de la conception, alors que l'outil n'identifie qu'un seul scénario de contre exemple, c'est à dire le scénario de contre-exemple résolu, alors le processus doit être modifié de manière à pouvoir identifier tous les autres contre-exemples.
3. Le cas le plus difficile à résoudre est celui où une preuve ne peut pas être produite et où un scénario de contre exemple ne peut pas être identifié. Une option possible consiste à reprendre la conception de manière à réduire l'effort de vérification. En outre, les activités de vérification peuvent être décomposées en identifiant clairement les cas traités par la preuve formelle, et ceux pour lesquels les exigences doivent être traitées par d'autre moyens. Les modifications de la conception et des exigences dérivées devraient être répercutées vers la FFPA.

3.3.3.3. Données des méthodes formelles

Les données produites lors de l'application des méthodes formelles sont :

1. La description de l'approche spécifique des méthodes formelles à utiliser et des composants ou FFPs auxquels les méthodes formelles sont appliquées.
2. Les expressions formelles des exigences.
3. Les modèles formels de composants.
4. La preuve, ou le scénario de génération de preuve suffisamment détaillé reliant les modèles de composants à l'expression formelle des exigences, y compris la corrélation avec les données de traçabilité.
5. L'identification des outils utilisés et les résultats d'évaluation des outils.
6. L'identification des cas de test de vérification et des exigences ajoutées et modifiées à la suite de l'analyse.
7. L'expression du niveau de complétude de la vérification obtenu pour les FFPs traités par l'analyse. Elle comprend la liste des divergences de l'analyse non résolues par la modification des cas de test ou des exigences, et les raisons pour lesquelles ces divergences ont été acceptées.

ANNEXE C

GLOSSAIRE

Ces définitions correspondent aux termes tels qu'ils sont utilisés dans ce document. Si un terme n'est pas défini dans cette Annexe, il peut avoir été défini dans le texte associé.

Acceptation (Acceptance) - Reconnaissance par l'autorité de certification de la satisfaction des exigences applicables par les données, arguments, ou déclarations d'équivalence soumises

Analyse (Analysis) - Processus mathématique, ou autre forme de raisonnement logique, qui conduit à partir de prémices établies, à une conclusion relative aux capacités propres d'un équipement ou d'un article matériel, à satisfaire à une application particulière.

Analyse de la Couverture (Coverage Analysis) - Détermination du degré auquel une activité du processus de vérification du matériel satisfait à ses objectifs.

Analyse de Marge de Conception (Design Margin Analysis) - Processus qui permet de déterminer que les effets cumulés des marges de conception des différents composants utilisés donnent un produit qui atteint ou dépasse les exigences de performance, ainsi que les exigences propres à sa fabrication et à son exploitation.

Approbation (Approval) - Acte ou instance par lequel s'exprime une opinion favorable ou une sanction formelle ou officielle.

Architecture Système (System Architecture) - Structure choisie pour le matériel et le logiciel afin de satisfaire aux exigences du système.

Article (Item) - Terme générique utilisé pour désigner un composant matériel, un système ou un logiciel.

Article de Configuration (Configuration Item) - Un ou plusieurs composants, outils ou données considérés comme un tout du point de vue de la gestion de la configuration.

Article Matériel (Hardware Item) - Un article qui a une existence physique. S'applique en général aux LRUs, aux cartes équipées, aux alimentations et aux composants.

Article Matériel Complexe (Complex Hardware Item) - Tous les articles qui ne sont pas simples sont considérés comme "complexes". Voir la définition d'Article Matériel Simple.

Article Matériel Simple (Simple Hardware Article) - Un article matériel est considéré comme simple lorsqu'une combinaison jugée suffisante de tests et d'analyses déterministes détaillés peut garantir des performances fonctionnelles correctes, sans comportements anormaux pour la totalité des conditions opérationnelles envisageables.

Assemblage (Assembly) – Composants, ou combinaisons de ceux-ci, reliés entre eux afin d'implémenter une fonction particulière.

Assurance (Assurance): Résultat d'actions planifiées et systématiques nécessaires pour donner une confiance suffisante et apporter la preuve qu'un produit ou qu'un processus satisfait à des exigences données.

