



## ED-80 / RTCA DO254 application guide

## Guide d'application de l'ED-80 / RTCA DO254

Copyright © BNAE. All rights reserved.  
Any complete or partial reproduction is  
unlawful, except as may be expressly  
permitted in writing by the publisher. The  
same applies to translation, adaptation,  
transformation or arrangement by any  
technical means. Copies or reproductions  
are only authorized and strictly reserved  
for the private use and not intended for  
collective use.

Copyright © BNAE. Tous droits réservés.  
Toute reproduction intégrale ou partielle  
est illicite sauf accord explicite écrit  
accordé par l'éditeur. Il en est de même  
pour la traduction, l'adaptation, la  
transformation ou l'arrangement par un  
procédé quelconque. Seules sont  
autorisées les copies ou reproductions  
strictement réservées à l'usage privé et  
non destinées à une utilisation collective.

Edition 09/2005

BNAE would like to thank all the companies and organizations members of BNAE Committee and Working Group which have contributed to the preparation of this document.

Le BNAE remercie les sociétés et organismes membres de la Commission de Branche  
et du Groupe de travail qui ont participé à l'élaboration de ce document.

| GENERAL RECOMMENDATIONS                          |                                                                                                    | ED-80 / RTCA DO254 APPLICATION GUIDE | Recommendation<br><b>RG.Aéro 000 28</b><br>September 2005 |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------|
| <b>CONTENTS</b>                                  |                                                                                                    |                                      |                                                           |
|                                                  |                                                                                                    |                                      | Page                                                      |
| <b>0</b>                                         | <b>Foreword .....</b>                                                                              |                                      | <b>2</b>                                                  |
| <b>1</b>                                         | <b>Scope of the recommendation .....</b>                                                           |                                      | <b>2</b>                                                  |
| <b>2</b>                                         | <b>Bibliography .....</b>                                                                          |                                      | <b>2</b>                                                  |
| <b>3</b>                                         | <b>Scope of application of the Recommendation .....</b>                                            |                                      | <b>3</b>                                                  |
| <b>4</b>                                         | <b>Comments on terminology .....</b>                                                               |                                      | <b>3</b>                                                  |
| <b>5</b>                                         | <b>General presentation of ED-80 .....</b>                                                         |                                      | <b>6</b>                                                  |
| 5.1                                              | Objective and purpose .....                                                                        |                                      | 6                                                         |
| 5.2                                              | Scope .....                                                                                        |                                      | 6                                                         |
| 5.3                                              | How to use this document (extract from ED-80) .....                                                |                                      | 6                                                         |
| <b>6</b>                                         | <b>Links/consistency with other documents .....</b>                                                |                                      | <b>8</b>                                                  |
| 6.1                                              | Links/consistency with IEC 61508 .....                                                             |                                      | 8                                                         |
| 6.2                                              | Links/consistency with RAMS documents described in RG.Aéro 000 40A and its support documents ..... |                                      | 11                                                        |
| <b>7</b>                                         | <b>Comprehension/recommendations per ED-80 chapter .....</b>                                       |                                      | <b>11</b>                                                 |
| 7.1                                              | Introduction .....                                                                                 |                                      | 11                                                        |
| 7.2                                              | System aspect of hardware design assurance .....                                                   |                                      | 13                                                        |
| 7.3                                              | Hardware design life cycle .....                                                                   |                                      | 15                                                        |
| 7.4                                              | Planning process .....                                                                             |                                      | 16                                                        |
| 7.5                                              | Hardware design processes .....                                                                    |                                      | 17                                                        |
| 7.6                                              | Validation and verification process .....                                                          |                                      | 18                                                        |
| 7.7                                              | Configuration management process .....                                                             |                                      | 24                                                        |
| 7.8                                              | Process assurance .....                                                                            |                                      | 25                                                        |
| 7.9                                              | Certification liaison process .....                                                                |                                      | 25                                                        |
| 7.10                                             | Hardware design life cycle data .....                                                              |                                      | 26                                                        |
| 7.11                                             | Additional considerations .....                                                                    |                                      | 31                                                        |
| <b>Annex A</b>                                   | <b>.....</b>                                                                                       |                                      | <b>34</b>                                                 |
| <b>Annex B</b>                                   | <b>.....</b>                                                                                       |                                      | <b>35</b>                                                 |
| <b>Annex C</b>                                   | <b>.....</b>                                                                                       |                                      | <b>38</b>                                                 |
| <b>Approved by BNAE</b><br><b>September 2005</b> |                                                                                                    |                                      |                                                           |

© All rights reserved

| RECOMMANDATIONS GÉNÉRALES                             |                                                                                                                    | GUIDE D'APPLICATION DE L'ED-80 / RTCA DO254 | Recommandation<br><b>RG.Aéro 000 28</b><br>Septembre 2005 |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------------------------------------------------|
| <b>SOMMAIRE</b>                                       |                                                                                                                    |                                             |                                                           |
|                                                       |                                                                                                                    |                                             | Page                                                      |
| <b>0</b>                                              | <b>Avant-propos .....</b>                                                                                          |                                             | <b>2</b>                                                  |
| <b>1</b>                                              | <b>Objet de la recommandation .....</b>                                                                            |                                             | <b>2</b>                                                  |
| <b>2</b>                                              | <b>Références bibliographiques .....</b>                                                                           |                                             | <b>2</b>                                                  |
| <b>3</b>                                              | <b>Domaine d'application de la Recommandation .....</b>                                                            |                                             | <b>3</b>                                                  |
| <b>4</b>                                              | <b>Commentaires sur la terminologie .....</b>                                                                      |                                             | <b>3</b>                                                  |
| <b>5</b>                                              | <b>Présentation générale de l'ED-80 .....</b>                                                                      |                                             | <b>6</b>                                                  |
| 5.1                                                   | Objectif et but .....                                                                                              |                                             | 6                                                         |
| 5.2                                                   | Domaine d'application .....                                                                                        |                                             | 6                                                         |
| 5.3                                                   | Modalités d'utilisation du document (extrait de l'ED-80) .....                                                     |                                             | 6                                                         |
| <b>6</b>                                              | <b>Liaisons/cohérence avec autres documents .....</b>                                                              |                                             | <b>8</b>                                                  |
| 6.1                                                   | Liaisons/cohérence avec CEI 61508 .....                                                                            |                                             | 8                                                         |
| 6.2                                                   | Liaisons/cohérence avec les documents SdF de la logique RG.Aéro 000 40A et de ses documents d'accompagnement ..... |                                             | 11                                                        |
| <b>7</b>                                              | <b>Compréhension/recommandations par chapitre de l'ED-80 .....</b>                                                 |                                             | <b>11</b>                                                 |
| 7.1                                                   | Introduction .....                                                                                                 |                                             | 11                                                        |
| 7.2                                                   | Aspect système de l'assurance de la conception du matériel .....                                                   |                                             | 13                                                        |
| 7.3                                                   | Cycle de vie de la conception du matériel .....                                                                    |                                             | 15                                                        |
| 7.4                                                   | Processus de planification .....                                                                                   |                                             | 16                                                        |
| 7.5                                                   | Processus de conception du matériel .....                                                                          |                                             | 17                                                        |
| 7.6                                                   | Processus de validation et de vérification .....                                                                   |                                             | 18                                                        |
| 7.7                                                   | Processus de gestion de la configuration .....                                                                     |                                             | 24                                                        |
| 7.8                                                   | Assurance processus .....                                                                                          |                                             | 25                                                        |
| 7.9                                                   | Processus de liaison avec la certification .....                                                                   |                                             | 25                                                        |
| 7.10                                                  | Données du cycle de vie de la conception du matériel .....                                                         |                                             | 26                                                        |
| 7.11                                                  | Considérations complémentaires .....                                                                               |                                             | 31                                                        |
| <b>Annexe A</b>                                       | <b>.....</b>                                                                                                       |                                             | <b>34</b>                                                 |
| <b>Annexe B</b>                                       | <b>.....</b>                                                                                                       |                                             | <b>35</b>                                                 |
| <b>Annexe C</b>                                       | <b>.....</b>                                                                                                       |                                             | <b>38</b>                                                 |
| <b>Approuvée par le BNAE</b><br><b>Septembre 2005</b> |                                                                                                                    |                                             |                                                           |

