

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Process management for avionics – Counterfeit prevention –
Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic
components**

**Gestion des processus pour l'avionique – Prévention de la contrefaçon –
Partie 1: Prévention de l'utilisation de composants électroniques contrefaits,
frauduleux et recyclés**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2019 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Process management for avionics – Counterfeit prevention –
Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic
components**

**Gestion des processus pour l'avionique – Prévention de la contrefaçon –
Partie 1: Prévention de l'utilisation de composants électroniques contrefaits,
frauduleux et recyclés**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.50; 31.020; 49.060

ISBN 978-2-8322-7249-7

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	6
1 Scope.....	8
2 Normative references	8
3 Terms, definitions and abbreviated terms	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms.....	13
4 Technical requirements	15
4.1 General.....	15
4.2 Minimum avionics OEM requirements	16
4.3 Intellectual property	19
4.3.1 General	19
4.3.2 Definition of intellectual property.....	20
4.4 Counterfeit consideration	20
4.4.1 General	20
4.4.2 Legal definition of counterfeit.....	21
4.4.3 Fraudulent components	21
4.4.4 How to establish traceability	21
4.4.5 Reasons for the loss of component traceability	22
4.5 The counterfeit problem	22
4.5.1 General	22
4.5.2 General worldwide activities combating counterfeit issues	23
4.5.3 Cultural differences	23
4.5.4 Counterfeiting activities and avionics equipment.....	23
4.5.5 Electronic components direct action groups	26
4.6 Recycled components	26
4.6.1 General	26
4.6.2 Why the avionics industry does not use recycled components	27
4.6.3 How recycled components become suspect and potentially fraudulent.....	27
4.7 Original component manufacturer (OCM) anti-counterfeit guidelines	27
4.7.1 General.....	27
4.7.2 Chinese Reliable Electronic Component Supplier (RECS) audit scheme	28
4.7.3 Original component manufacturer (OCM) ISO 9001 and AS/EN/JISQ 9100 Third Party Certification	28
4.7.4 Original component manufacturer's (OCM) trademarks	28
4.7.5 Original component manufacturer's (OCM) IP control.....	28
4.7.6 Original component manufacturer's (OCM) physical part marking and packaging marking.....	28
4.7.7 The Semiconductor Industries Association Anti Counterfeit Task Force (ACTF)	29
4.7.8 USA Trusted Foundry Program	29
4.7.9 USA Trusted IC Supplier Accreditation Program	30
4.7.10 Physical unclonable function (PUF)	30
4.7.11 Original component manufacturer (OCM) best practice	30
4.8 Distributor minimum accreditations	30
4.9 Distributor AS/EN/JISQ 9120 Third Party Certification.....	31
4.10 Franchised distributor network	31
4.10.1 General	31

4.10.2	SAE AS6496.....	32
4.10.3	Control stock through tracking schemes	32
4.10.4	Control of scrap	33
4.10.5	RECS	33
4.11	Non-franchised distributor anti-counterfeit guidelines	33
4.11.1	General	33
4.11.2	CCAP-101 certified program for independent distributor	33
4.11.3	SAE AS6081.....	33
4.11.4	OEM managed non-franchised distributors	34
4.11.5	Brokers.....	34
4.12	Avionics OEM anti-counterfeit guidelines when procuring components.....	34
4.12.1	Anti-counterfeiting general approach	34
4.12.2	Buy from approved sources	34
4.12.3	Traceable components	34
4.12.4	Certificate of conformance and packing slip.....	35
4.12.5	Plan and buy sufficient quantities	36
4.12.6	Use of non- franchised distributors	36
4.12.7	Brokers.....	36
4.12.8	Contact the original manufacturer	37
4.12.9	Obsolete components and franchised aftermarket sources	37
4.12.10	IEC 62239-1 approved alternatives	37
4.12.11	Product redesign	37
4.12.12	Non traceable components	38
4.12.13	OEM anti-counterfeit plans including SAE AS5553 and SAE AS6174.....	38
4.13	OEM anti-counterfeit guidelines for their products	43
4.13.1	IP control.....	43
4.13.2	Tamper-proofing the OEM design	43
4.13.3	Tamper-proof labels.....	43
4.13.4	Use of ASICs and FPGAs with IP protection features.....	43
4.13.5	Control the final OEM product marking	44
4.13.6	Control OEM scrap	44
4.13.7	OEM trademarks and logos.....	44
4.13.8	Control delivery of OEM products and spares and their useful life.....	44
4.13.9	MRO activities	45
4.14	Counterfeit, fraud and component recycling reporting	46
4.14.1	General	46
4.14.2	USA FAA suspected unapproved parts (SUP) program	46
4.14.3	EASA.....	46
4.14.4	UK counterfeit reporting.....	46
4.14.5	EU counterfeit reporting.....	46
4.14.6	UKEA anti-counterfeiting forum.....	46
4.15	Anti-counterfeit awareness training	46
4.16	Information to support the management of the supply chain.....	47
Annex A	(informative) Useful contacts	48
A.1	World Intellectual Property Organization (WIPO).....	48
A.1.1	General	48
A.1.2	What is WIPO?	48
A.1.3	WIPO Intellectual Property Services	49
A.1.4	WIPO global network on Intellectual Property (IP) Academies.....	50

A.2	Anti-Counterfeiting Trade Agreement (ACTA).....	50
A.2.1	ACTA.....	50
A.2.2	Global Anti-Counterfeiting Network (GACG).....	51
A.3	World Semiconductor Council (WSC) and GAMS	51
A.4	SEMI.....	52
A.5	Electronics Authorized Directory	53
A.6	UK	53
A.6.1	The UK intellectual property office	53
A.6.2	Alliance for IP	54
A.6.3	UK Chartered Trading Standards Institute.....	54
A.6.4	UK HM Revenue and Customs.....	54
A.6.5	Anti-Counterfeiting Forum.....	54
A.6.6	Electronic Component Supplier Network (ESCN)	55
A.6.7	UK Ministry of Defence	55
A.7	Europe.....	55
A.7.1	Europa Summaries of EU Legislation.....	55
A.7.2	Europol, the European Law Enforcement Agency.....	55
A.7.3	European Patent Office	55
A.7.4	EUIPO	55
A.7.5	European Aviation Safety Agency (EASA).....	56
A.7.6	IECQ audit schemes	57
A.7.7	BEAMA.....	57
A.8	USA.....	57
A.8.1	United States Patent and Trademark Office	57
A.8.2	The International Trade Administration, US Department of Commerce.....	58
A.8.3	International Intellectual Property Alliance	58
A.8.4	The Federal Aviation Administration (FAA)	58
A.8.5	Trusted Access Program Office (TAPO).....	59
A.8.6	Independent Distributors of Electronics Association (IDEA)	59
A.8.7	ECIA formerly National Electronic Distributors Association (NEDA)	60
A.8.8	Components Technology Institute Inc. (CTI)	61
A.8.9	Defense Logistics Agency (DLA).....	61
A.8.10	DFARS	61
A.8.11	IAQG	62
A.8.12	USA Homeland Security	62
A.9	China.....	62
A.9.1	CNIPA.	62
A.9.2	Chinese Patent and Trademark Office	62
A.9.3	China Electronics Associations:.....	62
A.9.4	China Quality Certification Centre (CQC).....	62
A.9.5	Civil Aviation Administration of China (CAAC).....	62
A.9.6	China lawinfo.Co Ltd., for Law info China	62
A.10	Japan – Japanese Patent Office (JPO)	63
A.11	Physical unclonable function	63
A.12	PUF and tags initiative and solutions	64
A.12.1	The Hardware Intrinsic Security (HIS) initiative	64
A.12.2	Examples of tag providers	64
A.13	Examples of tamper-proof design companies	65
A.14	Examples of FPGA die serialization	65

A.15	Examples of NVRAM manufacturers	65
A.16	SAE G-19	65
A.17	iNEMI.....	69
A.18	OECD	69
A.19	ICC	69
A.20	Applied DNA Sciences	70
A.21	Safety Directors' Forum	70
A.22	'Stop fake bearings' video	70
A.23	Industrial company's online anti-counterfeit awareness training	70
A.24	Subscription based anti-counterfeit awareness training.....	70
A.25	USA Government anti-counterfeit publications and awareness training	70
A.26	IECQ WG6	71
A.27	Anti-counterfeiting videos.....	71
Annex B	(informative) Examples of aftermarket sources	72
B.1	Examples of franchised aftermarket sources	72
B.2	Examples of sources of franchised die which can be packaged.....	72
B.3	Examples of third party custom packaging houses which provide aftermarket solutions	72
B.4	Examples of emulated aftermarket providers.....	72
Annex C	(informative) Typical example of a RECS certificate.....	74
Annex D	(informative) Flowchart of IEC 62668-1 requirements	75
Annex E	(Informative) Typical use of anti-counterfeit standards in supply chains	77
Bibliography		83
Figure 1	– Suspect components perimeter	21
Figure D.1	– Flowchart of IEC 62668-1 requirements and their relationship to external standards.....	76
Figure E.1	– Available anti-counterfeit standards for supply chains.....	77
Figure E.2	– Overview of typical relationships for anti-counterfeit standards in an avionics supply chain.....	79
Figure E.3	– Overview of typical anti-counterfeit standards in an avionics OEM supply chain.....	80
Figure E.4	– IECQ OD 3702 traceability audit	81
Figure E.5	– Typical IECQ OD 3702 coverage in any supply chain.....	82
Table 1	– Anti-counterfeit awareness training guidelines.....	18
Table.2	– IEC 62668-1 requirements satisfied or not if OEM has an approved SAE AS5553A plan.....	39
Table.3	– IEC 62668-1 requirements satisfied or not if OEM has an approved SAE AS5553B plan.....	41

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROCESS MANAGEMENT FOR AVIONICS – COUNTERFEIT PREVENTION –

Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62668-1 has been prepared by IEC technical committee 107: Process management for avionics.

This first edition cancels and replaces the third edition of IEC TS 62668-1 published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) added a reference to AS/EN/JISQ 9100 and AS/EN/JISQ 9110 which contain anti-counterfeit requirements which may be used to satisfy the requirements of 4.2;
- b) added reference to USA DFAR rule 252.246.7008 and to UK Defence Standard 05-135;
- c) added reference to more GAO, OECD and ICC reports in 4.5.1;

- d) updated weblinks and other references;
- e) added new Annex E with figures describing how anti-counterfeit documents can be used in supply chains;
- f) added a reference to the new IECQ OD 3702 traceability audit;
- g) added new definition for re-manufactured components with a warning that these are not recommended.

The text of this International Standard is based on the following documents:

CDV	Report on voting
107/335/CDV	107/346A/RVC

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62668 series, published under the general title *Process management for avionics – Counterfeit prevention*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours, which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

PROCESS MANAGEMENT FOR AVIONICS – COUNTERFEIT PREVENTION –

Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components

1 Scope

This part of IEC 62668 defines requirements for avoiding the use of counterfeit, recycled and fraudulent components used in the aerospace, defence and high performance (ADHP) industries. It also defines requirements for ADHP industries to maintain their intellectual property (IP) for all of their products and services. The risks associated with purchasing components outside of franchised distributor networks are considered in IEC 62668-2. Although developed for the avionics industry, this document can be applied by other high performance and high reliability industries at their discretion.

NOTE IEC 62668 (all parts) does not address the restriction on the re-use of a component in maintenance, repair and overhaul (MRO) operations and only addresses MRO activities when they are under the OEM's responsibility.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62239-1, *Process management for avionics – Management plan – Part 1: Preparation and maintenance of an electronic components management plan*

IEC 62668-2, *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*

ISO 9001, *Quality management systems – Requirements*

AS/EN/JISQ 9100, *Quality Management Systems – Requirements for Aviation, Space and Defense Organizations*

AS/EN/JISQ 9110, *Quality Maintenance Systems – Aerospace – Requirements for Maintenance Organizations*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1

aftermarket source

reseller which may or may not be under contract with the original component manufacturer (OCM), or is sometimes a component “re-manufacturer”, under contract with the OCM

Note 1 to entry: The reseller accumulates inventories of encapsulated or non-encapsulated (wafer) components whose end of life date has been published by the OCM. These components are then resold at a profit to fill a need within the market for components that have become obsolete.

3.1.2

broker

individual or corporate organization that serves as an intermediary between buyer and seller

Note 1 to entry: In the electronic component sector a broker specifically seeks to supply obsolete or hard to find components in order to turn a profit. To do so it may accumulate an inventory of components considered to be of strategic value or may rely on inventories accumulated by others. The broker operates within a worldwide component exchange network.

3.1.3

COTS product

commercial off-the-shelf product

one or more components, assembled and developed for multiple commercial consumers, whose design and/or configuration is controlled by the manufacturer's specification or industry standard

Note 1 to entry: COTS products can include electronic components, subassemblies or assemblies, or top level assemblies. Electronic COTS subassemblies or assemblies include circuit card assemblies, power supplies, hard drives, and memory modules. Top-level COTS assemblies include a fully integrated rack of equipment such as raid arrays, file servers to individual switches, routers, personal computers, or similar equipment.

Note 2 to entry: This note applies to the French language only.

3.1.4

counterfeit, verb

action of simulating, reproducing or modifying a material good or its packaging without authorization

Note 1 to entry: It is the practice of producing products which are imitations or are fake goods or services. This activity infringes the intellectual property rights of the original manufacturer and is an illegal act. Counterfeiting generally relates to wilful trademark infringement.

3.1.5

counterfeited component

material good imitating or copying an authentic material good which may be covered by the protection of one or more registered or confidential intellectual property rights

Note 1 to entry: A counterfeited component is one whose identity or pedigree has been altered or misrepresented by its supplier.

Identity = original manufacturer, part number, date code, lot number, testing, inspection, documentation or warranty, etc.

Pedigree = origin, ownership history, storage, handling, physical condition, previous use, etc.

Note 2 to entry: When a material good has no registered or confidential intellectual property rights, then the material good has no intellectual property protection. Examples include situations where the original component manufacturer (OCM) has ceased to trade and has not sold or passed on the intellectual property rights to another entity.

3.1.6

customer device specification

device specification written by a user and agreed by the supplier

3.1.7 customer user

original equipment manufacturer (OEM) which purchases electronic components, including integrated circuits and/or semiconductor devices compliant with this document, and uses them to design, produce, and maintain systems

3.1.8 data sheet

document prepared by the manufacturer that describes the electrical, mechanical, and environmental characteristics of the component

3.1.9 franchised distributor or agent

individual or corporate organization that is legally independent from the franchiser (in this case the electronic component manufacturer or OCM) and agrees under contract to distribute products using the franchiser's name and sales network

Note 1 to entry: Distribution activities are carried out in accordance with standards set and controlled by the franchiser. Shipments against orders placed can be despatched either directly from the OCM or the franchised distributor or agent. In other words, the franchised distributor enters into contractual agreements with one or more electronic component manufacturers to distribute and sell the said components. Distribution agreements may be stipulated according to the following criteria: geographical area, type of clientele (avionics for example), maximum manufacturing lot size. Components sourced through this route are protected by the OCM's warranty and supplied with full traceability.

3.1.10 fraudulent component

electronic component produced or distributed either in violation of regional or local law or regulation, or with the intent to deceive the customer

Note 1 to entry: This includes but is not limited to the following which are examples of components which are fraudulently sold as new ones to a customer:

- 1) a stolen component;
- 2) a component scrapped by the original component manufacturer (OCM) or by any user;
- 3) a recycled component, that becomes a fraudulent recycled component when it is a disassembled (for example disassembled from a PCB assembly) component resold as a new component (see Figure 1), where typically there is evidence of prior use and rework (e.g. solder, re-plating or lead re-attachment activity) on the component package terminations;
- 4) a counterfeit component, a copy, an imitation, a full or partial substitute of brands;
- 5) fraudulent designs, models, patents, software or copyright sold as being new and authentic. For example: a component whose production and distribution are not controlled by the original manufacturer;
- 6) unlicensed copies of a design;
- 7) a disguised component (re-marking of the original manufacturer's name, reference date/code or other identifiers etc.), which may be a counterfeit component (see Figure 1);
- 8) a component without an internal silicon die or with a substituted silicon die which is not the original manufacturer's silicon die.

3.1.11 intellectual property

creations of the mind such as inventions, literary and artistic works, and symbols, names, images, and designs used in commerce

Note 1 to entry: This is property created through intellectual or creative activity.

Note 2 to entry: It includes patents, trademarks, copyright and designs. It can be owned, rented out, licensed, sold or given away.

**3.1.12
microcircuit
component
device**

electrical or electronic device that is not subject to disassembly without destruction or impairment of design use and is a small circuit having a high equivalent circuit element density which is considered as a single part composed of interconnected elements on or within a single substrate to perform an electronic circuit function

Note 1 to entry: This excludes printed wiring boards/printed circuit boards, circuit card assemblies and modules composed exclusively of discrete electronic components.

**3.1.13
MRO
maintenance, repair and overhaul**

operations, such as tests, measurements, replacements, adjustments, and repairs, intended to retain or restore a functional unit in or to a specified state in which the unit can perform its required functions

Note 1 to entry: This activity includes inspection, rebuilding, alteration and the supply of spare parts, accessories, raw materials, adhesives, sealants, coatings and consumables.

Note 2 to entry: This note applies to the French language only.

**3.1.14
non-franchised distributor
company which does not fall under a franchised distributor or OCM**

Note 1 to entry: These distributors may purchase components from component manufacturers, franchised distributors, or through other supply channels (open markets). These distributors cannot always provide the guarantees and support provided by the franchised distributor network; components sourced through this source are usually protected by the source's warranty only.

Note 2 to entry: Some non-franchised distributors are able to purchase traceable components from the OCM or their franchised distributors and to provide traceability paperwork and/or are able to return stock for investigation to the OCM. Such non-franchised distributors can satisfy the USA DFARS 252.246.7008 requirements (see A.8.10).

**3.1.15
OCM
original component manufacturer
company specifying and manufacturing the electronic component**

Note 1 to entry: This note applies to the French language only.

**3.1.16
OEM
original equipment manufacturer**

manufacturer which defines the electronic subassembly that includes the electronic components or defines the components used in an assembly and/or test specification

Note 1 to entry: This note applies to the French language only.

**3.1.17
piracy
willful copyright infringement****3.1.18
re-manufactured component
recycled element**

electronic component that includes a recycled silicon die or technology element as documented and disclosed by the electronic component re-manufacturer and that is fully tested before being sold

Note 1 to entry: Examples include a silicon or other die extracted from another electronic component, either new or used, which is externally marked and disclosed using the re-manufacturer's name, logo and different part number.

Note 2 to entry: Re-manufacturing an electronic component can necessitate the original engineering data and schematics of the product. This does not mean that a re-manufactured product is identical to the new product.

Note 3 to entry: Electronic re-manufactured components often come with warranties.

3.1.19 reseller

general supplier which offers a selection of electronic components to order from a catalog

3.1.20 recycled component

electrical component removed from its original product or assembly and available for reuse

Note 1 to entry: The component has authentic logos, trademarks and markings. However, it typically has no output to measure the useful life remaining for its reuse. A recycled component can fail earlier than a new one when re-assembled into another product or assembly. A recycled component may also be physically damaged or damaged through electro static discharge (ESD) during the removal process.

3.1.21 semiconductor

electronic component in which the characteristic distinguishing electronic conduction takes place within a semiconductor

Note 1 to entry: This includes semiconductor diodes which are semiconductor devices having two terminals and exhibiting a nonlinear voltage-current characteristic and transistors which are active semiconductor devices capable of providing power amplification and having three or more terminals.

3.1.22 subcontractor

manufacturer of electronic subassemblies or supplier manufacturing items in compliance with customer design data pack and drawings, and under the authority of the OEM

Note 1 to entry: This supplier can potentially procure all or part of the electronic components required to produce a subassembly and is often referred to as the contract electronic manufacturer (CEM) or electronics manufacturing services (EMS).

3.1.23 supplier

company which provides to another an electronic component which is identified by the logo or name marked on the device

Note 1 to entry: A supplier can be an OCM, a franchised distributor or agent, a non-franchised distributor, broker, reseller, OEM, CEM, and EMS, etc.

3.1.24 suspect component

electronic component which has lost supply chain traceability back to the original manufacturer and which may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent or counterfeit component

Note 1 to entry: Suspect components may include but are not limited to:

- 1) counterfeit components;
- 2) recycled components coming from uncontrolled recycling operations carried outside of the OEM, franchised network and OEM business where typically it has been fraudulently sold to the OEM as being in a new unused condition.

3.1.25 traceability

ability to have, for an electronic component, its full trace back to the original component manufacturer

Note 1 to entry: This traceability means that every supplier in the supply chain is prepared to legally declare in writing that they know and can identify their source of supply, which goes back to the original manufacturer and can confirm that the electronic components are brand new and were handled with appropriate ESD and MSL handling precautions. This authenticates that the electronic components being supplied are unused, brand new components with no ESD, MSL or other damage. This ensures that the electronic components are protected by any manufacturer's warranties, have all of their useful life remaining and function according to the manufacturer's published data sheet, exhibiting the expected component life in the application for the OEM's reliability predictions and product warranty.

3.1.26

untraceable

property of electronic components which have lost their traceability (see 3.1.25)

3.2 Abbreviated terms

AAIPT	Alliance Against IP Theft
ACTA	Anti-Counterfeit Trade Agreement
ACTF	Semiconductor Industries Association Anti Counterfeit Task Force
ADHP	aerospace, defence and high performance
ASIC	application specific integrated circuit
ATP	acceptance test procedure
BEAMA	British Electrotechnical Allied Manufacturers' Association
BoM	bill of materials
CAAC	Civil Aviation Administration of China
CATA	China Anti-counterfeit Technology Association
CB	certifying body (third party)
CNIPA	China National Intellectual Property Administration, PRC
COTS	commercial off-the-shelf
CofC	certificate of conformance
CEC	China Electronics Corporation
CECA	China Electronic Components Association
CEEI	China Electrical Equipment Association
CEM	contract electronic manufacturer
CESI	China Electronics Standardization Institute
CMM	component maintenance manuals
CQAE	China Quality Management Association for Electronics Industry
CMOS	complementary metal oxide semiconductor
DFARS	Defense Federal Acquisition Regulation System
DLF	direct line feed
DOD	Department of Defence (US)
DMEA	Defense MicroElectronics Activity
DMSMS	diminishing manufacturing sources and material shortages
DNA	deoxyribonucleic acid
DSCC	Defence Supply Centre Columbus
DLA	Defense Logistics Agency (former DSCC)
EASA	European Aviation Safety Agency
ECIA	Electronic Components Industry Association
ECMP	electronic component management plan
ECSN	electronic component supplier network

EMS	electronic manufacturing services
ERAI	Electronic Reseller Association International (see web-page http://www.eraf.com)
ESD	electrostatic discharge
ESIA	European Semiconductor Industries Association
EOS	electrical overstress
EU	European Union
EUIPO	European Union Intellectual Property Office
FAA	Federal Aviation Administration
FAR	Federal Avionic Regulations
FFF	form, fit and function
FIT	failures in time
FPD	flat panel display
FPGA	field-programmable gate array
FSC	Federal Supply Class
G-19	SAE Counterfeit Electronic Parts Committee
GAMS	Government/Authorities meeting on Semiconductors
GIFAS	French Aerospace Association
HAST	highly accelerated stress test
HIS	hardware intrinsic security
HTOL	high temperature operating life
IAQG	International Aerospace Quality Group – SAE
ICC	International Chamber of Commerce
ID	independent distributors
IDEA	Independent Distributors of Electronics Association
IEC	International Electrotechnical Commission
iNEMI	International Electronics Manufacturing Initiative
IP	intellectual property
IPR	intellectual property rights
ISP	internet service provider
ITAR	International Traffic in Arms Regulations
IUID	Item Unique Identification
JEDEC	Joint Electron Device Engineering Council
JIT	just in time
JPO	Japanese Patent Office
LED	light-emitting diode
LDC	lot data code
LTB	last time buy
MEMS	micro-electromechanical systems
MOD	Ministry of Defence, UK
MRO	maintenance, repair and overhaul (related to operations intended to retain or restore a functional unit)
MTBF	mean time between failure
MTTF	mean time to failure

MSL	moisture sensitivity level
NATO	North Atlantic Treaty Organization
NDAA	National Defense Acquisition Act
NEDA	National Electronics Distributors Association
NVRAM	non-volatile random access memory
OCM	original component manufacturer
OECD	Organisation for Economic Co-operation and Development
OEM	original equipment manufacturer
PCB	printed circuit board
PCN	product change notice
PQDR	product quality deficiency report
PRC	People's Republic of China
PV	photovoltaic
QTSL	Qualified Testing Suppliers List
RECS	Reliable Electronic Component Supplier
PUF	physical unclonable function
RFID	radio frequency identity detection
RAM	random access memory
ROM	read only memory
SAE	Society of automotive engineers
SEE	single event effect
SEU	single event upset
SER	soft error rate
SIA	Semiconductor Industry Association
SRAM	static random access memory
TAPO	Trusted Access Program Office
TSO	Trading Standards Officers
UK	United Kingdom
UKEA	UK Electronics Alliance
UNG	unique number generator
USA	United States of America
WIPO	World Intellectual Property Organization
WSC	World Semiconductor Council

4 Technical requirements

4.1 General

This document minimises counterfeiting, recycling and fraudulent activities by maintaining intellectual property and allowing the purchasing of traceable components.

Minimum avionics OEM requirements are defined in 4.2. This, in whole or in part, applies to MRO operations under the OEM's responsibility.

Subclauses 4.3 to 4.14.6 provide supporting information to 4.2.

Informative annexes are provided at the end of this document and their content is subject to change. Users of this document are encouraged to review the latest data available whenever referencing the content of these annexes.

- Annex A provides further cross-reference information for all the institutions and organizations discussed in Clause 4.
- Annex B provides examples of aftermarket sources which shall be considered in obsolescence situations (see 4.12.9).
- Annex C provides an example of a typical Chinese RECS certificate (see 4.7.2).
- Annex D provides a flowchart of IEC 62668-1 requirements and their relationship to external standards.
- Annex E provides typical examples of how to deploy anti-counterfeit standards in the supply chain.

The key elements to control and understand are:

- the definition of intellectual property (see 4.3);
- the limitations of the term counterfeit (see 4.4);
- the better description of “fraudulent components” (see 4.4.3);
- what recycling is and why the avionics industry minimises recycling to in-house activities only (see 4.6);
- the use of original component manufacturers (OCMs) which protect their intellectual property (see 4.7);
- the use of approved franchised distributors or sources (see 4.10);
- the use of risk management and component test processes when buying suspect untraceable components from non-franchised distributors in accordance with IEC 62668-2 (see 4.12.6);
- the protection of the OEM's intellectual property, throughout its product lifecycles including management of all spares;
- the reporting of violations of intellectual property through customer dialogue and local law enforcement (see 4.14, A.7.2, and Clause A.8 for useful contacts);
- the training of relevant employees (see 4.15);
- the use of obsolescence management (see 4.12.1) to mitigate the risk of buying counterfeit components.

4.2 Minimum avionics OEM requirements

The avionics OEMs shall:

- a) Protect their intellectual property rights (see 4.3, 4.4, 4.5, 4.12 and 4.13).
- b) Select components from original component manufacturers (OCMs) which control their intellectual property rights (see 4.3, 4.7) and which include unique configuration controlled part numbers and physical part markings (see 4.7.6), avoiding the use of re-manufactured components (see 3.1.18) wherever possible.
- c) Have an anti-counterfeit, fraudulent and recycled component process, in compliance with the requirements herein, which may include an anti-counterfeit management plan in accordance with this document and which can be based on plans such as SAE-AS5553A or SAE AS5553B or others similar (see 4.12.13). The OEMs shall flow this requirement down to lower level suppliers (see 4.12.13.3).

NOTE 1 Figures E.1, E.2, E.3, E.4 and E.5 can assist in the deployment of anti-counterfeit standards.

NOTE 2 AS/EN/JISQ 9100 and/or AS/EN/JISQ 9110 contain high level requirements for anti-counterfeit management for all types of electrical and mechanical components and materials and can be used to satisfy this need (see 4.7.3 and 4.12.1). Some documents such as IEC TS 62239-2 and SAE AS6174 (see 4.12.13) can also aid for anti-counterfeit management.

- d) Have a process (see 4.12) to audit all sources of supply of components.

NOTE 3 AS/EN/JISQ 9100 and/or AS/EN/JISQ 9110 can satisfy this requirement.

- e) Have a process only allowing the purchase of traceable components (see 4.4.4), as follows:

- 1) from the original component manufacturer (OCM) (see 4.7) with any appropriate traceability measures such as the use of Semiconductor Industries Association Anti Counterfeit Task Force (ACTF) measures (see 4.7.7) or physical unclonable function (PUF) features (see 4.7.10);
- 2) direct from the USA Trusted Foundry Program (see 4.7.8) and/or from the USA Trusted IC Supplier Accreditation Program (see 4.7.9) where required by customer contract or considered appropriate;
- 3) in situations where the component is obsolete, by purchasing directly from the franchised aftermarket manufacturer (see 4.12.9 and Annex B);
- 4) from franchised distributors (see 4.10)
 - which are preferably AS/EN/JISQ 9120 approved (see 4.9);
 - which are also ISO 9001 approved as a minimum requirement (see 4.8); or
 - which comply with SAE AS 6496 requirements (see Clause A.16);
 - from non-franchised distributors (see 4.11) using IEC 62668-2.

NOTE 4 SAE AS6171 can assist with the use of IEC 62668-2.

NOTE 5 Some tracking schemes (see 4.10.3) or tamper-proof initiatives can assist with traceability and authentication.

NOTE 6 AS/EN/JISQ 9100 and/or AS/EN/JISQ 9110 can satisfy the traceability requirements.

- f) Have a process which avoids the use of unapproved brokers (see 4.11.5).

NOTE 7 AS/EN/JISQ 9100 and/or AS/EN/JISQ 9110 can satisfy this requirement.

- g) In the rare event an avionics OEM considers it is necessary to purchase untraceable components:

- 1) conduct and document an exhaustive search for traceable alternatives, including the review of possible design changes to accommodate traceable alternatives and aftermarket sources (see 4.12, in particular 4.12.9, 4.12.10, 4.12.11, and Annex B);
- 2) use and document a risk management process to assess the additional requirements needed to determine that the components are not counterfeited, recycled or fraudulent components, using the requirements of IEC 62668-2. This risk management process will include conformity, quality, reliability and maintenance performances aspects.

NOTE 8 SAE AS6171 can satisfy the requirements of IEC 62668-2.

- h) Have a process for repair and rework operations (see 4.13.9) which shall include AS/EN/JISQ 9110 certification for all maintenance operation.
- i) Report incidents of counterfeit and fraudulent activities in accordance with local law (see 4.14) and customer requirements.
- j) Establish an anti-counterfeit awareness training for relevant personnel based on Table 1 which is provided for guidance and which identifies the relevant personnel and training records (see 4.15). In the case of newly hired personnel, initiate immediate training for the specific discipline or department.
- k) Have a process to verify that any components are not counterfeit or fraudulently recycled and meet the requirements as defined in the contract.

NOTE 9 AS/EN/JISQ 9100 and/or AS/EN/JISQ 9110 can satisfy this requirement.

NOTE 10 This also applies to returned components and surplus components purchased as a "buy back" scheme, for example when buying back surplus stock from a subcontractor or internal transfers.

- l) Have an obsolescence process to mitigate the instances of buying obsolete components.

NOTE 10 IEC 62239-1, IEC TS 62239-2, IEC 62402 or SAE STD016 can be used to satisfy this requirement.

- m) Apply in whole or in part, according to the application, the requirements listed in items a) to l) for their MRO operations, and/or have a process to cascade the applicable requirements and control their implementations if MRO operations are subcontracted to MRO organizations.

Table 1 – Anti-counterfeit awareness training guidelines

Discipline or department	Type of awareness training	Frequency	Comments
Sourcing, buying or procurement	Traceability in the supply chain, differences between brokers, the different types of distributor (franchised, non-franchised), the OCM etc. When to raise issues.	Every 2 years	Change frequency to annual if there is a new major change or development to be flowed down or if the department has a poor anti-counterfeit management record.
Subcontract procurement	How the subcontractors should control their supply chain for an avionics product, how changes are to be managed and approved by the OEM before implantation.	Every 2 years	
Hardware design	Why sourcing cannot be done directly off the internet; why approved suppliers are necessary; why franchised distributors are necessary, etc.	Every 2 years	
Program management	Why sourcing cannot be done directly off the internet, why approved suppliers are necessary, etc. How obsolescence management mitigates the risk to supply counterfeit components.	Every 2 years	
Component engineering	Type of testing which can be used to minimise the use of counterfeit components; how part numbers and non-conformances should be managed, etc. How obsolescence management mitigates risk to supply counterfeit components.	Every 2 years	
Goods receiving. Goods inwards Stock room Kitting, material kitting department	Why visual inspection is necessary and why attention to detail regarding part numbers, labelling, certificates of conformance and paperwork is necessary. How to raise concerns.	Every 2 years	
Supplier quality	How to audit for anti-counterfeit. Checklists, etc. Whom to discuss issues with and how to manage corrective actions.	Every 2 years	

Discipline or department	Type of awareness training	Frequency	Comments
Production assembly department	General awareness; how to report any concerns if part marking looks suspicious, etc. Review production test failure trends and investigate low yields which may be caused by counterfeit or fraudulent components.	Every 2 years	
Test department	General awareness for consideration of counterfeit to be included in fault analyses or fault findings.	Every 2 years	

4.3 Intellectual property

4.3.1 General

Anti-counterfeit activities start with the definition and knowledge of what intellectual property (IP) is. Counterfeit occurs when the original manufacturer's IP is fraudulently infringed. Therefore, anti-counterfeit activities are concerned about the maintenance of intellectual property.