Assurance Conception (Design Assurance) - Toutes les actions planifiées et systématiques utilisées pour justifier, avec un niveau de confiance suffisant, que les erreurs de conception ont été identifiées et corrigées de telle sorte que le matériel satisfait aux exigences de certification.

Assurance Processus (Process Assurance) - L'objectif de l'assurance processus est de garantir que les plans sont suivis, que les objectifs du cycle de vie de la conception du matériel ont été atteints et que les activités ont été effectuées complètement.

Autorité de Certification (Certification Authority) - Organisation ou personne, responsable dans l'Etat ou le pays concerné de la certification de la conformité aux exigences.

NOTA : Un dossier concernant la certification de type de l'aéronef, du moteur, ou de l'hélice, ou l'approbation d'un équipement doit habituellement être traité par l'autorité de certification. Les sujets concernant le maintien de la navigabilité peuvent être traités par l'entité considérée comme autorité de navigabilité.

Base de la Certification (Certification Basis) - Définie par l'Autorité de certification en coopération avec le postulant comme exigence particulière de la certification, accompagnée de toute condition spécifique qui peut compléter les règles publiées, elle devient la base de la certification de l'aéronef, du moteur ou de l'hélice.

Cas de Défaillance / Condition de Panne (Failure Condition) - Effet sur l'aéronef et ses occupants, à la fois directement ou par voie de conséquence, provoqué par une ou plusieurs défaillance(s), en considérant les conditions opérationnelles et environnementales dangereuses applicables.

Certification (Certification) - Reconnaissance légale par l'autorité de certification de la conformité d'un produit, d'un service, d'une organisation ou d'une personne, aux exigences applicables. La certification concerne l'activité de contrôle technique du produit, du service, de l'organisation ou de la personne, ainsi que la reconnaissance formelle de la conformité aux exigences applicables, par l'émission d'un certificat, d'une autorisation, d'une approbation ou d'un autre document en fonction des lois et procédures nationales. En particulier la certification d'un produit implique :

a. Le processus d'évaluation de la conception du produit dans le but de garantir qu'il est conforme à un ensemble de règles applicables à ce type de produit, afin de démontrer un niveau de sécurité acceptable.

b. Le processus d'évaluation d'un produit individuel dans le but de garantir qu'il est conforme à la conception de type certifiée.

c. L'émission d'un certificat exigé par les lois nationales, qui déclare que l'on a constaté la conformité avec les règles en suivant les deux points ci-dessus.

Chemin de Propagation des Défaillances (Functional Failure Path) - Ensemble spécifique de circuits interdépendants susceptibles de provoquer un comportement anormal du matériel qui implémente la fonction, ou du matériel qui est lui même dépendant de cette fonction.

Chemin Fonctionnel (Functional Path) - Ensemble de circuits spécifiques interdépendants qui implémentent une fonction.

Circuit Intégré Spécifique [ASIC] - Circuits intégrés développés pour implémenter une fonction. Dans ce terme sont inclus sans que ce soit limitatif: les pré-diffusés, les pré-caractérisés, les composants entièrement personnalisés recouvrant les technologies des composants linéaires, numériques et mixtes.

Circuits Intégrés (Integrated Circuits) - Circuit comprenant des éléments associés de manière non sécable et réalisés "in situ" sur ou à l'intérieur d'un substrat unique afin d'implémenter une fonction de circuit électronique.

Classe d'Equivalence (Equivalence Class) - Découpage de l'espace des entrées d'une fonction de telle sorte que le test d'une valeur représentative de la classe équivaut à tester les autres valeurs de cette classe.

Comportement Anormal - (Anomalous Behavior): Comportement non conforme par rapport aux exigences spécifiées.

Composant (Component) - Partie indivisible, combinaison de parties, sous-ensembles ou éléments unitaires qui implémentent une fonction du système distincte.

Composant Logique Programmable [PLD] (Programmable Logic Device) - Composant acheté comme un composant électronique et qui est modifié pour implémenter une fonction spécifique à une application. Les PLDs comprennent, sans que ce soit limitatif: les "Programmable Array Logic Components" [PAL], les "General Array Logic Components" [GAL], les "Field Programmables Gate Arrays components" [FPGA] et les "Erasable Programmable Logic Devices" [EPLD].