## 0 Foreword

Increasing numbers of standardisation documents are currently being issued by international bodies (IEC, EUROCAE, SAE, OCCAR, NATO, etc.). These documents are intended to define a certain number of recommendations or even contractual requirements affecting the field of RAMS (reliability, availability, maintainability, safety).

The scope of these documents is far wider than initially envisaged and are now applicable to fields covered by the BNAE. The question then arises of correct understanding of these documents by the industrial parties using the BNAE baseline (whether or not contractors) and knowledge of the good practices to be associated with these various requirements.

ED-80 (RTCA DO254) applies to the electronic hardware aspects and to the field of safety with a view to certification. This guide will in particular apply to highlighting system and RAMS links.

**ED-80 must be read before this recommendation is used.**

## 1 Scope of the recommendation

The purpose of this guide is to create links between the EUROCAE ED-80 document "Design Assurance Guidance for Airborne Electronic Hardware" and the BNAE documents more specifically related to RAMS and describing the good practices and the pitfalls to be avoided:

- RAMS Section of RG.Aéro 000 40A,
- RG.Aéro 000 27 and RG.Aéro 000 33A,
- RE.Aéro 703 05A, 06A.

Certain other BNAE documents may be used:

- Configuration Management Section of RG.Aéro 000 40A,
- RG.Aéro 000 23B,

The main body of the BNAE's RAMS documents can provide solutions reflecting the particularity of the four individual components of RAMS.

## 2 Bibliography

ISO 9000, *Quality management systems – Fundamentals and vocabulary*

EN 9100, *Aerospace series – Quality management systems – Requirements (based on ISO 9001:2000) and Quality systems – Model for quality assurance in design, development, production, installation and servicing (based on ISO 9001:1994)*

EN 9200, *Aerospace series – Programme management – Guidelines for project management specification*

X 60-500, *Terminology relating to reliability, maintainability and availability*

ED-80, *Design assurance guidance for airborne electronic hardware*

EUROCAE ED-12B/RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*

EUROCAE ED-14D/RTCA DO-160D, *Environmental Conditions and Test Procedures for Airborne Equipment*

## 0 Avant-propos

**À l'heure actuelle, de plus en plus de documents à caractère normatif sont édités par des instances internationales (CEI, EUROCAE, SAE, OCCAR, OTAN, etc.). Ces documents sont destinés à définir un certain nombre de recommandations voire d'exigences contractuelles qui touchent le domaine de la Sûreté de Fonctionnement.**

Ces documents ont des domaines d'application bien plus larges que ceux initialement prévus. Ces documents deviennent applicables aux domaines couverts par le BNAE. Il se pose alors la question de la bonne compréhension de ces documents par les industriels utilisant le référentiel BNAE (contractants ou non) et de la connaissance des bonnes pratiques à associer à ces diverses exigences.

L'ED-80 (RTCA DO254) s'applique aux aspects matériels électroniques et au domaine de la sécurité en vue de la certification. En particulier, le présent guide s'appliquera à mettre en évidence les liens sous l'aspect système et Sûreté de Fonctionnement.

**La lecture de l'ED-80 est un préalable à l'utilisation de cette recommandation.**

Vis-à-vis de la version française de l'ED-80, seule la version anglaise fait foi.

## 1 Objet de la recommandation

Le propos de ce guide est de créer des liens entre le document EUROCAE ED-80 "Design Assurance Guidance for Airborne Electronic Hardware" et les documents du BNAE relatifs plus particulièrement à la Sûreté de Fonctionnement qui décrivent les bonnes pratiques et les pièges à éviter :

- chapitre Sûreté de Fonctionnement de la RG.Aéro 000 40A,
- RG.Aéro 000 27 et RG.Aéro 000 33A,
- RE.Aéro 703 05A, 06A.

Certains autres documents BNAE pourront être utilisés :

- chapitre "Gestion de la Configuration" de la RG.Aéro 000 40A,
- RG.Aéro 000 23B,

Le corpus de documents Sûreté de Fonctionnement du BNAE est apte à apporter des solutions reflétant la particularité de la Sûreté de Fonctionnement telle que prise en compte dans l'ensemble de ses quatre composantes.

## 2 Références bibliographiques

ISO 9000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

EN 9100, *Série aérospatiale – Systèmes de management de la Qualité – Exigences (basé sur ISO 9001:2000) et Systèmes qualité – Modèle pour l'assurance qualité en conception, développement, production, installation et exploitation (basé sur ISO 9001:1994)*

EN 9200, *Série aérospatiale – Management de programme – Recommandation pour une spécification de management de projet*

X 60-500, *Terminologie relative à la fiabilité – Maintenabilité – Disponibilité*

ED-80, *Recommandations pour l'assurance conception de matériel électronique de bord*

EUROCAE ED-12B/RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*

EUROCAE ED-14D/RTCA DO-160D, *Environmental Conditions and Test Procedures for Airborne Equipment*

EUROCAE ED-79/SAE ARP 4754, *Certification Considerations for Highly Integrated or Complex Aircraft Systems*

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

SAE ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

RE.Aéro 701 10A, *Safety construction principle for a missile or space product*

RE.Aéro 701 11A, *Guide of safety analysis running methods for a missile or space product*

RE.Aéro 701 12A, *Guide for the elaboration of safety objectives for a missile or space product*

RE.Aéro 703 05A, *Guide for reliability control*

RE.Aéro 703 06A, *Guidelines for reliability growth control*

RG.Aéro 000 23B, *Programme Management – A guide for the application of the principles of configuration management*

RG.Aéro 000 27, *Programme management – Guide to RAMS management*

RG.Aéro 000 33A, *Programme Management – FRACAS : Failure Reporting Analysis and Corrective Actions System*

RG.Aéro 000 40A, *General recommendation for the project management specification*

### 3 Scope of application of the Recommendation

This recommendation applies to the aeronautical field but may be extended to any other area. It concerns the design aspect of electronic equipment and the field of safety with a view to certification.