The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations. It is dedicated to developing a balanced and accessible international IP system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest.

WIPO was established by the WIPO Convention in 1967 with a mandate from its Member States to promote the protection of IP throughout the world through cooperation among states and in collaboration with other international organizations. Its headquarters are in Geneva, Switzerland. For further information about WIPO see Clause A.1. The following are regional Intellectual Property offices:

- a) USA: The United States Patent and Trademark Office (see A.8.1).
- b) UK: The Intellectual Property Office (see A.6.1), which provides further information and details of the on-line IP Health check diagnostic tool.
- c) Europe: The Europa webpage contains summaries of EU legislation for intellectual property (see A.7.1).
- d) China: The State Intellectual Property office of the P.R.C (see A.9.1).

The following are additional resources for intellectual property information:

- 1) WIPO webpage (see A.1.3) has links to the treaties administered by WIPO, with details of legislations from a wide range of countries and other related information (see A.1.4) and includes the present members of the Global Network on Intellectual Property (IP) Academies.
- 2) The International Intellectual Property Alliance is a private sector coalition, formed in 1984, of trade associations representing the US copyright based industries in bilateral and multilateral efforts working to improve international protection and enforcement of copyrighted materials and open up foreign markets closed by piracy and other market access barriers (see A.8.4).
- 3) The International Trade Administration, U.S. Department of Commerce Stopfakes webpage (see A.8.2) has links to Intellectual Property Toolkits for other countries.
- 4) The USA Embassy in China webpage (see A.8.3) has very useful data for IP control when importing goods into China.

4.3.2 Definition of intellectual property

4.3.2.1 General

Intellectual property (IP) is defined in 3.1.11 and can be controlled by the use of:

- patents
- trademarks
- copyright protection
- design registration

4.3.2.2 Patents

Patents are territorial rights. Therefore, they apply in one country, in the European Union (EU), or through the Patent Cooperation Treaty. A granted patent becomes property and can be sold or licensed out. A patent can last up to 20 years. For further information see:

- WIPO (see A.1.3);
- the European Patent Office (see A.7.3.);
- the Chinese Patent and Trademark Office (see A.9.2); or
- the Japanese Patent Office (see Clause A.10).

4.3.2.3 Trademarks

These are signs, for example words, logos, pictures, or any combination thereof. Trademarks are territorial and must be filed in each country where protection is sought.

Trademarks should be registered at:

- WIPO for the Madrid System for the International Registration of Trademarks which offers a route to trademark protection in multiple countries by filing a single application (see A.1.3); or
- EUIPO in Europe (see A.7.4) for a "Community Trade Mark" applicable to all EU member states; or
- the Chinese Patent and Trademark Office in China (see A.9.2); or
- the United States Patent and Trademark Office in the USA (see A.8.1).

4.3.2.4 Copyright

This is an automatic right which can be licensed or sold. Use © after your name.

4.3.2.5 Design

A design relates to the physical appearance of an item or part of it. Designs should be registered in your country or with the EU at EUIPO (see A.7.4) or with WIPO (see A.1.3).

4.4 Counterfeit consideration

4.4.1 General

There are various definitions of "counterfeit" being used in the avionics industry at present, which is essentially infringement of intellectual property rights. However counterfeit definitions need to use the legal definition to ensure law enforcement can proceed with managing counterfeit issues through the judiciary. The definition of counterfeit should not be confused with recycling (see 4.6).

4.4.2 Legal definition of counterfeit

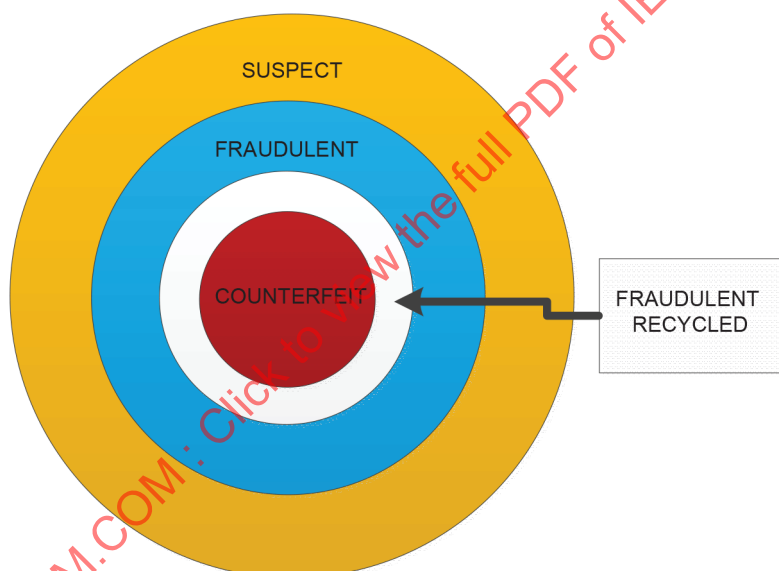
See 3.1.4 for the definition of "counterfeit" and 3.1.5 for the definition of "counterfeited component". These definitions are based on ISO 16678.

Each country typically has a slightly differently worded legal definition but generally all are based on trademark infringement.

4.4.3 Fraudulent components

See 3.1.10 for the definition of "fraudulent component". Fraudulent components are considered to be a subset within the suspect components perimeter; see 3.1.24 for the definition of "suspect component" and Figure 1. Suspect components require further investigation to determine if they are fraudulent, fraudulent recycled or counterfeit components.

NOTE It is relatively easy for law enforcement to follow the trail of money derived from fraudulent activities through the banking system and therefore there are many more successful legal convictions for fraud than for counterfeit activities. Also, as the electronic component recycling market expands, there is a huge temptation for unscrupulous brokers to trade hard to find recycled components as being in a new 'unused' condition in order to realize a greater profit. The sale of fraudulent recycled components as being in a new 'unused' condition is therefore increasing as the electronics recycling industry expands.



IEC

Figure 1 – Suspect components perimeter

4.4.4 How to establish traceability

See 3.1.24 for the definition of "traceability". Traceability is typically demonstrated by certificates of conformance (CofC) or packing slips (see 4.12.4) or other means of tracking components back to the OCM.

Where this is not available, the necessary information may be obtained from the supplier's business systems or through other databases.

Indeed, the distributor or franchised aftermarket manufacturer may not always be in possession of an original certificate of conformance or packing slip from the OCM, but can have business system database entries confirming the date of receipt from the supplier (which should be the OCM or one of their franchised distributors), the quantity and lot date code. This business system information together with a copy of the franchised agreement should provide sufficient information to satisfy traceability requirements back to the OCM.

NOTE 1 IECQ OD 3702 traceability audit can be used as a second party or third party audit process for verification purposes at any part of the supply chain (see Figure E.3 and E.4).

NOTE 2 IPC-1782 can also assist with the traceability of critical items based on risk.

4.4.5 Reasons for the loss of component traceability

Many components lose their traceability (see 3.1.26 for the definition of "untraceable") back to the original manufacturer. This can be caused by:

- Poor housekeeping and record retention either by distributors or OEMs. Many OEMs move stock from one location to another and in the process lose the traceability paperwork.
- Often OEMs sell off surplus stock back into the supply chain, without the traceability paperwork and then attempt to buy it back in. Such components are then identified as 'suspect'. As there is no traceability, this stock becomes known as possible 'counterfeit' stock.
- Distributors not checking back through the supply chain as to whether the components have traceability back to the original manufacturer. Many non-franchised distributors will not be able to manage this traceability. The supply chain may be very long and after a certain point down the supply chain, information may not be obtainable. This lack of knowledge makes the components 'suspect' and hence considered as possible counterfeit stock.
- Using inappropriate distributors for the avionics market, which are not AS/EN/JISQ 9120 certified. Although they may typically supply direct from manufacturers, they cannot prove that this is the case as their warehouse operations and traceability processes are not able to track individual lots of components and where they originate from.
- Commercial grade components which are not supplied with full traceability back to the OEM.

4.5 The counterfeit problem

4.5.1 General

Recent reports, published by the US Government Accountability Office, detail the extent to which counterfeiting activity affects the US economy:

- GAO-10-423;
- GAO-12-375;
- GAO-12-213T;
- GAO-13-762T;
- GAO-03-713T;
- GAO-16-236;
- USA Homeland Security report 'Supporting Innovation, Creativity and enterprise, charting the path ahead FY2017-2019' (see A.8.12).

Europol also reports on the impact of counterfeiting activity (see A.7.2).

The Japanese Patent Office also includes a 'FY2004 Survey Reports on Losses Caused by Counterfeiting' (see Clause A.10).

The OECD (Organisation for Economic Co-operation and Development) has published several reports concerning the impact of the counterfeit trade (see Clause A.18).

The International Chamber of Commerce (ICC) also tracks the impact of counterfeiting and piracy providing projections up to 2016 (see Clause A.19).

There are also several on-line videos highlighting the link between organised crime and counterfeiting (see Clause A.27).

NOTE Counterfeiting is a growing trade as there are usually minimal penalties in the criminal justice systems when caught. Typical punishments are a low value financial fine with no incarceration. Weak criminal justice system penalties allow the accused to walk out of the court room and recommence their counterfeiting operations on the same day.

4.5.2 General worldwide activities combating counterfeit issues

4.5.2.1 General

There are currently several ongoing anti-counterfeit activities which will assist law enforcement activities, as follows.

4.5.2.2 Anti-Counterfeiting Trade Agreement (ACTA)

The Anti-Counterfeiting Trade Agreement (ACTA) is a multinational treaty for the purpose of establishing international standards for intellectual property rights enforcement, see A.2.1. Unfortunately, it has failed to obtain worldwide acceptance.

4.5.2.3 Government/Authorities Meetings on Semiconductors (GAMS)

GAMS, founded in 1999 by a multilateral Joint Statement on Semiconductors, aims to promote the fair and open global trade and growth of the global semiconductor market through improved mutual understanding between industries and governments and reports into the World Semiconductor council. GAMS is undertaking counterfeit prevention issues, see Clause A.3.

4.5.3 Cultural differences

Many cultures are not familiar with the concept of intellectual property and fail to comply with the WTO intellectual property definitions (see 4.3). As worldwide trade increases it is essential that all worldwide organizations comply with intellectual property definitions. Failure to comply can result in claims of counterfeiting when there is no intent to deceive. For example, it is common for components and materials to be locally sourced but these may not comply completely with the customers' requirements. A local substitute is often the only solution for a quick delivery. However, it is essential that any substitute components or materials are declared to the customer and that customer approval is obtained before shipping these alternatives. Failure to inform the customer can result in the customer declaring the components are 'suspect' and hence 'counterfeit'.

4.5.4 Counterfeiting activities and avionics equipment

4.5.4.1 General

Avionics component obsolescence issues may result in the following situations:

- the obsolete components are difficult to find and sourced from franchised distributors or the OCM, which may have ceased trading;
- long deliveries (for example higher than 26 weeks) may be quoted for special assembled lots from franchised aftermarket sources or the OCM;
- limited quantities may only be available.

These situations typically have a high value market where the component cost at this stage of the component lifecycle may be considerably more than the original component cost. In addition, the avionics OEM typically has a short term requirement and wishes to avoid costly redesigns. These situations are very attractive to fraudsters and counterfeiters wishing to exploit the avionics industry.

A market is therefore created where there is an urgent demand which can be filled by counterfeit and fraudulent components.

This is an ongoing problem particularly where the avionics OEM has a requirement to support past designed avionics equipment. In these situations, the current production activity can address for example a repair activity with future obsolescence issues. The temptation for counterfeiters to continue to produce components for this avionics obsolescence market is very high and has become 'easy' money. Counterfeiting activities have become more sophisticated as knowledge of this activity increases and the avionics community procurement activities improve.

Today it is quite common for counterfeit and fraudulent electronic components to visually appear genuine, operate electrically at room temperature and somewhat over temperature extremes. Counterfeit detection methods today therefore have to be more sophisticated than just a visual inspection and knowledge of where the component was last purchased from.

However counterfeit activities can have a more malicious intent. As counterfeit sophistication increases, it will become more difficult in the future to distinguish between counterfeiting activities which are just commercial endeavours to make a profit and those which are genuinely intended as sabotage.

4.5.4.2 DOD counterfeit issues in the USA

The recent report GAO-10-389, published by US Government Accountability Office on 28 April 2010, highlights the risks of counterfeit parts to the USA DOD.

In addition, the January 2010 report "Defense Industrial Base Assessment: Counterfeit Electronics" published by the US Department of Commerce extensively reviews counterfeit activities and strongly recommends:

- buying components directly from the original component manufacturer or the approved franchised distributor;
- maintaining component traceability back to the original manufacturer, typically through the use of certificates of conformance or test certifications;
- maintaining approved supplier lists and criteria of supplier approval;
- ensuring supply chain anti-counterfeit procedures are established and are maintained;
- using escrow accounts operated by ERAI when purchasing potentially suspect components;
- using IDEA-STD-1010 type visual inspection regimes and test suspect components, for example X-ray, electrical test, as required;
- using databases to track suspect or counterfeit components, using GIDEP;
- that DOD entities should use Product Quality Deficiency Reports (PQDRs) to report non-working electronic components;
- proposing that FAR regulations are changed for the procurement of components for mission critical applications;
- that a centralised US federal reporting mechanism and database be set up for collecting counterfeit data with close ties to law enforcement. [10]¹

At the July 9th 2013 Oversight and Investigations subcommittee meeting on Intellectual Property (see GAO-13-762T), the Chief Economist reviewed insights gained from efforts to quantify the effects of counterfeit and pirated goods in the US economy. The conclusion is that IP theft is growing, heightened by the use of digital technologies.

¹ Numbers in square brackets refer to the Bibliography.

The USA Homeland Security ‘Supporting Innovation, Creativity and enterprise, charting the path ahead FY2017-2019’ (see A.8.12) indicates that a small number of ‘provenance economies’ constitutes the largest suppliers of counterfeit goods to the USA and EU.

4.5.4.3 Reliability impact and danger to general public

Counterfeit, suspect or untraceable components are a serious threat to the safety of avionics equipment as they do not have the expected reliability that the original authentic component has. Reliability is a result of good design controlled by the original manufacturer, with controlled manufacturing and handling. Reliability can never be screened into a component afterwards.

Traceable components perform as expected to the manufacturer’s published data sheets, exhibiting the expected component life in the application for the OEM’s reliability predictions and product warranty.

Untraceable or suspect components, which may or may not be counterfeit, have no information as to how the component has been stored or handled and whether it has been subjected to ESD latent damage, moisture damage, shock or vibration, etc. As a result of this lack of knowledge, it is impossible to attribute untraceable components with having the same reliability as traceable components.

4.5.4.4 Defense Logistics Agency (DLA)

The DLA sources various US Military specified component categories for various US defence programs.

The DLA has recently established the Qualified Testing Suppliers List (QTSL) to assist with the sourcing of near obsolete components using SAE AS6081 (see A.8.9) but also when sourcing components from non-franchised sources.

As of August 2012, a new clause in the Defense Logistics Acquisition Directive, DLAD 52.211-9074, related to the deoxyribonucleic acid (DNA) marking on high risk items, will be included in new solicitations and contracts for Federal Supply Class (FSC) 5962 electronic microcircuits when the microcircuit description states that the microcircuit requires DNA marking. The clause requires contractors to provide microcircuits that have been marked with botanically-generated DNA produced by Applied DNA Sciences Inc. or its authorized licensees if any; see A.8.9.

However, this marking requirement is unpopular with the Semiconductor Industry Association (SIA) and many of their members are refusing to bid for working with the DLA. As a result, the DLA has arranged a re-imbursement scheme for those Trusted Suppliers who use Applied DNA Science (see Clause A.20). This scheme, initially mandatory, was discontinued in December 2016 due to the high cost of licence fees and non-recurring charges to create the DNA sequence. However, the DLA has obtained funding to continue with this scheme for other types of components.

4.5.4.5 USA DFARS and related FARS for USA supply chains

The USA President signed the National Defence Acquisition Act (NDAA), which included section 818 on anti-counterfeit measures, on December 31st 2012. Section 818 addresses how to minimise counterfeit components in the US defence supply chain. Severe penal and financial penalties will be levied on organizations and individual personnel found to be involved in deliberately supplying counterfeit or fraudulent components to the US defence organizations. This applies to all parts of the supply chain including brokers, distributors and OEMs and MRO organizations. This was converted into an Anti-counterfeit Prevention Policy, number DoDI 4140.67 and a new Defence Federal Acquisition Regulation System (DFARS) 252.246.7007 for use in contracts (see A.8.10). DFARS 252.246.7008 on trusted suppliers was issued in 2016 which supplements DFARS 252.246.7007. Another DFAR 252.246.7008 amendment is due soon.

There is no requirement for any supplier to comply with SAE AS5553 to satisfy DFAR 252.246.7007 and DFAR 252.246.7008 requirements.

NOTE 1 SAE AS5553 is under revision again (revision C) whereby the SAE committee is attempting to include as many DFARS requirements as possible but there will be a compromise as SAE AS5553 is intended as good practice for all industry and not just for USA defence supply chains. The committee also plans to publish the document AIR 6860 to explain the extent of compliance of SAE AS5553 revision C to the DFARS requirements.

There is also the possibility that a USA Government Body will audit suppliers to DFARS requirements.

All penalties are alleviated if the OEM or distributor publishes an anti-counterfeit management plan.

All instances of suspected components are to be reported into GIDEP, a USA database for use within Canada and the USA (see A.8.12). This poses difficulties for other international suppliers as they cannot obtain access to GIDEP. Most international suppliers take exceptions to the DFARS GIDEP clauses.

NOTE 2 GIDEP is now in the process of being modified in 2017 where the plan is for suspect component counterfeit data to be hosted at three levels of sensitivity whereby it is hoped the first two levels of data will be viewable internationally.

In addition, DoDI 7050.05 concerning remedies for fraud and corruption-related procurement activities is already published.

4.5.4.6 UK MOD anti-counterfeit guidance

The UK MOD has created an interactive webpage (see A.6.7), to provide guidance for their supply chain. It has also published their 'Counterfeit Avoidance Maturity Model' which includes the Defence Standard 05-135 which is now revised to version 2.0 (it includes the requirement for obsolescence management). Defence Standard 05-135 and associated auditing and assessment awareness guidelines together provide high level counterfeit avoidance requirements for managing complex supply chains covering the procurement of missiles, munitions, ships, tanks, airplanes to bandages, food, clothing and medicines for the armed forces.

4.5.4.7 North Atlantic Treaty Organization (NATO)

NATO has now acknowledged the risk of counterfeit materiel in the supply chain and is working on an assessment of counterfeit issues.

4.5.5 Electronic components direct action groups

Several electronic components manufacturers take direct action working with local law enforcement to seize their counterfeited components and associated tooling. An example is the non-profit organization BEAMA for the electro-technical industry in the UK and Europe, which represents over 300 manufacturing companies and conducts raids of suspected factories and distributors passing on counterfeited components (see A.7.7). In addition, the anti-counterfeiting task force of the WSC (see Clause A.3) works with customs and law enforcement to eliminate counterfeits in the supply chain.

4.6 Recycled components

4.6.1 General

See 3.1.20 for the definition of "recycled component".

This is a legal activity when the components are sold as being recycled. Many industries use this practice to recover expensive chipsets, for example the telecommunications industry where expensive ASIC components are recycled from returned mobile phone handsets. In

itself recycling is not illegal if all parties in the transaction understand that the components are recycled.

NOTE The electronic recycling industry is increasing massively as the world uses more consumer products that are typically replaced by upgraded models every few years. The replaced discarded consumer products are sent to worldwide recycling centres, many of which recycle the components using uncontrolled processes, potentially causing component ESD and physical damage, making them unsuitable for future ADHP use.

4.6.2 Why the avionics industry does not use recycled components

The avionics industry has to ensure that all flight equipment produced has a predicted product life in line with the predicted repair and service life to ensure the public is not endangered. Typically an OEM will calculate a mean time between failure (MTBF) and possibly a mean time to failure (MTTF) prediction in order to establish maintenance operations. These calculations assume that all components are new, or considered as "unused", at the point of introduction into flight use and that no useful component life and/or any "unsafe" component conditions have been used.

Generally recycled components have no output for users to measure and determine how much useful life has already been used before being recycled and therefore the predicted remaining life cannot be accurately calculated for maintenance operations established by the OEM. Also the process of recycling itself, if carried out in an uncontrolled process, can introduce component damage such as inducing ESD or EOS latent damage which cannot be immediately detected but which is a long term failure mechanism and which could affect the remaining component reliability.

4.6.3 How recycled components become suspect and potentially fraudulent

ADHP OEMs typically purchase new unused components for their products and their purchase orders have terms and conditions excluding the delivery and acceptance of recycled components. Delivered components or products entering ADHP OEMs are therefore considered to be "suspect fraudulent recycled components" when evidence of prior use is observed on the component package or termination, for example where there is evidence of solder present on the terminations or the terminations have been re-plated or re-attached. Typically, in these situations, the supply chain traceability back to the OCM (see 3.1.25) has also been lost and the recycled components have been fraudulently sold into the ADHP supply chain as being "new" or "unused". For more information on fraudulent components see 4.4.3. Law enforcement agencies would typically consider this to be "fraudulent" activity rather than "counterfeit" activity, where the fraud is the selling of recycled components as being new or unused.

NOTE This practice is increasing particularly for hard-to-find expensive obsolete components as the electronic component recycling industry increases due to the turnover in consumer products for upgraded modules.

However, ADHP OEMs may use an internal recycling practice when repairing their assemblies in-house, using their internally controlled repair conditions, which include supply chain traceability back to the OCM, as defined in the IEC 62239-1 ECMP, which is approved by their customer.

4.7 Original component manufacturer (OCM) anti-counterfeit guidelines

4.7.1 General

It is important that all OCMs use anti-counterfeit measures when manufacturing, producing and selling their components. The following are typical measures which should be used on a worldwide basis unless the scheme is specific to a region or country as stated in the respective paragraphs of 4.7.2 to 4.7.11.

4.7.2 Chinese Reliable Electronic Component Supplier (RECS) audit scheme

This auditing scheme operated in China and was promoted by GAMS 2009 and by the WSC. The RECS scheme announced the first thirteen qualified enterprises in January 2008. Unfortunately this audit scheme has not been maintained and is now considered to be of historical interest only.

4.7.3 Original component manufacturer (OCM) ISO 9001 and AS/EN/JISQ 9100 Third Party Certification

When OCMs are third party audited by accredited registrars, this process also authenticates manufacturers and their manufacturing facilities and product lines, as all addresses listed on the certificates have to be physically visited and audited by the third party auditors. It is therefore highly recommended that all components are purchased from AS/EN/JISQ 9100 (see 4.2) or as a minimum from ISO 9001 Third Party Certified manufacturers. Note that ISO 9001 has no minimum benchmark workmanship standards and therefore does not guarantee component quality.

The IAQG online Oasis database (see A.8.11), can be used to verify AS/EN/JISQ 9100, AS/EN/JISQ 9110 and AS/EN/JISQ 9120 certificates.

4.7.4 Original component manufacturer's (OCM) trademarks

All OCMs shall protect their intellectual property and have a registered trademark or logo registered with WIPO, etc. The Semiconductor Association recommends that trademarks be registered within all countries within a trade free zone to ensure counterfeiters do not import their components through the member country where the trademark is not registered. In Europe trademarks can be registered with EUIPO (see A.7.4) for a "Community Trade Mark" applicable to all EU member states. Component trademark infringement is the most common cause of counterfeiting.

4.7.5 Original component manufacturer's (OCM) IP control

Manufacturer intellectual property control is typically by control of patents, control of design, use of trademarks and logos. A crucial part of the design control is the control of the final acceptance test program (ATP test software and test stations) and control of the published data sheets. ATP test software and test stations should be numbered and critically controlled. Data sheets (see 3.1.8) should be published in a locked format so that they cannot be edited and should also contain the manufacturer's logo or trademark. For COTS parts, only the data published in the OCM data sheet is the OCM's design information which is controlled by their intellectual property rights.

4.7.6 Original component manufacturer's (OCM) physical part marking and packaging marking

OCMs secretly control their final part marking activities, typically through in-house operations. However, it is essential that the OCM's trademark which is physically marked on the component is the same as the trademark registered with WIPO (see Clause A.1) and is as expected as per the OCM information. OCMs add additional physical markings to authenticate their products, using special font size, font spacing, letter and number positioning, special laser or ink marking, etc., with:

- trademarks;
- lot date codes;
- unique location codes;
- wafer lot date codes;
- special exterior package marking;
- other proprietary codes for traceability.

OCMs may assist OEMs with validating their part marking if required. However, there is a limit to the control that can be employed with this method alone. Most OCMs also use some proprietary die and packaging marking techniques (see 4.7.9, 4.7.10, 4.7.11). Note that:

- ISO 12931 has been issued to assist with the authentication methods required to combat counterfeit risks.
- ISO 16678 was developed for tracking and trace methods for shipment.
- US defence components may be uniquely identified using DoDI 8320.04 Item Unique Identification (IUID) methods.

4.7.7 The Semiconductor Industries Association Anti Counterfeit Task Force (ACTF)

SEMI is a global industry association (see Clause A.4) and provides guidance on practical measures which can be used to avoid counterfeit issues.

Chip or die traceability is a new emerging activity for wafer foundries. The following new documents have been published focusing on IC chip counterfeiting:

- SEMI T18-1106 (reapproved 0812), *Specification of Parts and Components Traceability*
- SEMI T20-0710, *Specification for authentication of semiconductors and related products*
- SEMI T20.1, *Specification for object labelling to authenticate semiconductors and related products in an open market*
- SEMI T20.2, *Guide for qualifications of authentication service bodies for detecting and preventing counterfeiting of semiconductors and related products.*
- SEMI T21-0314, *Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain*
- SEMI T22-0212, *Specification for Traceability by Self Authentication Service Body and Authentication Service Body*

These new documents help trusted manufacturers of authentic goods and use strongly-encrypted batch numbers. Using a free authentication service, anyone considering the purchase of a batch of goods can use the encrypted batch number as the basis for a validation check. Secure serialization is a major deterrent to counterfeiters. Although secure serialization systems alone do not prevent the copying or theft of codes, they can be effective at detecting that such fraud has occurred. Thus, secure serialization serves as a deterrent and an early warning system. Developed for use with semiconductor circuits and devices, these procedures can also be extended to apply to other electronic parts and other types of products.

The SIA has published a white paper in August 2013 where they discuss their recent activities in the fight against counterfeit components (see Clause A.3). This white paper concludes that the best strategy is to buy components from OCMs and their franchised distributors including franchised aftermarket distributors and to avoid buying on the open market or from non-franchised sources.

4.7.8 USA Trusted Foundry Program

The USA DOD in response to several counterfeit issues has set up new policies, including the Trusted Access Program Office (TAPO) (see A.8.5), which are responsible for finding and maintaining suppliers of trusted microelectronic parts per DoD DODI 5200.44.

Trusted suppliers are now managed by the Defence Micro Electronics Activity (DMEA) (see A.8.5) where a list of accredited suppliers is maintained.

This currently protects custom ASIC components used in critical US applications. Such items are typically designated ITAR controlled components. Users should check the ITAR status of any components used from 'Trusted Foundry' manufacturers.

4.7.9 USA Trusted IC Supplier Accreditation Program

USA trusted suppliers, in addition to those listed in 4.7.8, which are now managed by DMEA (see A.8.5), also include Trusted Test Houses, brokers, post processing facilities, packaging/assembly/test facilities, etc. Accredited trusted suppliers are awarded Trusted Supplier certificates for a period of time (with an expiry date listed on the certificate) which can be found on the company's website.

4.7.10 Physical unclonable function (PUF)

For a good definition of PUF, which is a cryptography term, see Clause A.11 where various silicon, SRAM, IC coating and magnetic PUF examples are given. This is a new emerging technology with immediate applications for preventing counterfeit activities, for example RFID tags and military applications.

NOTE ISO 17367, ISO/IEC 20243 (all parts) and ISO/IEC TR 24729-1 can assist with RFID tags.

However, new research is concerned that this technology can be tampered with and suggests this should be used with caution (see Clause A.11).

Organizations and products which can assist with this new technology include the Hardware Intrinsic Security (HIS) Initiative, launched in May 2010 (see Clause A.12). This technology exploits the unique 'electronic fingerprint' found on each semiconductor (see 3.1.21), the physical unclonable function (PUF). Semiconductor components are now being manufactured using PUF as part of their secure device manager system.

4.7.11 Original component manufacturer (OCM) best practice

OCMs should ensure that rigorous control is maintained over their subcontractors, including CEMs or EMSs to ensure that scrap, pilot runs and bad yield components are disposed of beyond use. This will ensure that these components are not sold onto the open market through non-franchised suppliers to OEMs. OCMs should also aid their distributors and OEMs by stating on their documentation when components have been legitimately re-marked. OCMs should also provide part marking verification processes, for example websites with look-up information for OEMs and other users to verify physical component markings and tamperproof labels or tags (see Clause A.13).

4.8 Distributor minimum accreditations

It is recommended that all distributors should have the following minimum third party accreditations:

- International Organization for Standardization (ISO) 9001: a quality management system standard;
- ISO 14001: an environmental management system;
- Standard Occupational Health and Safety Assessment Series (OHSAS) 18001: an occupational health and safety management system specification or equivalent procedure;
- American National Standards Institute/Electrostatic Discharge ANSI/ESD S20.20: an ESD control program standard or IEC 61340-5-1 or equivalent procedure.

4.9 Distributor AS/EN/JISQ 9120 Third Party Certification

AS/EN/JISQ 9120 is a subsection of ISO 9001 and is the complementary aerospace standard for stockists/distributors. It manages avionics distribution requirements and is in line with the OEM AS/EN/JISQ 9100 requirements. The purchase of traceable components, with traceability back to the original manufacturer is a key aspect of this AS/EN/JISQ 9120 certification process. The contract review section of the AS/EN/JISQ 9120 audit requires that all distributors in the scheme clearly define when quoting, whether the quote is for traceable components or untraceable components. The distributors will lose their AS/EN/JISQ 9120 certification if they supply untraceable components when the order is for traceable components.

Both franchised distributors and non-franchised distributors may acquire AS/EN/JISQ 9120 certification.

It is recommended that all distributors and in particular non-franchised distributors used by avionics OEMs are AS/EN/JISQ 9120 third party audited. The IAQG online Oasis database (see A.8.11), can be used to verify AS/EN/JISQ 9100, AS/EN/JISQ 9110, and AS/EN/JISQ 9120 certificates.

4.10 Franchised distributor network

4.10.1 General

Manufacturers can sell their components directly through approved franchised distributor networks (see 3.1.9 for the definition of “franchised distributor”).

These franchised distributors are approved for a stated time frame by the OCM, for example annually or every 2 years. Additionally, a distributor may only be franchised for one manufacturer and not for all the manufacturers on their line card. There appears to be no central database whereby all franchised distributors and their approval/disapproval dates are maintained historically over time. OEMs are advised to keep their own records of when a distributor is franchised for a given manufacturer and when this franchise ends.

Information about authorized franchised distributors of semiconductors is available as follows:

- The Electronics Authorized Directory (see Clause A.5), is organised by Rochester Electronics for the Semiconductor Industry Association (SIA) and has been established by the SIA as an anti-counterfeit measure.

However, the most up-to-date information should be checked on the OCM website page dedicated to: local sales, distribution offices, sales and distributors.

Franchised distributor associations are now becoming more stringent on standards for membership. These are evolving from networking clubs into standard bearers for best practices.

Examples of distributor associations are:

- 1) Electronics Components Industry Association (ECIA), a non-profit organization in North America (see A.8.7) which produces guidelines including:
 - NIGP 113: *NEDA Guidelines for Product Returns*;
 - NIGP 109: *Guidelines for Distributor Assessment of Manufacturer Performance*;
 - NIGP 107: *Guidelines for the format of Military Certificates of Conformance*;
 - NIGP 111: *Guidelines for the format of Packing Slips*
 - NIGP 115: *Guidelines for Certificates of Conformance for Commercial Electronic Parts*;
 - NGIP 116: *ECIA Guidelines for Disposition of Excess Inventory*;

- a new authorised inventory search site that supports authorised distribution.
- 2) Electronic Component Supplier Network (ECSN), a non-profit UK trade association (see A.6.6), which publishes several guides and can act as an arbitrator for franchise agreements.
 - 3) International Independent Distributors of Electronics Association (IDEA) (see A.8.6) which created the IDEA-STD-1010 visual inspection anti-counterfeit standard and operates the certified IDEA-ICE-3000 training courses. In addition, IDEA publishes white papers, operates suspect counterfeit parts lists and guidelines for independent non-franchised distributors.