Composants du Commerce sur Etagère [COTS] - Composant, circuit intégré, ou sous-système développé par un fournisseur pour des utilisateurs multiples, dont la conception et la configuration sont assurées suivant les spécifications du fournisseur ou de l'industrie.

NOTA : Des exemples de composants COTS peuvent être les résistances, les condensateurs, les microprocesseurs, les circuits programmables sur site [FPGA] et les composants effaçables programmables [EPLD] avant programmation et autres types de circuits intégrés ainsi que leurs modèles implémentables, les circuits imprimés et les LRUs complets disponibles sur catalogue chez un fournisseur.

Conduite de test (Testing) - Processus de vérification du fonctionnement d'un article matériel.

Configuration (Configuration) - Liste des articles de configuration qui définit entièrement l'implémentation d'une fonction.

Conformité (Compliance) - Accomplissement satisfaisant de toutes les activités obligatoires; adéquation entre les résultats attendus ou spécifiés et les résultats réels.

Conformité (Conformance) - Caractérise le respect d'une règle, d'une spécification ou d'un dossier.

Conformité (Conformity) - Constat d'adéquation de la réalisation physique de l'article matériel par rapport à ses documents de définition.

Crédit de Certification (Certification Credit) - Acceptation par l'Autorité de certification du fait qu'un processus, ou une démonstration satisfait à une exigence de certification.

Cycle de Vie (Life-Cycle) - Intervalle de temps allant du début de la conception ou de la modification d'un article matériel, à l'achèvement de la conception ou de la modification et jusqu'à la transition vers la production.

NOTA : Dans ce document, sauf si cela est défini autrement dans le texte, ceci signifie "cycle de vie de la conception du matériel".

Cycle de Vie du Processus de Conception du Matériel (Hardware Design Life Cycle Process) - Une des combinaisons des processus de conception ou des processus transverses, définie par une organisation suffisante pour la conception de l'article matériel.

Défaillance (Failure) - Incapacité d'un système ou d'un composant du système à exécuter une fonction requise dans les limites spécifiées. Une défaillance peut subvenir lorsqu'il y a une faute.

Défaut (Defect) - Toute non conformité d'une caractéristique par rapport à une exigence spécifiée.

Défauts de Contrainte Excessive (Over-stress defects) - Défauts qui provoquent soit le dépassement des limites de conception autorisées d'un composant, ou qui sont le résultat de contraintes excessives rencontrées au cours du cycle de vie de la conception du matériel.

Défauts de Fiabilité (Reliability Defects) - Défauts qui provoquent un taux excessif de défaillances du matériel lorsqu'il est soumis à des contraintes qui n'excèdent pas les limites autorisées. Les défauts de contraintes excessives tout comme les défauts de fiabilité peuvent être mis en évidence par des taux excessifs de défaillances aléatoires, des mortalités infantiles excessives, ou des taux de vieillissement excessifs.

Défauts de Robustesse (Robustness Defects) - Défauts qui entraînent des défaillances du matériel ou un fonctionnement incorrect lorsqu'il est soumis à des contraintes et à une exploitation qui ne dépasse pas les limites de conception. Les conséquences de ces défauts peuvent se traduire par des susceptibilités aux contraintes d'environnement et des instabilités en cours d'exploitation.

Défauts Fonctionnels (Functional Defects) - Défauts qui entraînent des fonctionnements incorrects du matériel, même s'il n'y a pas eu une défaillance physique de celui-ci. Le fonctionnement incorrect du matériel qui en résulte peut à son tour entraîner un fonctionnement incorrect des fonctions du logiciel.

Détarage de composant (Component de-Rating) - Il s'agit d'une méthode de conception qui augmente les marges opérationnelles des composants en imposant des limitations d'usage plus restrictives que les limitations d'usage habituelles ou publiées par les fabricants.

Disponibilité (Availability) - Probabilité pour qu'un article ou une fonction soit dans un état utilisable.

Dysfonctionnement (Malfunction) - Occurrence d'une situation au cours de laquelle le fonctionnement est en dehors des limites spécifiées.

Effet d'une Défaillance (Failure Effect) - (1) Description du fonctionnement d'un article à la suite d'une défaillance ; (2) Conséquences d'un mode de défaillance sur l'utilisation, le fonctionnement ou l'état d'un système ou d'un article.