### 4 Comments on terminology

The definitions of a certain number of terms are not harmonized in the existing documents (standards, general documents, etc.), in particular with regard to those used in RG.Aéro 000 40A and in its support documents. The specific terminology of ED-80 and the clarifications provided in this chapter must be taken into account.

Specific Note for the english version : this version does not include terminology to clarify french translation of ED-80.

The comments applying to the ED-80 terminology are as follows:

#### 4.1 acceptance

#### 4.2 airworthiness

#### 4.3 analysis

#### 4.4 anomalous behavior

EUROCAE ED-79/SAE ARP 4754, *Certification Considerations for Highly Integrated or Complex Aircraft Systems*

CEI 61508, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

SAE ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

RE.Aéro 701 10A, *Principes de construction de la sécurité d'un produit missile ou spatial*

RE.Aéro 701 11A, *Guide des méthodes courantes d'analyse de la sécurité d'un produit missile ou spatial*

RE.Aéro 701 12A, *Guide d'élaboration des objectifs de sécurité d'un produit missile ou spatial*

RE.Aéro 703 05A, *Guide pour la maîtrise de la fiabilité*

RE.Aéro 703 06A, *Guide pour le pilotage de la croissance de fiabilité*

RG.Aéro 000 23B, *Management de Programme – Guide pour la mise en oeuvre des principes de la Gestion de la Configuration*

RG.Aéro 000 27, *Management de programme – Guide pour la maîtrise de la Sûreté de Fonctionnement*

RG.Aéro 000 33A, *Management de Programme – Logique de traitement des incidents*

RG.Aéro 000 40A, *Recommandation générale pour la Spécification de Management de Programme*

### 3 Domaine d'application de la Recommandation

Cette recommandation s'applique au domaine aéronautique et peut être étendue à tout autre domaine. Elle concerne les aspects de la conception des matériels électroniques et le domaine de la sécurité en vue de la certification.

### 4 Commentaires sur la terminologie

Les définitions d'un certain nombre de termes ne sont pas harmonisées dans les documents existants (normes, documents généraux, ...), en particulier vis-à-vis de celles utilisées dans la RG.Aéro 000 40A et dans ses documents d'accompagnement. Il est nécessaire de bien prendre en compte la terminologie spécifique de l'ED-80 et les précisions apportées par ce chapitre.

Les commentaires utilisés sur la terminologie de l'ED-80 sont les suivants :

#### 4.1

##### **acceptance**

correspond à la notion d'acceptation

#### 4.2

##### **airworthiness**

équivalent de navigabilité

#### 4.3

##### **analyse**

correspond à "analyse". Utilisé ou restreint à un procédé de justification

#### 4.4

##### **anomalous behavior**

comportement non conforme avec les exigences spécifiées

**4.5****approval**

approval in the broadest sense

RG.Aéro 000 40A definition is more restrictive: *Formal agreement allowing the use or application of a document.*

NOTE The approving authority commits its own responsibility on the document contents use.

**4.6****assessment****4.7****assumption****4.8****design assurance****4.9****process assurance**

corresponds to the concept of quality assurance

**4.10****availability**

aptitude of a product to be in a condition to perform a required function in given conditions, at a given time or for a given period, assuming that the necessary maintenance resources are supplied [availability according to X 60-500]

**4.11****certification****4.12****component****4.13****configuration**

use RG.Aéro 000 23B as a means of comparison with the various ED-80 definitions concerning configuration.

**4.14****conformity****4.15****derived requirement****4.16****failure**

the definition is consistent with the usual meaning of "défaillance", the second sentence is typically "software"

**4.17****failure condition**

**4.5****approval**

approbation au sens très général

La définition de la RG.Aéro 000 40A est plus restrictive : *Accord formel permettant l'utilisation ou l'application d'un document.*

NOTE L'autorité qui approuve engage sa propre responsabilité sur l'utilisation du contenu du document.

**4.6****assessment**

évaluation basée sur des travaux d'ingénierie (justification)

**4.7****assumption**

hypothèse

**4.8****assurance conception**

dans ce document, l'assurance conception concerne le traitement des erreurs de conception

**4.9****assurance processus**

correspond à la notion d'assurance qualité

**4.10****availability**

aptitude d'un produit à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens de maintenance nécessaires soit assurée [disponibilité selon X 60-500]

**4.11****certification**

identique à "certification"

**4.12****component**

ce terme est pris dans son acception anglo-saxonne, c'est-à-dire plus large que son acception française qui est "composant"

**4.13****configuration**

utiliser la RG.Aéro 000 23B en tant qu'élément de comparaison avec les différentes définitions de l'ED-80 concernant la configuration

**4.14****conformity**

se traduit par "conformité" qui lui-même est traduit également en anglais par "compliance" et "conformance"

La "conformity" est déclarée sur la base de la "compliance" du produit et la "conformance" du processus.

**4.15****derived requirement**

exigence dérivée

exigence complémentaire résultant des processus de conception du matériel qui peut ne pas être directement tracée vers les exigences de niveau plus élevé

**4.16****failure**

la définition est cohérente avec celle de "défaillance", hormis la deuxième phrase qui est typiquement "logiciel"

**4.17****failure condition**

cas de défaillance/condition de panne : effet d'une ou plusieurs défaillance sur l'aéronef et sur ses occupants

**4.18  
failure effect****4.19  
firmware****4.20  
implementation**

equipment implementation is taken to mean the conversion of system requirements allocated to the hardware into one or more hardware items.

**4.21  
inspection****4.22  
item**

The term "item" does not appear in RG.Aéro 000 40A and its support documents. It is included in the notion of product.

**4.22.1  
simple hardware item****4.22.2  
complex hardware item**

the definition of the various levels of complexity is here based on the feasibility and on the level of difficulty in obtaining an acceptable check by deterministic means

**4.23  
prototype**  
the definition is limited to the product representative of the production definition**4.24  
release****4.25  
reliability defect****4.26  
validation**

**4.18****failure effect**

effet d'une défaillance

Conséquence d'une défaillance sur un article ou un système

**4.19****firmware microgiciels**

Le mot firmware n'est pas dans le glossaire de la CEI 61508 : le terme utilisé est « programmable electronic ». La définition donnée est : technologie basée sur l'informatique, pouvant comprendre du matériel, du logiciel, ainsi que les unités d'entrée et/ ou de sortie.

**EXEMPLES**

- Microprocesseurs
- Microcontrôleurs
- Automates programmables
- Circuits intégrés spécifiques à une application (ASIC)
- Automates logiques programmables (PLC)
- Autres appareils basés sur la technologie informatique.

**4.20****implementation**

par implémentation du matériel, il faut comprendre la transformation des exigences système allouées au matériel en un ou plusieurs articles matériels.

**4.21****inspection**

contrôle

**4.22****item**

article

Le terme "article" n'apparaît pas dans la RG.Aéro 000 40A et ses documents d'accompagnement. Il est inclus dans la notion de produit.