Franchised distributors have enormous advantages for the avionics industry as they can assist with enhanced traceability information and can provide considerable guidance and information for obsolescence issues.

Franchised distributors can also sell to other franchised distributors. It is highly recommended that OEMs and customers request that all franchised stock comes directly from the OCM, and not from stock obtained from another franchised distributor which could potentially contain returned customers stocks with risk of components commingling; indeed this case contravenes for example the DFARS 252.246-7007 and DFARS 252-246-7008 requirements for not using “commingled” stocks on USA defence hardware.

There are many franchised distributors that also act as non-franchised distributors. These types of distributors, often called ‘mixed’ distributors are often difficult to manage, particularly if the OEM is part of a DFARS 252.246.7007 or DFARS 252-246-7008 supply chain. The concern is that their stock may be mixed up or commingled.

It is strongly recommended that OEMs and customers of distributors insert clauses in their contracts prohibiting the purchase of returned or “commingled” stocks and insist that they only receive new stocks directly from the OCM.

NOTE 1 “Commingling” refers to returned stock being mixed with new stock received straight from the OCM; the resultant stock is named “commingled” stock.

NOTE 2 Franchised distributors are increasingly concerned about the rise of the giant internet distribution fulfilment, which could eventually take over their business for general industry.

4.10.2 SAE AS6496

A new franchised distributor specification has been published by the SAE G-19 committee, SAE AS6496 (see Clause A.16), to address how the franchised distribution supply chain mitigates the risk of counterfeit components. One of its key features is that the franchised distributor shall re-inspect any returned stock to ensure returns are not composed of counterfeit or recycled components.

4.10.3 Control stock through tracking schemes

Franchised distributors control manufacturers' stock through relevant tracking schemes and can accept back unused stock from the OEMs and MRO organizations, and resell to other customers with the required traceability (see 4.10.1 for NIGP 113 and 4.10.2 for SAE AS6496).

US defence components can be tracked using DoDI 8320.04 IUID tracking standards.

There are various additional tracking schemes available such as the ‘Digital DNA’ marking scheme (see Clause A.20) and tamper-proof design companies (see Clause A.13).

See 4.13.8 for the control of products in the supply chain.

4.10.4 Control of scrap

Franchised distributors also control OCM scrap and are legally allowed to scrap and destroy 'suspect' counterfeit or fraudulent stock on behalf of the OCM (see 4.10.2 for SAE AS6496).

4.10.5 RECS

All franchised distributors in the Far East were recommended to be RECS audited some years ago (see 4.7.2). However, this scheme is no longer maintained and RECS certificates are now considered out of date and not relevant for current supply chain management.

4.11 Non-franchised distributor anti-counterfeit guidelines

4.11.1 General

See 3.1.14 for the "non-franchised distributor" definition.

The supply chain for components purchased through non-franchised distributors can be very long. There is the possibility that several distributors and brokers will be involved. The non-franchised distributor will not always know the other sources in this long supply chain and at some stage in this supply chain the components may become 'suspect' components.

It is recommended that OEMs manage non-franchised distributors in accordance with 4.11.4.

Non-franchised distributors can also be AS/EN/JISQ 9120 Third Party Certified. The IAQG online Oasis database (see A.8.11), can be used to verify AS/EN/JISQ 9100, AS/EN/JISQ 9110 and AS/EN/JISQ 9120 certificates.

Non-franchised distributors also need to establish a procedure for how to deal with suspect components as they cannot return them back again into the supply chain without being legally liable for handling counterfeit components and being accused of fraud.

SAE ARP 6178, which is an audit checklist, is a useful tool in assessing sources of supply (see Clause A.16), and when completed, could become part of the non-franchised distributor anti-counterfeit management plan.

For more information, see IEC 62668-2.

4.11.2 CCAP-101 certified program for independent distributor

The Components Technology Institute Inc. (CTI) in the USA has established the CCAP-101 certified program for independent distributors (see A.8.8), to define mandatory practices to detect and avoid the delivery of counterfeit electronic components to their customers. There are approximately ten certified distributors, mainly in the USA.

4.11.3 SAE AS6081

SAE AS6081 is published for the non-franchised distributors which offer components for sale with some testing as detailed in SAE AS6081 to avoid counterfeit, fraudulent and recycled components in the supply chain. SAE AS6301 is the verification standard. Such components may not have any traceability back to the original component manufacturer (OCM).

The IECQ has established an audit program for non-franchised distributors using SAE AS6081, see A.7.6.

The DLA has adopted SAE AS6081 on June 10th 2013 for use by the DOD. The DLA audits the distributor which tests components to SAE AS6081 and which becomes listed on the Qualified Testing Suppliers List (QTSL) when the audit is successful (see A.8.9).

However, an OEM needs to take precautions when using components tested to SAE AS6081 as there may be no traceability back to the OCM, testing can be customised in SAE AS6081, and the parts are not risk assessed for the application as the non-franchised distributor has no knowledge of the intended application. Avionics OEMs may prefer to take direct action themselves and manage the entire supply chain and select appropriate testing using IEC 62668-2 (see 4.11.4).

4.11.4 OEM managed non-franchised distributors

Most OEMs need to use some non-franchised distributors occasionally to source traceable components as it is impossible, with the vendor (OCM or franchised distributor) reduction programs in place today, to supply all the components needed from franchised distributors.

There is a small group of non-franchised distributors that only purchase directly from OCMs or their franchised distributors for the avionics market. Such distributors typically have AS/EN/JISQ9120 and SAE AS6081 Third Party Certification. These distributors typically operate with full traceability and can be useful suppliers to the avionics industry, and can comply with DFARS 252.246-7007 and DFARS 252-246-7008 requirements. These distributors are sometimes referred to "pass-through" suppliers.

For more information, see IEC 62668-2.

4.11.5 Brokers

Use of brokers (see 3.1.2) for the purchase of avionics components is not recommended.

For more information, see IEC 62668-2.

4.12 Avionics OEM anti-counterfeit guidelines when procuring components

4.12.1 Anti-counterfeiting general approach

OEMs shall have anti-counterfeit management plans in place based on:

- AS/EN/JISQ 9100 procedures (see 4.2);
- IEC 62239-1 (ECMP) which includes obsolescence management.

NOTE Obsolescence management is a major contributor in counterfeiting prevention. IEC 62402 and SAE STD-0016 provide guidelines regarding component obsolescence management.

4.12.2 Buy from approved sources

All components, which should be selected from approved manufacturers which use trademarks, logos and other intellectual property controls, should be bought from authorised sources with traceability back to the OCM, using the OEMs AS/EN/JISQ 9100 approved processes. All authorised sources should be either ISO 9001 or preferably AS/EN/JISQ 9100 or AS/EN/JISQ 9120 approved and should be either the OCM or their authorised approved franchised distributor (see 4.10). The IAQG online Oasis database (see A.8.11), can be used to verify AS/EN/JISQ 9100, AS/EN/JISQ 9110 and AS/EN/JISQ 9120 certificates.

SAE ARP 6178, which is an audit checklist, may be a useful tool in assessing sources of supply (see Clause A.16) and could become part of the OEM AS/EN/JISQ 9100 approved supplier process.

NOTE ISO 22380, under development, can assist with managing product fraud risk.

4.12.3 Traceable components

AS/EN/JISQ 9100 requires demonstration of conformity to the product definition. For electronic components this can be shown by traceability back to the original manufacturer to validate they are genuine and conform to the stated specification/data sheets.

Most avionics OEMs therefore require that all components purchased are traceable back to the original manufacturer, as most OEMs operate common stock procedures for all their programs where the buyer at the point of ordering does not know where the component will be used and whether the application is flight critical or not. The OEM buyers shall ensure there is full traceability on all stock ordered and raise special non-conformance purchase queries when only non-traceable stock can be found. This shall apply to any procurement process including direct line feed (DFL) operations via a typical replacement system and/or any traditional stockroom situation.

Components have full traceability when purchased from the original manufacturer, their franchised distributor or their franchised aftermarket supplier of packaged final product or die or wafers or their OEM managed non-franchised distributors (see 4.11.4). Traceable stock is also available through AS/EN/JISQ 9120 certified distributors which may be franchised or non-franchised distributors. A certificate of conformance and/or a copy of the OCM packing slip can be requested confirming this traceability (see 3.1.25 and 4.12.4). The franchise agreement letter or the contract with the OCM together with the supplier's business system database entries showing the dates of receipt, quantity and lot date codes, etc. can satisfy traceability requirements back to the OCM.

It is advisable to periodically audit these suppliers, for example using the IECQ OD 3407-1 traceability audit checklists.

Franchised aftermarket distributors often struggle to provide sufficient traceability paperwork back to the OCM as they may have acquired stock many years ago before traceability throughout the supply chain had to be audited and demonstrated.

It may be necessary for the OEM to establish special contractual agreements with distributors to ensure that their orders are fully traceable back to the OCM prior to the placement of any orders. This contractual agreement should be part of the OEM AS/EN/JISQ 9120 distributor assessment and approval process (see 4.12.2).

All OEMs should order traceable stock as a first priority as safety is paramount.

Supply chain delivery tracking schemes can assist this process, for example DoDI 8320.04 Item Unique Identification (IUID) methods.

4.12.4 Certificate of conformance and packing slip

4.12.4.1 Certificate of conformance

A certificate of conformance is the traditional way of checking traceability back to the original component manufacturer. A certificate of conformance signed by the OCM not only shows traceability but also conformity to the product design. These OCM certificates of conformance are routinely used by avionics OEMs to underwrite their airworthiness certificates, as the certificates of conformance provide evidence that the components have been validated as conforming to their product design characteristics. It is typically a written statement signed by the quality manager of the distributor or company selling the component with a written guarantee that the component supplied is new, unused and traceable back to the original manufacturer. This information may be held electronically in a database or in paper form.

In the USA, certificates of conformance for USA defence components follow JESD31 requirements.

Note that certificates of conformance may only be the supplier's certificate of conformance and not the OCM's certificate of conformance. These may also be counterfeited.

4.12.4.2 Packing slip

For non-defence components, traceability may be demonstrated by the distributor 'packing slips' which typically follow the ECIA publications (see A.8.7):

- NIGP 111, *Guidelines for the Format of Packing Slips*, which allows for the certificate of conformance to be either printed directly on the front of the packing slip or as a separate document included with the pack list;
- NIGP 115, *Certificates of Conformance for Commercial Electronic Parts*.

In this case, as there is an information transfer, the OEM has to make sure with the distributor that the traceability towards the OCM is reliable.

4.12.5 Plan and buy sufficient quantities

OEMs often only buy components with a two-year forecast as that is the only order cover that they themselves have for the products they deliver to their customers, even though the product has a lifetime of 15 years plus maintenance time. Often the OEM also operates 'just in time' (JIT) ordering procedures. The result is that OEMs typically do not buy enough components or even miss last time buy (LTB) opportunities. It is essential that every OEM operates an obsolescence management process which may be in accordance with its IEC 62239-1 ECMP or its SAE STD-0016 DMSMS management plan and monitors component requirements throughout the lifecycle of its product.

OEMs JIT policies have to be rationalised with their obsolescence management policies. Risk could be better managed by arranging more 'one time buys' depending on the application or by ordering periodically to maintain the link with the OCM for components which are on the verge of obsolescence than waiting for the last time buy (LTB) announcement. In addition, LTB stock requires careful management and storage (see the guidelines of IEC 62435-1).

4.12.6 Use of non- franchised distributors

The use of non-franchised distributors (see 4.11), should be minimised wherever possible as they require direct management. Their use has an inherent risk of possible counterfeit stock being procured. The OEM has to manage them carefully to know when they are shipping fully traceable components and when they are shipping untraceable components. It is highly recommended that all non-franchised distributors be AS/EN/JISQ 9120 certified as this distinction will be clearly identified on all quotations to the OEM. Also the OEM may consider the use of various tools which are now available to assess the risks when using non-franchised distributors, for example:

- 1) SAE ARP 6178 (see Clause A.16);
- 2) iNEMI anti-counterfeit risk assessment calculators (see Clause A.17);
- 3) SAE AS6171 which includes the use of a web-based Counterfeit Defect Coverage Tool (see Clause A.16).

When non-franchised distributors are shipping untraceable components, the OEM shall follow the requirements of IEC 62668-2 for more information, which requires that all purchased components be analysed for risk, and risk mitigation tested prior to use. Prior approval by the customer, generally the OEM (see 3.1.15), is typically required.

4.12.7 Brokers

The use of unapproved brokers (see 3.1.2) for the purchase of avionics components is not recommended, especially brokers which operate off the internet (see IEC 62668-2 for more information).

4.12.8 Contact the original manufacturer

The OCM may organise a new production run of an obsolete product or infrequently manufactured product, if there is enough die left over in wafer storage. This may not be visible on the website and direct contact with the OCM is necessary to determine if this is possible.

4.12.9 Obsolete components and franchised aftermarket sources

Obsolete components are often the greatest sources of counterfeit or recycled components in the supply chain. Obsolete components may be available in franchised distribution for a considerable time after the last time buy (LTB) announcements. Care should be taken to monitor the lot date codes (LDCs) in the LTB announcements to ensure the parts offered for sale are genuine. The OCM may assist with this LDC verification. In addition, various obsolescence and active counterfeit monitoring tools are now available to assist OEMs in monitoring LTBs, PCNs and counterfeit reports so that the LDCs can be quickly verified.

Obsolete components which are still available from franchised 'sunset' or manufacturer approved 'aftermarket' sources (see 3.1.1) shall be used before sourcing untraceable components. See Annex B for examples of aftermarket sources.

It may be necessary to verify the franchised agreement between the franchised 'sunset' or 'aftermarket' manufacturer and the original manufacturer, for example by asking for the franchised agreements, letters, searching for press releases, published statements, etc.

The franchised aftermarket manufacturer or distributor may not always be in possession of an original certificate of conformance or packing slip from the OCM but will have business system database entries confirming the date of receipt from the supplier (which should be the OCM or one of their franchised distributors), the quantity and lot date code. This business system information together with a copy of the franchised agreement should provide sufficient information to satisfy traceability requirements back to the OCM (see also 4.12.3).

Where only franchised die is available, the die may be packaged up by third party custom packaging houses (see Clause B.3) and approved in accordance with the OEMs' IEC 62239-1 ECMP or SAE STD-0016.

Obsolete or soon to be obsolete components should be identified early using pro-active obsolescence procedures based on one or more of the following:

- IEC 62239-1;
- SAE STD-0016;
- IEC 62402;
- SD-22.

4.12.10 IEC 62239-1 approved alternatives

Where no traceable or aftermarket components can be found, the OEMs should consider using their IEC 62239-1 electronic component management plan (ECMP) process to find traceable IEC 62239-1 approved components which are form, fit and function alternatives suitable for the application.

4.12.11 Product redesign

Where there is no franchised aftermarket or IEC 62239-1 alternatives available, the OEM should consider a redesign so that traceable components can be used. The redesign could be limited to developing a small 'electronic mezzanine' or 'daughter electronic board' rather than redesigning the entire electronic board.

4.12.12 Non traceable components

Where all other sources of supply are exhausted and there is no opportunity for a product redesign, untraceable stock is often considered to be the only solution. However, procuring untraceable stock is a high risk process with no guarantee of success as it is highly likely that counterfeit or recycled components will be found. Also, the legal implications of what to do if the components are proved to be counterfeit have to be considered as they cannot be mixed up with good traceable stock and cannot be returned into the supply chain. Returning such components back into the supply chain means that the returner is trading illegally and may be liable for prosecution. Components found to be counterfeited should be quarantined and retained for evidence and the matter should be reported to the relevant enforcement authority (see 4.14, A.7.2, and Clause A.8 for useful contacts). Non traceable stock shall be managed within an OEM anti-counterfeit management plan (see 4.12.13) using IEC TS 62668-2.

4.12.13 OEM anti-counterfeit plans including SAE AS5553 and SAE AS6174

4.12.13.1 General

The OEM shall have an anti-counterfeit, fraudulent and recycling plan in accordance with this document (see 4.2 and in particular 4.2 c)).

The OEMs which do not have an SAE AS5553 plan shall meet the requirements specified in 4.2 c).

The OEMs that have an SAE AS5553A or AS5553B anti-counterfeit plan for electronic components may consider it in their IEC 62668-1 anti-counterfeit plans; Table 2 and Table 3 identify the IEC 62668-1 requirements which can be satisfied or not, respectively, by SAE AS5553A or AS5553B requirements.

SAE AS5553, currently at revision B, with revision C in progress, is a very comprehensive document targeted at the general and high reliability industry and written mainly for USA users (see Clause A.17 for further information) but only applies to electronic components coming into a business.

Note that the new SAE AS5553 revision C currently in progress may, when published, have different traceability requirements with regard to the previous revisions and so it may respond differently to IEC 62668-1 requirements, leading Table 2 or Table 3 not to be satisfactory. In addition to the management of electronic components coming into a business, IEC 62668-1 also includes the management of an OEM's IP of all the products sold out of the business, including the management of spares (either sold as separate individual components or assemblies) and repairs.

Table 2 – IEC 62668-1 requirements satisfied or not if OEM has an approved SAE AS5553A plan

IEC 62668-1 requirement	Satisfied by SAE AS5553A requirement	Comments	Notes for avionics OEMs when writing an SAE AS5553A plan as a basis for an IEC 62668-1 plan
4.2 a)	No.		
4.2 b)	No.	SAE AS5553A has no minimum specific component selection rules reviewing the component IP, only rules for maximizing the availability of parts with an obsolescence management plan and rules for sourcing or buying components.	Refer to an IEC 62239-1 ECMP plan addressing obsolescence management and component selection and qualification rules for avionics OEMs.
4.2 c)	An SAE AS5553A plan only satisfies how components are purchased and brought into a business. The IEC 62668-1 plan also has to address all the 4.2 requirements including how plan owners manage their own IP, spares, repairs and sale of individual spares into the market place.		Issue a cross reference matrix based on Table 2 to show how the SAE AS5553A plan satisfies the IEC 62668-1 requirements.
4.2 d)	No – not unless AS/EN/JISQ 9100 is invoked.	SAE AS5553A is written for general industry and does not mandate the use of AS/EN/JISQ 9100.	Base your SAE AS5553A plan on your AS/EN/JISQ 9100 procedures.
4.2 e)	Yes.		Base your SAE AS5553A plan on traceability through the supply chain back to the original manufacturer.
4.2 e) 1)	Yes.		Base your SAE AS5553A plan on traceability through the supply chain.
4.2e) 2)	Optional requirement depending on customer contract. No.	SAE AS5553A does not acknowledge this optional contract requirement using USA trusted sources.	Allow your SAE AS5553A plan to be customised using USA trusted suppliers where required by contract if you have USA customers.
4.2 e) 3)	Yes.		Base your SAE AS5553A plan on using franchised aftermarket sources when the part is obsolete.
4.2 e) 4)	Yes.		Base your SAE AS5553A plan on traceability through the supply chain.
4.2 f)	Partially.	SAE AS5553A is written for general industry and does not mandate the use of AS/EN/JISQ 9100.	Base your anti-counterfeit plan on your AS/EN/JISQ 9100 procedures.
4.2 g) 1)	Partially.	SAE AS5553A does not ask for the search to be exhaustive and that alternate solutions should be considered before going to an untraceable part sourced from a non-franchised source.	Base your anti-counterfeit plan on using IEC 62239-1 for assessing the risks and considering alternate solutions based on a traceable part before derogating and procuring an untraceable part outside the OCMs and franchised distributors network.

IEC 62668-1 requirement	Satisfied by SAE AS5553A requirement	Comments	Notes for avionics OEMs when writing an SAE AS5553A plan as a basis for an IEC 62668-1 plan
4.2 g) 2)	No.	SAE AS5553A minimum requirements do not refer to IEC 62668-2 and do not mandate the use of AS/EN/JISQ 9100 non-conformance procedures.	Base your anti-counterfeit plan on using IEC 62668-2 for managing non-franchised distributors.
4.2 h)	No.	SAE AS5553A does not apply to product or spares leaving the OEM.	
4.2 i)	Yes.		
4.2 j)	Yes.		
4.2 k)			
4.2 l)	Yes.		

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

Table 3 – IEC 62668-1 requirements satisfied or not if OEM has an approved SAE AS5553B plan

IEC 62668-1 requirement	Satisfied by SAE AS5553B requirement	Comments	Notes for avionics OEMs when writing an SAE AS5553B plan as a basis for an IEC 62668-1 plan
4.2 a)	No.		
4.2 b)	No.	SAE AS5553B has no minimum specific component selection rules reviewing the component IP, only rules for maximizing the availability of parts with an obsolescence management plan and rules for sourcing or buying components.	Refer to an IEC 62239-1 ECMP plan addressing obsolescence management and component selection and qualification rules for avionics OEMs.
4.2 c)	An SAE AS5553B plan only satisfies how components are purchased and brought into a business. The IEC 62668-1 plan also has to address all the 4.2 requirements including how plan owners manage their own IP, spares, repairs and sale of individual spares into the market place.		Issue a cross reference matrix based on Table 2 to show how the SAE AS5553B plan satisfies the IEC 62668-1 requirements.
4.2 d)	No – not unless AS/EN/JISQ 9100 is invoked.	SAE AS5553B is written for general industry and does not mandate the use of AS/EN/JISQ 9100.	Base your SAE AS5553B plan on your AS/EN/JISQ 9100 procedures.
4.2 e)	Yes.		Base your SAE AS5553B plan on traceability through the supply chain back to the original component manufacturer using your AS/EN/JISQ quality management plan.
4.2 e) 1)	Yes.		Base your SAE AS5553B plan on traceability through the supply chain back to the original manufacturer.
4.2 e) 2)	Optional requirement depending on customer contract.	SAE AS5553B does not acknowledge this optional contract requirement using USA trusted sources.	Allow your SAE AS5553B plan to be customised using USA trusted suppliers where required by contract if you have USA customers.
4.2 e) 3)	Yes.		Base your SAE AS5553B plan on using franchised aftermarket sources when the part is obsolete with traceability back to the original manufacturer.
4.2 e) 4)	Yes.		Base your SAE AS5553B plan on traceability through the supply chain.
4.2 f)	Partially.	SAE AS5553B is written for general industry and does not mandate the use of AS/EN/JISQ 9100.	Base your anti-counterfeit plan on your AS/EN/JISQ 9100 procedures.

IEC 62668-1 requirement	Satisfied by SAE AS5553B requirement	Comments	Notes for avionics OEMs when writing an SAE AS5553B plan as a basis for an IEC 62668-1 plan
4.2 g) 1)	Partially.	SAE AS5553B does not ask for the search to be exhaustive and that alternate solutions should be considered before going to an untraceable part sourced from a non-franchised source.	Base your anti-counterfeit plan on using IEC 62239-1 for assessing the risks and considering alternate solutions based on a traceable part before derogating and procuring an untraceable part outside the OEMs and franchised distributors network.
4.2 g) 2)	No.	SAE AS5553B minimum requirements do not refer to IEC 62668-2 and do not mandate the use of AS/EN/JISQ 9100 non-conformance procedures.	Base your anti-counterfeit plan on using IEC 62668-2 for managing non-franchised distributors (which includes reference to SAE AS6171).
4.2 h)	No.	SAE AS5553B does not apply to product or spares leaving the OEM.	
4.2 i)	Yes.		
4.2 j)	Yes.		
4.2 k)	No		SAE AS5553B does not address the inspection of returned stock or products
4.2 l)	Yes	SAE AS5553B does require an obsolescence process.	

4.12.13.2 GIFAS guide for OEMs using non-franchised distributors

The GIFAS 5052 guide is published by the GIFAS French National Committee. It was adopted and modified to be published as IEC 62668-2.

4.12.13.3 Flow down to lower level subcontractors

The OEM shall flow down the requirements for an anti-counterfeit plan to the lower level subcontractors or shall manage them effectively; this includes MRO operations under the OEM's responsibility.

NOTE Figures E.1, E.2, E.3, E.4 and E.5 can assist in the deployment of anti-counterfeit standards.

Contract electronic manufacturers (CEMs), which carry out subcontracted manufacturing operations for OEMs and which have SAE AS5553 anti-counterfeit plans may also be monitored by the use of IECQ OD 3702 traceability second party or third party audits.

4.12.13.4 Re-manufactured components

See 3.1.18 for the definition of "re-manufactured component". Such components may be manufactured to fulfil the market need for components in different packages or different temperature grades or to solve obsolescence problems, etc. Die extraction techniques are considered potentially damaging as the extraction process may be uncontrolled and may induce ESD, mechanical and temperature damage. The die also may have been previously used in an application and therefore is a recycled die with an unknown long term reliability and lifetime when applied in a new application.

Re-manufactured components are not considered counterfeit or fraudulent if the re-manufacturer uses their logo, name and part numbers to describe these components and discloses in their datasheet the technical information such as electrical, functional and physical characteristics and re-manufacturing process.

Such re-manufactured components do not produce the same long-term reliability as components produced by the OCM. Re-manufactured components are therefore not addressed in this document and it is recommended that they be avoided for civil avionics use as they can lead to an unacceptable risk of equipment MTBF reduction.

4.13 OEM anti-counterfeit guidelines for their products

4.13.1 IP control

The OEMs should control their design through a combination of patents, trade agreements, franchise agreements, control of design, trademarks and logos. The OEMs should also control their final ATP and test stations, bills of material (BoMs), drawings and specifications securely.

4.13.2 Tamper-proofing the OEM design

There are many ways of configuring an OEM design with tamper-proofing features either in hardware or software.

There are many specialised external subcontractors which offer a full tamper-proof service for a complete design (see Clause A.13 for examples).

Alternatively, custom ASICs and FPGAs can be designed using physical unclonable function (PUF) technology (see 4.7.10) or similar technologies.

Recent tamper-proof articles include:

- Adam Waksman, Simha Sethumadhavan, 'Tamper Evident Microprocessors', Department of Computer Science, Columbia University, NY. [11]

4.13.3 Tamper-proof labels

Tamper-proof labels are available in different styles and can be applied throughout the assembly to indicate when unauthorised disassembly or repair has been carried out. Units can be sealed externally with tamper-proof hardware or labels (see Clause A.13).

4.13.4 Use of ASICs and FPGAs with IP protection features

4.13.4.1 General

ASICs and FPGAs are complex microcircuits containing OEM proprietary software code, which is typically the OEM's intellectual property. This code requires IP protection.

4.13.4.2 FPGA and peripheral microcircuit packaging

Some FPGA solutions (RAM based FPGA) have been manufactured as a single microcircuit, assembled onto a PCB with PCB traces between it and adjacent separately packaged and assembled semiconductor memories. These PCB traces can be intercepted by counterfeiters, who can read the signals coming through the PCB traces. Anti-fused FPGA solutions or FPGA with on board semiconductor memory in one stacked microcircuit package, are better IP solutions as no external memory is required. FPGA manufacturers are now also including additional peripheral microcircuits with the FPGA into one highly complex microcircuit thereby providing a one-microcircuit package solution for assembly onto the PCB.

4.13.4.3 FPGA die serialization

FPGA confidential randomly generated single die serialization is now available from some manufacturers (see Clause A.14 for examples).

4.13.4.4 NVRAM

Some NVRAMs contain an internal microprocessor, which can be factory programmed to destroy the internal code (see Clause A.15).

4.13.5 Control the final OEM product marking

The OEM shall ensure that the equipment marking is in accordance with the regulatory requirements and provides full traceability. Note that radio frequency ID tags are becoming common in order to distinguish genuine components from counterfeit ones (see Clause A.12).

The user can note the following:

- ISO 12931 has been issued to assist with the authentication methods required to combat counterfeit risks;
- ISO 16678 assists with tracking and trace methods for shipment to deter counterfeiting and illicit trade;
- ISO/IEC 15459-8 has been issued to assist with specifying unique, non-significant string of characters for the unique identifier for grouping of transport units which may be represented in a bar code label or other media that make up the grouping to meet supply chain needs and regulatory needs;
- ISO 17367 has been issued to define the basic features of RFID for the use in the supply chain and can assist with the traceability of products at each stage of the production process;
- ISO/IEC 20243 (all parts) has been issued to constitute the Open Trusted Technology Provider Standard (O-TTPS) for mitigating maliciously tainted and counterfeit products;
- ISO/IEC TR 24729-1 has been issued to provide guidance on the use of RFID enabled labels and packaging in the supply chain;
- MIL-STD-130 specifies the identification marking of US defence property;
- MIL-STD-129 defines the US defence marking practices for shipment and storage.

4.13.6 Control OEM scrap

All internal rejects should be physically destroyed to ensure potential counterfeiters cannot reconstruct rejects and sell them fraudulently as original components or units. US defence equipment should be disposed of using DoD 4160.21-M.

4.13.7 OEM trademarks and logos

All trademarks should be registered (see A.1.3). The OEMs should take as many precautions as possible to protect their products with the use of special serial numbers, lot date code markings, exterior markings, package markings and product shipping processes.

4.13.8 Control delivery of OEM products and spares and their useful life

The OEM should consider the use of special tracking schemes for mission critical components such as engines, which are FAA Class I products.

For further information on the FAA and its product classifications, see A.8.4.

The FAA has webpages for engine identification and registration marking requirements (see A.8.4.2).

The FAA recently published an advisory circular AC 00-56B about their “voluntary industry distributor accreditation program” for accrediting civil aircraft electronic components distributors based on voluntary oversight.

Also, see DI-MISC-81356 for certificates of compliance when delivering equipment to US defence customers.

4.13.9 MRO activities

4.13.9.1 General

See 3.1.13 for the definition of “MRO”. It is recommended that all maintenance organizations be Third Party Certified to AS/EN/JISQ 9110 quality management system to ensure full traceability of all components and repaired units. In addition, AS/EN/JISQ 9110 has a specific clause, requiring that appropriate measures be taken to prevent purchase of counterfeit/unapproved products. See 4.4.4 for traceability in MRO activities.

4.13.9.2 Civil avionics repairs to OEM products

Most civil OEMs repair their equipment internally, in their own approved MRO repair centres, to ensure authentic components are used and repairs are carried out in a controlled manner. The OEMs also issue component maintenance manuals (CMMs) for their products which detail the design and the replacement component information. Often the replacement component can only be purchased from the OEM and this again is an anti-counterfeit measure.

Some civil air framers also carry out repairs. Some of them use FAA approved facilities as follows:

- FAR Part 43 describes the rules for any aircraft having a US air-worthiness certificate;
- FAA AC (advisory circular) 20-62 defines the quality, eligibility and traceability of aeronautical parts and materials intended for installation on USA type certified products;
- FAR Part 145 describes the certification, training, facility requirements and operating rules for aeronautics and space repair stations.

EASA (see A.7.5) certifies civil aircraft in Europe and repair facilities:

- EASA Part M establishes common technical requirements and administrative procedures for ensuring continuing airworthiness of aircraft;
- EASA Part 145 deals with approved maintenance organizations.

Some aircraft engine manufacturers operate real time tracking schemes for engine health management which provide full traceability through satellite tracking schemes on their engines throughout the engine operational life. Processes using this concept are highly recommended.

CAAC certifies civil aircraft in China and repair facilities (see A.9.5):

- CAAC CCAR 145 establishes civil aircraft maintenance regulations together with advisory circular CAAC AC-145-06R1.

4.13.9.3 Defence avionics repairs to OEM products

Defence customers typically use their approved defence MRO repair centres and order replacement components for repairs. USA military repairs are made in accordance with the anti-counterfeit DFARs 242.256.7007 and DFARS 242-256-7008 (see 4.5.4.5). Where components are obsolete and impact the repair of a product, it is recommended that the customer research reliable alternatives, including potentially equipment redesign activity, rather than use for example re-manufactured components, which have no predictable reliability.

4.14 Counterfeit, fraud and component recycling reporting

4.14.1 General

It is recommended that evidence of counterfeiting, fraudulent and electronic component recycling activities be forwarded on to the relevant local law enforcement agencies in a timely manner, preferably before the suspect component crosses the border control.

4.14.2 USA FAA suspected unapproved parts (SUP) program

Suspected counterfeit component issues can be e-mailed to the Aviation Safety Hotline office (see A.8.4.3).

4.14.3 EASA

EASA issue Safety Information Bulletins (SIBs) on potential hazards which may include reporting of counterfeit or fraudulent components (see A.7.5).

4.14.4 UK counterfeit reporting

The UK Revenue and Customs webpage (see A.6.4) has a reporting facility for suspected counterfeit components. In addition, the local Trading Standards office (see A.6.3) has a facility for reporting counterfeit goods.

4.14.5 EU counterfeit reporting

Counterfeit reporting within the EU should be reported locally. The Europa webpage (see A.7.1, second bullet point) contains forms and details of how to process national and EU wide applications for IP action by customs authorities.

4.14.6 UKEA anti-counterfeiting forum

See A.6.5 which is managed by the UK Electronic Alliance (UKEA).

Their website contains awareness information and links for industry in their fight to beat counterfeit components from entering their supply chains. It contains an on-line directory of relevant free-to-access information including articles, best practice, events, presentations, reliable component sources, reports and solution providers. Visitors may register free of charge to contribute to and search a database of suspect counterfeit components.