Erreur (Error) - Erreur commise dans les exigences, la conception ou l'implémentation.

Evaluation (Assessment) - Estimation basée sur l'expérience en ingénierie.

Evaluation de la Sécurité du Système [SSA] (System Safety Assessment) - Evaluation détaillée continue et systématique du système proposé pour montrer que les exigences de sécurité sont satisfaites.

Evaluation d'Outil (Tool Assessment) - Ensemble des activités d'évaluation des outils utilisés dans la conception et la vérification de l'article matériel pour donner confiance en la capacité de ces outils à exécuter correctement leurs fonctions, en cohérence avec le niveau d'assurance conception des fonctions que doit implémenter l'article matériel.

Evaluation Préliminaire de la Sécurité du Système - [PSSA] (Preliminary System Safety Assessment): Evaluation systématique de l'architecture du système et de son implémentation, fondée sur l'évaluation des risques fonctionnels et la classification des cas de défaillance, pour déterminer les exigences de sécurité de tous les éléments de l'architecture.

NOTA : L'évaluation préliminaire de la sécurité du système s'applique au système en développement. Elle est utilisée pour déterminer les activités d'analyses plus détaillées nécessaires à l'évaluation complète de la sécurité du système.

Exigence (Requirement) - Elément identifiable et vérifiable d'une spécification.

Exigence Dérivée (Derived Requirement) - Exigence complémentaire résultant des processus de conception du matériel qui peut ne pas être directement tracée vers les exigences de niveau plus élevé.

Expérience du Produit en Exploitation (Product Service Experience) - Période pendant laquelle le matériel est utilisé dans un environnement connu et au cours de laquelle les défaillances successives sont enregistrées.

Faute (Fault) - (1) Manifestation d'une anomalie dans le matériel due à une erreur ou à un événement aléatoire. Une faute lorsqu'elle se produit peut provoquer une défaillance. (2) Anomalie non souhaitée d'un article.

Fiabilité (Reliability) - Probabilité pour qu'un article assure une fonction requise pendant une durée spécifiée dans des conditions établies.

Gestion de Configuration (Configuration Management) - (1) Processus d'Identification de la Configuration et de contrôle des problèmes et des évolutions des Identités de Configuration. (2) Activité d'orientation et de surveillance à la fois technique et administrative ayant pour but d'identifier et d'enregistrer les caractéristiques fonctionnelles et physiques d'un article de configuration; de gérer les modifications de ces caractéristiques, d'enregistrer et de rendre compte de la gestion des modifications et de l'état de leur mise en oeuvre.

Gestion des Modifications (Change Control) - (1) Processus d'enregistrement, d'évaluation, d'approbation ou de désapprobation, et de coordination des modifications des articles de configuration après l'établissement formel de leur identification ou de la définition du référentiel. (2) L'évaluation, la coordination, l'approbation ou la désapprobation et la réalisation systématiques des modifications approuvées de la configuration d'un article, après l'établissement formel de son identité ou du référentiel.

"Glitch" (Glitch) - Transition sur une entrée ou pointe de tension qui survient pendant une durée inférieure au retard de propagation jusqu'à la sortie de la logique affectée.

Hypothèse (Assumption) - Déclaration ou principe proposé sans preuve.

Identificateur (Part Number) - Ensemble de nombres, lettres ou autres caractères utilisés pour identifier un item de configuration, une identité de configuration.

Identification de Configuration (Configuration Identification) - Processus de définition et de désignation d'un article de configuration.

Identité de Configuration (Configuration Identity) - Nom unique donné à un article de configuration ou à une configuration résultant d'une Identification de Configuration.

Implémentation (Implementation) - Acte de création d'une réalité physique à partir d'une spécification.

Indépendance (Independance) - Séparation des responsabilités qui garantit l'aboutissement d'une évaluation objective. A rapprocher de l'indépendance intellectuelle telle que celle d'un autre individu, et non de celle d'un département ou d'une entreprise:

1. Pour la vérification, l'indépendance est obtenue par l'évaluation de l'exactitude des données du point de vue technique au moyen, soit d'une personne, soit d'une entité autre que celles utilisées pour produire cette donnée.
2. Pour l'assurance processus, l'indépendance est obtenue par l'évaluation de la conformité du processus par des personnes ou des entités autres que celles utilisées pour exécuter ce processus.