**4.22.1****simple hardware item**

article matériel simple

(par opposition à article complexe) : vérification acceptable par des moyens déterministes capables de garantir les performances fonctionnelles

**4.22.2****complex hardware item**

article complexe

la définition des 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

**4.23****prototype**

la définition est restreinte au produit représentatif de la définition série (appelé parfois prototype d'identification)

**4.24****release**

la traduction française de l'ED-80 (mise à disposition) est inappropriée

Cela signifie « Mise en gestion de configuration ».

**4.25****reliability defect**

ne concerne que les défauts qui amènent au non-respect des exigences de fiabilité

**4.26****validation**

terme restreint à la validation des exigences en terme d'exhaustivité et d'exactitude

Selon l'ED-80 : Processus de détermination de la complétude et de l'exactitude des exigences.

## 4.27 verification

NOTE In chapter 11, the term "qualification" is used.

# 5 General presentation of ED-80

## 5.1 Objective and purpose

ED-80 gives recommendations for the design assurance of airborne electronic equipment so that it will reliably carry out the expected functions according to the design errors in the specified environments, with a view to certification (possibly non-civil aeronautics).

## 5.2 Scope

The scope concerned by the ED-80 is aeronautical, for which the FAR and CS regulations apply. The ED-80 is generally considered by the authorities (FAA and EASA) to be an acceptable means of conformity with the applicable certification requirements.

During negotiation of the applicable regulations with the Authority, it may decide to issue additional requirements (via a CRI: Certification Review Item for example) for the purposes of clarification, addition or exemption.

Nonetheless, for other fields, programmes could require the use of ED-80. In this case, a certain number of topics would have to be adjusted, in particular the notion of certification, with specification of the criticality of the system covered by the programme. These adjustments and specifications must be agreed by the customer and the supplier.

ED-80 concerns airborne electronic equipment, from design up to certification, including post-certification developments.

The following are primarily concerned:

- Line Replaceable Units (LRU);
- printed circuit boards;
- customisable microcoded components such as Application Specific Integrated Circuits (ASICs), Programmable Logic Devices (PLDs), including all associated macro-functions;
- integrated technology components such as hybrid circuits and multi-chip modules;
- commercial off-the-shelf articles (COTS).

ED-80 explicitly requests a decision on whether firmware is to be dealt with via ED-80 or ED-12.

The functions to be involved in application of the document and the corresponding responses, both from the customer and the supplier sides, are:

- Quality assurance,
- certification,
- RAMS,

which means that right from the outset, these three entities must have a clear distribution of responsibilities and the respective tasks.

## 5.3 How to use this document (extract from ED-80)

Figure 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.

#### 4.27

##### verification

comprendre "qualification"

Selon l'ED-80 : Évaluation de l'implémentation des exigences afin de déterminer si elles ont été satisfaites.

NOTE Au chapitre 11 est utilisé le terme "qualification".

## 5 Présentation générale de l'ED-80

### 5.1 Objectif et but

L'ED-80 fournit des recommandations pour l'assurance conception du matériel électronique de bord, de telle sorte que celui-ci exécute de manière sûre les fonctions attendues au regard des erreurs de conception dans les environnements spécifiés, en vue de la certification (le cas échéant hors aéronautique civile).

### 5.2 Domaine d'application

Le domaine concerné par l'ED-80 est le domaine aéronautique pour lesquels les règlements FAR et CS sont applicables. L'ED-80 est généralement considéré par les Autorités (FAA et EASA) comme un moyen de conformité acceptable, aux exigences de certification applicables.

Lors des négociations des règlements applicables avec l'Autorité, celle-ci peut décider d'éditer des exigences complémentaires (via un CRI : Certification Review Item par exemple) pour clarifier, ajouter ou exempter.

Néanmoins, pour d'autres domaines, des programmes pourraient exiger l'ED-80. Dans ce cas il conviendra de moduler un certain nombre de thèmes dont en particulier la notion de certification et de préciser la criticité du système objet du programme. Ces modulations et précisions doivent faire l'objet d'accords entre le client et le fournisseur.

L'ED-80 s'adresse au matériel électronique de bord des aéronefs, de la conception jusqu'à la certification, y compris les évolutions post-certification.

Sont principalement concernés :

- les Unités Remplaçables en Ligne (LRU) ;
- les assemblages sur cartes (cartes électroniques) ;
- les composants microcodés personnalisés tels que les Circuits Intégrés pour Applications Spécifiques (ASICs), les Composants Logiques Programmables (PLDs), y compris toutes les macro-fonctions associées ;
- les composants à technologie intégrée tels que les circuits hybrides et les modules multipuces ;
- les articles du Commerce sur Etagère (COTS).

L'ED-80 demande explicitement de décider si les microgiciels (firmware) doivent être traités à travers l'ED-80 ou l'ED-12.

Les fonctions qui doivent être impliquées dans l'application du document et les réponses à lui apporter, tant du côté client que du côté fournisseur, sont :

- l'assurance Qualité,
- la certification,
- la Sûreté de Fonctionnement,

ce qui implique que ces trois entités, dès les premières phases, aient défini une répartition claire des responsabilités et des tâches respectives.

### 5.3 Modalités d'utilisation du document (extrait de l'ED-80)

La Figure 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.