4.15 Anti-counterfeit awareness training

Anti-counterfeit awareness training is essential to ensure counterfeit and fraudulent components are identified and managed. There are various anti-counterfeiting training videos and training packages available in the public domain which include the following examples:

- the Nuclear Industry 'Safety Directors Forum' which has recently published an online video (see Clause A.21);
- the World Bearing Association (WBA) has an excellent webpage and on-line awareness training 'Stop Fake Bearings' video (see Clause A.22);
- industrial companies' on-line counterfeit awareness training videos are available, which are targeted at specific industry sectors (see Clause A.23 for an example);
- subscription based training packages, for example from ERAI (see Clause A.24);
- USA Government publications (see Clause A.25);
- IECQ WG6 anti-counterfeit webpage (see Clause A.26);
- various videos on the Internet explaining the link between organised crime and the anti-counterfeit world.

4.16 Information to support the management of the supply chain

Some documents such as ISO 28000, ISO 28001, ISO 28002, ISO 28003 and ISO 28004 (all parts) can assist in managing and securing the supply chain with regard to the reduction of the risks related to acts of piracy and fraud.

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

Annex A (informative)

Useful contacts²

A.1 World Intellectual Property Organization (WIPO)

A.1.1 General

WIPO has its headquarters in Geneva: 34 Chemin des Colombettes, 1211 Geneva 20, Switzerland, tel: (+41-22) 338 9111 and its regional offices are as follows:

- WIPO Brazil Office, Avenida Atlântica, Nº 1130, 5th Floor – Part B, Copacabana, Rio de Janeiro, Brazil, Zip code: 22021-000 tel: (+5521) 2513-3506, see webpage: <https://www3.wipo.int/contact/en/area.jsp?area=wbo>
- WIPO China Office, No.2 Dongkoudai Hutong, Xicheng District, Beijing 100009, China, tel: + 86 10 83 22 02 38 /+ 86 10 83 22 08 33, Fax: + 86 10 83 22 03 23 see webpage <http://www.wipo.int/about-wipo/en/offices/china/>
- WIPO Japan Office Daido Seimei Kasumigaseki Bldg. 7F, 1-4-2 Kasumigaseki, Chiyoda-ku Tokyo 100-0013, Japan tel: (+81) 3 5532 5030 see webpage <http://www.wipo.int/about-wipo/en/offices/japan/>
- WIPO Moscow Office, 5 Nobelya str. Skolkovo Innovation Center Moscow, 143026 Russian Federation , Tel: +7 499 940 04 82, Fax: +7 499 940 04 83, see webpage <http://www.wipo.int/about-wipo/en/offices/russia/>
- WIPO New York Office, WIPO Coordination Office, 2 UN Plaza, Suite 2525, New York, NY 10017, tel:(+1) 212-963-6813 see http://www.wipo.int/about-wipo/en/new_york/
- WIPO Singapore Office, 29 Heng Mui King Terrace, #06-16, Singapore, 119620, Singapore, tel: (+65) 6774 6406 and see(+65) 6774 4298 webpage <http://www.wipo.int/about-wipo/en/offices/singapore/>

The WIPO webpage is <http://www.wipo.int/portal/index.html.en>. It contains the following information.

A.1.2 What is WIPO?

The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations. It is dedicated to developing a balanced and accessible international intellectual property (IP) system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest.

WIPO was established by the WIPO Convention in 1967 with a mandate from its Member States to promote the protection of IP throughout the world through cooperation among states and in collaboration with other international organizations. Its headquarters are in Geneva, Switzerland.

² The information contained in Annex A is given for the convenience of the users of this document and does not constitute an endorsement by the IEC of the organizations or software named.

A.1.3 WIPO Intellectual Property Services

- **International patent protection – Patent Cooperation Treaty (PCT) System**

The PCT System (see webpage <http://www.wipo.int/pct/en/>) allows inventors and applicants to seek patent protection internationally by filing a single international application with a single patent office. Filing and processing patent applications through the PCT:

- brings the world within reach;
- postpones the major costs associated with international patent protection;
- provides valuable information about potential patentability of the invention;
- is safe and easy with WIPO's electronic filing software.

- **International trademark registration (Madrid System)**

The Madrid System (see webpage <http://www.wipo.int/madrid/en/> or <http://www.wipo.int/trademarks/en/>) offers trademark owners the possibility to protect a trademark in up to 115 countries by filing a single application with a national or regional trademark office. Trademarks are distinctive signs, used to differentiate between identical or similar goods and services offered by different producers or services providers. Trademarks are a type of industrial property, protected by intellectual property rights.

WIPO is not in a position to offer legal advice to individuals or businesses on specific questions. You may wish to consult your national IP office, an IP agent, or the relevant national or regional legislation (WIPO Lex).

International trademark registration through the Madrid System offers the following advantages:

- avoids having to file multiple applications at different offices;
- covers 115 countries from around the world;
- facilitates management of the mark, as changes or renewals can be recorded through a single procedural step;
- trademark owners simply need to fill in, from their national office, one form, in one language, pay one set of fees, in one currency, to obtain and modify an international registration;
- trademark owners benefit from online tools to search existing marks, browse the WIPO gazette, estimate filing costs, make e-payments and renewals and check registration status;
- this unique service offered by the Madrid System eases the registration and management of a mark or a large portfolio: it empowers businesses and helps expand their market abroad;
- WIPO works with Member States to develop international laws and standards for trademarks. See Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications (SCT);
- to search international trademark registrations, see the ROMARIN (Read-Only-Memory of Madrid Active Registry Information) database at webpage <http://www.wipo.int/madrid/en/romarin/>

- **International design registration (Hague System)**

The Hague System (see webpage <http://www.wipo.int/hague/en/>) allows applicants to register an industrial design in up to 66 countries with a minimum of formalities and expense. Choosing the Hague System to protect industrial designs internationally:

- avoids having to file multiple registrations at different offices;
- enables applicants to register up to 100 industrial designs with a single form;
- facilitates management of registered designs, as changes or renewals can be recorded through a single procedural step.

- **International registration of appellations of origin (Lisbon System)**

The Lisbon System (see webpage <http://www.wipo.int/lisbon/en/>) facilitates the international protection of appellations of origin through one single registration procedure. The Lisbon System:

- avoids having to file multiple registrations at different offices;
- covers over two dozen countries in Africa, Asia, Europe, and Latin America.

- **Alternative dispute resolution**

The WIPO Arbitration and Mediation Center (see webpage <http://www.wipo.int/amc/en/>) is the leading resource in the resolution of IP disputes outside the courts. It offers specialized procedures including neutral arbitration, expedited mediation and expert determination for the resolution of international commercial disputes between private parties. The Center's procedures are designed as efficient and inexpensive alternatives to court proceedings and may take place in any country, in any language and under any law.

- **Domain name dispute resolution**

The WIPO Arbitration and Mediation Center (see webpage <http://www.wipo.int/amc/en/>) is internationally recognized as the leading dispute resolution service provider for challenges related to abusive registration and use of Internet domain names, a practice commonly known as "cybersquatting." Applicable to all international domains and a growing number of country code domains, the resolution procedure is conducted in electronic format and results in enforceable decisions within two months.

- **International classifications**

Applicants for national or international IP protection are required to determine whether their creation is new or is owned or claimed by someone else. To determine this, huge amounts of information must be searched. International classification systems (see webpage <http://www.wipo.int/classifications/en/>) facilitate such searches by organizing information concerning inventions, trademarks and industrial designs into indexed, manageable structures for easy retrieval.

- **Protection of State emblems (Article 6ter of the Paris Convention)**

The protection of State emblems, and names, abbreviations and emblems of international intergovernmental organizations is governed by Article 6ter (see webpage <http://www.wipo.int/article6ter/en/>) of the Paris Convention, administered by WIPO.

A.1.4 WIPO global network on Intellectual Property (IP) Academies

See webpages <http://www.wipo.int/academy/en/> and http://www.wipo.int/academy/en/about/startup_academies/, which contains the following information:

The WIPO Academy is the core entity in WIPO for training and human capacity-building activities, particularly for developing countries, least-developed countries (LDCs) and countries in transition.

Contact the WIPO Academy using the webpage <http://www.wipo.int/contact/en/area.jsp?area=academy>

A.2 Anti-Counterfeiting Trade Agreement (ACTA)

A.2.1 ACTA

For more information, see the information on the Office of the US Trade Representatives (see webpage <https://ustr.gov/acta>) where the final text of the agreement can be found at http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf

The agreement aims to establish an international legal framework for targeting counterfeit goods, generic medicines and copyright infringement on the Internet, and would create a new

governing body outside existing forums, such as the World Trade Organization, the World Intellectual Property Organization, and the United Nations.

The agreement was initially signed in October 2011 by Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea, and the United States. In 2012, Mexico, the European Union and 22 countries which are member states of the European Union signed it as well. One signatory (Japan) has ratified (formally approved) the agreement, which would come into force in countries that ratified it after ratification by six countries (see Clause A.2). However, the EU withdrew from the agreement in July 2012.

A.2.2 Global Anti-Counterfeiting Network (GACG)

The GACG is an informal network of national and regional IP protection and enforcement organizations which have a strong international dimension to their activities. There are currently 21 members covering 40 countries plus direct informal contacts with many other national and industry associations. The objectives are to exchange and share best practices and information and to participate in appropriate joint activities to solve IPR enforcement challenges (see webpage <http://www.gacg.org/>).

A.3 World Semiconductor Council (WSC) and GAMS

The webpage is <http://www.semiconductorcouncil.org/> where the following information is available:

"The World Semiconductor Council (WSC) is an international forum that brings together industry leaders to address issues of global concern to the semiconductor industry. Comprised of the semiconductor industry associations (SIAs) of the United States, Korea, Japan, Europe, China and Chinese Taipei, the goal of the WSC is to promote international cooperation in the semiconductor sector in order to facilitate the healthy growth of the industry from a long-term, global perspective.

It also supports expanding the global market for information technology products and services and promoting fair competition, technological advancement, and sound environmental, health and safety practices.

WSC activities shall be undertaken on a voluntary basis and shall be guided by principles of fairness, respect for market principles, and consistency with WTO rules and with laws of the respective countries or regions of each Member. The WSC recognizes that it is important to ensure that markets will be open without discrimination. The competitiveness of companies and their products should be the principal determinant of industrial success and international trade."

Reference: "Agreement Establishing a New World Semiconductor Council", June 10, 1999; Brussels, Belgium.

WSC meets annually. At the May 2017 meeting, the WSC agreed to intensify counterfeiting activities through its anti-counterfeit task force. At the May 2015 Hangzhou China meeting, WSC recognised the importance of trade secret protection. Members have agreed a set of 'core' elements in model trade secret legislation and are calling for government authorities including GAMS to support the core elements.

GAMS has members from the Semiconductor Industries Associations in China, Chinese Taipei, EU, Japan, USA and Korea. The Joint Statement is reviewed every five years. The Joint Statement provides for industry to make reports and recommendations to governments on policies that may affect the future outlook and competitive conditions within the global semiconductor industry through a CEO-level World Semiconductor Council (WSC). Topics under discussion include counterfeit prevention issues. The 2009 meeting affirmed the members' agreement to undertake enforcement measures against semiconductor

counterfeiting. The European Semiconductor Industry Association (ESIA) (see Clause A.3) is chair of the counterfeit committee. This committee has recently published a white paper on anti-counterfeit measures (see 4.7.7 and Clause A.3) and has excluded DNA fingerprint marking of components as a viable technique to mitigate against anti-counterfeiting (see 4.5.4.4). The October 2014 meeting was held in Fukuoka Japan and GAMS continues to work with the WSC to eliminate counterfeits from the supply chain. Recently ESIA has seized a large amount of counterfeit components, working with EU customs operations and 12 EU member states in 2016.

The WSC anti-counterfeit task force (ACTF) is working to eliminate counterfeits from the semiconductor market and has published a white paper in May 2014 "Winning the battle against counterfeit semiconductor products".

The webpage provides links to the Semiconductor Industry Associations from China, Chinese Taipei, Europe, Japan, Korea and the USA which are all members of the World Semiconductor Council. The webpage <http://www.semiconductorcouncil.org/about-wsc/members/> provides information on WSC membership.

The Semiconductor Industry Association USA webpage for viewing their statements on anti-counterfeit is: http://www.semiconductors.org/issues/anticounterfeiting/anti_counterfeiting/

The European Electronic Semiconductor Industry Association (EECA) is chair of the counterfeit committee (see webpage <http://www.eusemiconductors.eu/esia/home>). Their counterfeit webpage is <https://www.eusemiconductors.eu/esia/public-policy/anti-counterfeiting>

A.4 SEMI

SEMI global headquarters are located at 673 South Milpitas Blvd. Milpitas, CA 95035, USA (tel: +1 408 943 6900) (see webpage <http://www.semi.org/About/ContactUs>). SEMI is a global industry association serving the manufacturing supply chain for the micro and nano-electronics industries with worldwide offices, see webpage <http://www.semi.org/en/About/> where the following information is found:

"SEMI is the global industry association serving the manufacturing supply chain for the micro-and nano-electronics industries, including:

- Semiconductors – Device Manufacturers, Equipment, Material and other Service Providers
- Flexible, Hybrid and Printed Electronics
- Micro-ElectroMechanical Systems (MEMS)
- Sensors
- High-Brightness LED
- Photovoltaics (PV)
- Flat Panel Display (FPD)
- Related micro- and nano-electronics

The industries, companies, and people SEMI represents are the architects of the electronics revolution. SEMI members are responsible for the innovations and technologies that enable smarter, faster, more powerful, and more affordable electronic products and devices that bring the power of the digital age to more people every day.

For more than 40 years, SEMI has served its members and the industries it represents through programmes, initiatives, and actions designed to advance business and market growth worldwide. SEMI supports its members through a global network of offices, activities, and events in every major electronics manufacturing region around the world.

Our purpose:

The industries that comprise the microelectronics supply chain are increasingly complex, capital intensive, and interdependent. Delivering cutting-edge electronics to the marketplace requires:

- Construction of new manufacturing (fabrication) facilities;
- Development of new processes, tools, materials, and manufacturing standards;
- Advocacy and action on policies and regulations that encourage business growth;
- Investment in organizational and financial resources;
- Integration across all segments of the industry around the world;
- Addressing these needs and challenges requires organized and collective action on a global scale.

SEMI facilitates the development and growth of our industries and manufacturing regions by organizing regional trade events (expositions), trade missions, and conferences; by engaging local and national governments and policy makers; through fostering collaboration; by conducting industry research and reporting market data; and by supporting other initiatives that encourage investment, trade, and technology innovation.

In addition to supporting access to regional markets, SEMI helps its members explore diversified business opportunities and contributes to the growth and advance of emerging and adjacent technology markets."

The SEMI Intellectual Property webpage

<http://www.semi.org/en/Issues/IntellectualProperty/> provides further information.

Also see webpage <http://ams.semi.org/ebusiness/standards/semistandard.aspx?volumeid=17> for a list of published specifications.

A.5 Electronics Authorized Directory

The Electronics Authorized Directory had a website for searching for Authorised Component Distributors, but this is now operated by the ECIA, see A.8.7.

A.6 UK

A.6.1 The UK intellectual property office

The interactive webpage is <http://www.ipo.gov.uk/>

This website contains information to decide what type of IP protection is required:

- Patents (see webpage <https://www.gov.uk/intellectual-property/patents>) which are *discussed with details about how to apply for a patent and manage them. Details are also provided for using other people's patents and patent infringement.*
- Trademarks (see webpage <https://www.gov.uk/intellectual-property/trade-marks>) which are discussed with details of how to apply and manage these. Details are also provided for other people's trademarks and trademark infringement.
- Designs (see webpage <https://www.gov.uk/intellectual-property/designs>) which are discussed with details of how to apply to register a design.
- Copyright (see webpage <https://www.gov.uk/intellectual-property/copyright>) which is discussed with details of ownership and how to legally apply to use other people's copyright works.

Also see the in-line tool at webpage www.ipo.gov.uk/iphealthcheck. This tool provides information related to how to use intellectual property for protecting the business and answers to typical IP questions.

The UK Information Centre will also be able to assist, tel: 0300 300 2000 within the UK or 44 (0)1633 814000 outside of the UK or e-mail enquiries@ipo.gov.uk

A.6.2 Alliance for IP

The Alliance for Intellectual Property is located at 2nd Floor, Riverside Building, County Hall, Westminster Bridge Road, London, SE1 7JA, phone +44 020 7803 1319, see webpage <http://www.allianceforip.co.uk/> where the following information is found:

"Established in 1998, the Alliance Against Intellectual Property (IP) Theft is a UK-based coalition of 20 associations and enforcement organizations with an interest in ensuring intellectual property rights receive the protection they need and deserve. Our members include representatives of the audio-visual, music, video games and business software, and sports industries, branded manufactured goods, publishers, authors, retailers and designers."

A.6.3 UK Chartered Trading Standards Institute

The Chartered Trading Standards Institute (see webpage <http://www.tradingstandards.uk/>) has the following information:

"CTSI represents trading standards professionals working in the UK and overseas – in local authorities, business and consumer sectors and central government.

CTSI exists to:

- promote and protect the success of a modern vibrant economy, and
- safeguard the health, safety and wellbeing of citizens by enhancing the professionalism of its members".

A.6.4 UK HM Revenue and Customs

HM Revenue and Customs has a webpage: www.hmrc.gov.uk. For IP rights see webpage http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageLibrary_ShowContent&id=HMCE_CL_000244&propertyType=document and webpage <https://www.gov.uk/fraud-and-international-trade>.

The following means allow to report fraud including counterfeit items:

- UK custom hotline 0800 788 887:
- Webpage <https://www.gov.uk/government/news/hmrc-launches-new-fraud-hotline>; or
- On-line digital form located on webpage <https://www.gov.uk/report-an-unregistered-trader-or-business>.

A.6.5 Anti-Counterfeiting Forum

The ESCO Anti-Counterfeiting Forum is now the Anti-counterfeiting Forum , see webpage <http://www.anticounterfeitingforum.org.uk/counterfeiting.aspx>, and provides guidance on how to avoid counterfeit components.

Reports of suspect counterfeit items can be reported on this webpage and accessed by members. This webpage provides the UK customs hotline for reporting counterfeit items: 0800 788 887

A.6.6 Electronic Component Supplier Network (ESCN)

The Electronic Component Supplier Network (see webpage <http://www.ecsn-uk.org/>) is a member managed, not-for-profit trade association based in the UK which supports counterfeit avoidance measures.

A.6.7 UK Ministry of Defence

Guidance for MOD delivery teams on the avoidance of fraudulent and counterfeit material is provided on the interactive webpage:

https://www.aof.mod.uk/aofcontent/tactical/quality/content/counterfeitavoid/counterfeit.htm?zoom_highlight=Counterfeit.

NOTE Registration (as a “civilian” to the “AOF (Acquisition Operating Framework)”) is necessary to access the website.

Reporting should be directed at the Defence Irregularity Reporting Cell (DIRC) using e-mail: DIRCellMailbox@mdpga.mod.uk

A new high level anti-counterfeit training video has recently been created and is available for use by industry.

A.7 Europe

A.7.1 Europa Summaries of EU Legislation

- The ‘Fight against Fraud’ webpage linking to the ‘Fight against counterfeiting’ webpage is http://eur-lex.europa.eu/summary/chapter/fight_against_fraud.html?root_default=SUM_1_CODED%3D22,SUM_2_CODED%3D2203&obsolete=false
- The Europa webpage for the EU Taxations and Customs Union entitled ‘How can right holders protect themselves from counterfeiting and piracy’ provides details and forms for reporting counterfeit activities, see webpage http://ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/right_holders/index_en.htm
- See the following Europa webpage for the published ACTA http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf

A.7.2 Europol, the European Law Enforcement Agency

See webpage <https://www.europol.europa.eu/content/page/about-us>

Europol is the European Union’s law enforcement agency whose main goal is to help achieve a safer Europe for the benefit of all EU citizens. Europol does this by assisting the European Union’s Member States in their fight against serious international crime and terrorism.

The Europol Counterfeit Goods webpage is <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime/counterfeit-goods>

A.7.3 European Patent Office

See the interactive webpage <http://www.epo.org/>. (phone +00 800 80 20 20 20), where a search or application can be made.

A.7.4 EUIPO

See webpage <https://euipo.europa.eu/ohimportal/en/> to access the trademark webpage for information regarding the ‘Community Trade Mark’ applicable to all EU member states.

Trademarks are discussed at webpage <https://euipo.europa.eu/ohimportal/en/trade-marks> which contains the following information:

"A trade mark may consist of any signs capable of being represented graphically, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings."

"Why register your trade mark?"

A trade mark has three essential functions:

- it identifies the origin of goods and services;
- it guarantees consistent quality by showing an organization's commitment to its users and consumers;
- it is a form of communication, a basis for publicity and advertising.

A trade mark can become one of the most important assets of a company.

Trade mark registration is one of the strongest ways to defend a brand; a way to ensure that no one else uses it. If you do not register your trade mark, others may do so and acquire your rights to distinguish their goods and services.

Trade marks influence consumer decisions every day. A strong trade mark creates an identity, builds trust, distinguishes you from the competition, and makes communication between seller and buyer simpler. Because so much money and time is often invested in a trade mark, it is worth paying something to protect it from misuse.

What is a good or a service?

In law, a good is any kind of item which may be traded. A service is the provision of activities in accordance with human demands.

What is the difference between a trade mark and other industrial property rights such as patents and designs?

All industrial property rights are intended to protect the creativity of businesses and individuals. However, they do not cover the same aspects.

A trade mark identifies the origin of goods and services of one undertaking so as to differentiate them from those of its competitors.

A design covers the appearance of a product. A design cannot protect the function of a product.

A patent covers the function, operation or construction of an invention. To be patentable, a function must be innovative, have an industrial application and be described in such a way as to permit reproduction of the process."

A.7.5 European Aviation Safety Agency (EASA)

The European Aviation Safety Agency is located at Ottoplatz 1, D-50679 Koeln, Germany, tel +49 221 8999 000, info@easa.europa.eu and has a webpage <http://www.easa.europa.eu/>. EASA controls Design Organisation Approvals (DOA), Production Organisations Approvals (POA) and Maintenance Organisations Approvals (MOA).

EASA publishes Safety Information Bulletins on webpage <http://ad.easa.europa.eu/sib-docs/page-1>.

A.7.6 IECQ audit schemes

The IECQ is the assessment side of the IEC (see IECQ WG06 Counterfeit avoidance webpage <http://www.iecq.org/workgroups/wg06/>).

IECQ Working Group 6 (WG6) is establishing audit rules of procedure and auditor training requirements for Certifying Bodies such as BSI, DNV, etc., to operate Third Party SAE and IEC anti-counterfeit schemes which include:

- 1) SAE AS6081 auditing for non-franchised distributors which offer components with some testing to their customers which include the DLA;
- 2) SAE AS5553 auditing;
- 3) IEC 62668-1 for avionics OEMs, which can use SAE AS5553 compliance towards IEC 62668-1 compliance
- 4) new traceability audit IECQ OD 3702 whereby the part number required (and original manufacturer) is compared against the part number and source ordered from to the part number and source received, checking that all data matches and that there is sufficient traceability in the supply chain to eliminate potential counterfeits and fraudulent recycled components.

A.7.7 BEAMA

BEAMA is the independent expert knowledge base and forum for the electro-technical industry for the UK and across Europe. Representing over 300 manufacturing companies in the electro-technical sector, the organisation has significant influence over UK and international political, standardisation and commercial policy (see webpage <http://www.beama.org.uk/about-beama.html> and webpage <http://www.beama.org.uk/anti-counterfeiting-working-group.html> for anti-counterfeit activities).

Also see webpage <http://www.counterfeit-kills.co.uk/uk/index.php> which has access to an excellent on-line video at webpage <http://www.youtube.com/embed/11SAAiiGX08?rel=0>

A.8 USA

A.8.1 United States Patent and Trademark Office

The United States patent and Trademark office (USPTO) is headquartered at: Madison Buildings (East and West), 600 Dulany Street, Alexandria, VA 22314, USA, phone: 1-800-786-9199. The USPTO has many customer support centres which can be found on their webpage.

The USPTO website is <http://www.uspto.gov/>.

- Patents: see which at webpage <https://www.uspto.gov/patents-getting-started/general-information-concerning-patents> contains the following information:

“What is a patent?

A patent for an invention is the grant of a property right to the inventor, issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions. Under certain circumstances, patent term extensions or adjustments may be available.

The right conferred by the patent grant is, in the language of the statute and of the grant itself, “the right to exclude others from making, using, offering for sale, or selling” the invention in the United States or “importing” the invention into the United States. What is granted is not the right to make, use, offer for sale, sell or import, but the right to exclude others from making, using, offering for sale, selling or importing the invention. Once a patent is issued, the patentee must enforce the patent without aid of the USPTO.

There are three types of patents

- Utility patents may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof. Design patents may be granted to anyone who invents a new, original, and ornamental design for an article of manufacture; and
- Plant patents may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant."
- Trademarks: see webpage: <http://www.uspto.gov/trademarks/index.jsp>

A.8.2 The International Trade Administration, US Department of Commerce

The International Trade Administration, U.S. Department of Commerce [Stopfakes.gov](https://www.stopfakes.gov) has a webpage <https://www.stopfakes.gov/welcome> which contains very useful information for protecting IP.

A.8.3 International Intellectual Property Alliance

See webpage <https://iipa.org/> where the following information is provided:

"The International Intellectual Property Alliance (IIPA) is a private sector coalition, formed in 1984, of trade associations representing U.S. copyright-based industries in bilateral and multilateral efforts working to improve international protection and enforcement of copyrighted materials and open up foreign markets closed by piracy and other market access barriers.

IIPA's five member associations represent over 3,200 U.S. companies producing and distributing materials protected by copyright laws throughout the world—all types of computer software, including entertainment software (interactive games for videogame consoles, handheld devices, personal computers and the Internet), and educational software; theatrical films, television programs, DVDs and home video and digital representations of audio visual works; music, records, CDs, and audiocassettes; and fiction and non-fiction books, education instructional and assessment materials, and professional and scholarly journals, databases and software in all formats. Members of the IIPA include Association of American Publishers, Entertainment Software Association, Independent Film & Television Alliance, Motion Picture Association of America, and Recording Industry Association of America. The U.S. copyright-based industries are one of the fastest-growing and most dynamic sectors of the U.S. economy. Inexpensive and accessible reproduction and transmission technologies, however, make it easy for copyrighted materials to be pirated in other countries. IIPA and its member associations, working with U.S. government, each foreign government, and local rights holder representatives, analyse copyright laws and enforcement regimes in countries around the globe and seek improvements that will foster technological and cultural development in these countries, deter piracy, and improve market access, all of which encourages local investment, creativity, innovation and employment. As technology rapidly changes, IIPA is working to ensure that high levels of copyright protection and effective enforcement become a central component in the legal framework for the growth of global electronic commerce. Strong protection and enforcement, both in-law and in-practice, against the theft of intellectual property are essential for achieving the full economic and social potential of global e-commerce."

A.8.4 The Federal Aviation Administration (FAA)

A.8.4.1 General

The FAA is located at 800 Independence Avenue, SW Washington, DC 20591, and has an interactive website, see webpage <http://www.faa.gov/>.

A.8.4.2 FAA engines approvals

The FAA identification and registration marking requirements webpage for engines is http://www.faa.gov/aircraft/air_cert/design_approvals/engine_prop/engine_approvals/

A.8.4.3 FAA aviation safety hotline office

The webpage <https://hotline.faa.gov/> contains an on-line reporting form to be used to report safety concerns.

A.8.5 Trusted Access Program Office (TAPO)

The Trusted Access Program Office (TAPO) webpage is <https://www.dmea.osd.mil/tapo.html> where the following information is found:

"US Government acquisition programs must actively manage their IC supply chains, anticipate potential threats posed by outsourcing practices, formally assess their system's vulnerabilities and employ trusted suppliers and/or pursue other means of risk mitigation. Trust is defined as 'the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components'.

The Trusted Access Program Office (TAPO) has been chartered by the U. S. Government to find and maintain suppliers of trusted microelectronic parts. TAPO has successfully developed a reliable source of parts that gives the Intelligence Community needed access to state of the art commercial processes, fabrication tools and fabrication services. In so doing, TAPO has effective cost-avoidance advantages by not having to upgrade or replace government owned wafer fabrication tools. TAPO has made it possible for the Intelligence Community to design and obtain advanced mission critical systems via commercial, state of the art manufacturing processes. Finally, TAPO's long term contract assures long term access to the latest and most capable commercial IC technologies in the world.

TAPO has established a contractual relationship with GLOBALFOUNDRIES U.S. 2 LLC (GFUS2) to produce advanced microelectronics parts in a trusted environment. GFUS2 maintains domestic facilities, providing capabilities to the government with yearly options through fiscal year 2023. Other facilities are currently under review including sources for design, packaging, test and fabrication. TAPO is entering its fourth year of operation, in support of the US Government. TAPO brokers cost-effective access to trusted suppliers of customized leading edge microelectronic technologies in order to improve the security of mission-critical U.S. Government information and operations.

TAPO resources are made available for government use only and therefore access requests require a valid government sponsor."

TAPO has accredited suppliers which are listed at webpage <https://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf>. The Defense Microelectronics Activity (DMEA) provides microelectronics technology solutions and addresses complex microelectronics issues such as obsolescence. The DMEA Trusted IC Supplier Accreditation Program webpage is: <http://www.dmea.osd.mil/> where the Trusted IC webpage is found at webpage <http://www.dmea.osd.mil/trustedic.html> which supports DoD Instruction 5200.44 and DODI 5200.39. The Defense Microelectronics Activity (DMEA), which provides microelectronics technology solutions, has been designated by the Department of Defense as the accrediting authority for this program. Send questions or comments to TrustedIC@dmea.osd.mil or call (916) 231-1514 for more information on trusted electronic components suppliers.

A.8.6 Independent Distributors of Electronics Association (IDEA)

The Independent Distributors of Electronics Association (IDEA) organisation is located at 2250 Double Creek Drive #6474, Round Rock, TX 78683-0061, USA, phone: 714-670-0200. See webpage <http://www.idofea.org/> where the following information is available:

"The Independent Distributors of Electronics Association (IDEA) is a global trade association comprised of organizations dedicated to quality initiatives that provide Responsible Procurement Solutions™ to the supply chain.

IDEA employs a comprehensive approach that focuses on programs and best practices that establish and increase quality standards, provide industry with a conduit to improve the access to and sharing of relevant knowledge, and advance industry ethics and integrity.

The foundation of these solutions resides within the sustained leadership in the implementation of quality standards, certifications, best practices, and counterfeit detection methods as well as the cooperation and education of all stakeholders responsible for procurement and inspection practices and policies. IDEA seeks to fulfil this mission through the development and dissemination of relevant standards, training, and certification programs.”

IDEA hosts a series of IDEA-STD-1010 USA based training courses.

A.8.7 ECIA formerly National Electronic Distributors Association (NEDA)

The Electronic Component Industry Association in North America is located at 310 Maxwell Road. Suite 200, Alpharetta, GA 30005, USA, phone: 678-393-9990. See webpage <http://www.ecianow.org/> which contains the following information:

“ECIA provides resources and opportunities for members to improve their business performance while enhancing the industry’s overall capacity for growth and profitability. From driving critical conversations and process optimization to product authentication and industry advocacy, ECIA is your trusted source for support, insight and action.

Bringing together the talent and experience of broad array of industry leaders and professionals representing all facets of the electronics components supply chain, ECIA is uniquely positioned to enable individual connection as well as industry-wide collaboration. As the supply chain becomes increasingly more complex, ECIA serves as a vital nexus for refinement and progress.

Expansion and uncertainty seem to be the only true constants in the electronics industry today. In this dynamically shifting environment, reliable market intelligence is at a premium. Because ECIA’s members are the marketplace, we provide a level of visibility into the supply chain otherwise unavailable. From individual anecdotes gleaned from conversations at an ECIA event, to our exclusive market reports, we help keep you in the know.

As an organization made up of the leading electronic component manufacturers, their manufacturer representatives and authorized distributors, ECIA members share a common goal of promoting and improving the business environment for the authorized sale of electronic components to the end customer. In doing so, we contribute to making the Americas region more competitive in the design and production of electronic goods.”

Documents such as NIGP best practices and guidelines can be downloaded from their webpage <http://www.ecianow.org/standards-practices/general-best-practices-guidelines/>. Visit <http://www.eciaauthorized.com/> the only US industry’s website that fully supports authorized distribution with an easy-to-use tool to find available inventory from authorized sources. The search results are random, unbiased and not influenced by advertising.

Advocacy efforts:

The ECIA supported SAE AS6496 and has a created dedicated webpage for this, see <http://www.ecianow.org/industry-issues/sae-as6496-anti-counterfeiting-standard-3/>

The industry advocacy effort delivers the message that electronic component users and buyers can’t go wrong dealing with supplier authorized distributors. The campaign features a significant online presence every month to grab the attention of prospective customers.

A.8.8 Components Technology Institute Inc. (CTI)

CTI is a multi-discipline company providing engineering and consulting services, training courses, and component conferences, see webpage <http://www.cti-us.com/CCAP.htm>. Its counterfeit components avoidance program (CCAP) has developed the CCAP-101 certified program for use by independent distributors to detect and avoid the delivery of counterfeit electronic components to their customers.