Ingénierie Concurrente (Concurrent Engineering) - Processus dans lequel des disciplines multiples contribuent au processus de conception du matériel afin de garantir que les exigences propres aux disciplines sont prises en compte.

Inspection (Inspection) - Examen et test des fournitures et services, y compris, lorsque cela est approprié, des matériaux bruts, des composants, des assemblages intermédiaires et des services afin de déterminer s'ils sont conformes aux exigences spécifiées.

Inspection du Premier Article (First Article Inspection) - Inspection qui vérifie au titre de l'Assurance Processus que le matériel présenté est conforme à la documentation du processus de fabrication. Elle est effectuée sur un article matériel représentatif de la configuration des premiers produits issus de la chaîne, en tant que condition préalable à l'approbation de la production.

Intégration Matériel/Logiciel (Hardware/Software Integration) - Réunion du matériel et du logiciel afin d'implémenter une application ou une fonction.

Intégrité (Integrity) - Attribut d'un article indiquant que l'on peut lui faire confiance pour la réalisation de la fonction attendue.

Langage de Description du Matériel [HDL] (Hardware Description Language) - Est utilisé dans ce document pour représenter tous les langages de description du matériel, y compris le "Verilog HDL", le langage de Description des Circuits Intégrés à Très Haute Vitesse et le Langage de Description du Matériel Analogique.

Logiciel (Software) - Programme informatique et éventuellement sa documentation associée ainsi que les données faisant partie de l'utilisation du système informatique.

Maintenabilité (Maintenability) - Caractéristique de la conception et de l'installation qui s'exprime par la probabilité qu'un article soit conservé ou restauré dans un état spécifique au cours d'une période de temps donnée, lorsque la maintenance est réalisée conformément aux procédures et ressources prescrites.

Manufacturabilité (Manufacturability) - Caractéristique de la conception d'un produit qui améliore la rentabilité de la production de masse par l'optimisation des matériaux, des outils de fabrication et par l'utilisation de techniques de conception qui minimisent l'impact des dispersions des composants sur la fonctionnalité.

Mise à disposition (Release) - Acte formel de mise sous le contrôle de la gestion de la configuration d'une donnée de l'article matériel.

Mode Commun (Common Mode) - Evénement qui provoque un comportement anormal de deux ou plusieurs articles, sous-articles ou fonctions.

Mode de Défaillance (Failure Mode) - Manière dont la défaillance d'un article se produit.

Moyens de Démonstration de Conformité (Means of Compliance) - Méthodes à utiliser par le postulant afin de satisfaire les exigences exprimées dans la base de certification pour un aéronef ou un moteur. Par exemple: les instructions, les dessins, les analyses, les calculs, les tests, la simulation, les inspections et les qualifications environnementales. Les circulaires d'information diffusées par l'autorité de certification sont utilisées quand cela est approprié.

Navigabilité (Airworthiness) - Etat d'un article qui peut être un aéronef, un système d'aéronef ou un composant, dans lequel cet article fonctionne de manière sûre dans l'accomplissement des fonctions attendues.

Outil de vérification (Verification tool) - Outil utilisé pour garantir les performances vis à vis de règles préétablies ou des exigences. Cet outil n'introduit pas d'erreurs mais il peut être incapable de les détecter. Exemple: un simulateur de circuits numériques ou analogiques, ou un testeur automatisé qui mesure les performances d'un circuit réel.

Outils de Conception (Design Tools) - Outils dont les sorties font partie de la conception du matériel et qui par conséquent peuvent y introduire des erreurs : par exemple un routeur d'ASIC ou un outil qui crée le placement d'une carte ou d'une puce à partir d'un schéma ou de toute autre exigence détaillée.

Partitionnement du Matériel (Hardware Partitioning) - Méthode d'amélioration de la fiabilité et de la sécurité par la séparation physique et par l'isolement du matériel qui implémente les fonctions, y compris les redondances pour prévenir les effets des défaillances dues aux fautes communes.