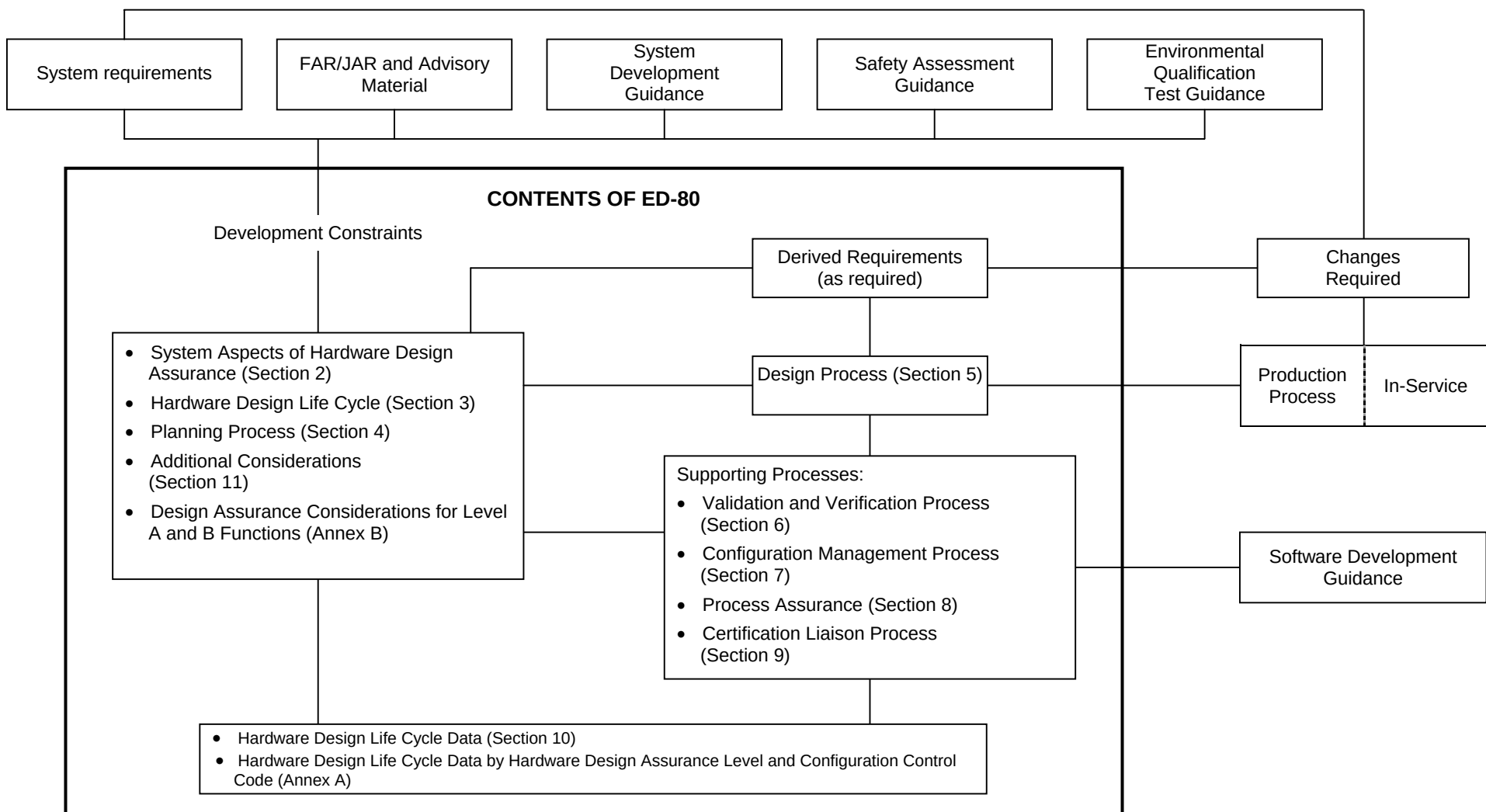


Figure 1 – Document overview

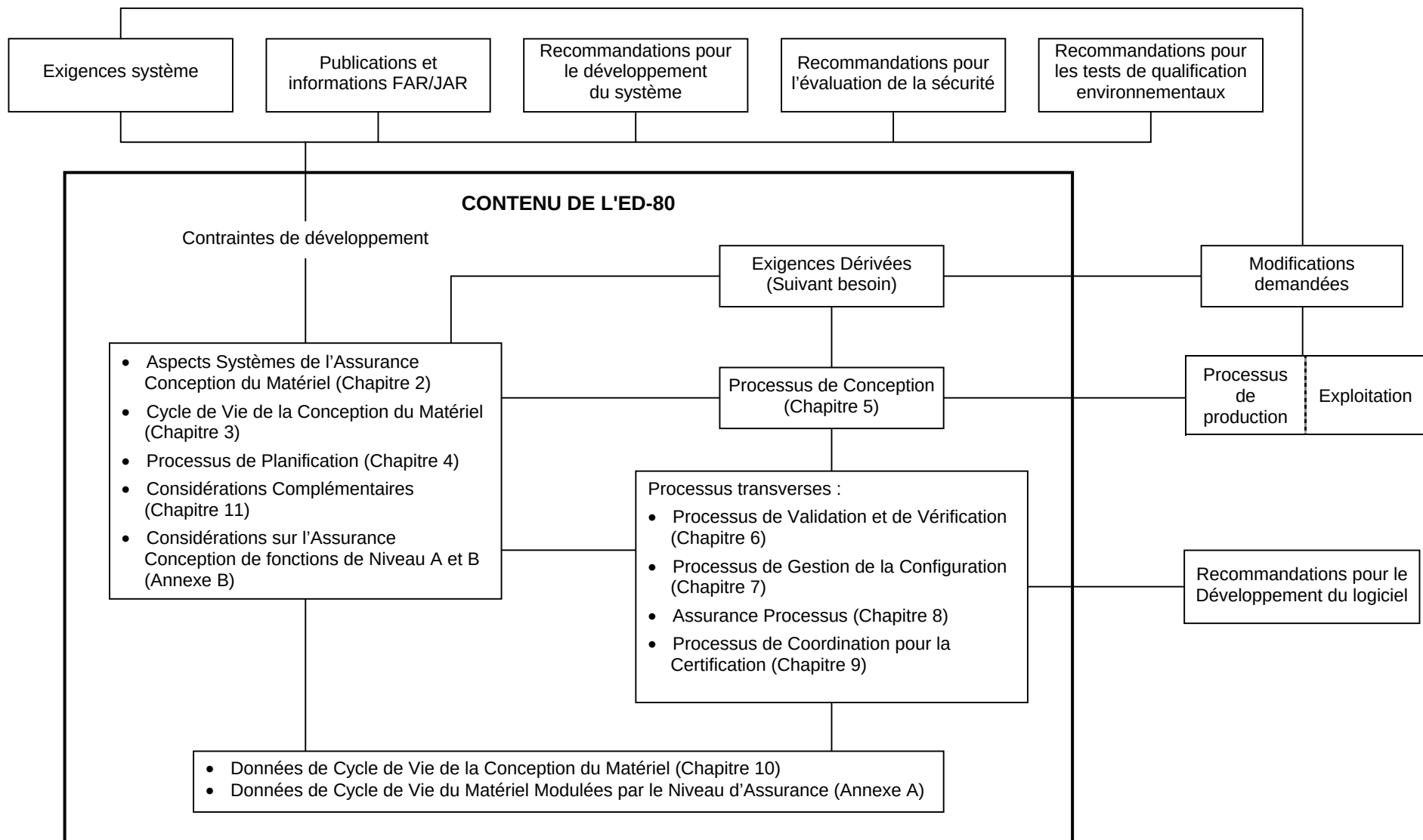


Figure 1 – Vue générale du document

## 6 Links/consistency with other documents

Figure 2 presents the interactions between documents in the aeronautical baseline.