CCAP-101 certified independent distributors are listed on webpage <http://www.cti-us.com/CCAPCertifiedDist.htm> The CTI contact address is:

2608 Artie St., Suite 4
Huntsville, AL 35805
Tel: 256-536-1304
Fax: 256-536-1308
CTIinc.82@gmail.com

A.8.9 Defense Logistics Agency (DLA)

The DLA audits non-franchised distributors to SAE AS6081 which combine accepted counterfeit mitigation practices with quality assurance processes for selected Federal Stock Class (FSC) 5961 and 5962 electronic microcircuits and, if successful, lists the distributor on the Qualified Testing Suppliers List (QTSL), see webpage https://landandmaritimeapps.dla.mil/Offices/Sourcing_and_Qualification/qtsl.aspx

where approximately 26 USA based distributors are listed.

The DLA also operates the Qualified Suppliers List of Distributors (QSLD) program for 5961 and 5962 electronic microcircuits, see webpage https://landandmaritimeapps.dla.mil/offices/sourcing_and_qualification/offices.aspx?Section=QSL

The DLA now maintains a list of commercial laboratories suitable for testing military devices (see https://landandmaritimeapps.dla.mil/offices/sourcing_and_qualification/labsuit.aspx).

The DLA has now abandoned the application of the deoxyribonucleic acid (DNA) marking due to industry objections. The Appraisal of Select Provisions of US FY 2013 National Defense Authorization Act, "Section 807: Item-Unique Identification requirements", that discusses the new DLA DNA marking scheme for 5962 microcircuits, can be viewed on webpage <http://www.rjo.com/PDF/FederalContractsReport-01082013.pdf>.

The DLA hotline number for reporting suspected fraud, waste, abuse or mismanagement is 0001 800 411-9127 (see <http://www.dla.mil/HQ/InspectorGeneral/Business/Hotline.aspx>).

A.8.10 DFARS

DFARS 252.246-7007 and DFARS 252.246-7008, Contractor Counterfeit Electronic Part Detection and Avoidance System, can be found on webpage: <https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>

See webpage http://www.acq.osd.mil/dpap/dars/case_status.html for DFARS case status.

There are DFARS supplements, DFARS Case 2016-D013 and DFARS Case 2016-D010 which address respectively sources of electronic parts and costs related to counterfeit electronics parts.

A.8.11 IAQG

The IAQG (see webpage <http://www.sae.org/iaqg/>), is affiliated to the SAE and provides a forum for collaboration within the aviation, space and defence companies. There are several initiatives including:

- the online OASIS database for looking up the latest AS/EN/JISQ 9100, AS/EN/JISQ 9110 and AS/EN/JISQ 9120 certificates (see webpage <https://www.iaqg.org/oasis/login>);
- an interactive Supply Chain Management Handbook (SCMH) which is being expanded to include a new section on anti-counterfeit guidance.

A.8.12 USA Homeland Security

The USA Homeland Security has released a recent 'Joint Strategic Plan on Intellectual Property Enforcement (FY 2017-2019)' report titled 'Supporting innovation, creativity and enterprise, charting the path ahead' which is available at the following webpage: <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2016jointstrategicplan.pdf>.

A.9 China

A.9.1 CNIPA

See the interactive webpage <http://english.sipo.gov.cn/> and <http://www.chinaipr.gov.cn/>.

A.9.2 Chinese Patent and Trademark Office

See the webpage <http://www.chinatrado.com/> where further information can be found.

A.9.3 China Electronics Associations

Select search engines that translate Chinese into English:

- The China Electronics Corporation (CEC) is located at: Building A, Tri-Tower, No 66-1 Zhongguancun, Haidian District, Beijing, 100190 The CEC webpage is <http://en.cec.com.cn/index.html>
- China Electrical Equipment Industry Association (CEEIA), is located at Fengtai District, Building 30, No. 188, No. 188, South Fourth Ring Road, Beijing, Zip code: 100070; see <https://translate.google.com/translate?hl=en&sl=zh-CN&u=http://www.ceeia.com/&prev=search>
- China Electronics Standardization Institute (CESI), see webpage <http://www.cc.cesi.cn/english.aspx>

A.9.4 China Quality Certification Centre (CQC)

CQAE is located at Section 9, No. 188, Nansihuan (the South Fourth Ring Road), Xilu (West Road), Beijing, 100070, see webpage <http://www.cqc.com.cn/www/english/>

A.9.5 Civil Aviation Administration of China (CAAC)

CAAC, is located at NO.155 Dongsu West Avenue, Dongcheng District, Beijing 100710, PRC (see webpage <http://www.caac.gov.cn/en/SY/>).

A.9.6 China lawinfo.Co Ltd., for Law info China

See webpage <http://www.lawinfochina.com/>. It is a hi-tech legal company, established by Peking University, to develop Chinese laws in electronic database format also available in English.

For other information, see webpage <http://www.chinatradeoffice.com/index.php/tdreg/>

A.10 Japan – Japanese Patent Office (JPO)

The Japanese Patent Office (JPO) is located at 3-4-3- Kasumigaseki, Chiyoda-ku Tokyo, 100-8915, Japan. The e-mail address for industrial property system questions is PA0842@jpo.go.jp.

The JPO interactive webpage is <http://www.jpo.go.jp/> where patents, trademarks and designs can be registered.

A.11 Physical unclonable function

See webpage https://en.wikipedia.org/wiki/Physical_unclonable_function where the following is extracted:

A **physical unclonable function**, or **PUF**, is a “digital fingerprint” that serves as a unique identity for a semiconductor device such as a microprocessor. PUFs are based on physical variations which occur naturally during semiconductor manufacturing, and which make it possible to differentiate between otherwise identical semiconductors. PUFs are usually utilized in [cryptography](#). A physical unclonable function (sometimes also called **physically unclonable function**) is a physical entity that is embodied in a physical structure. Today, PUFs are usually implemented in [integrated circuits](#) and are typically used in applications with high security requirements

Early references about systems that exploit the physical properties of disordered systems for authentication purposes date back to Bauder in 1983 and Simmons in 1984. Naccache and Frémanteau provided an authentication scheme in 1992 for memory cards. The terms POWF (physical one-way function) and PUF (physical unclonable function) were coined in 2001 and 2002, the latter publication describing the first integrated PUF where unlike PUFs based on optics, the measurement circuitry and the PUF are integrated onto the same electrical circuit (and fabricated on silicon).

From 2010 to 2013, PUF gained attention in the smartcard market as a promising way to provide “silicon fingerprints”, creating cryptographic keys that are unique to individual smartcards.

PUFs are now established as a secure alternative to battery-backed storage of secret keys in commercial FPGAs, such as the Xilinx Zynq Ultrascale++ and Altera.

PUFs depend on the uniqueness of their physical microstructure. This microstructure depends on random physical factors introduced during manufacturing. These factors are unpredictable and uncontrollable, which makes it virtually impossible to duplicate or clone the structure.

Rather than embodying a single cryptographic key, PUFs implement challenge–response authentication to evaluate this microstructure. When a physical stimulus is applied to the structure, it reacts in an unpredictable (but repeatable) way due to the complex interaction of the stimulus with the physical microstructure of the device. This exact microstructure depends on physical factors introduced during manufacture which are unpredictable (like a fair coin). The applied stimulus is called the challenge, and the reaction of the PUF is called the response. A specific challenge and its corresponding response together form a challenge–response pair or CRP. The device's identity is established by the properties of the microstructure itself. As this structure is not directly revealed by the challenge-response mechanism, such a device is resistant to spoofing attacks.

Using a fuzzy extractor or key extractor PUFs can also be used to extract a unique strong cryptographic key from the physical microstructure. The same unique key is reconstructed every time the PUF is evaluated. The challenge-response mechanism is then implemented using cryptography.

PUFs can be implemented with a very small hardware investment. Unlike a ROM containing a table of responses to all possible challenges, which would require hardware exponential in the number of challenge bits, a PUF can be constructed in hardware proportional to the number of challenge and response bits. In some cases PUFs can even be built from existing hardware with the right properties.

Unclonability means that each PUF device has a unique and unpredictable way of mapping challenges to responses, even if it was manufactured with the same process as a similar device, and it is infeasible to construct a PUF with the same challenge–response behavior as another given PUF because exact control over the manufacturing process is infeasible. Mathematical unclonability means that it should be very hard to compute an unknown response given the other CRPs or some of the properties of the random components from a PUF. This is because a response is created by a complex interaction of the challenge with many or all of the random components. In other words, given the design of the PUF system, without knowing *all* of the physical properties of the random components, the CRPs are highly unpredictable. The combination of physical and mathematical unclonability renders a PUF truly unclonable.

Because of these properties PUFs can be used as a unique and untamperable device identifier. PUFs can also be used for secure key generation and storage as well as for a source of randomness.

A.12 PUF and tags initiative and solutions

A.12.1 The Hardware Intrinsic Security (HIS) initiative

See the website <https://www.intrinsic-id.com/about/> where the following information is available:

“About Intrinsic ID’

Mission:

“Our mission is to authenticate everything and everyone and make the connected world safer. Our silicon SRAM PUF technology can be applied to almost any chip, from tiny microcontrollers to high performance FPGAs. Our fuzzy extractor can turn noisy data like a fingerprint or SRAM PUF into secure cryptographic keys and reliable identifiers.”.

Partners include: Intel, NXP, TSMC, Microsemi, Renesas, ARM, Coherent Logic, SELEX.

Various white papers are available to download at webpage <https://www.intrinsic-id.com/resources/white-papers/> for example on ‘The reliability of SRAM PUF’.

Also semiconductor manufacturers are now embedding PUF features in their new designs, for example Altera Stratix 10 with Intrinsic ID’S PUF technology.

A.12.2 Examples of tag providers

- a) The company Verayo, which is located at 1054 S. De Anza Blvd, Suite 201, San Jose, CA 95129, USA, tel 408-996-0352 has a webpage <http://www.verayo.com/> where the following information is found:

“Verayo develops solutions based on its proprietary PUF technology to revolutionize digital authentication of products, people and machine. We provide complete

authentication solutions. Our solutions include: unclonable chips, authentication software, consumer engagement, back-end data analysis enabling platforms and key generation.

Since its founding in 2005, our team has designed, built, and tested silicon chips based on its PUF technology and built-up a growing body of additional Intellectual Property (IP) and substantive know-how beyond the core technology that Verayo licensed from MIT. Verayo is funded by Khosla Ventures and has assembled an experienced advisory board drawn from the semiconductor, mobile and security industries. In the past year, the company has also deepened its relationships with US Department of Defense agencies and has received multiple contracts.”.

- b) The company ProofTag, which is located at 1100, Avenue de l'Europe, F-82 000 Mountauban, France, tel: +33 (0)5 63 21 10 50 and has a webpage <http://www.prooftag.net/bubble-tag/> develops security solutions to guarantee product and document authenticity and traceability based on one of the most reliable authentication systems in the world, the Bubble Tag™, now complemented by the Fiber Tag™ which is an intrinsic authentication solution for printed labels and documents.

ProofTag has been deploying solutions since 2004 to protect brands (wines, spirits, watches, jewelry, cosmetics, electronic goods, etc.), to guarantee document authenticity (diplomas and customs, financial, voting, identity documents, etc.) and fiscal stamps (cigarettes, spirits, beers).

The high level of security conferred by the Bubble Tag™ has further strengthened ProofTag's legitimacy worldwide. For instance, ProofTag has been approved by the Chinese authorities (CATA – China Anti-Counterfeiting Technology Association) for its anti-counterfeiting technology.

A.13 Examples of tamper-proof design companies

See for example:

- CCL Design Electronics, 4 Redwood Crescent, East Kilbride, Glasgow, UK at webpage <https://www.ccldesignelectronics.com/Brand-Protection-Authentication.aspx>
- Xilinx which provides design security solutions for their FPGA microcircuit products at webpage <http://www.xilinx.com/products/technology/design-security.html>

A.14 Examples of FPGA die serialization

- Xilinx device DNA security feature, see webpage <http://www.xilinx.com/products/technology/design-security.html>

A.15 Examples of NVRAM manufacturers

- Cypress semiconductor NVRAMs, see webpage <http://www.cypress.com/?id=65&source=products>.

A.16 SAE G-19

SAE International (see webpage <http://www.sae.org/>), is a global organisation of more than 128 000 engineers and related technical experts in the aerospace, automotive and commercial-vehicles industries.

The SAE G-19 Counterfeit Electronic Parts committee (see webpage <http://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG19>) has published the following documents:

- **SAE AS5553B³**, Counterfeit Electrical, Electronic and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation and Disposition

The scope is as follows:

This standard is for use by organizations that procure and/or integrate EEE parts and/or assemblies containing such items. The requirements of this standard are generic and intended to be applied/flowed down, as applicable, through the supply chain to all organizations that procure EEE parts and/or assemblies, regardless of type, size, and product provided. The mitigation of counterfeit EEE parts in this standard is risk-based and these mitigation steps will vary depending on the application, desired performance, and reliability of the equipment/hardware.

The requirements of this document are intended to supplement the requirements of a higher level quality standard (e.g., AS/EN/JISQ9100, ISO-9001, ANSI/ASQC E4, ASME NQA-1, AS9120, AS9003, and ISO/TS 16949 or equivalent) and other quality management system documents. They are not intended to stand alone, supersede, or cancel requirements found in other quality management system documents; requirements imposed by contracting authorities, or applicable laws and regulations unless an authorized exemption/variance has been obtained. This document is not intended to make a legal determination of fraud, and appropriate legal counsel should be consulted for further action.

- **SAE AS6081⁴**, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition -Distributors

The scope is as follows:

This SAE Aerospace Standard standardizes practices to:

- a) identify reliable sources to procure parts;
- b) assess and mitigate risk of distributing fraudulent/counterfeit parts;
- c) control suspect or confirmed fraudulent/counterfeit parts; and
- d) report suspect and confirmed fraudulent/counterfeit parts to other potential users and Authority having jurisdiction.

SAE AS6081 will reference SAE AS6171 which will define test methods at its next revision.

- **SAE AS6171⁵**, Test Methods Standard: General Requirements, Suspect/Counterfeit Electrical, Electronic and Electromechanical Parts

The scope is as follows:

Scope:

This SAE Aerospace Standard (AS) standardizes inspection and test procedures, workmanship criteria, and minimum training and certification requirements to detect Suspect/Counterfeit (SC) Electrical, Electronic, and Electromechanical (EEE) parts. The requirements of this document apply once a decision is made to use parts with unknown chain of custody that do not have pedigree back to the original component manufacturer or have been acquired from a broker or independent distributor, or when there are other known risk elements that result in the User/Requester to have concerns about potential SC EEE parts. The tests specified by this standard may also detect occurrences of malicious tampering, although the current version of this standard is not designed specifically for this purpose.

This standard ensures consistency across the supply chain for test techniques and requirements based on assessed risk associated with the application, component, supplier, and other relevant risk factors. The requirements of this document supplement the requirements of a higher level quality standard (for example AS9100, AS9003,

³ Reprinted with permission from the published version of SAE document AS5553B ©2017 SAE International.

⁴ Reprinted with permission from the published version of SAE document AS6081 © 2017 SAE International.

⁵ Reprinted with permission from the published of SAE document AS6171 © 2017 SAE International.

AS9120, ISO 9001) and other quality management system documents. They are not intended to stand alone, supersede, or cancel requirements found in other quality management system documents, or requirements imposed by contracting authorities.

This SAE Aerospace Standard (AS) standardizes inspection and test procedures, workmanship criteria, and minimum training and certification requirements to detect Suspect/Counterfeit (SC) Electrical, Electronic, and Electromechanical (EEE) parts. The requirements of this document apply once a decision is made to use parts with unknown chain of custody that do not have pedigree back to the original component manufacturer or have been acquired from a broker or independent distributor, or when there are other known risk elements that result in the User/Requester to have concerns about potential SC EEE parts. The tests specified by this standard may also detect occurrences of malicious tampering, although the current version of this standard is not designed specifically for this purpose.

This standard ensures consistency across the supply chain for test techniques and requirements based on assessed risk associated with the application, component, supplier, and other relevant risk factors. The requirements of this document supplement the requirements of a higher level quality standard (e.g., AS9100, AS9003, AS9120, ISO 9001) and other quality management system documents. They are not intended to stand alone, supersede, or cancel requirements found in other quality management system documents, or requirements imposed by contracting authorities.

This standard should be implemented when other risk mitigation methods for avoiding the use of SC EEE parts (e.g., acquiring all parts from Authorized Sources, redesigning the system, having obsolete parts emulated, etc.) are either unavailable or inadequate. This standard mitigates the technical risk of performing insufficient inspection and test to determine suspect counterfeit EEE parts. This standard is not intended to be used to assess quality or reliability issues that may arise because of component production issues or due to mishandling, improper storage, or other attributes specific to quality or reliability.

The following terminology is used throughout this document and associated AS6171 Slash Sheets:

- a) Shall = is mandatory;
- b) Should = is recommended; and
- c) Will = is planned (is considered to be part of a standard process).

This standard should be utilized when parts are not available from sources with known traceability to the Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM), or authorized manufacturer. The requirements of this document specify testing based on acceptable levels of risk for a program or customer, to identify anomalies or performance issues that may indicate suspect counterfeit and counterfeit activity. No amount of testing can confirm an item as authentic; this would require that there be a known, unbroken chain of custody to the OCM/OEM or authorized manufacturer. Therefore, organizations should attempt to obtain parts from sources that have known traceability to the OCM or authorized manufacturer to avoid receiving counterfeit parts. All intermediaries from the origin (i.e., OCM/OEM or authorized manufacturer) to the final destination should consist of Trusted Suppliers, and transportation should be provided by logistics carriers that have documented processes and procedures to avoid tampering or substitution during the journey to the parts' final destination. A preference should be given to parts with known pedigree over parts with unknown pedigree to avoid counterfeit parts. This standard does not apply to parts obtained directly from a Trustworthy Authorized Supplier with traceability to the OCM/OEM or authorized manufacturer. This standard does not have specific test methods to determine if an item is a Fraudulent Part beyond what is considered counterfeit. Test data on anomalies can be gathered for potential legal determination of fraudulent intent or negligence. This document does not make a legal determination of fraud, and appropriate legal counsel should be consulted for further action.

Unless otherwise specified in the SOW (statement of work) or PO (purchase order) by the User/Requester, the information in the Appendices is not considered mandatory.

SAE Counterfeit Defect Coverage Tool:

The SAE Counterfeit Defect Coverage (CDC) Tool is a dynamic, web-based application, that supplements SAE Standard AS6171 authored by the SAE G-19A Test Laboratory Standards Development Committee. It provides potential test sequences for the identification of counterfeit electrical, electronic, and electromechanical (EEE) parts along a range of risk levels and EEE part types. Allowing users to compare alternative test sequences as a function of resources needed to implement those tests, the SAE CDC Tool is appropriate for those ordering counterfeit detection tests as well as those performing the tests.

See <http://www.sae.org/standardsdev/cdctool/>

- **SAE ARP 6178⁶**, Fraudulent/Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors

The scope is as follows:

Scope: This SAE Aerospace Recommended Practice is applicable for all organizations that procure electronic components from sources other than the original component manufacturer. It is especially applicable for assessing distributors that sell electronic components without contractual authorization from the original component manufacturer.

- **SAE AS6174A⁷**, Counterfeit Materiel: Assuring Acquisition of Authentic and conforming materiel.

The scope is as follows:

This SAE Standard standardizes practices to: a. maximize availability of authentic materiel, b. procure materiel from reliable sources, c. assure authenticity and conformance of procured materiel, including methods such as certification, traceability, testing and inspection appropriate to the commodity/item in question, d. control materiel identified as fraudulent/counterfeit, e. and report suspect or confirmed fraudulent/counterfeit materiel to other potential users and Authority Having Jurisdiction.

- **SAE AS6496⁸**, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution

The scope is as follows:

This SAE Aerospace Standard (AS) identifies the requirements for mitigating counterfeit products in the Authorized Distribution supply chain by the Authorized Distributor. If not performing Authorized Distribution, such as an Authorized Reseller, Broker, or Independent Distributor, refer to another applicable SAE standard.

- **SAE AIR6273⁹ (draft)**, Terms, Definitions and Acronyms–Counterfeit Materiel or Electrical, Electronic and Electromechanical Parts

The scope is as follows:

This document is to be used and cited as a standard reference by other SAE G-19 Committee documents that address the mitigation of Fraudulent/Counterfeit Electronic Parts.

- **SAE AS6301¹⁰**, Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors

The scope is as follows:

This set of criteria is intended for use by accredited Certification Bodies (CBs) to establish compliance, and grant certification to AS6081, Aerospace Standard;

⁶ Reprinted with permission from the published version of SAE document AS6178 © 2018 SAE International.

⁷ Reprinted with permission from the published version of SAE document AS6174A © 2018 SAE International.

⁸ Reprinted with permission from the published version of SAE document AS6496 © 2018 SAE International.

⁹ Reprinted with permission from the draft version of SAE document AIR6273 ©2018 SAE International.

¹⁰ Reprinted with permission from the published version of SAE document AS6301 ©2018 SAE International.

Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition-Distributors: It may also be used by others to assess compliance to AS6081 requirements.

- **SAE ARP6328**¹¹, Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems

The scope is as follows:

This document contains guidance for implementing a counterfeit mitigation program in accordance with AS5553.

The information contained in this document is intended to supplement the requirements of a higher level quality standard (e.g., AS9100) and other quality management system documents. This is not intended to stand alone, supersede, or cancel requirements found in other quality management system documents, requirements imposed by contracting authorities, or applicable laws and regulations unless an authorized exemption/variance has been obtained

- **SAE AS6462A**¹², AS5553A Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria

This set of criteria shall be utilized by accredited Certification Bodies (CBs) to establish compliance, and grant certification to AS5553A, Aerospace Standard; Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.

A.17 INEMI

INEMI has created a webpage on counterfeit components assessment methodology and metric development containing a counterfeit calculator (see webpage <http://www.inemi.org/development-of-a-methodology-to-determine-risk-of-counterfeit-use-whitepaper>) which is based on Excel:

- 1) risk of counterfeit use;
- 2) risk of untrusted sources;
- 3) counterfeit loss and total cost estimations.

This tool is free to download and use. Feedback is appreciated.

A.18 OECD

The Organisation for Economic Co-operation and Development (OECD) promotes policies that improve the economic and social well-being of people around the world (see <http://www.oecd.org/about/>). OECD has published various reports on the impact of counterfeits, see webpage

<http://www.oecd.org/general/searchresults/?q=counterfeit&cx=012432601748511391518:xzea-dub0b0a&cof=FORID:11&ie=UTF-8>.

A.19 ICC

The International Chamber of Commerce (ICC) produces statistics and reports concerning the economic and social impacts of counterfeiting and piracy (see webpages <https://iccwbo.org/global-issues-trends/innovation-ip/counterfeiting-piracy/> and <https://iccwbo.org/?s=counterfeit>).

¹¹ Reprinted with permission from the published version of SAE document ARP6328 ©2018 SAE International.

¹² Reprinted with permission from the published version of SAE document AS6462 ©2018 SAE International.

A.20 Applied DNA Sciences

Applied DNA Sciences (see webpage <http://adnas.com/solutions/>), uses biotechnology as a forensic foundation to create unique security solutions for modern commerce situations. Applied DNA Sciences's electronic product labelling/tracking scheme is explained on webpage <http://www.adnas.com/electronics>. This technology can be expensive to implement and industry has complained about the cost of the licence fees. As a result, the DLA has agreed to reimburse trusted suppliers who provide them with DNA labelled 5962-XXXXX components and is expanding the scheme through the Rapid Innovation Fund (RIF) to develop a single authentication platform for six types of commodity.

A.21 "Safety Directors" Forum

The Nuclear Industry 'Safety Directors' Forum has published an anti-counterfeit awareness on-line video which can also be viewed at webpage <https://www.youtube.com/watch?v=YwFUGeuZspg>

A.22 "Stop fake bearings" video

The World Bearing Association (WBA) has an excellent 'Stop Fake Bearings' webpage (see <http://stopfakebearings.com/>) where the on-line anti-counterfeit video can be viewed at webpage <http://stopfakebearings.com/video/>

A.23 Industrial company's online anti-counterfeit awareness training

An example of a specific industry sector 'on line' anti-counterfeit training package is from the USA company Raytheon which is working with the USA Defense Industry, located at webpage <http://www.raytheon.com/media/modules/corpcou0012/scolist.htm>

A.24 Subscription based anti-counterfeit awareness training

An example of subscription based on-demand anti-counterfeit awareness training modules is:

- ERAI (see <http://www.erai.com/>) is proposing a new web-based training program, with a primary focus on counterfeit mitigation, which is called "InterCEPT" (see webpage http://www.erai.com/InterCEPT_International_Counterfeit_Electronics_Personnel_Training_Overview). Their older 2011 presentation is located at <https://www.slideshare.net/KristalSnider-ERAI/erai-counterfeit-awarenessavoidance-training-02132011-6992436>

A.25 USA Government anti-counterfeit publications and awareness training

There are various USA Government publications and awareness training, for example:

- The Office of the Assistant Secretary of the Navy (Research, Development & Acquisition) Acquisition and Business Management published in June 2017 the document DON¹³ COUNTERFEIT MATERIEL PROCESS GUIDEBOOK titled "COUNTERFEIT MATERIEL PROCESS GUIDEBOOK – Guidelines for Mitigating the Risk Of Counterfeit Materiel in the Supply Chain, NAVSO P-7000" (see [http://www.secnav.navy.mil/rda/Policy/2017%20Policy%20Memoranda/Counterfeit-Materiel-Process-Guidebook,-NAVSO-P-7000-\(June-2017\)-and-associated-cover-memo.aspx](http://www.secnav.navy.mil/rda/Policy/2017%20Policy%20Memoranda/Counterfeit-Materiel-Process-Guidebook,-NAVSO-P-7000-(June-2017)-and-associated-cover-memo.aspx));

¹³ DON : Department of Navy

- The NASA Jet Propulsion Laboratory established a training course titled "Counterfeit Parts Awareness and Inspection" (see webpage https://mttc.jpl.nasa.gov/files/NASA%20Counterfeit%20Training_unlimited%20distribution%20handout.pdf).

A.26 IECQ WG6

IECQ WG6 is related to counterfeit avoidance (see webpage <http://www.iecq.org/workgroups/wg06/wg06-home.htm>).

A.27 Anti-counterfeiting videos

Examples videos showing the link between organised crime and the anti-counterfeiting world can be found at webpages:

- https://www.ted.com/talks/alastair_gray_how_fake_handbags_fund_terrorism_and_organized_crime
- <https://www.youtube.com/watch?v=4ZlwOoaCPxI> "Combatting the Counterfeit Drug Trade: Ashifi Gogo at TEDxBoston"

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

Annex B (informative)

Examples of aftermarket sources¹⁴

B.1 Examples of franchised aftermarket sources

- a) Rochester Electronics, see webpage <http://www.rocelec.com/>
- b) Teledyne E2V, see webpage <https://www.e2v.com/products/semiconductors/high-reliability-ics-qp-semi-product/> ,
- c) Lansdale, see webpage <http://www.lansdale.com/>
- d) Micross Components, see webpage <http://www.micross.com>
- e) Sensitron Semiconductor, see webpage <http://www.sensitron.com>
- f) Defence Logistics Agency, Columbus Ohio, see webpage <http://www.dla.mil/>
- g) Arrow/Zeus Electronics, Melville, NY, North America, see webpage <http://www.arrow.com/>
- h) Xtreme Semiconductor for Analog to Digital converters, see webpage <http://www.xtremesemi.com/products.htm>

B.2 Examples of sources of franchised die which can be packaged

- a) Micross formerly Chip Supply, see webpage <http://www.micross.com/> (over 20 franchised manufacturers)
- b) Semidice, see webpage <http://www.semidice.com/>

B.3 Examples of third party custom packaging houses which provide aftermarket solutions

- a) Force Technologies, see webpage <http://www.forcetechnologies.co.uk/>
- b) Technograph Microcircuits, see webpage <http://www.technographmicro.com/>
- c) Micross, see webpage <http://www.eltek-semi.com/>
- d) Sac-Tec Labs Inc., see webpage <http://www.sactec.com/index.htm>
- e) IDMOS, see webpage <http://www.id-mos.com> part of Serma Technologies
- f) Microsemi, formerly T.S.I Microelectronics, see webpage <http://www.microsemi.com/design-support/module-hybrid-design>.
- g) Integra Technologies, see webpage <https://www.integra-tech.com/>
- h) Teledyne E2V, see webpage <https://www.e2v.com/> Pantronix Corporation, see webpage <http://www.pantronix.com/>

B.4 Examples of emulated aftermarket providers

Through the “Advanced Microcircuit Emulation” (AME) and the “Generalized Emulation of Microcircuits (GEM)” programs, the Defense Logistics Agency (DLA) and SRI International (SRI) with its Sarnoff Corporation Division developed an emulation process (see webpages <http://www.gemes.com> and http://www.gemes.com/about_us/emulation_process/) offering an emulated replacement solution to obsolescence of an electronic component.

¹⁴ The information contained in Annex B is given for the convenience of the users of this document and does not constitute an endorsement by the IEC of the organizations named.

This approach allows electronic components that were originally manufactured in diverse technologies to be reproduced from a managed inventory of standardized base wafers.

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

Annex C (informative)

Typical example of a RECS certificate¹⁵

NOTE The RECS scheme is no longer in use and this is included for historical reference purposes only.



IEC

¹⁵ Reproduced with the permission of Avnet Technology Solutions Ltd., Bracknell, Berks, RG12 2PW, UK on behalf of Avnet Asia PTE Ltd.

Annex D
(informative)

Flowchart of IEC 62668-1 requirements

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

Figure D.1 provides a flowchart of IEC 62668-1 requirements and their relationship to external standards.

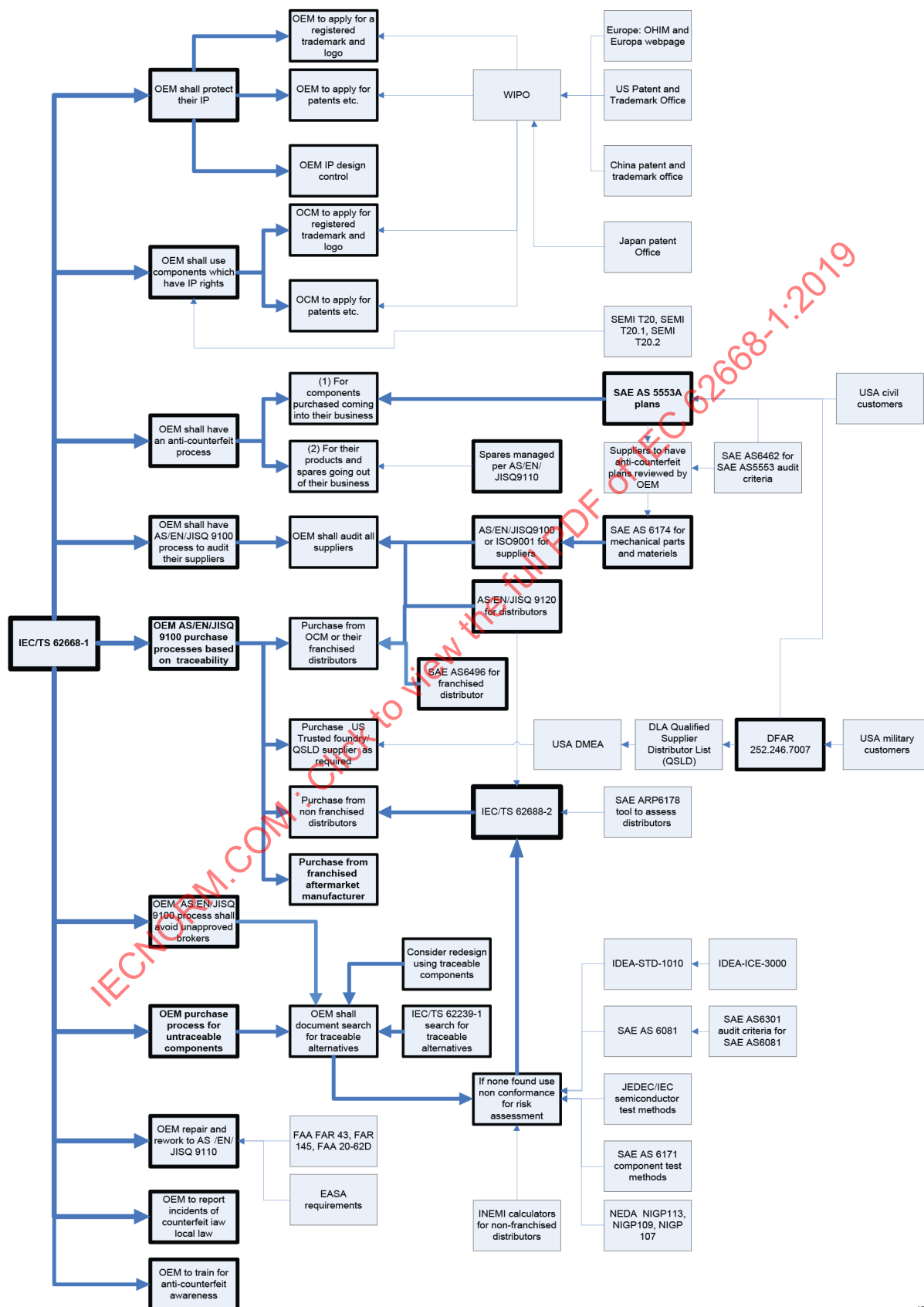


Figure D.1 – Flowchart of IEC 62668-1 requirements and their relationship to external standards

Annex E (Informative)

Typical use of anti-counterfeit standards in supply chains

Figures E.1, E.2, E.3, E.4 and E.5 provide examples of how to deploy anti-counterfeit standards in the supply chain.