Postulant (Applicant) - Une personne ou une organisation qui demande une approbation à l'autorité de certification.

Premier Article (First Article) - Unité soumise à une inspection afin de vérifier les dossiers de production, les outils et les procédures.

Procédure de test (Test Procedure) - Instructions détaillées pour le contrôle des conditions d'exécution d'une suite donnée de tests.

Processus (Process) - Ensemble d'activités interconnectées réalisées afin de produire un résultat ou un produit attendu.

Processus de Conception (Design Process) - Processus de création d'un article matériel à partir d'un jeu d'exigences en utilisant un ensemble de processus: recueil des exigences, conception générale, conception détaillée, implémentation et transition vers la production.

Processus de Planification (Planning Process) - Processus de définition et de coordination des activités des processus de conception et de développement.

Processus Transverse (Supporting Process) - Processus utilisé afin de soutenir le processus de conception, il consiste en l'un des processus suivants: validation, vérification, gestion de la configuration, assurance processus ou coordination pour la certification.

Production (Production) - Fabrication du produit par une séquence de processus documentés et maîtrisés.

Produit (Product) - Matériel, logiciel, article ou système élaborés en réponse à un ensemble défini d'exigences.

Prototype (Prototype) - Article matériel de pré-production totalement représentatif du produit final utilisant des composants approuvés et appropriés pour une évaluation complète de la forme, de la conception et des performances.

Qualification d' Outil (Tool Qualification) - Processus nécessaire à l'obtention d'un crédit de certification pour un outil dans le contexte particulier des systèmes de bord.

Recommandation (Guidance) - Conseil ou aide qui permet de satisfaire aux exigences de certification.

Référentiel (Baseline) - Configuration identifiée et approuvée qui sert ensuite de référence pour une conception ultérieure, et qui n'est modifiée qu'au travers des procédures de gestion des modifications.

Règle (Standard) - Directive ou base de comparaison utilisée pour fournir à la fois des recommandations et l'évaluation d'une activité donnée ou le contenu d'un item de donnée spécifiée.

Rétroingénierie (Reverse Engineering) - Reconstitution de la conception d'un article matériel par l'étude de sa construction, de ses fonctions et de ses performances dans un environnement particulier.

Revue (Review) - Evaluation qualitative conduite afin d'évaluer les plans, les exigences, les données de conception, le concept ou l'implémentation de la conception, afin de démontrer avec un degré de confiance élevé que les exigences ont été ou seront satisfaites.

Risque (Risk) - Combinaison de la fréquence et des conséquences d'un état dangereux spécifié.

Sécurité (Safety) - Etat dans lequel le risque est inférieur à la limite du risque. La limite du risque est la valeur supérieure du risque acceptable. Elle est spécifique d'un processus technique ou d'un état. Le risque est défini par le taux ou la probabilité d'occurrence ainsi que les dommages et blessures attendues.

Similitude (Similarity) - S'applique aux systèmes comparables en caractéristiques et en utilisation sur un aéronef, précédemment certifié par le postulant. Il est de plus supposé qu'il n'y a pas de parties du système qui sont soumises à davantage de risques d'environnement ou d'installation et que les contraintes opérationnelles ne sont pas plus sévères que pour le système analogue.

Simulateur (Simulator) - Dispositif, programme informatique ou système utilisé lors de la vérification du matériel, qui accepte les mêmes entrées et produit les mêmes sorties qu'un système donné.

Spécification (Specification) - Ensemble d'exigences, qui prises ensemble, constituent les critères qui définissent les fonctions et les attributs d'un article.

Structure (Structure) - Arrangement ou interconnexion spécifié de parties qui forment un tout.

Surveillance (Monitoring) - (1) **Sécurité -** Fonctionnalité interne à un système qui est conçue afin de détecter les comportements anormaux de ce système. (2) **Assurance processus** - Action d'attester ou d'examiner des exemples choisis de tests, d'inspection ou d'autres activités, ou enregistrements de ces activités, afin de garantir que ces activités sont maîtrisées et que les résultats enregistrés sont représentatifs des résultats attendus. La surveillance est généralement associée à des activités exécutées sur une longue durée au cours de laquelle un contrôle à 100% est considéré comme impossible à réaliser ou non nécessaire. La surveillance apporte la confirmation que l'activité demandée a été réalisée comme prévu.