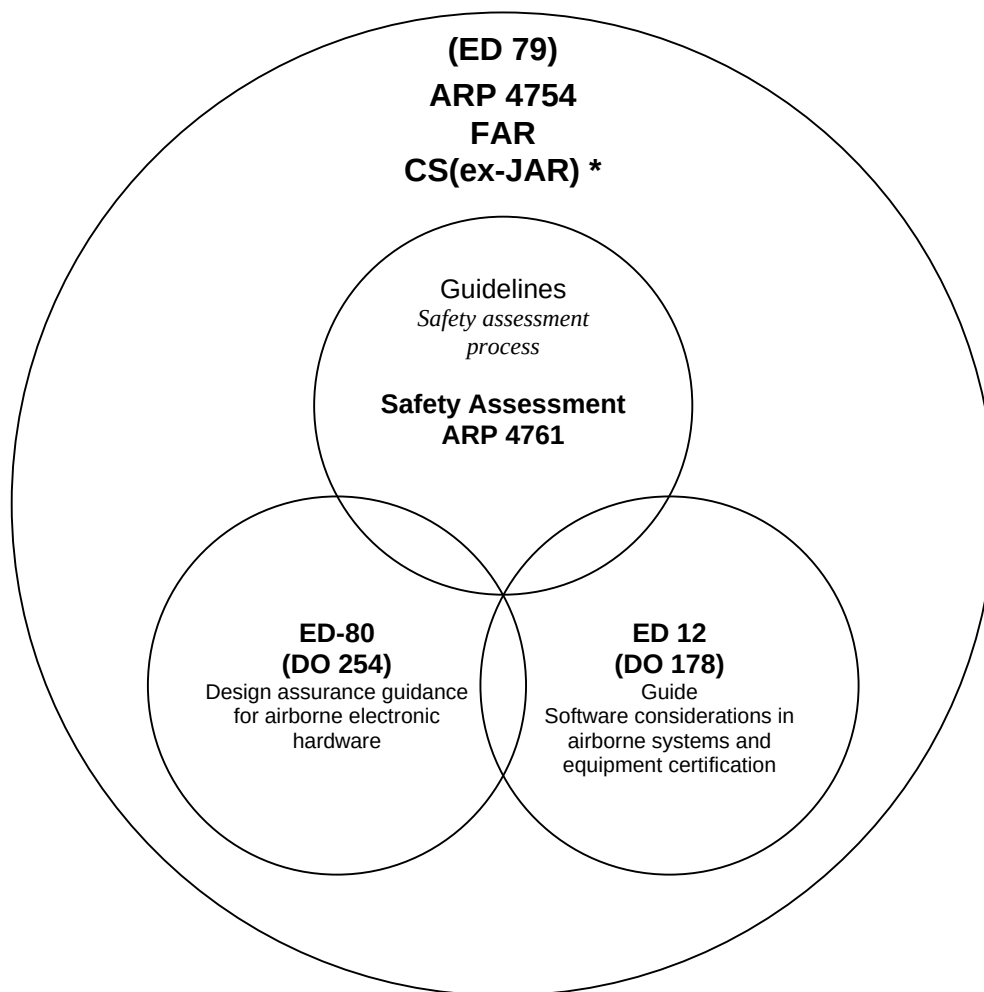


**Figure 2**

**\* The term JAR is today replaced by: Certification Specifications (CS)**

The FAR and CS are applicable regulations while the ARP are simply recommendations.

### 6.1 Links/consistency with IEC 61508

IEC 61508 could constitute an alternative as envisaged in paragraph 1.7 of ED-80, although IEC 61508 is not currently recognized by the civil aviation certification authorities. Caution! certification of a given programme by an authority using IEC 61508 in no way implies that it will be accepted by another civil aviation authority.

The scope of application of IEC 61508 corresponds to all the scopes of application of ED-80 (hardware part), ED-12 (software part) and ED-79 (system part).

This paragraph underlines the common aspects and the differences between IEC 61508 and ED-80.

## 6 Liaisons/cohérence avec autres documents

La Figure 2 présente les interactions entre documents dans le référentiel aéronautique.

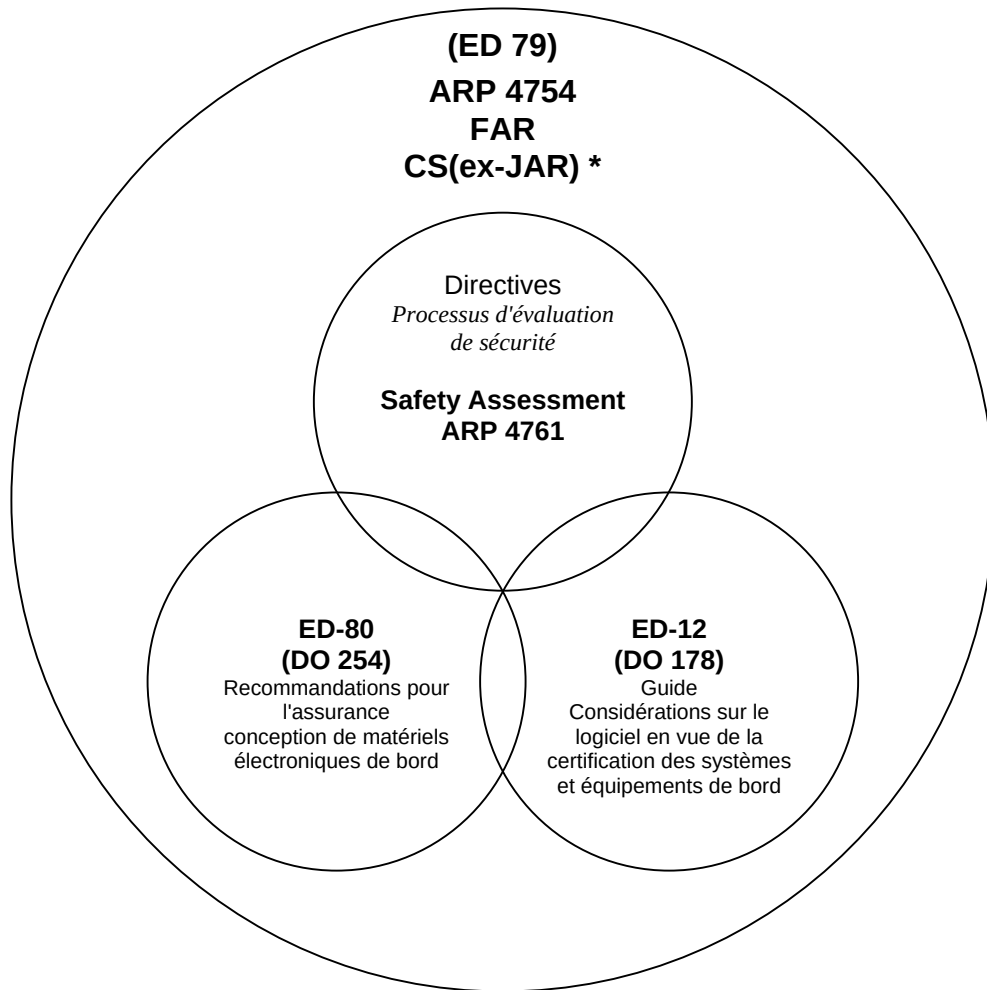


**Figure 2**

**\* Le terme JAR est aujourd'hui remplacé par : Certification Specifications (CS)**

Les FAR et CS sont des règlements applicables alors que les ARP sont des recommandations.

### 6.1 Liaisons/cohérence avec CEI 61508

La CEI 61508 peut constituer une alternative telle qu'envisagée dans le paragraphe 1.7 de l'ED-80, sachant que la CEI 61508 n'est pas actuellement reconnue par les autorités de certification de l'aéronautique civile. Attention ! Une certification sur un programme donné par une autorité selon la CEI 61508 ne préjuge pas de son acceptation par une autre autorité de l'aéronautique civile.