International anti-counterfeit standards for supply chains

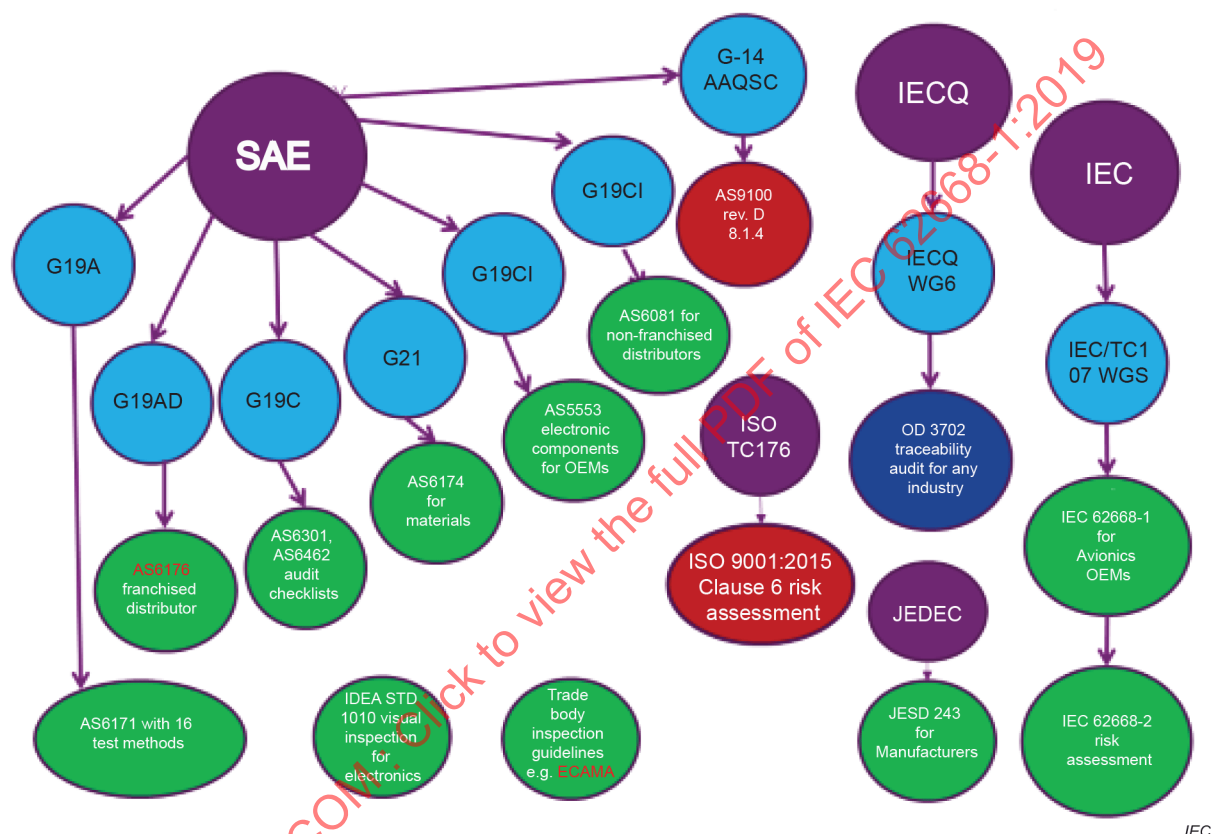


Figure E.1 – Available anti-counterfeit standards for supply chains

Referenced organizations:

IEC, International Electrotechnical Commission, see <http://www.iec.ch/>

- **TC107 WG3 , Counterfeit electronic parts; avoidance, detection, mitigation, and disposition in avionics applications** , see http://www.iec.ch/dyn/www/f?p=103:29:11713616250956:::FSP_ORG_ID,FSP_LANG_ID:1304,25#1

Guidance for the development of a management plan to avoid the use of counterfeit electronic parts in avionic applications. The plan will maximize the use of authentic parts with correct traceability and conformance documentation. It will also provide the risk mitigation methodologies to assess supplied components and require the formal reporting of any counterfeit and non-conforming parts and materials identified. This plan may be applied to other applications.

IECQ, International Electrotechnical Commission Quality Assessment System for Electronics, see <http://www.iecq.org/index.htm>

- **IECQ WG6, Counterfeit avoidance**, see <http://www.iecq.org/workgroups/wg06/wg06-home.htm>

In accordance with IECQ and industry requirements develop the necessary documentation to enable IECQ Counterfeit Avoidance – Approved Process Certification under the IECQ Approved Process Scheme. The initial IECQ Programme will begin by meeting the needs of the aerospace, avionics and military industry, however the Programme shall be developed such that it allows for industries other than the aerospace, avionics and military industries, noting that different industries may require differing criteria.

SAE Society of Automotive Engineers, see <https://www.sae.org/>

- **G-14 Americas Aerospace Quality Standards Committee (AAQSC)** is a technical committee established under the Aerospace General Projects Division of the SAE Aerospace Council. The AAQSC creates and maintains technical reports in the form of Aerospace Recommended Practices (ARP) and Aerospace Standards (AS) related to quality management systems and supporting quality-related processes. The committee has responsibilities to:
 - Review, approve/disapprove and prioritize proposals for new and revised technical reports
 - Charter project teams to develop and maintain technical reports
 - Recommend technical reports for publication
- **G-21 Counterfeit Materiel Committee** is chartered to address aspects of preventing, detecting, responding to and counteracting the threat of counterfeit materiel. The objective of the SAE G-21 committee is to develop standards suitable for use in high performance/high reliability applications to mitigate the risks of counterfeit materiel. In this regard, the standard will document recognized best practices in materiel management, supplier management, procurement, inspection, test/evaluation methods and response strategies when suspect or confirmed counterfeit materiel is detected.
- **G-19 Test Laboratory Standards Development Committee**, is chartered to address aspects of preventing, detecting, responding to and counteracting the threat of counterfeit electronic components.
 - G-19A Inspection and Test Matrix Committee
 - To develop an inspection/test matrix plan for different classes of Electrical, Electronic, and Electromechanical (EEE) commodities to detect suspect and confirmed counterfeit components.
 - G-19AD Authorized Distributor
 - G-19C Standard Compliance Verification
 - G-19CI Continuous Improvement
 - G-19D Distributor
 - G-19DR Distributor Risk Characterization
 - G-19T Terms and Definitions

For additional information on this SAE Technical Standards Committee, please visit:

<http://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG19>

ISO International Standard organization see <https://www.iso.org/>

- **ISO/TC176 Quality management and quality assurance**, see <https://www.iso.org/committee/53882.html>

JEDEC, Joint Electron Device Engineering Council see <https://www.jedec.org/>

JEDEC is the global leader in developing open standards for the microelectronics industry, with more than 3,000 volunteers representing nearly 300 member companies.

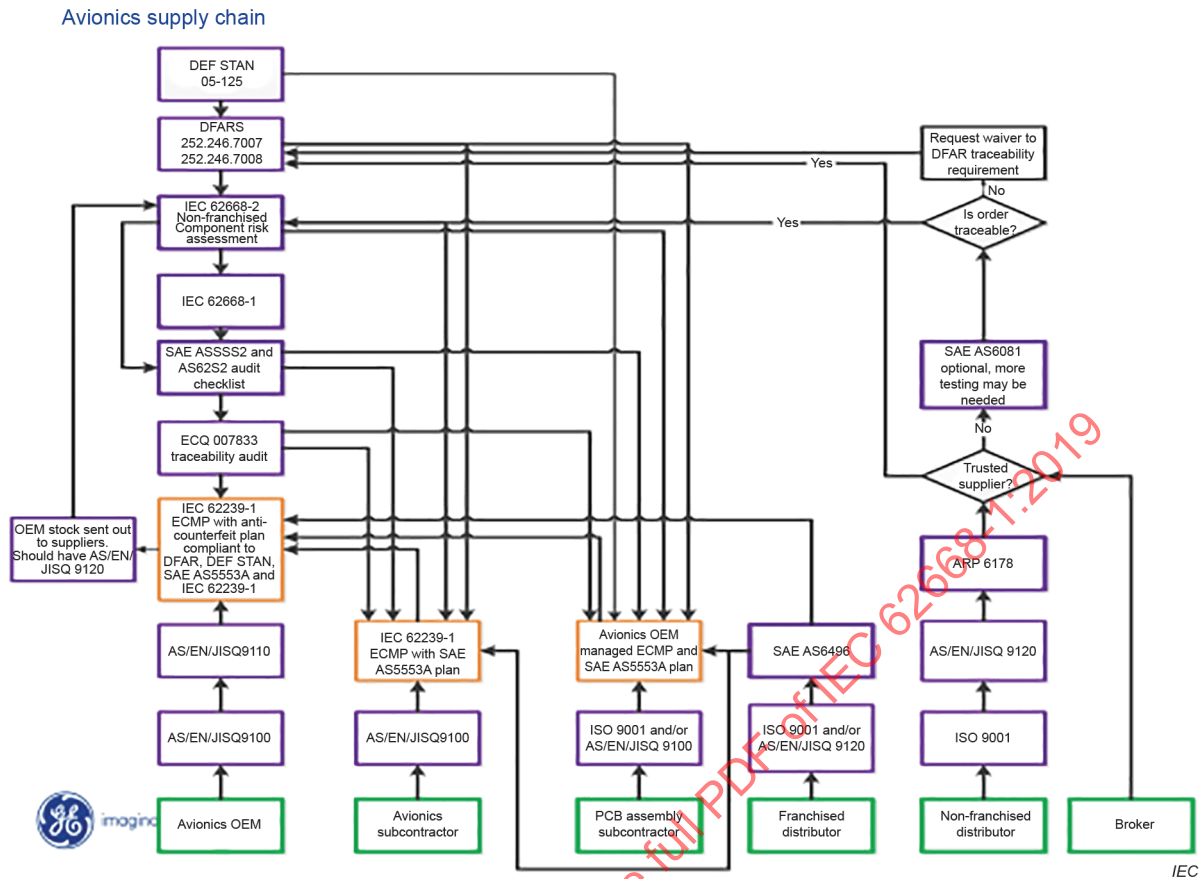
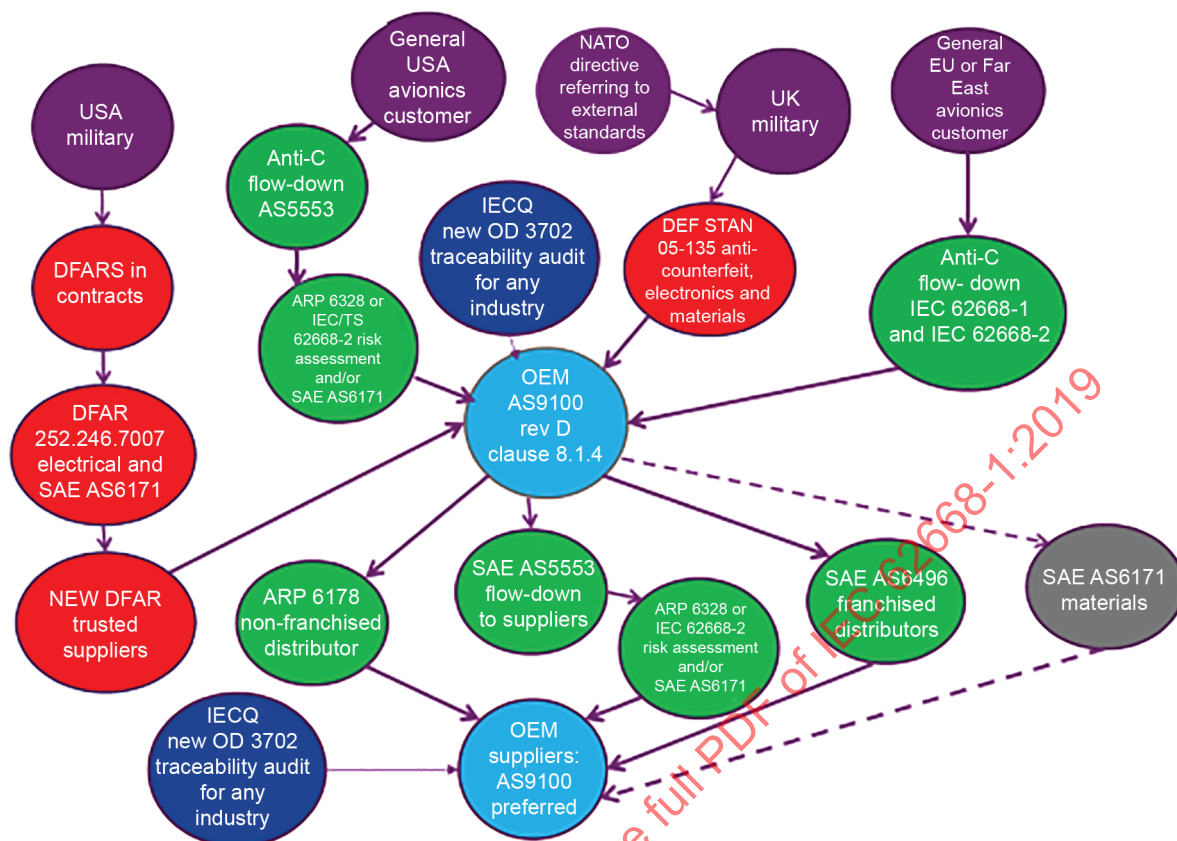


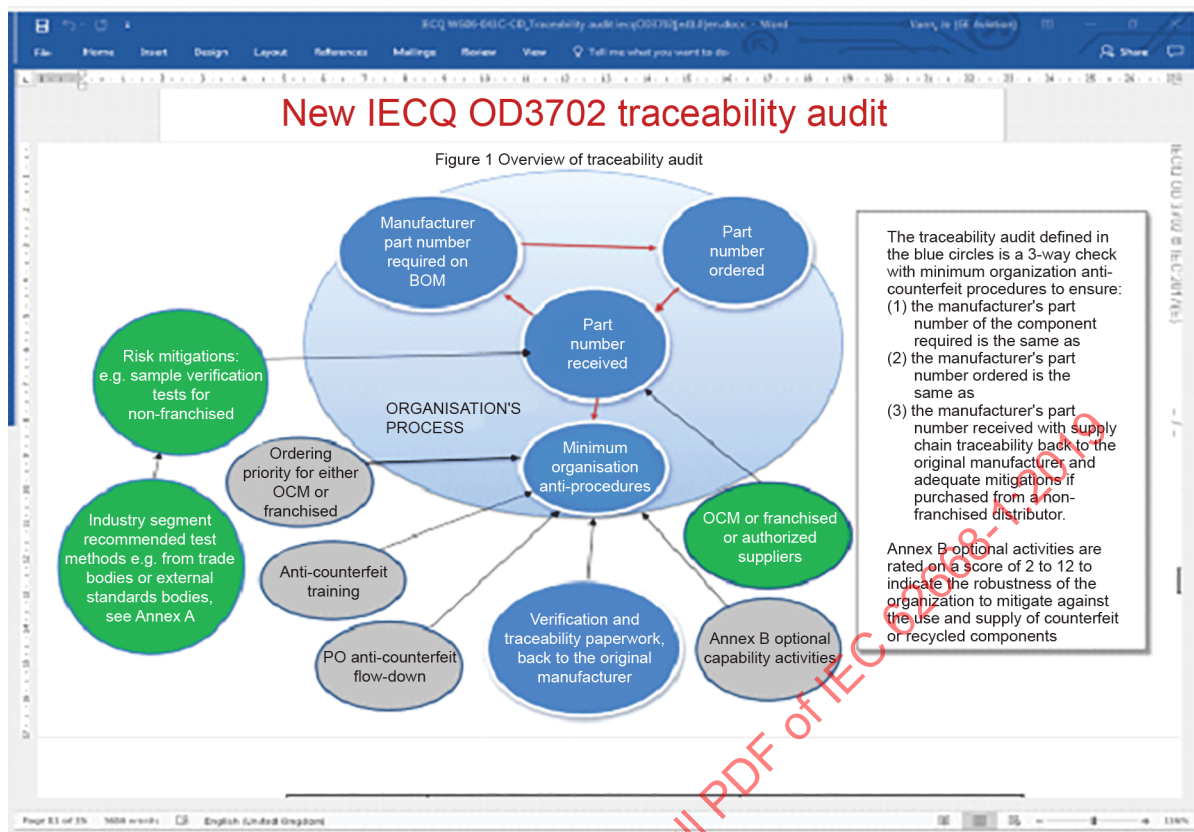
Figure E.2 – Overview of typical relationships for anti-counterfeit standards in an avionics supply chain

Avionics supply chains and contract flow-down which includes AS9100 flow down



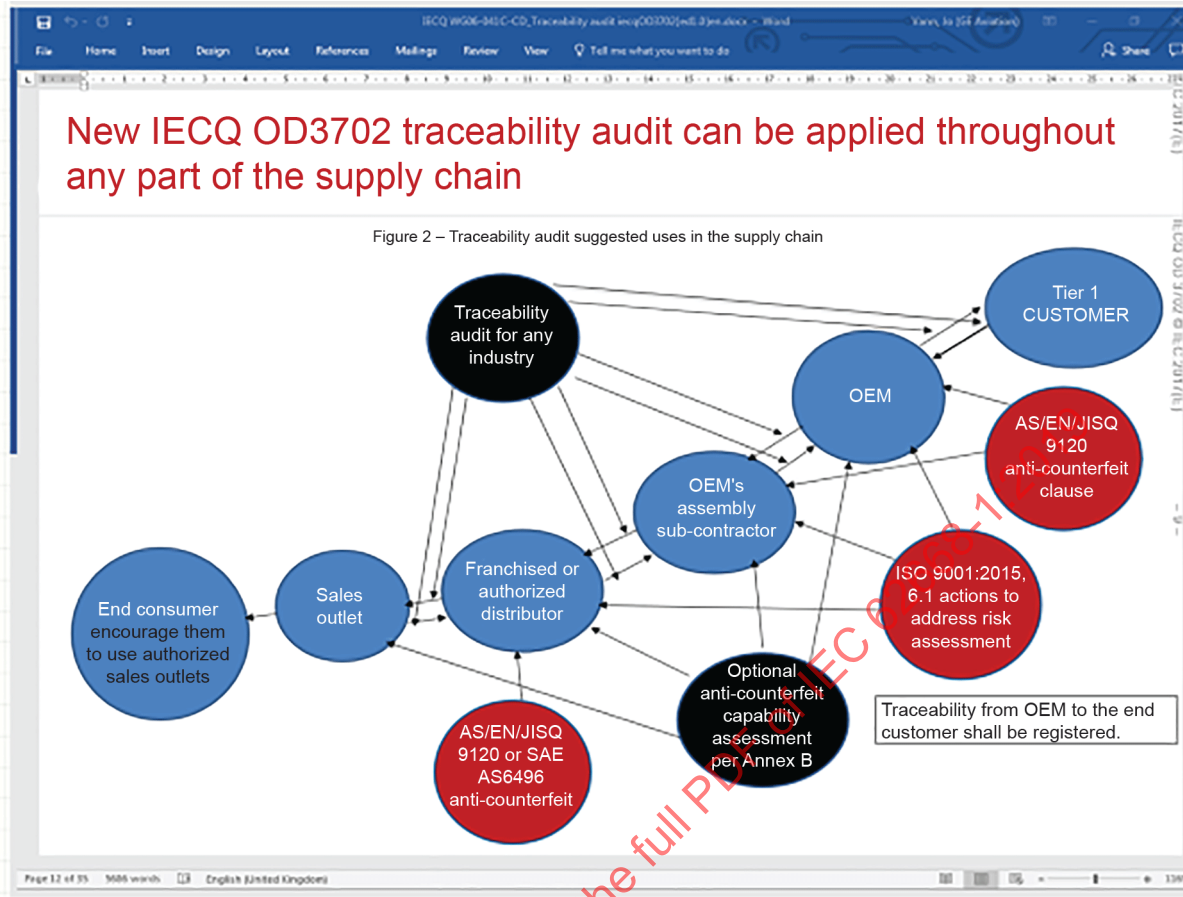
IEC

Figure E.3 – Overview of typical anti-counterfeit standards in an avionics OEM supply chain



IEC

Figure E.4 – IECQ OD 3702 traceability audit



IEC

Figure E.5 – Typical IECQ OD 3702 coverage in any supply chain

Bibliography

IEC 61340-5-1, *Electrostatics – Part 5-1: Protection of electronic devices from electrostatic phenomena – General requirements*

IEC 62402:2007, *Obsolescence management – Application guide*

IEC 62435-1, *Electronic components – Long-term storage of electronic semiconductor devices – Part 1: General*

IECQ OD 3407-1, *IECQ Subcontractor ECMP Programme Assessment, Evidence of Compliance Summary and Assessment Reporting Form, related to Assembly Subcontractor Quality and Process Management*

IECQ OD 3702, *IECQ Counterfeit Avoidance Programme assessment, evidence of compliance summary and assessment reporting form – Anti-counterfeit traceability audit for any industry segment*

ISO 12931, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*

ISO 14001, *Environmental management systems – Requirements with guidance for use*

ISO 16678, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*

ISO 17367, *Supply chain applications of RFID – Product tagging*

ISO/IEC 20243-1 *Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products- Part 1: Requirements and recommendations*

ISO 22380, *Security and resilience – Authenticity, integrity and trust for products and documents – General principles for product fraud risk and countermeasures*

ISO/IEC TR 24729-1, *Information technology – Radio frequency identification for item management – Implementation guidelines – Part 1: RFID-enabled labels and packaging supporting ISO/IEC 18000-6C*

ISO 28000, *Specification for security management systems for the supply chain*

ISO 28001, *Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance*

ISO 28002, *Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use*

ISO 28003, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*

ISO 28004 (all parts), *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000*

ISO 28004-1, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*

ISO 28004-2, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations*

ISO 28004-3, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)*

ISO 28004-4, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective*

AC 00-56B, *Voluntary Industry Distributor Accreditation Program*

ANSI/ESD S20.20, *Protection of Electrical and Electronic parts, Assemblies and Equipment (excluding electrically initiated explosive device)*

AS/EN/JISQ 9120, *Quality Management Systems – Requirements for Aviation, Space and Defense Distributors*

CAAC CCAR 145, *Civil Aircraft Maintenance Organisation Certification Regulations*

CAAC AC-145-06R1, *Aircraft Line Maintenance*

Defence Standard 05-135, *Avoidance of Counterfeit Materiel*

DFARS Case 2016-D010, *Defense Federal Acquisition Regulation Supplement: Costs Related to Counterfeit Electronic Parts*

DFARS Case 2016-D013, *Defense Federal Acquisition Regulation Supplement: Amendments Related to Sources of Electronic Parts*

DFARS 252.246.7007, *Contractor Counterfeit Electronic Part Detection and Avoidance System*

DFARS 252.246.7008, *Sources of Electronic Parts*

DI-MISC-81356, *Certificate of Compliance*

DLAD 52.211-9074, *Solicitation Provisions and Contract clauses – Deoxyribonucleic Acid (DNA) Marking-Federal Supply Class (FSC) 5962 Electronic Microcircuits*

DoD 4160.21-M, *DoD Disposition Manual*

DoDI 4140.67, *DoD Counterfeit Prevention Policy*

DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*

DODI 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense.*

DoDI 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities*

DoDI 8320.04 DoD, *Instruction 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property*

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*

DON Counterfeit Materiel Process Guidebook, *Counterfeit Materiel Process Guidebook – Guidelines for Mitigating the Risk Of Counterfeit Materiel in the Supply Chain*, NAVSO P-7000 (June 2017)

EASA Part M, *Continuing Airworthiness Requirements*

EASA Part 145, *Maintenance Organisation Approvals*

FAR Part 43, *Maintenance, Preventive Maintenance, Rebuilding and Alterations*

FAR Part 145, *Repair Stations*

FAA AC (advisory circular) 20-62, *Eligibility, quality and Identification of Aeronautical Replacement parts*

GAO-10-389, *DOD should leverage on-going initiatives in developing its program to mitigate risk of counterfeit parts*

GAO-10-423, *Observations on Efforts to Quantify the Economic effects of Counterfeit and Pirated Goods*

GAO-12-213T, *DoD Supply Chain: Preliminary observations indicate that counterfeit electronic parts can be found on internet purchasing platforms*

GAO-12-375, *DoD Supply chain: Suspect Counterfeit Electronic Parts can be found on internet purchasing platforms.*

GAO-03-713T, *Counterfeit documents used to enter the US from certain western hemisphere countries not detected.*

GAO-13-762T, *Intellectual property: Insight gained from Efforts to Quantify the Effects of counterfeit and Pirated Goods in the US Economy*

GAO-16-236, *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk*
GIFAS 5052, *Guide for managing electronic component sourcing through non-franchised distributors, preventing fraud and counterfeiting*

IDEA-STD-1010, *Acceptability of electronic components distributed in the open market*

IDEA-ICE-3000, *Professional Inspector Certification Exam*

IPC-1782, *Standard for Treaceability of Critical Items based on risk.*

JESD31, *General Requirements for Distributors of Commercial and Military Semiconductor Devices*

MIL-HDBK-103, *Department of Defense Handbook: List of Standard Microcircuit Drawings*

MIL-STD-129, *Military marking for Shipment and Storage*

MIL-STD-130, *Identification Marking of U.S. Military Property*

NASA/JPL, *Counterfeit Parts Awareness and Inspection*
(https://mttc.jpl.nasa.gov/files/NASA%20Counterfeit%20Training_unlimited%20distribution%20handout.pdf)

NIGP 107, *Guidelines for the format of Military Certificates of Conformance*

NIGP 109, *Guidelines for Distributor Assessment of Manufacturer Performance*

NIGP 111: *Guidelines for the format of Packing Slips*

NIGP 113, *NEDA Guidelines for Product Returns*

NIGP 115, *Certificates of Conformance for Commercial Electronic Parts*

NIGP 116, *ECIA Guidelines for Disposition of Excess Inventory*

OHSAS 18001, *Occupational health and safety*

SAE AIR6273¹⁶, *Terms and Definitions – Fraudulent/Counterfeit Electronic Parts*

SAE ARP 6178¹⁷, *Fraudulent/Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors*

SAE ARP 6328¹⁸, *Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems*

SAE AS5553A¹⁹, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition*

SAE AS6081²⁰, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition – Distributors Counterfeit Electronic parts; Avoidance Protocol, Distributors*

SAE AS6171²¹, *Test Methods Standard: Counterfeit Electronic Parts*

SAE AS6174²², *Counterfeit Material: Detection, Mitigation and Disposition*

SAE AS6301²³, *Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors*

¹⁶ Reprinted with permission from the draft version of SAE document AIR6273 (c) 2018 SAE International.

¹⁷ Reprinted with permission from the published version of SAE document ARP6178 (c) 2018 SAE International.

¹⁸ Reprinted with permission from the published version of SAE document ARP6328 (c) 2018 SAE International.

¹⁹ Reprinted with permission from the published version of SAE document AS5553 (c) 2018 SAE international.

²⁰ Reprinted with permission from the published version of SAE document AS6081 (c) 2018 SAE International.

²¹ Reprinted with permission from the draft version of SAE document AS6171 (c) 2018 SAE International.

²² Reprinted with permission from the published version of SAE document AS6174 (c) 2018 SAE International.

²³ Reprinted with permission from the published version of SAE document AS6301 (c) 2018 SAE International.

SAE AS6462²⁴, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria*

SAE AS6496²⁵, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution*

SAE STD-0016²⁶, *Standard for Preparing a DMSMS Management Plan*

SD-22, *Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook*

SEMI T18-1106 (Reapproved 0812), *Specification of Parts and Components Traceability*

SEMI T20, *Specification for authentication of semiconductors and related products*

SEMI T20.1, *Specification for object labelling to authenticate semiconductors and related Products in an open market*

SEMI T20.2, *Guide for qualifications of authentication service bodies for detecting and preventing counterfeiting of semiconductors and related products*

SEMI T20-0710, *Specification for Authentication of Semiconductors and Related Products*

SEMI T21-0314, *Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain*

SEMI T22-0212, *Specification for Traceability by Self Authentication Service Body and Authentication Service Body*

USA Homeland Security – *Joint Strategic Plan on Intellectual Property Enforcement (FY 2017-2019), Supporting innovation, creativity and enterprise, charting the path ahead*

²⁴ Reprinted with permission from the published version of SAE document AS6462 (c) 2018 SAE International.

²⁵ Reprinted with permission from the published version of SAE document AS6496 (c) 2018 SAE International.

²⁶ Reprinted with permission from the published version of SAE STD-0016 document (c) 2018 SAE International.