Système (System) - Ensemble de composants matériels et logiciels structurés pour accomplir une fonction ou un ensemble de fonctions spécifiques.

Taux de défaillance (Failure Rate) - Nombre total de défaillances pour une population d'articles, donnée divisé par le nombre total d'heures de mise sous tension dans des conditions données.

Temps d'Exposition (Exposure Time) - Intervalle de temps entre l'instant où un article matériel a été reconnu fonctionner correctement pour la dernière fois, et celui où il sera reconnu fonctionner correctement à nouveau.

Test (Test) - Procédure quantitative qui prouve la performance en utilisant des critères objectifs formalisés associés à des résultats du type succès ou échec.

- Approximativement synonyme de contrôle.
- De calculs en électronique numérique - Pour vérifier l'état ou la condition d'un élément, d'un composant, d'un programme, etc.
- D'un article matériel - Pour déterminer ses caractéristiques de performance lorsqu'il fonctionne dans des conditions contrôlées.
- Un des points d'une inspection qui dénote en général la détermination par des moyens techniques des propriétés d'éléments, de fournitures, ou de commentaires sur celles-ci, incluant le fonctionnement opérationnel, et qui implique la mise en œuvre de procédures et de principes scientifiques établis.
- Utilisé dans certain cas comme terme générique pour inclure à la fois les procédures d'essais et de diagnostic.

Testabilité (Testability) - (1) Capacité à tester un article matériel de manière suffisante pour garantir qu'il fonctionne suivant ses spécifications dans tous les états possibles. (2) Facilité avec laquelle un article matériel peut être testé afin de fournir la preuve de la conformité à ses exigences.

Traçabilité (Traceability) - Association identifiable entre des articles matériel ou des processus, telle qu'entre une exigence et la source de l'exigence ou entre une méthode de vérification et l'exigence de référence.

"Upset" (Upset) - Interférence résultant d'événements externes tels que le foudroiement ou tout autre événement environnemental.

Validation (Validation) - Processus de détermination de la complétude et de l'exactitude des exigences.

Vérification (Verification) - Evaluation de l'implémentation des exigences afin de déterminer si elles ont été satisfaites.

ANNEXE D

ABREVIATIONS

ALU	Unité arithmétique et logique
ARP	Pratiques aéronautiques recommandées
ASIC	Circuit intégré à application spécifique
HC1	Catégorie 1 de contrôle de données
HC2	Catégorie 2 de contrôle des données
COTS	Composant du commerce sur étagère
EUROCAE	Organisation Européenne pour l'Equipement de l'Aviation Civile
FAR	Règlements de l'aviation fédérale
FFP	Chemin de propagation des défaillances
FFPA	Analyse des chemins de propagation des défaillances
FHA	Evaluation des risques fonctionnels
AMDE_F	Analyse des modes et effets des défaillances fonctionnelles
FTA	Analyse de l'arbre des fautes
HDL	Langage de description du matériel
JAR	Exigences aéronautiques conjointes
LRU	Unité remplaçable en ligne
PHAC	Plan pour les aspects matériel de la certification
PLD	Composant logique programmable
PSSA	Evaluation préliminaire de la sécurité du système
RTCA	RTCA, Inc
SAE	Society of Automotive Engineers
SC	Comité spécial
SSA	Evaluation de la sécurité du système
WG	Groupe de travail

MEMBERSHIP

EUROCAE WG-46/RTCA SC-180

Chairmen:

EUROCAE WG-46	Arnaud Demichelis	DGA/SPAe (FR)
RTCA SC-180	Robert Clark	Honeywell, Inc.
RTCA SC-180	Lee Johnson	Rockwell Collins, Inc.

Secretaries:

EUROCAE WG-46	William Betts	Lucas Electronics (UK)
EUROCAE WG-46	Cleland Newton	DERA (UK)
RTCA SC-180	Connie Beane	Federal Aviation Administration

EUROCAE Representative:	**RTCA Representative:**
Francis Grimal	Jack Cattilini
Geoffrey Hunt	Jerry Bryant
	Rudy Ruana

Joint Team 1 Co-Chairs:

Jacques Azum	Aerospatiale
Denis Mayfield	Boeing Commercial Airplane Group

Joint Team 2 Co-Chairs:

Ken Hunt	British Aerospace Airbus
Ted Parker	Honeywell, Inc.