Le domaine d'application de la CEI 61508 correspond à l'ensemble des domaines d'application de l'ED-80 (partie matérielle), l'ED-12 (partie logiciel) et l'ED-79 (partie système).

Ce paragraphe souligne les points communs et les différences entre la CEI 61508 et l'ED-80.

### 6.1.1 Presentation of documents

#### 6.1.1.1 ED-80

ED-80 is:

- a recommendation document for use by companies designing electronic hardware performing mission-critical functions in an aircraft, in order to prepare for certification.
- a document recognised by the certification authorities.

ED-80 is a guide for developing electronic hardware in a specific environment so that it safely performs the functions for which it is intended.

ED-80 describes the activities to be systematically performed in order to meet the safety objectives linked to the design of the electronic hardware.

ED-80 models electronic hardware development in the form of processes:

- "Planning" process: to define electronic hardware development organisation documents,
- "Hardware design" process: for development of electronic hardware (this process itself being broken down into sub-processes),
- "Verification and Validation" process,
- "Configuration management" process,
- "Quality Assurance" process,
- "Communication with the certification authorities" process.

Standard ED-80 requires that initiation of each process be subject to compliance with transition criteria. These criteria must be commensurate with the risk linked to initiation of this process with incomplete, ambiguous or incorrect input data, or the risk linked to the use of resources which do not meet the process objectives in full.

Standard ED-80 defines typical documents to be produced during the processes and for each document, the data it contains.

Standard ED-80 gives suggestions for adapting the process used in development of the electronic equipment to the criticality of this equipment.

Standard ED-80 is organised in the following way:

- For each process involved in the design of the electronic equipment, define this process's safety objectives.
- Provide information so that the activities of each process can attain the process safety objectives defined by ED-80.
- Define the means for demonstrating conformity, so that for each process, compliance with the safety objectives allocated to each process by ED-80 can be assessed.

#### 6.1.1.2 IEC 61508

IEC 61508 is a functional safety standard dedicated to management of automated safety systems.

This standard, combining hardware, software and system, applies to the specification, development, production, operation and maintenance of automated safety systems by managing risks throughout the lifecycle. It uses the SIL (Safety Integrity Level) concept.

### 6.1.2 Comparison

#### 6.1.2.1 Common points

The two standards cover the **safety of electronic equipment**.

Both propose a breakdown of activities by lifecycle (called process breakdown in ED-80)



## 6.1.1 Présentation des documents

### 6.1.1.1 ED-80

L'ED-80 est :

- Un document de recommandation à l'usage des entreprises qui conçoivent du matériel électronique réalisant des fonctions critiques d'un aéronef dans le but de préparer la certification.
- Un document reconnu par les autorités de certification.

L'ED-80 est un guide pour développer, dans un environnement spécifié, du matériel électronique qui satisfasse de façon sécuritaire les fonctions pour lesquelles il est prévu.

L'ED-80 décrit les activités qui doivent être réalisées systématiquement pour satisfaire les objectifs de sécurité liés à la conception de matériel électronique.

L'ED-80 modélise le développement de matériel électronique sous forme de processus :

- Processus « Planification » : pour définir les documents d'organisation d'un développement de matériel électronique,
- Processus « Conception du matériel » : pour développer un matériel électronique (ce processus est lui-même décomposé en sous-processus),
- Processus « Vérification et Validation »,
- Processus « Gestion de la Configuration »,
- Processus « Assurance de la Qualité »,
- Processus « Communication avec les autorités de certification ».

La norme ED-80 demande que l'engagement de chaque processus soit soumis au respect de critères de transition. Ces critères doivent être en relation avec le risque lié à l'engagement de ce processus avec des données d'entrée incomplètes, ambiguës ou incorrectes ou le risque lié à l'utilisation de moyens ne répondant pas totalement aux objectifs du processus.

La norme ED-80 définit des documents types à produire au cours des processus et pour chacun de ces documents les données contenues dans ce document.

La norme ED-80 donne des indications pour adapter les processus participant au développement du matériel électronique en fonction de la criticité de ce matériel.

La norme ED-80 est organisée suivant le schéma ci-après :

- Définir, pour chaque processus intervenant dans la conception du matériel électronique, les objectifs de sécurité de ce processus.
- Fournir des indications pour que les activités de chaque processus permettent d'atteindre les objectifs de sécurité du processus définis par l'ED-80.
- Définir les moyens de démonstration de conformité qui permettent d'évaluer pour chaque processus, la satisfaction des objectifs de sécurité alloués par l'ED-80 à chaque processus.

### 6.1.1.2 CEI 61508

La CEI 61508 est une norme de sécurité fonctionnelle dédiée au management des systèmes automatisés de sécurité.

Cette norme, combinant matériel, logiciel et système, s'applique à la spécification, au développement, à la réalisation, à l'exploitation, et au maintien des automatismes de sécurité en maîtrisant les risques durant tout le cycle de vie. Elle utilise le Concept de SIL (Safety Integrity Level): Niveau d'intégrité de sécurité.

## 6.1.2 Comparaison

### 6.1.2.1 Points communs

Les deux normes traitent de la **sécurité du matériel électronique**.

Toutes deux proposent un découpage des activités par cycle de vie (appelé découpage par processus dans l'ED-80).

### 6.1.2.2 Differences

| ED-80                                                                                                                                                                                                                                                                                                                                                                                                             | IEC 61508                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain coverage: civil aviation</b><br>Electronic system<br>Hardware<br>Safety                                                                                                                                                                                                                                                                                                                                 | <b>Domain coverage: all activity sectors</b><br>Electrical/electronic/programmable electronic systems:<br>- Hardware<br>- Software<br>- Safety                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Objectives</b><br>To guarantee that any hardware design errors are dealt with consistently and verifiably during the design and certification process.                                                                                                                                                                                                                                                         | <b>Objectives</b><br>The objectives of standard IEC 61508 target the "Satisfaction of the safety requirements with respect to the required SIL".<br>The choice of SIL level is the responsibility of the industrial firm or is formalised in an application document per activity sector.                                                                                                                                                                                                                                                                                                    |
| <b>Processes</b><br>ED-80 presents the development of aeronautical equipment with designed-in safety in the form of processes:<br>- Planning,<br>- Hardware design (requirements capture, conceptual then detailed design, implementation & production transition),<br>- Verification and Validation,<br>- Configuration management,<br>- Quality Assurance,<br>- Communication with the certification authority. | <b>Lifecycle</b><br>The standard presents the development of electronic equipment (Hardware and software) in the form of lifecycle:<br>- Specification,<br>- Realisation,<br>- Installation/Commissioning,<br>- Operation and maintenance,<br>- Disposal.                                                                                                                                                                                                                                                                                                                                    |
| <b>Central concept</b><br>The ED-80 guide is a reference recommendation for qualification of electronic hardware, which will be integrated into certification of an aircraft, engine, etc., in other words an aeronautical system, with a view to type certification (and thus airworthiness).<br>This ED-80 guide also applies to systems which do not require certification.                                    | <b>Central concept</b><br>The standard postulates that the effects of random failures (failures which can occur at random moments and which result from equipment internal deterioration mechanisms) must be forecast quantitatively, using the normal RAMS methods, via an availability calculation.<br>It also postulates that there is no point in quantifying malfunctions linked to systematic failures (failures which occur with a particular combination of inputs in a given phase), as these must be avoided through organisational measures, or controlled by technical measures. |
| <b>Principle</b><br>ED-80 stresses the need for each process to define transitional criteria which determine initiation.<br>These transitional criteria are defined at the beginning of each phase.<br>They are checked or validated at the end of each process.                                                                                                                                                  | <b>Principle</b><br>The purpose of checking each lifecycle phase is to demonstrate that the output data in all respects meet the objectives and specific requirements of this phase.<br>The verification plan must be drawn up in parallel with development of this phase.                                                                                                                                                                                                                                                                                                                   |