SOMMAIRE

AVANT-PROPOS	93
1 Domaine d'application	95
2 Références normatives	95
3 Termes, définitions et termes abrégés	95
3.1 Termes et définitions	95
3.2 Termes abrégés	100
4 Exigences techniques	103
4.1 Généralités	103
4.2 Exigences minimales concernant le fabricant d'équipements avioniques d'origine	104
4.3 Propriété intellectuelle	107
4.3.1 Généralités	107
4.3.2 Définition de la propriété intellectuelle	108
4.4 Prise en compte de la contrefaçon	109
4.4.1 Généralités	109
4.4.2 Définition légale de la contrefaçon	109
4.4.3 Composants frauduleux	109
4.4.4 Comment mettre en place la traçabilité	110
4.4.5 Motifs de perte de traçabilité d'un composant	110
4.5 Le problème de la contrefaçon	111
4.5.1 Généralités	111
4.5.2 Activités mondiales relatives aux questions de lutte contre la contrefaçon	111
4.5.3 Différences culturelles	112
4.5.4 Equipements avioniques et contrefaçon	112
4.5.5 Groupes d'intervention directe contre la contrefaçon de composants électroniques	116
4.6 Composants recyclés	116
4.6.1 Généralités	116
4.6.2 Pourquoi l'industrie avionique n'utilise pas de composants recyclés	116
4.6.3 De quelle manière les composants recyclés deviennent suspects et potentiellement frauduleux	117
4.7 Lignes directrices des fabricants de composants d'origine (OCM) en matière de lutte contre la contrefaçon	117
4.7.1 Généralités	117
4.7.2 "Fournisseur fiable de composants électroniques" (RECS): le mécanisme de vérification chinois	117
4.7.3 Certification tierce des fabricants de composants d'origine au titre de l'ISO 9001 et de l'AS/EN/JISQ 9100	118
4.7.4 Marques déposées des fabricants de composants d'origine	118
4.7.5 Contrôle de la propriété intellectuelle des fabricants de composants d'origine	118
4.7.6 Marquage physique des pièces et des emballages des fabricants de composants d'origine	118
4.7.7 Groupe de travail anticontrefaçon (ACTF) de l'Association de l'industrie des semiconducteurs	119
4.7.8 Les fonderies de confiance: le programme américain	120
4.7.9 Programme américain d'accréditation des fournisseurs de confiance de circuits intégrés	120

4.7.10	Fonction physique non clonable (PUF)	120
4.7.11	Meilleures pratiques des fabricants de composants d'origine	121
4.8	Accréditations minimales des distributeurs	121
4.9	Certification tierce AS/EN/JISQ 9120 des distributeurs	121
4.10	Réseau de distributeurs franchisés	122
4.10.1	Généralités	122
4.10.2	SAE AS6496	123
4.10.3	Contrôle des stocks par le biais de mécanismes de suivi	123
4.10.4	Contrôle des rebuts	124
4.10.5	Fournisseur fiable de composants électroniques (RECS)	124
4.11	Lignes directrices des distributeurs non franchisés en matière de lutte contre la contrefaçon	124
4.11.1	Généralités	124
4.11.2	Programme certifié CCAP-101 destiné aux distributeurs indépendants	124
4.11.3	SAE AS6081	125
4.11.4	Distributeurs non franchisés gérés par les fabricants d'équipements d'origine	125
4.11.5	Courtiers	125
4.12	Lignes directrices des fabricants d'équipements avioniques d'origine en matière de lutte contre la contrefaçon lors de l'achat de composants	125
4.12.1	Approche générale de la lutte contre la contrefaçon	125
4.12.2	Achat auprès de sources agréées	126
4.12.3	Composants avec une traçabilité jusqu'au fabricant d'origine	126
4.12.4	Certificat de conformité et bordereau d'expédition	127
4.12.5	Planification et achat de quantités suffisantes	128
4.12.6	Recours à des distributeurs non franchisés	128
4.12.7	Courtiers	128
4.12.8	Recours au fabricant d'origine	129
4.12.9	Composants obsolètes et sources franchisées du marché secondaire	129
4.12.10	Substituts agréés au titre de l'IEC 62239-1	130
4.12.11	Reconception produit	130
4.12.12	Composants d'origine inconnue	130
4.12.13	Plans de lutte contre la contrefaçon des OEM comprenant la SAE AS5553 et la SAE AS6174	130
4.13	Lignes directrices des fabricants d'équipements d'origine en matière de lutte contre la contrefaçon concernant leurs produits	135
4.13.1	Contrôle de la propriété intellectuelle	135
4.13.2	Rendre les conceptions des fabricants d'équipements d'origine inviolables	136
4.13.3	Étiquettes inviolables	136
4.13.4	Utilisation de circuits intégrés spécifiques et de réseaux de portes programmables in situ disposant de fonctions de protection de la propriété intellectuelle	136
4.13.5	Contrôle du marquage final du produit du fabricant d'équipements d'origine	137
4.13.6	Contrôle des rebuts des fabricants d'équipements d'origine	137
4.13.7	Logos et marques déposées des fabricants d'équipements d'origine	137
4.13.8	Contrôle des livraisons des produits et pièces détachées des fabricants d'équipements d'origine et de leur durée de vie utile	137
4.13.9	Activités MRO	138
4.14	Déclaration de contrefaçon, de fraude et de recyclage de composants	139

4.14.1	Généralités	139
4.14.2	Programme relatif aux pièces non approuvées suspectes de la FAA aux Etats-Unis.....	139
4.14.3	AESA.....	139
4.14.4	Déclaration de contrefaçon au Royaume-Uni	139
4.14.5	Déclaration de contrefaçon dans l'Union européenne	139
4.14.6	Forum de l'UKEA contre la contrefaçon	139
4.15	Formation de sensibilisation à la prévention de la contrefaçon	140
4.16	Informations pour la prise en charge de la gestion de la chaîne d'approvisionnement	140
Annexe A (informative) Contacts utiles		141
A.1	Organisation mondiale de la propriété intellectuelle (OMPI)	141
A.1.1	Généralités	141
A.1.2	Présentation de l'OMPI	141
A.1.3	Services de la propriété intellectuelle de l'OMPI	141
A.1.4	Réseau mondial d'académies de la propriété intellectuelle de l'OMPI	143
A.2	Accord commercial anticontrefaçon (ACAC).....	144
A.2.1	ACAC	144
A.2.2	Réseau mondial anticontrefaçon (GACG - Global Anti-Counterfeiting Network).....	144
A.3	Conseil mondial des semiconducteurs (WSC - World Semiconductor Council) et GAMS	144
A.4	SEMI.....	145
A.5	Electronics Authorized Directory	147
A.6	Royaume-Uni.....	147
A.6.1	Bureau de la propriété intellectuelle du Royaume-Uni.....	147
A.6.2	Alliance for IP	147
A.6.3	UK Chartered Trading Standards Institute.....	148
A.6.4	UK HM Revenue and Customs.....	148
A.6.5	Anti-Counterfeiting Forum.....	148
A.6.6	Electronic Component Supplier Network (ESCN)	148
A.6.7	Ministère de la Défense britannique.....	148
A.7	Europe.....	149
A.7.1	Synthèses européennes de la législation de l'UE	149
A.7.2	Europol, agence européenne de lutte contre la criminalité	149
A.7.3	Office européen des brevets	149
A.7.4	EUIPO	149
A.7.5	Agence européenne de la sécurité aérienne (AESA).....	150
A.7.6	Schémas d'audit IECQ.....	150
A.7.7	BEAMA.....	151
A.8	Etats-Unis	151
A.8.1	Bureau américain des brevets et des marques commerciales	151
A.8.2	International Trade Administration, US Department of Commerce.....	152
A.8.3	International Intellectual Property Alliance	152
A.8.4	Federal Aviation Administration (FAA)	153
A.8.5	Trusted Access Program Office (TAPO).....	153
A.8.6	Independent Distributors of Electronics Association (IDEA)	154
A.8.7	ECIA, anciennement National Electronic Distributors Association (NEDA).....	154
A.8.8	Components Technology Institute Inc. (CTI)	155

A.8.9	Defense Logistics Agency (DLA).....	155
A.8.10	DFARS	156
A.8.11	IAQG	156
A.8.12	USA Homeland Security	156
A.9	Chine	157
A.9.1	CNIPA	157
A.9.2	Bureau chinois des brevets et des marques commerciales	157
A.9.3	Associations chinoises des composants électroniques.....	157
A.9.4	China Quality Certification Centre (CQC).....	157
A.9.5	Civil Aviation Administration of China (CAAC).....	157
A.9.6	China lawinfo.Co Ltd., pour Law info China	157
A.10	Japon – Japanese Patent Office (JPO)	157
A.11	Fonction physique non clonable	158
A.12	PUF et initiatives et solutions en matière de tags	159
A.12.1	Initiative Sécurité intrinsèque du matériel (HIS)	159
A.12.2	Exemples de fournisseurs de tags	159
A.13	Exemples de sociétés de conception de solutions inviolables	160
A.14	Exemples de sérialisation de puce FPGA.....	160
A.15	Exemples de fabricants de mémoire vive non volatile.....	160
A.16	SAE G-19	160
A.17	iNEMI.....	164
A.18	OCDE	165
A.19	CCI	165
A.20	Applied DNA Sciences	165
A.21	Safety Directors' Forum	165
A.22	Vidéo "Stop fake bearings" (Halte aux roulements contrefaits)	165
A.23	Formation de sensibilisation à la prévention de la contrefaçon des sociétés industrielles	165
A.24	Formation de sensibilisation à la prévention de la contrefaçon reposant sur les abonnements.....	165
A.25	Publications et formation de sensibilisation à la prévention de la contrefaçon du gouvernement américain	166
A.26	IECQ WG6.....	166
A.27	Vidéos de lutte contre la contrefaçon	166
Annexe B (informative)	Exemples de marchés secondaires.....	167
B.1	Exemples de sources franchisées du marché secondaire.....	167
B.2	Exemples de sources de puces franchisées qui peuvent être placées dans un boîtier	167
B.3	Exemples de boîtiers d'emballage tiers offrant des solutions de marché secondaire	167
B.4	Exemples de fournisseurs du marché secondaire émulsés.....	167
Annexe C (informative)	Exemple classique de certificat RECS	169
Annexe D (informative)	Diagramme des exigences de l'IEC 62668-1	170
Annexe E (informative)	Utilisation classique des normes anticontrefaçon dans les chaînes d'approvisionnement.....	172
Bibliographie.....		178
Figure 1 – Zone des composants suspects		110

Figure D.1 – Diagramme des exigences de l'IEC 62668-1 et de leur relation avec les normes externes	171
Figure E.1 – Normes anticontrefaçon disponibles pour les chaînes d'approvisionnement	172
Figure E.2 – Vue d'ensemble des relations classiques pour des normes anticontrefaçon dans une chaîne d'approvisionnement avionique.....	174
Figure E.3 – Vue d'ensemble des normes anticontrefaçon classiques dans une chaîne d'approvisionnement OEM avionique	175
Figure E.4 – Audit de traçabilité IECQ OD 3702	176
Figure E.5 – Couverture IECQ OD 3702 classique dans une chaîne d'approvisionnement	177
Tableau 1 – Lignes directrices pour la formation de sensibilisation à la prévention de la contrefaçon.....	106
Tableau 2 – Respect ou non des exigences de l'IEC 62668-1 en fonction de la présence d'un plan agréé au titre de la SAE AS5553A chez le fabricant d'équipements d'origine.....	131
Tableau 3 – Respect ou non des exigences de l'IEC 62668-1 en fonction de la présence d'un plan agréé au titre de la SAE AS5553B chez le fabricant d'équipements d'origine.....	133

IECNORM.COM : Click to view the full PDF of IEC 62668-1:2019

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES PROCESSUS POUR L'AVIONIQUE – PRÉVENTION DE LA CONTREFAÇON –

Partie 1: Prévention de l'utilisation de composants électroniques contrefaits, frauduleux et recyclés

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62668-1 a été établie par le comité d'études 107 de l'IEC: Gestion des processus pour l'avionique.

Cette première édition annule et remplace la troisième édition de l'IEC TS 62668-1 parue en 2016. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- a) ajout d'une référence à l'AS/EN/JISQ 9100 et l'AS/EN/JISQ 9110, qui contiennent les exigences de prévention de la contrefaçon qui peuvent être utilisées pour satisfaire aux exigences du 4.2;
- b) ajout d'une référence à la règle 252.246.7008 de la DFAR (Etats-Unis) et à la Defence Standard 05-135 (Royaume-Uni);
- c) ajout d'une référence à plusieurs rapports du GAO, de l'OCDE et de la CCI en 4.5.1;
- d) mise à jour de liens Internet et d'autres références;
- e) ajout de la nouvelle Annexe E contenant des figures représentant la manière dont les documents de prévention de la contrefaçon peuvent être utilisés dans les chaînes d'approvisionnement;
- f) ajout d'une référence au nouvel audit de traçabilité OD 3702 de l'IECQ;
- g) ajout d'une nouvelle définition pour les composants refabriqués avec un avertissement précisant que ces composants ne sont pas recommandés.

Le texte de cette Norme internationale est issu des documents suivants:

CDV	Report on voting
107/335/CDV	107/346A/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62668, publiées sous le titre général *Gestion des processus pour l'avionique – Prévention de la contrefaçon*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

GESTION DES PROCESSUS POUR L'AVIONIQUE – PRÉVENTION DE LA CONTREFAÇON –

Partie 1: Prévention de l'utilisation de composants électroniques contrefaits, frauduleux et recyclés

1 Domaine d'application

La présente partie de l'IEC 62668 définit les exigences permettant d'éviter l'utilisation de composants contrefaits, recyclés et frauduleux dans le secteur de l'aérospatial, de la défense et des hautes performances (ADHP). Elle définit également les exigences permettant de maintenir la propriété intellectuelle de tous les produits et services utilisés dans ce même secteur. Les risques associés à l'achat de composants en dehors des réseaux de distributeurs franchisés sont pris en compte dans l'IEC 62668-2. Bien que développé pour l'industrie avionique, le présent document peut être appliqué par d'autres secteurs à hautes performances et à haute fiabilité s'ils le souhaitent.

NOTE L'IEC 62668 (toutes les parties) ne traite pas de la restriction portant sur la réutilisation d'un composant en maintenance, en réparation et en révision; elle traite ces activités uniquement lorsqu'elles sont sous la responsabilité du fabricant d'équipements d'origine.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62239-1, *Gestion des processus pour l'avionique – Plan de gestion – Partie 1: Préparation et maintenance d'un plan de gestion des composants électroniques*

IEC 62668-2, *Gestion des processus pour l'avionique – Prévention de la contrefaçon – Partie 2: Gestion des composants électroniques achetés auprès de sources non franchisées*

ISO 9001, *Systèmes de management de la qualité – Exigences*

AS/EN/JISQ 9100, *Systèmes de management de la qualité – Exigences pour les organismes de l'aéronautique, l'espace et la défense*

AS/EN/JISQ 9110, *Quality Maintenance Systems – Aerospace – Requirements for Maintenance Organizations* (disponible en anglais seulement)

3 Termes, définitions et termes abrégés

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

3.1.1

source du marché secondaire

revendeur qui peut ou non être sous contrat avec le fabricant de composants d'origine (OCM), ou qui est parfois une "entreprise de refabrication" de composants, sous contrat avec l'OCM

Note 1 à l'article: Le revendeur cumule les stocks de composants encapsulés ou non encapsulés (tranche) dont la date de fin de vie a été publiée par l'OCM. Ces composants sont ensuite revendus avec un bénéfice afin de répondre à un besoin du marché concernant les composants devenus obsolètes.

3.1.2

courtier

organisation individuelle ou corporative qui sert d'intermédiaire entre l'acheteur et le vendeur

Note 1 à l'article: Dans le secteur des composants électroniques, un courtier cherche spécifiquement à fournir des composants obsolètes ou rares afin d'engendrer des bénéfices. Pour ce faire, il peut cumuler un stock de composants jugés comme ayant une valeur stratégique ou il peut compter sur les stocks cumulés par d'autres organisations. Le courtier évolue au sein d'un réseau international d'échange de composants.

3.1.3

produit COTS

produit disponible dans le commerce

un ou plusieurs composants, assemblés et développés à destination de différents consommateurs, dont la conception et/ou la configuration est contrôlée par une spécification du fabricant ou une norme industrielle

Note 1 à l'article: Les produits COTS peuvent inclure les composants, sous-assemblages ou assemblages, ou assemblages de niveau supérieur électroniques. Les sous-assemblages ou assemblages COTS électroniques incluent les assemblages de cartes à circuit, les alimentations, les disques durs et les modules de mémoire. Les assemblages COTS de niveau supérieur incluent un rack entièrement intégré d'équipements tels que des groupes RAID, des serveurs de fichiers et des interrupteurs individuels, des routeurs, des ordinateurs personnels ou tout équipement similaire.

Note 2 à l'article: L'abréviation "COTS" est dérivée du terme anglais développé correspondant "commercial off-the-shelf".

3.1.4

contrefaire, verbe

action de simuler, reproduire ou modifier un bien matériel ou son emballage, sans autorisation

Note 1 à l'article: Pratique consistant à produire des produits qui constituent des imitations ou de faux produits ou services. Cette activité enfreint les droits de propriété intellectuelle du fabricant d'origine et constitue un acte illégal. La contrefaçon concerne généralement la contrefaçon délibérée de marques.

3.1.5

composant contrefait

bien matériel imitant ou copiant un bien matériel authentique qui peut être protégé par un ou plusieurs droits de propriété intellectuelle enregistrés ou confidentiels

Note 1 à l'article: Un composant contrefait est un composant dont l'identité ou la lignée a été altérée ou déformée par le fournisseur.

Identité = fabricant d'origine, numéro de pièce, code de date, numéro de lot, essais, inspection, documentation ou garantie, etc.

Lignée = origine, historique de propriété, stockage, manipulation, état, utilisation antérieure, etc.

Note 2 à l'article: Lorsqu'un bien matériel ne possède aucun droit de propriété intellectuelle enregistré ou confidentiel, sa propriété intellectuelle n'est pas protégée. Les exemples incluent les cas où le fabricant de composants d'origine (OCM) a cessé son activité et n'a pas vendu ou transmis les droits de propriété intellectuelle à une autre entité.

3.1.6

spécification de dispositif client

spécification de dispositif rédigée par un utilisateur et convenue par le fournisseur

3.1.7

client

utilisateur

fabricant d'équipements d'origine (OEM) qui achète des composants électroniques, y compris des circuits intégrés et/ou des dispositifs à semiconducteurs conformes au présent document, et qui les utilise pour concevoir, produire et assurer la maintenance des systèmes

3.1.8

fiche technique

document élaboré par le fabricant qui décrit les caractéristiques électriques, mécaniques et environnementales du composant

3.1.9

distributeur ou agent franchisé

organisation individuelle ou corporative, juridiquement indépendante du franchiseur (dans ce cas, le fabricant de composants électroniques ou OCM), qui accepte de distribuer des produits, dans le cadre d'une relation contractuelle, en utilisant le nom et le réseau de vente du franchiseur

Note 1 à l'article: Les activités de distribution sont réalisées conformément aux normes établies et contrôlées par le franchiseur. Les commandes effectuées peuvent être expédiées directement par l'OCM ou par le distributeur ou l'agent franchisé. En d'autres termes, le distributeur franchisé conclut un accord contractuel avec un ou plusieurs fabricants de composants électroniques pour distribuer et vendre ces composants. Les accords de distribution peuvent être stipulés selon les critères suivants: zone géographique, type de clientèle (avionique par exemple), taille maximale du lot de fabrication. Les composants fournis par ce biais sont protégés par la garantie OCM et livrés avec une traçabilité complète.

3.1.10

composant frauduleux

composant électronique produit ou distribué soit en violation de la loi ou de la réglementation régionale ou locale, soit dans le but de tromper le client

Note 1 à l'article: Sont inclus, entre autres, les exemples suivants de composants frauduleusement vendus en tant que nouveaux composants à un client:

- 1) composant volé;
- 2) composant mis au rebut par le fabricant de composants d'origine (OCM) ou par un utilisateur, quel qu'il soit;
- 3) composant recyclé, qui devient un composant recyclé frauduleux lorsqu'il s'agit d'un composant démonté (d'un assemblage de circuits imprimés par exemple), puis revendu en tant que composant neuf (voir Figure 1), avec généralement des signes d'utilisation antérieure et de reprise (par exemple, soudures, nouvelle métallisation ou refixation des broches) sur les terminaisons du boîtier du composant;
- 4) composant contrefait, copie, imitation, substitut total ou partiel de marques;
- 5) données de conception, modèles, brevets, logiciels ou droits d'auteur frauduleux vendus comme étant nouveaux et authentiques. Par exemple: composant dont la production et la distribution ne sont pas contrôlées par le fabricant d'origine;
- 6) copies non autorisées de données de conception;
- 7) composant déguisé (indiquant le nom du fabricant d'origine, la date ou le code de référence ou d'autres identificateurs, etc.), pouvant être un composant contrefait (voir Figure 1);
- 8) composant sans puce en silicium interne ou avec une puce en silicium de substitution, qui n'est pas la puce en silicium du fabricant d'origine.

3.1.11

propriété intellectuelle

créations de l'esprit telles que inventions, œuvres littéraires et artistiques, et symboles, noms, images et données de conception utilisés dans le commerce

Note 1 à l'article: Il s'agit de la propriété créée par l'intermédiaire d'une activité intellectuelle ou créative.

Note 2 à l'article: Sont inclus les brevets, marques, droits d'auteur et données de conception. La propriété intellectuelle peut être détenue, louée, concédée sous licence, vendue ou donnée.

3.1.12 microcircuit composant dispositif

dispositif électrique ou électronique qui ne peut pas être démonté sans être détruit ou porter atteinte à son utilisation prévue et qui est un circuit de petite taille avec une forte densité d'éléments de circuit équivalent, considéré comme une seule pièce incluant des éléments interconnectés sur ou dans un substrat unique afin de réaliser une fonction de circuit électronique

Note 1 à l'article: Sont exclus les cartes à circuit imprimé, les assemblages de cartes à circuit et les modules composés exclusivement de composants électroniques séparés.

3.1.13 MRO maintenance, réparation et révision

opérations, telles que des essais, des mesures, des remplacements, des réglages et des réparations, destinées à conserver ou restaurer une unité fonctionnelle à un état spécifié dans lequel l'unité peut réaliser ses fonctions exigées

Note 1 à l'article: Cette activité inclut l'inspection, la reconstruction, la modification et l'approvisionnement des pièces détachées, des accessoires, des matières premières, des adhésifs, des matériaux d'étanchéité, des revêtements et des consommables.

Note 2 à l'article: L'abréviation "MRO" est dérivée du terme anglais développé correspondant "maintenance, repair and overhaul".

3.1.14 distributeur non franchisé

entreprise qui n'appartient pas à un distributeur franchisé ou un OCM

Note 1 à l'article: Ces distributeurs peuvent acheter des composants à des fabricants de composants, des distributeurs franchisés ou en passant par d'autres canaux d'approvisionnement (marchés libres). Ils ne peuvent pas toujours fournir les garanties et l'assistance offertes par le réseau de distributeurs franchisés; les composants fournis par cette source sont généralement protégés par la garantie de la source uniquement.

Note 2 à l'article: Certains distributeurs non franchisés peuvent acheter des composants traçables auprès de l'OCM ou de leurs distributeurs franchisés et fournir les documents de traçabilité et/ou peuvent renvoyer leur stock à l'OCM à des fins d'investigation. Ces distributeurs non franchisés peuvent satisfaire aux exigences du DFARS 252.246.7008 américain (voir A.8.10).

3.1.15 OCM fabricant de composants d'origine

entreprise qui spécifie et fabrique le composant électronique

Note 1 à l'article: L'abréviation "OCM" est dérivée du terme anglais développé correspondant "original component manufacturer".

3.1.16 OEM fabricant d'équipements d'origine

fabricant qui définit le sous-assemblage électronique incluant les composants électroniques ou qui définit les composants utilisés dans un assemblage et/ou une spécification d'essai

Note 1 à l'article: L'abréviation "OEM" est dérivée du terme anglais développé correspondant "original equipment manufacturer".

3.1.17 piratage

violation délibérée des droits d'auteur

3.1.18**composant refabriqu^é
élément recyclé**

composant électronique qui inclut une puce en silicium recyclée ou un élément technologique comme cela est attesté et communiqué par l'entreprise de refabrication du composant électronique et qui est soumis à un essai complet avant d'être vendu

Note 1 à l'article: Les exemples incluent une puce en silicium ou toute autre puce extraite d'un autre composant électronique, nouveau ou usagé, sur laquelle sont apposés le nom et le logo de l'entreprise de refabrication ainsi qu'un numéro de pièce différent.

Note 2 à l'article: La refabrication d'un composant électronique peut nécessiter les données d'ingénierie et les schémas d'origine du produit. Cela ne signifie pas qu'un produit refabriqu^é est identique au nouveau produit.

Note 3 à l'article: Les composants électroniques refabriqués sont souvent accompagnés de garanties.

3.1.19**revendeur**

fournisseur général qui offre un choix de composants électroniques à commander dans un catalogue

3.1.20**composant recyclé**

composant électrique retiré de son produit ou de son assemblage d'origine, et disponible pour réutilisation

Note 1 à l'article: Le composant comprend des logos, des marques déposées et des marques authentiques. Cependant, il n'existe généralement pas de données permettant de mesurer la durée de vie utile restante pour sa réutilisation. Un composant recyclé peut tomber en panne plus tôt qu'un composant neuf lorsqu'il est réassemblé dans un autre produit ou assemblage. Un composant recyclé peut également avoir subi des dommages physiques ou des dommages liés aux décharges électrostatiques (DES) pendant le processus de dépose.

3.1.21**semiconducteur**

composant électronique dont la principale caractéristique est la conduction électronique qui a lieu dans un semiconducteur

Note 1 à l'article: Sont inclus les diodes à semiconducteurs qui sont des dispositifs à semiconducteurs équipés de deux bornes et d'une caractéristique tension/courant non linéaire, et les transistors qui sont des dispositifs à semiconducteurs actifs capables d'assurer une amplification de puissance et équipés de trois bornes ou plus.

3.1.22**sous-traitant**

fabricant de sous-assemblages électroniques ou fournisseur qui fabrique des éléments conformément à l'ensemble des données de conception et aux dessins du client, sous l'autorité de l'OEM

Note 1 à l'article: Ce fournisseur peut éventuellement obtenir tout ou partie des composants électroniques exigés pour produire un sous-assemblage; il est souvent désigné comme fabricant électronique contractuel (CEM) ou services de fabrication de composants électroniques (EMS).

3.1.23**fournisseur**

entreprise qui fournit à une autre entreprise un composant électronique et dont le logo ou le nom est apposé sur le dispositif

Note 1 à l'article: Un fournisseur peut être un OCM, un distributeur franchisé ou un agent, un distributeur non franchisé, un courtier, un revendeur, un OEM, un CEM, un EMS, etc.

3.1.24**composant suspect**

composant électronique dont la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant d'origine a été perdue, qui peut avoir été dénaturé par le fournisseur ou le fabricant, et qui peut correspondre à la définition de composant frauduleux ou contrefait

Note 1 à l'article: Les composants suspects peuvent inclure, entre autres:

- 1) des composants contrefaits;
- 2) les composants recyclés provenant d'opérations de recyclage non contrôlées, effectuées en externe de l'OEM, du réseau franchisé et d'entreprises OEM, vendus frauduleusement à l'OEM comme étant neufs et inutilisés.

3.1.25

traçabilité

capacité de disposer de la trace complète d'un composant électronique remontant jusqu'au fabricant de composants d'origine

Note 1 à l'article: Cette traçabilité signifie que chaque fournisseur de la chaîne d'approvisionnement est prêt à déclarer juridiquement par écrit qu'il connaît et peut identifier sa source d'approvisionnement, qui remonte au fabricant d'origine, et qu'il peut confirmer que les composants électroniques sont neufs et qu'ils ont été manipulés en prenant les mesures appropriées afin d'éviter tout dommage lié aux décharges électrostatiques et à la sensibilité à l'humidité. Elle authentifie que les composants électroniques fournis sont inutilisés, neufs et qu'ils n'ont subi aucun dommage lié aux décharges électrostatiques, à la sensibilité à l'humidité ou autre. Elle garantit que les composants électroniques sont protégés par les garanties du fabricant, qu'ils disposent de l'intégralité de leur durée de vie restante et de leur fonction conformément à la fiche technique publiée par le fabricant, qui présente la durée de vie prévue du composant dans l'application pour les prévisions de fiabilité et la garantie de produit de l'OEM.

3.1.26

non traçable

propriété des composants électroniques qui ont perdu leur traçabilité (voir 3.1.25)

3.2 Termes abrégés

AAIPT	Alliance Against IP Theft (Alliance contre le vol de propriété intellectuelle)
ACAC	Accord Commercial Anticontrefaçon
ACTF	Semiconductor Industries Association Anti Counterfeit Task Force (Groupe de travail anticontrefaçon de l'Association de l'industrie des semi-conducteurs)
ADHP	Aerospace, Defence And High Performance (aérospatial, défense et hautes performances)
ASIC	Application Specific Integrated Circuit (circuits intégrés spécifiques à l'application)
ATP	acceptance test procedure (procédure d'essai d'acceptation)
BEAMA	British Electrotechnical Allied Manufacturers' Association
BoM	bill of materials (nomenclature des matériels)
CAAC	Civil Aviation Administration of China (Administration de l'aviation civile de Chine)
CATA	China Anti-counterfeit Technology Association
CB	certifying body (organisme de certification tiers)
CNIPA	China National Intellectual Property Administration (Administration nationale chinoise de la propriété intellectuelle), RPC
COTS	commercial off the shelf (produit disponible dans le commerce)
CdC	certificat de conformité
CEC	China Electronics Corporation (Société chinoise des composants électroniques)
CECA	China Electronic Components Association (Association chinoise des composants électroniques)
CEEI	China Electrical Equipment Association (Association chinoise des équipements électroniques)
CEM	contract electronic manufacturer (fabricant électronique contractuel)
CESI	China Electronics Standardization Institute (Institut chinois de normalisation des composants électroniques)
CMM	component maintenance manuals (manuels de maintenance des composants)
CQAE	China Quality Management Association for Electronics Industry

CMOS	complementary metal oxide semiconductor (semiconducteur à oxyde de métal complémentaire)
DFARS	Defense Federal Acquisition Regulation System (Système de contrôle des acquisitions fédérales pour la défense)
DLF	direct line feed (approvisionnement en ligne directe)
DOD	Department of Defence (US) (Département de la Défense des Etats-Unis)
DMEA	Defense MicroElectronics Activity
DMSMS	diminishing manufacturing sources and material shortages (sources de fabrication en diminution et pénuries de matériaux)
ADN	acide désoxyribonucléique
DSCC	Defence Supply Centre Columbus (Centre d'approvisionnement de la défense de Colombus)
DLA	Defense Logistics Agency (Agence de logistique de la Défense) (anciennement DSCC)
AESA	Agence européenne de la sécurité aérienne
ECIA	Electronic Components Industry Association (Association des entreprises de composants électroniques)
ECMP	electronic components management plan (plan de gestion des composants électroniques)
ECSN	electronic component supplier network (réseau du fournisseur de composants électroniques)
EMS	electronics manufacturing services (services de fabrication de composants électroniques)
ERAI	Electronic Reseller Association International (Association internationale des revendeurs d'électronique) (voir http://www.eraï.com)
DES	Décharge électrostatique
ESIA	European Semiconductor Industries Association (Association européenne de l'industrie des semiconducteurs)
EOS	Electrical Overstress (surcharge électrique)
UE	Union européenne
EUIPO	European Union Intellectual Property Office (Office de l'Union européenne pour la propriété intellectuelle)
FAA	Federal Aviation Administration (Administration fédérale de l'aviation)
FAR	Federal Avionic Regulations (Règlements fédéraux relatifs à l'avionique)
FFF	form, fit and function (forme, conformité et fonction)
FIT	failures in time (défaillances dans le temps)
FPD	flat panel display (écran plat)
FPGA	field-programmable gate array (réseau de portes programmables in situ)
FSC	Federal Supply Class (Classification fédérale des approvisionnements)
G-19	Comité SAE Counterfeit Electronic Parts (pièces électroniques de contrefaçon)
GAMS	Government/Authorities meeting on Semiconductors (Réunion des gouvernements et des autorités sur les semiconducteurs)
GIFAS	Groupement des Industries Françaises Aéronautiques Et Spatiales
HAST	highly accelerate stress testing (essais accélérés de contrainte)
HIS	hardware intrinsic security (sécurisation matérielle intrinsèque)
HTOL	high temperature operating life (durée de vie en fonctionnement à haute température)

IAQG	International Aerospace Quality Group – SAE (Groupe international de qualité en aérospatiale)
CCI	Chambre de commerce internationale
ID	independent distributors (distributeurs indépendants)
IDEA	Independent Distributors of Electronics Association (Association des distributeurs d'électronique indépendants)
IEC	International Electrotechnical Commission (Commission électrotechnique internationale)
INEMI	International Electronics Manufacturing Initiative
PI	propriété intellectuelle
IPR	intellectual property rights (droits de propriété intellectuelle)
FAI	fournisseur d'accès à Internet
ITAR	International Traffic in Arms Regulations (Règlementation américaine sur le trafic d'armes au niveau international)
IUID	Item Unique Identification (identification unique d'un article)
JEDEC	Joint Electron Device Engineering Council (Conseil conjoint d'ingénierie pour les dispositifs électroniques)
JIT	just in time (juste à temps)
JPO	Japanese Patent Office (Office des brevets du Japon)
LED	light emitting diode (diode électroluminescente)
LDC	lot date code (code de date de lot)
LTB	last time buy (dernier achat)
MEMS	Micro-Electromechanical Systems (microsystèmes électromécaniques)
MOD	Ministry of Defence, UK (Ministère de la Défense, Royaume-Uni)
MRO	Maintenance, Repair and Overhaul (maintenance, réparation et révision) (concerne les opérations destinées à conserver ou restaurer une unité fonctionnelle)
MTBF	mean time between failure (temps moyen entre pannes)
MTTF	mean time to failure (temps moyen avant défaillance)
MSL	moisture sensitivity level (degré de sensibilité à l'humidité)
OTAN	Organisation du traité de l'Atlantique nord
NDAA	National Defense Acquisition Act (Acte d'acquisition de la défense nationale)
NEDA	National Electronics Distributors Association (Association nationale des distributeurs d'électronique)
NVRAM	non volatile random access memory (mémoire RAM non volatile)
OCM	original component manufacturer (fabricant de composants d'origine)
OCDE	Organisation de coopération et de développement économiques
OEM	original equipment manufacturer (fabricant d'équipements d'origine)
PCB	printed circuit board (circuit imprimé)
PCN	product change notice (notice de modification du produit)
PQDR	product quality deficiency report (rapport sur la qualité et la défectuosité des produits)
RPC	République populaire de Chine
PV	photovoltaïque
QTSL	Qualified Testing Suppliers List (liste des fournisseurs d'essai certifiés)

RECS	Reliable Electronic Component Supplier (fournisseur fiable de composants électroniques)
PUF	physical unclonable function (fonction physique non clonable)
RFID	radio frequency identity detection (radio-identification)
RAM	random access memory (mémoire vive)
ROM	read only memory (mémoire morte)
SAE	Society of Automotive Engineers (Société des ingénieurs automobiles)
SEE	single event effect (effet singulier)
SEU	single event upset (effet singulier de basculement)
SER	soft error rate (taux d'erreurs logicielles)
SIA	Semiconductor Industries Association (Association de l'industrie des semiconducteurs)
SRAM	static random access memory (mémoire vive statique)
TAPO	Trusted Access Program Office
TSO	Trading Standards Officers (professionnels des normes de commercialisation)
UK	United Kingdom (Royaume-Uni)
UKEA	UK Electronics Alliance
UNG	unique number generator (générateur de nombre unique)
USA	United States of America (Etats-Unis d'Amérique)
OMPI	Organisation mondiale de la propriété intellectuelle
WSC	World Semiconductor Council (Conseil mondial des semiconducteurs)

4 Exigences techniques

4.1 Généralités

Le présent document réduit le plus possible les activités frauduleuses, de contrefaçon et de recyclage en respectant la propriété intellectuelle et en permettant l'achat de composants traçables.

Les exigences minimales concernant le fabricant d'équipements avioniques d'origine sont définies en 4.2. Elles s'appliquent, en intégralité ou en partie, aux opérations de MRO sous la responsabilité de l'OEM.

Les paragraphes 4.3 à 4.14.6 fournissent des informations complémentaires au 4.2.

Les annexes informatives sont fournies à la fin du présent document et leur contenu est susceptible d'être modifié. Les utilisateurs du présent document sont invités à examiner les dernières données disponibles chaque fois que le contenu de ces annexes est cité en référence.

- L'Annexe A fournit des informations de référence croisée concernant toutes les institutions et organisations traitées à l'Article 4.
- L'Annexe B fournit des exemples de sources du marché secondaire qui doivent être prises en compte dans les cas d'obsolescence (voir 4.12.9).
- L'Annexe C fournit un exemple de certificat de RECS chinois type (voir 4.7.2).
- L'Annexe D fournit un organigramme des exigences de l'IEC 62668-1 et leur relation aux normes externes.
- L'Annexe E fournit des exemples types de déploiement de normes de prévention de la contrefaçon dans la chaîne d'approvisionnement.