Joint Team 3 Co-Chairs:

Brian Davis	Smiths Industries
David Richter	Rockwell Collins, Inc.

Joint Team 4 Co-Chairs:

David Austin	AlliedSignal
Francis Capecchi	Aerospatiale

Editorial Team:

Connie Beane	Federal Aviation Administration
Steven Beland	Boeing Commercial Airplane Group
Thierry Bickard	SNECMA
Francis Capecchi	Aerospatiale
Arnaud Demichelis	DGA/SPAe (FR)
Ken Hunt	British Aerospace Airbus
Lee Johnson	Rockwell Collins, Inc.
Thomas Neveling	Daimler Chrysler Aerospace Airbus
Cleland Newton	DERA (UK)
Ted Parker	Honeywell, Inc.
Dave Richter	Rockwell Collins, Inc.
William Struck	Federal Aviation Administration
Chris Wilkinson	Smiths Industries
Timothy Zimmerman	Cessna

MEMBERS

Ian Alderton	Ultra Electronics, Ltd.
Jozef van Baal	RLD
Barry Beaman	Woodward Governor Co.
Denys Bernard	Aerospatiale
Barbara BonJour	Boeing - Commercial Avionics Systems
Carmine Cifaldi	RAI
Christophe Conge	Dassault Aviation
Joe Costello	Rockwell Collins, Inc.
Rich Cuplin	Woodward Governor Co.
Dale Davidson	Honeywell, Inc.
Mike DeWalt	Certification Services, Inc.
William Donoghue	Pratt & Whitney
Cheryl Dorsey	Digital Flight
Joseph Eller	Liebherr-Aerospace
Brian Estep	Interstate Electronics Corp.
Bob Friday	AlliedSignal
Francois Gaffard	Intertechnique
Antoine Gautier	Dassault Aviation
John Glass	Smiths Industries
Bernard Gonzales	Bombardier Aerospace – Learjet, Inc.
Nathalie Goubert	STTE
Bill Greenleaf	Rockwell Collins, Inc.
Olivier Humez	Sextant Avionique
David Kirkland	Boeing Commercial Airplane Group
Tony Lambregts	Federal Aviation Administration
Dave Larkman	Boeing - Commercial Avionics Systems
Douglas Lee	Transport Canada
Michel Le Pimpec	Intertechnique
Brian Lucas	Proteus Corporation
Robert Maitan	Proteus Corporation
Joseph McHugh	ILC Data Device Corp.
Michael Miller	Honeywell, Inc.
Paul Miner	NASA, Langley Research
Ian Newton	GEC-Marconi Avionica
Jean Ofanowski	Dassault Aviation
Tom Olson	Rockwell Collins, Inc.
Steven Paasch	Certification Services, Inc.
Pascal Pampagnin	Aerospatiale
Chandrakant Patel	Litton Aero Products

Gerald Pilj	Bombardier Aerospace – Learjet, Inc.
Christian Pitot	Sextant Avionique
Benard Pro	AlliedSignal EAS
Misha Radich	Woodward Governor Co.
Leanna Rierson	Federal Aviation Administration
David Sandefur	Cessna
Paul Sapp	Universal Avionics Systems
Pete Saraceni	Federal Aviation Administration
Dennis Schmidt	Bombardier Aerospace – Learjet, Inc.
Kenneth Schmidt	Westinghouse ESG
Brian Shumaker	Proteus Corporation
Bruce Smith	Rockwell Collins, Inc.
Larry Smith	Honeywell, Inc.
Michael C. Smith	Ametek Aerospace
Pascal Thibault	Intertechnique
Laurie Thompson	Honeywell, Inc.
Jack Thornton	Rockwell Collins, Inc.
James Treacy	Federal Aviation Administration
Bertrand Voisin	Dassault Aviation
Kirk Walworth	Hamilton Sundstrand
Carl Ward	Lockheed Martin Aeronautical Systems
Brian Watkins	Bombardier Aerospace – Learjet, Inc.
Larry Yount	Honeywell, Inc.