## 6.1.2.2 Écarts

| ED-80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | CEI 61508                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domaine de couverture : aéronautique civile</b><br>Système électronique<br>Matériel<br>Sécurité                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Domaine de couverture : tous secteurs d'activités</b><br>Système électrique/électronique/électronique programmable :<br>- Matériel<br>- Logiciel<br>- Sécurité                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Objectifs</b><br>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.                                                                                                                                                                                                                                                                                                                 | <b>Objectifs</b><br>Les objectifs de la norme CEI 61508 visent la « Satisfaction des exigences de sécurité par rapport au SIL requis ».<br>Le choix du niveau SIL est de la responsabilité de l'industriel ou est formalisé dans un document d'application par secteur d'activité.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Processus</b><br>L'ED-80 présente le développement de matériels aéronautiques sûrs de conception sous forme de processus : <ul style="list-style-type: none"> <li>- Planification,</li> <li>- Conception du matériel (recueil des exigences, Conception générale puis détaillée, implémentation &amp; Transition vers la production),</li> <li>- Vérification et Validation,</li> <li>- Gestion de Configuration,</li> <li>- Assurance qualité,</li> <li>- Communication avec les autorités de certification.</li> </ul> | <b>Cycle de vie</b><br>La norme présente le développement de matériels électroniques (Matériel et Logiciel) sous forme de cycle de vie : <ul style="list-style-type: none"> <li>- Spécification,</li> <li>- Réalisation,</li> <li>- Installation / Démarrage,</li> <li>- Exploitation et maintenance,</li> <li>- Démantèlement.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Concept central</b><br>Le guide ED-80 est une recommandation de référence pour la qualification d'un matériel électronique, lequel sera intégré à la certification d'un avion, moteur ..., c'est à dire un système aéronautique en vue d'être certifié pour obtenir un certificat de type (et donc la navigabilité).<br>Ce guide ED-80 est également applicable pour des systèmes ne nécessitant pas de certification.                                                                                                   | <b>Concept central</b><br>La norme postule que les effets des défaillances aléatoires (défaillances se produisant à des instants aléatoires et résultant de mécanismes de dégradations internes du matériel) doivent être évalués prévisionnellement de manière quantitative, selon les méthodes habituelles de la sûreté de fonctionnement, par un calcul de disponibilité.<br>Elle postule également qu'il est inutile de quantifier les dysfonctionnements liés aux défaillances systématiques (défaillances se produisant à partir d'une combinaison particulière d'entrées survenant dans une phase quelconque), ceux-ci devant être évités, par des mesures organisationnelles, ou maîtrisés, par des mesures techniques. |
| <b>Principe</b><br>L'ED-80 met l'accent sur la nécessité de définir pour chaque processus des critères de transitions qui en conditionnent le démarrage.<br>Ces critères de transitions sont définis au début de chaque phase.<br>Ils sont vérifiés ou validés à la fin de chaque processus.                                                                                                                                                                                                                                | <b>Principe</b><br>La vérification de chaque phase du cycle de vie a pour but de démontrer que les données de sortie remplissent à tous les égards les objectifs et prescriptions spécifiques pour cette phase.<br>Le plan de vérification doit être établi en parallèle avec le développement de cette phase.                                                                                                                                                                                                                                                                                                                                                                                                                  |

### 6.1.3 Conclusion

#### **ED-80 is used when:**

One wishes to certificate electronic hardware to obtain an airworthiness certificate for an aircraft or engine (for software use ED-12 and for a system use ED-79).

#### **Standard IEC 61508 is used when:**

One wishes to demonstrate the level of safety of an electrical/electronic/programmable electronic system by using a multisectorial international standard.

## 6.2 Links/consistency with RAMS documents described in RG.Aéro 000 40A and its support documents

ED-80 comprises one purely Safety part (methods, tools, etc.) and one Quality Assurance and configuration management part. Chapter 8 of this document whenever necessary refers in detail to the RAMS good practices described in RG.Aéro 000 40A and its support documents. With regard to the other aspects (Quality assurance, configuration management, etc.), this document simply refers to RG.Aéro 000 40A.

## 7 Comprehension/recommendations per ED-80 chapter

### 7.1 Introduction

The French translation of ED-80 is sufficient for familiarisation purposes, however in a contractual context, we recommend using the English version.

| Section ED-80               | Definition of the text, with any proposed interpretations as necessary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Additional explanations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b><br><b>1.1, 1.2</b> | <p><u>Subject, scope, purpose</u></p> <p>Scope considered: National civil aviation,<br/>Subject: <u>Safety</u> and certification</p> <p>Risk source: Design errors<br/>"Hardware item" is the generic term used to describe the electronic hardware which is the subject of this document:</p> <ul style="list-style-type: none"> <li>• Line Replaceable Units (LRUs).</li> <li>• Circuit Board Assemblies.</li> <li>• Micro-coded components (ASICs, PLDs, FPGA, ...)</li> <li>• Integrated technology components (hybrids and multi-chips modules, ...)</li> <li>• COTS.</li> <li>• Non-exhaustive list</li> </ul> <p>Type of requirements breakdown: from system to hardware items (top-down)</p> | <p>The French version uses the term security, but we are in fact talking about safety.</p> <p>A new term is used in this recommendation, "Design assurance". It should be understood as a set of planned and systematic actions used to justify - with a sufficient level of confidence - that design errors have been identified and corrected, so that the hardware meets the certification requirements.</p> <p>This document only deals with the hardware design aspects linked to airworthiness. It only gives recommendations for implementing system functions allocated to the hardware.</p> |
| <b>1.3, 1.4</b>             | <p><u>Documents</u></p> <ul style="list-style-type: none"> <li>- EUROCAE ED-79/SAE ARP4754</li> <li>- SAE ARP 4761</li> <li>- EUROCAE ED-12B/RTCA DO-178B</li> <li>- EUROCAE ED-14D/RTCA DO-160D</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <p>See relations with chapter 6 of this document.</p> <p>The French version translates "rule" by the word "standard".</p> <p>The word "rule" only concerns those which are to be applied to the project:</p> <ul style="list-style-type: none"> <li>• Requirements rules</li> <li>• Equipment design rules</li> <li>• Verification and validation rules</li> <li>• Equipment archiving rules</li> </ul>                                                                                                                                                                                              |

continued