Les principaux éléments à contrôler et à comprendre sont les suivants:

- la définition de la propriété intellectuelle (voir 4.3);
- les limitations du terme "contrefaçon" (voir 4.4);
- la description correcte de "composants frauduleux" (voir 4.4.3);
- la définition du recyclage et la raison pour laquelle l'industrie avionique limite le recyclage aux activités internes uniquement (voir 4.6);
- l'utilisation de fabricants de composants d'origine (OCM) qui protègent leur propriété intellectuelle (voir 4.7);
- l'utilisation de distributeurs franchisés ou de sources approuvés (voir 4.10);
- l'utilisation de processus de gestion des risques et d'essai des composants lors de l'achat de composants suspects non traçables auprès de distributeurs non franchisés conformément à l'IEC 62668-2 (voir 4.12.6);
- la protection de la propriété intellectuelle de l'OEM, tout au long du cycle de vie des produits, y compris la gestion de l'ensemble des pièces détachées;
- le signalement de violations de la propriété intellectuelle en discutant avec les clients et en appliquant la loi locale (voir 4.14, A.7.2 et Article A.8 pour les contacts utiles);
- la formation des employés compétents (voir 4.15);
- l'utilisation de la gestion de l'obsolescence (voir 4.12.1) pour atténuer le risque d'achat de composants contrefaits.

4.2 Exigences minimales concernant le fabricant d'équipements avioniques d'origine

Les fabricants d'équipements avioniques d'origine doivent:

- a) Protéger leurs droits de propriété intellectuelle (voir 4.3, 4.4, 4.5, 4.12 et 4.13).
- b) Choisir les composants auprès de fabricants de composants d'origine (OCM) qui contrôlent leurs droits de propriété intellectuelle (voir 4.3, 4.7), qui précisent les numéros uniques des pièces dont la configuration est contrôlée et qui apposent un marquage sur les pièces (voir 4.7.6), tout en évitant l'utilisation de composants refabriqués (voir 3.1.18) dans la mesure du possible.
- c) Utiliser un processus de prévention des composants contrefaits, frauduleux et recyclés, conforme aux exigences définies dans le présent paragraphe, qui peut inclure un plan de gestion de la prévention de la contrefaçon conforme au présent document et qui peut reposer sur des plans tels que ceux de la SAE-AS5553A ou de la SAE AS5553B ou autres plans similaires (voir 4.12.13). Les OEM doivent transmettre cette exigence aux fournisseurs de niveau inférieur (voir 4.12.13.3).

NOTE 1 Les Figures E.1, E.2, E.3, E.4 et E.5 peuvent aider à déployer les normes de prévention de la contrefaçon.

NOTE 2 L'AS/EN/JISQ 9100 et/ou l'AS/EN/JISQ 9110 comportent des exigences de haut niveau concernant la gestion de la prévention de la contrefaçon pour tous les types de composants et matériaux électriques et mécaniques et peuvent être utilisées pour répondre à ce besoin (voir 4.7.3 et 4.12.1). Certains documents tels que l'IEC TS 62239-2 et la SAE AS6174 (voir 4.12.13) peuvent également aider à gérer la prévention de la contrefaçon.

- d) Utiliser un processus (voir 4.12) pour procéder à l'audit de l'ensemble des sources d'approvisionnement en composants.

NOTE 3 L'AS/EN/JISQ 9100 et/ou l'AS/EN/JISQ 9110 peuvent satisfaire à cette exigence.

- e) Utiliser un processus qui permet l'achat de composants traçables uniquement (voir 4.4.4), comme suit:
 - 1) auprès du fabricant de composants d'origine (OCM) (voir 4.7) en utilisant n'importe quelle mesure de traçabilité appropriée, telle que l'utilisation des mesures de l'ACTF (Semiconductor Industries Association Anti Counterfeit Task Force) (voir 4.7.7) ou de la fonction physique non clonable (PUF) (voir 4.7.10);

- 2) directement auprès du Trusted Foundry Program américain (voir 4.7.8) et/ou du Trusted IC Supplier Accreditation Program américain (voir 4.7.9) lorsque le contrat du client l'exige ou dans les cas appropriés;
- 3) dans les cas où le composant est obsolète, en achetant directement auprès du fabricant franchisé du marché secondaire (voir 4.12.9 et Annexe B);
- 4) auprès de distributeurs franchisés (voir 4.10):
 - de préférence approuvés par l'AS/EN/JISQ 9120 (voir 4.9);
 - également approuvés au minimum au titre de l'ISO 9001 (voir 4.8); ou
 - conformes aux exigences de la SAE AS 6496 (voir Article A.16);
 - auprès de distributeurs non franchisés (voir 4.11) conformes à l'IEC 62668-2.

NOTE 4 La SAE AS6171 peut aider à utiliser l'IEC 62668-2.

NOTE 5 Certains schémas de suivi (voir 4.10.3) ou initiatives inaltérables peuvent faciliter la traçabilité et l'authentification.

NOTE 6 L'AS/EN/JISQ 9100 et/ou l'AS/EN/JISQ 9110 peuvent satisfaire aux exigences de traçabilité.

- f) Utiliser un processus qui évite de recourir à des courtiers non approuvés (voir 4.11.5).

NOTE 7 L'AS/EN/JISQ 9100 et/ou l'AS/EN/JISQ 9110 peuvent satisfaire à cette exigence.

- g) Dans les rares cas où un fabricant d'équipements avioniques d'origine juge qu'il est nécessaire d'acheter des composants non traçables:

- 1) effectuer et documenter une recherche exhaustive portant sur les composants alternatifs traçables, y compris l'examen des modifications de conception possibles afin de prendre en charge les composants alternatifs traçables et les sources du marché secondaire (voir 4.12, en particulier 4.12.9, 4.12.10, 4.12.11 et Annexe B);
- 2) utiliser et documenter un processus de gestion des risques permettant d'évaluer les exigences supplémentaires nécessaires pour déterminer que les composants ne sont pas contrefaits, recyclés ou frauduleux, en utilisant les exigences définies dans l'IEC 62668-2. Le processus de gestion des risques inclut les aspects de conformité, qualité, fiabilité et performances de maintenance.

NOTE 8 La SAE AS6171 peut satisfaire aux exigences de l'IEC 62668-2.

- h) Utiliser un processus pour les opérations de réparation et de reprise (voir 4.13.9) qui doit inclure la certification AS/EN/JISQ 9110 pour l'ensemble des opérations de maintenance.
- i) Signaler les incidents liés aux activités frauduleuses et de contrefaçon conformément à la loi locale (voir 4.14) et aux exigences du client.
- j) Mettre en place une formation de sensibilisation à la prévention de la contrefaçon destinée au personnel compétent, fondée sur le Tableau 1 qui fournit des recommandations et identifie le personnel compétent et les registres de formation (voir 4.15). Si le personnel vient d'être engagé, initier une formation immédiate pour la discipline ou le département en question.
- k) Utiliser un processus permettant de vérifier que les composants ne sont pas contrefaits ou recyclés de manière frauduleuse et qu'ils satisfont aux exigences définies dans le contrat.

NOTE 9 L'AS/EN/JISQ 9100 et/ou l'AS/EN/JISQ 9110 peuvent satisfaire à cette exigence.

NOTE 10 Ce processus s'applique également aux composants renvoyés et aux composants excédentaires vendus avec promesse de rachat (technique du "buy back"), lors du rachat d'un stock excédentaire auprès d'un sous-traitant ou de transferts internes, par exemple.

- l) Utiliser un processus d'obsolescence pour réduire les achats de composants obsolètes.

NOTE 10 L'IEC 62239-1, l'IEC TS 62239-2, l'IEC 62402 ou la SAE STD016 peuvent être utilisées pour satisfaire à cette exigence.

- m) Appliquer, en intégralité ou en partie, conformément à l'application, les exigences définies aux points a) à l) pour leurs opérations de MRO, et/ou utiliser un processus permettant d'échelonner les exigences applicables et de contrôler leurs implémentations si les opérations de MRO sont sous-traitées à des organisations de MRO.

Tableau 1 – Lignes directrices pour la formation de sensibilisation à la prévention de la contrefaçon

Discipline ou département	Type de formation de sensibilisation	Fréquence	Commentaires
Sourcing, achat ou approvisionnement	Traçabilité dans la chaîne d'approvisionnement, différences entre les courtiers, différents types de distributeurs (franchisés, non franchisés), l'OCM, etc. Quand soulever des questions.	Tous les 2 ans	Passer à une formation tous les ans si une nouvelle modification ou un nouveau développement majeur(e) doit être transmis(e) ou si le département possède un bilan de gestion de la prévention de la contrefaçon médiocre.
Sous-traitance de l'approvisionnement	La manière dont il convient que les sous-traitants contrôlent leur chaîne d'approvisionnement pour un produit avionique, la manière dont les modifications doivent être gérées et approuvées par l'OEM avant leur implantation.	Tous les 2 ans	
Conception matérielle	La raison pour laquelle l'approvisionnement ne peut pas être effectué directement par Internet; la raison pour laquelle les fournisseurs approuvés et les distributeurs franchisés sont nécessaires, etc.	Tous les 2 ans	
Gestion du programme	La raison pour laquelle l'approvisionnement ne peut pas être effectué directement par Internet, la raison pour laquelle les fournisseurs approuvés sont nécessaires, etc. La manière dont la gestion de l'obsolescence atténue le risque de fournir des composants contrefaits.	Tous les 2 ans	
Ingénierie des composants	Type d'essai qui peut être utilisé pour réduire le plus possible l'utilisation des composants contrefaits; la manière dont il convient de gérer les numéros de pièces et les non-conformités, etc. La manière dont la gestion de l'obsolescence atténue le risque de fournir des composants contrefaits.	Tous les 2 ans	
Réception des produits Importation des produits Entrepôt Kitting, département de kitting des matériaux	La raison pour laquelle l'inspection visuelle est nécessaire et la raison pour laquelle le souci du détail concernant les numéros de pièces, l'étiquetage, les certificats de conformité et les documents est nécessaire. Comment soulever des préoccupations.	Tous les 2 ans	

Discipline ou département	Type de formation de sensibilisation	Fréquence	Commentaires
Qualité des fournisseurs	Comment effectuer un audit pour prévenir la contrefaçon. Listes de contrôle, etc. Avec qui discuter des problèmes et comment gérer les actions correctives.	Tous les 2 ans	
Département d'assemblage en production	Sensibilisation générale; comment signaler une préoccupation si le marquage d'une pièce semble suspect, etc. Examiner les tendances des défaillances des essais en production et enquêter sur les rendements faibles dont la cause peut être des composants contrefaits ou frauduleux.	Tous les 2 ans	
Département des essais	Sensibilisation générale pour la prise en compte de la contrefaçon dans les analyses ou les recherches de défauts.	Tous les 2 ans	

4.3 Propriété intellectuelle

4.3.1 Généralités

La définition et la connaissance de la propriété intellectuelle (PI) sont la base des activités de prévention de la contrefaçon. Il est question de contrefaçon lorsque la PI du fabricant d'origine est enfreinte de manière frauduleuse. Les activités de prévention de la contrefaçon sont donc liées au maintien de la propriété intellectuelle.

L'Organisation Mondiale de la Propriété Intellectuelle (OMPI) est une agence spécialisée des Nations Unies. Elle se consacre au développement d'un système de PI international équilibré et accessible, qui récompense la créativité, stimule l'innovation et contribue au développement économique tout en protégeant l'intérêt public.

L'OMPI a été créée par la Convention instituant l'OMPI en 1967 dans le cadre d'un mandat accordé par les Etats membres dans le but de promouvoir la protection de la PI à l'international par la coopération des Etats et en collaboration avec d'autres organisations internationales. Son siège social se trouve à Genève, en Suisse. Pour plus d'informations sur l'OMPI, voir Article A.1. La liste suivante répertorie les offices régionaux de propriété intellectuelle:

- a) Etats-Unis: le United States Patent and Trademark Office (voir A.8.1).
- b) Royaume-Uni: l'Intellectual Property Office (voir A.6.1), qui fournit des informations supplémentaires et des détails sur l'outil de diagnostic en ligne IP Health Check.
- c) Europe: la page web Europa contient des récapitulatifs de la législation de l'Union européenne pour la propriété intellectuelle (voir A.7.1).
- d) Chine: le State Intellectual Property Office de la RPC (voir A.9.1).

La liste suivante répertorie des ressources supplémentaires qui fournissent des informations sur la propriété intellectuelle:

- 1) La page web de l'OMPI (voir A.1.3) comporte des liens vers les traités administrés par l'OMPI, avec le détail des législations d'un grand nombre de pays et d'autres informations connexes (voir A.1.4). Elle inclut également les membres actuels du Réseau mondial d'académies de la propriété intellectuelle (PI).
- 2) L'International Intellectual Property Alliance est une coalition du secteur privé formée en 1984, constituée d'organisations professionnelles représentant les industries américaines fondées sur le droit d'auteur qui s'efforcent, dans le cadre d'efforts bilatéraux et multilatéraux, d'améliorer la protection et l'application des documents protégés par des droits d'auteur à l'international et d'ouvrir les marchés étrangers fermés par le piratage et autres barrières à l'accès au marché (voir A.8.4).
- 3) La page web Stopfakes de l'International Trade Administration du Département du Commerce des Etats-Unis (voir A.8.2) comporte des liens vers les toolkits de propriété intellectuelle pour d'autres pays.
- 4) La page web de l'ambassade des Etats-Unis en Chine (voir A.8.3) comporte des informations très utiles concernant le contrôle de la PI lors de l'importation de produits en Chine.

4.3.2 Définition de la propriété intellectuelle

4.3.2.1 Généralités

La propriété intellectuelle (PI) est définie en 3.1.11 et peut être contrôlée par l'emploi:

- de brevets;
- de marques;
- de la protection des droits d'auteur;
- d'enregistrements des données de conception.

4.3.2.2 Brevets

Les brevets sont des droits territoriaux. Ils s'appliquent donc dans un pays, dans l'Union européenne (UE), ou par le biais du Traité de coopération en matière de brevets. Un brevet délivré devient une propriété et peut être vendu ou faire l'objet d'une cession de licence. Un brevet a une durée de vie maximale de 20 ans. Pour plus d'informations, voir:

- l'OMPI (voir A.1.3);
- l'Office européen des brevets (voir A.7.3.);
- le Chinese Patent and Trademark Office (voir A.9.2); ou
- l'Office des brevets du Japon (voir l'Article A.10).

4.3.2.3 Marques

Les marques sont des symboles, comme des mots, des logos, des images ou toute combinaison de ceux-ci. Elles sont territoriales et doivent être classées dans chaque pays où la protection est sollicitée.

Il convient d'enregistrer les marques auprès:

- de l'OMPI pour le Système de Madrid concernant l'enregistrement international des marques qui offre une solution de protection des marques dans plusieurs pays par le dépôt d'une seule demande (voir A.1.3); ou
- de l'EUIPO en Europe (voir A.7.4) pour une "marque communautaire" applicable à tous les Etats membres de l'Union européenne; ou
- du Chinese Patent and Trademark Office en Chine (voir A.9.2); ou
- du United States Patent and Trademark Office aux Etats-Unis (voir A.8.1).

4.3.2.4 Droit d'auteur

Il s'agit d'un droit automatique qui peut être concédé sous licence ou vendu. Utiliser © en suffixe d'un nom donné.

4.3.2.5 Données de conception

Les données de conception font référence à l'apparence physique d'un élément ou d'une partie d'un élément. Il convient d'enregistrer les données de conception dans le pays concerné, auprès de l'EUIPO pour l'Union européenne (voir A.7.4) ou auprès de l'OMPI (voir A.1.3).

4.4 Prise en compte de la contrefaçon

4.4.1 Généralités

Différentes définitions du terme "contrefaçon" sont actuellement utilisées dans l'industrie avionique; elles concernent principalement la violation des droits de propriété intellectuelle. Ces définitions nécessitent toutefois d'utiliser la définition légale afin de garantir que le système judiciaire puisse continuer à gérer les problèmes de contrefaçon en appliquant la loi. Il convient de ne pas confondre la définition du terme "contrefaçon" avec celle du terme "recyclage" (voir 4.6).

4.4.2 Définition légale de la contrefaçon

Voir 3.1.4 pour obtenir la définition du terme "contrefaçon" et 3.1.5 pour la définition de "composant contrefait". Ces définitions reposent sur l'ISO 16678.

Chaque pays possède généralement une définition légale légèrement différente, mais toutes les définitions sont généralement fondées sur la contrefaçon de marque.

4.4.3 Composants frauduleux

Voir 3.1.10 pour la définition d'un "composant frauduleux". Les composants frauduleux sont vus comme un sous-ensemble dans la zone des composants suspects; pour obtenir la définition de "composant suspect", voir 3.1.24 et Figure 1. Les composants suspects exigent des recherches complémentaires afin de déterminer s'il s'agit de composants frauduleux, recyclés frauduleusement ou contrefaits.

NOTE Il est relativement facile pour le système judiciaire de suivre les traces de l'argent provenant d'activités frauduleuses par le biais du système bancaire; le nombre de condamnations juridiques pour fraude est donc bien plus élevé que pour les activités de contrefaçon. Avec le développement du marché du recyclage des composants électroniques, les courtiers peu scrupuleux sont également tentés d'intensifier leur activité pour trouver des composants recyclés à l'état neuf et "inutilisé" afin d'augmenter leurs bénéfices. Ainsi, la vente de composants à l'état neuf et "inutilisé" recyclés frauduleusement augmente à mesure que l'industrie de recyclage des composants électroniques se développe.

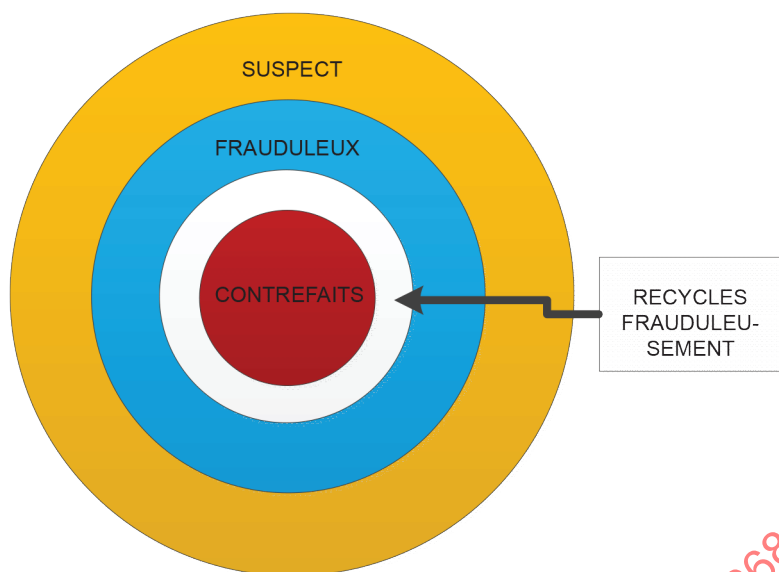


Figure 1 – Zone des composants suspects

4.4.4 Comment mettre en place la traçabilité

Voir 3.1.24 pour la définition de "traçabilité". La traçabilité est généralement attestée par des certificats de conformité (CdC), des bordereaux d'expédition (voir 4.12.4) ou toute autre méthode de suivi des composants permettant de remonter jusqu'à l'OCM.

Lorsque la traçabilité n'est pas disponible, les informations nécessaires peuvent être obtenues auprès des systèmes commerciaux du fournisseur ou par le biais d'autres bases de données.

En effet, le distributeur ou le fabricant franchisé du marché secondaire peut ne pas toujours être en possession du certificat de conformité ou du bordereau d'expédition d'origine transmis par l'OCM, mais peut disposer d'entrées dans la base de données du système commercial confirmant la date de réception du fournisseur (il convient que le fournisseur soit l'OCM ou l'un de ses distributeurs franchisés), la quantité et le code de date de lot. Il convient que ces informations issues du système commercial combinées à une copie du contrat de franchise fournissent suffisamment d'informations pour satisfaire aux exigences de traçabilité et remonter jusqu'à l'OCM.

NOTE 1 L'audit de traçabilité de l'IECQ OD 3702 peut être utilisé en tant que processus d'audit de seconde partie ou de tiers à des fins de vérification à n'importe quel stade de la chaîne d'approvisionnement (voir Figures E.3 et E.4).

NOTE 2 L'IPC-1782 peut également faciliter la traçabilité d'éléments critiques fondés sur le risque.

4.4.5 Motifs de perte de traçabilité d'un composant

Un grand nombre de composants perdent leur traçabilité (voir 3.1.26 pour obtenir la définition de "non traçable") et il est donc impossible de remonter jusqu'au fabricant d'origine. En voici les causes possibles:

- Un système de rangement médiocre et la rétention des documents par les distributeurs ou les OEM. Un grand nombre d'OEM déplacent leur stock d'un lieu à un autre et perdent leurs documents de traçabilité dans le processus.
- Les OEM liquident souvent leur stock excédentaire en le réinjectant dans la chaîne d'approvisionnement, sans fournir les documents de traçabilité, et tentent ensuite de racheter ce stock. Ces composants sont identifiés par la suite comme étant "suspects". Sans traçabilité, ce stock devient alors un possible stock de "contrefaçon".

- Les distributeurs qui ne contrôlent pas la chaîne d'approvisionnement pour savoir si les composants disposent d'une traçabilité permettant de remonter jusqu'au fabricant d'origine. La plupart des distributeurs non franchisés ne sont pas capables de gérer cette traçabilité. La longueur de la chaîne d'approvisionnement pouvant être très importante, les informations peuvent ne pas être disponibles à partir d'un certain point. Ce manque d'informations rend les composants "suspects" et ils sont donc jugés comme un possible stock de contrefaçon
- L'utilisation de distributeurs inappropriés pour le marché de l'avionique, qui ne sont pas certifiés AS/EN/JISQ 9120. Bien qu'ils puissent généralement se fournir directement auprès des fabricants, ces distributeurs ne peuvent pas le prouver, car leurs opérations d'entreposage et leurs processus de traçabilité ne sont pas capables de suivre les lots individuels de composants et leur origine.
- Les composants de qualité commerciale qui ne sont pas fournis avec leurs documents de traçabilité complets permettant de remonter jusqu'à l'OEM.

4.5 Le problème de la contrefaçon

4.5.1 Généralités

Les récents rapports publiés par le Government Accountability Office des Etats-Unis décrivent la mesure dans laquelle les activités de contrefaçon affectent l'économie américaine:

- GAO-10-423;
- GAO-12-375;
- GAO-12-213T;
- GAO-13-762T;
- GAO-03-713T;
- GAO-16-236;
- rapport du Département de la Sécurité intérieure des Etats-Unis intitulé "Supporting Innovation, Creativity and enterprise, charting the path ahead FY2017-2019" (voir A.8.12).

Europol rend également compte de l'impact des activités de contrefaçon (voir A.7.2).

L'Office des brevets du Japon a également rédigé le rapport intitulé "FY2004 Survey Reports on Losses Caused by Counterfeiting" (voir Article A.10).

L'OCDE (Organisation de coopération et de développement économiques) a publié plusieurs rapports concernant l'impact du commerce de produits de contrefaçon (voir Article A.18).

La Chambre de commerce internationale (CCI) effectue également un suivi de l'impact de la contrefaçon et du piratage en proposant des prévisions jusqu'en 2016 (voir Article A.19).

Plusieurs vidéos en ligne mettent également en évidence le lien entre le crime organisé et la contrefaçon (voir Article A.27).

NOTE La contrefaçon est un commerce en pleine croissance, car les sanctions prévues par les systèmes de justice pénale sont généralement minimales. Les sanctions types incluent une amende d'un faible montant sans emprisonnement. Les faibles sanctions prévues par le système de justice pénale permettent aux accusés de quitter la salle d'audience et de reprendre leurs opérations de contrefaçon le jour même.

4.5.2 Activités mondiales relatives aux questions de lutte contre la contrefaçon

4.5.2.1 Généralités

Il existe plusieurs activités anticontrefaçon en cours, qui viennent appuyer les activités de maintien de l'ordre, comme indiqué ci-après.

4.5.2.2 Accord commercial anticontrefaçon (ACAC)

L'accord commercial anticontrefaçon (ACAC) est un traité multinational dont le but est l'établissement de Normes internationales relatives à la mise en application des droits de propriété intellectuelle (voir A.2.1). Malheureusement, il n'a pas fait consensus sur le plan mondial.

4.5.2.3 Réunion des gouvernements et des autorités sur les semiconducteurs (GAMS)

Le GAMS, fondé en 1999 par une déclaration commune sur les semiconducteurs, a pour but la promotion d'un commerce et d'une croissance justes et équitables au sein du marché mondial des semiconducteurs, par le biais d'une meilleure compréhension mutuelle entre les industries et les gouvernements, ainsi que par le biais des rapports du Conseil mondial des semiconducteurs. Le GAMS s'occupe des questions relatives à la prévention de la contrefaçon (voir Article A.3).

4.5.3 Différences culturelles

De nombreuses cultures ne connaissent pas le concept de propriété intellectuelle et ne satisfont pas aux définitions de l'OMC relatives à la propriété intellectuelle (voir 4.3). Compte tenu du développement du commerce mondial, il est essentiel que l'ensemble des organisations mondiales satisfasse aux définitions relatives à la propriété intellectuelle. Tout manquement dans ce domaine peut se traduire par des réclamations pour contrefaçon alors qu'il n'y a aucune volonté de tromperie. Par exemple, il est courant que les composants et les matériaux locaux soient produits localement, mais cela peut ne pas correspondre complètement aux exigences du client. Un substitut local est souvent la seule possibilité en vue d'une livraison rapide. Il est cependant essentiel que tout composant ou matériau de substitution soit signalé au client et que celui-ci donne son accord avant l'expédition de ces substituts. Tout défaut d'information du client peut porter celui-ci à déclarer les composants "suspects" et par voie de conséquence "contrefaits".

4.5.4 Equipements avioniques et contrefaçon

4.5.4.1 Généralités

Les problèmes d'obsolescence des composants destinés à l'avionique peuvent se produire dans les situations suivantes:

- les composants obsolètes sont difficiles à trouver et proviennent de distributeurs franchisés ou des fabricants de composants d'origine, qui peuvent avoir cessé de les vendre;
- les livraisons à délai élevé (par exemple supérieur à 26 semaines) peuvent avoir lieu s'agissant de lots spécialement assemblés, provenant de sources franchisées du marché secondaire ou des fabricants de composants d'origine;
- seules de petites quantités peuvent être disponibles.

Ces situations créent généralement un marché à haute valeur ajoutée, où le coût du composant à cette étape de son cycle de vie peut être considérablement plus élevé que son coût originel. De plus, des exigences à court terme pèsent généralement sur les fabricants d'équipements avioniques d'origine et ceux-ci souhaitent éviter des reconceptions onéreuses. Ces situations sont très attirantes pour les fraudeurs et les contrefacteurs souhaitant abuser de l'industrie avionique.

Un marché caractérisé par une demande urgente se crée alors. Il peut être approvisionné par des composants frauduleux et contrefaits.

Il s'agit là d'un problème récurrent, particulièrement lorsque les exigences pesant sur les fabricants d'équipements avioniques d'origine comprennent la prise en charge d'équipements avioniques de conception ancienne. Dans ce type de situation, l'activité de production actuelle peut, par exemple, répondre à une activité de réparation où se poseront des problèmes d'obsolescence. La tentation est très forte pour les contrefacteurs de continuer à produire des composants destinés à ce marché de l'obsolescence avionique et par là même de créer une source d'argent "facile". Les activités de contrefaçon se sont complexifiées à mesure que cette activité a gagné en notoriété et que les activités du secteur de l'approvisionnement de l'avionique se sont étendues.

Aujourd'hui, il est assez courant que les composants électroniques contrefaits et frauduleux présentent un aspect authentique et fonctionnent à température ambiante, parfois même à des températures extrêmes. Les méthodes actuelles de détection de la contrefaçon se doivent d'être plus complexes que la simple combinaison d'une inspection visuelle et de la connaissance du dernier lieu d'achat.

La contrefaçon peut toutefois s'exercer dans des buts plus malveillants. Etant donné que la contrefaçon se complexifie, il devient plus difficile de distinguer les activités de contrefaçon qui ne sont que des entreprises commerciales de celles qui constituent de véritables actes de sabotage.

4.5.4.2 Problèmes relatifs à la contrefaçon rencontrés par le Ministère de la Défense américain

Le rapport GAO-10-389 publié par la commission d'audit du gouvernement américain (GAO) le 28 avril 2010 souligne les risques encourus par le Ministère de la Défense américain concernant la fourniture de pièces contrefaites.

De plus, le rapport "Defense Industrial Base Assessment: Counterfeit Electronics", publié en janvier 2010 par le Ministère américain du commerce, passe exhaustivement en revue les activités de contrefaçon et recommande fortement:

- d'acheter les composants directement auprès des fabricants de composants d'origine ou auprès des distributeurs franchisés agréés;
- de garantir la traçabilité des composants jusqu'au fabricant d'origine, généralement par l'utilisation de certificats de conformité ou d'épreuves d'homologation;
- de tenir à jour les listes de fournisseurs agréés ainsi que les critères d'agrément y afférant;
- de s'assurer que les procédures anticontrefaçon relatives à la chaîne d'approvisionnement sont bien en place et assurées;
- d'utiliser des comptes de garantie bloqués gérés par l'ERAI, lors de l'achat de composants potentiellement suspects;
- d'utiliser des régimes d'inspection visuelle de type IDEA-STD-1010 et de soumettre à essai les composants suspects, en utilisant par exemple les rayons X ou les essais électriques, comme exigé;
- d'utiliser des bases de données pour assurer le suivi des composants suspects ou contrefaits, d'utiliser le Programme d'échange de données entre le gouvernement et l'industrie (GIDEP);
- qu'il convienne que les entités liées au Ministère de la Défense utilisent les rapports sur la qualité et la défectuosité des produits (PQDR) afin de signaler tout composant électronique défectueux;
- de proposer que les règlements fédéraux relatifs à l'avionique (FAR) soient modifiés, en ce qui concerne l'approvisionnement en composants destinés à des applications essentielles aux missions entreprises;

- qu'un mécanisme de signalement ainsi qu'une base de données centralisés soient mis en place sur le plan fédéral, afin de recueillir les données relatives à la contrefaçon, en lien étroit avec les forces de l'ordre. [10]¹

Lors de la réunion du sous-comité de surveillance et d'enquête relative à la propriété intellectuelle (voir GAO-13-762T) qui s'est tenue le 9 juillet 2013, l'économiste en chef a passé en revue les renseignements tirés des efforts de quantification des effets des produits contrefaits et piratés sur l'économie américaine. Conclusion de cet état des lieux: le vol de propriété intellectuelle est en recrudescence et est exacerbé par l'utilisation de technologies numériques.

Le rapport "Supporting Innovation, Creativity and enterprise, charting the path ahead FY2017-2019" (voir A.8.12) du Ministère de la sécurité intérieure indique qu'un petit nombre d'"économies d'origine" constitue la masse des fournisseurs de produits contrefaits aux Etats-Unis et dans l'Union européenne.

4.5.4.3 Incidence sur la fiabilité et danger pour les populations

Les composants suspects, contrefaits ou d'origine inconnue représentent une grave menace envers la sécurité des équipements avioniques, compte tenu du fait qu'ils ne présentent pas la fiabilité attendue dont les composants d'origine font preuve. La fiabilité découle d'une conception adéquate contrôlée par le fabricant d'origine, ainsi que d'une fabrication et d'une manutention contrôlées. La fiabilité d'un composant ne peut pas être contrôlée ultérieurement.

Les composants avec une traçabilité jusqu'au fabricant d'origine présentent des performances conformes aux indications portées sur les fiches techniques du fabricant, et démontrent la durée de vie attendue, en application des prédictions de fiabilité du fabricant d'équipements d'origine et de la garantie du produit.

Les composants suspects ou d'origine inconnue, qui peuvent ou non s'avérer contrefaits, ne présentent aucune information permettant de savoir de quelle manière ils ont été conservés ou manipulés, mais également s'ils ont subi des dommages latents liés à des décharges électrostatiques, des dommages liés à l'humidité, aux chocs ou aux vibrations, etc. L'absence de ces informations rend impossible l'attribution aux composants d'origine inconnue d'une fiabilité identique à celle des composants ayant une traçabilité jusqu'au fabricant d'origine.

4.5.4.4 Defense Logistics Agency (DLA)

La DLA fournit de nombreux programmes liés à la défense américaine en composants militaires de catégorie spécifique.

Cet organisme a récemment établi la liste des fournisseurs d'essai certifiés (QTSL), afin de faciliter l'approvisionnement en composants quasi obsolètes en utilisant la SAE AS6081 (voir A.8.9), mais également lors de l'approvisionnement en composants auprès de sources non franchisées.

Depuis août 2012, un nouvel article de la directive d'acquisition de la logistique de défense, la DLAD 52.211-9074, relative au marquage des éléments à haut risque à l'acide désoxyribonucléique (ADN), est inséré dans les nouveaux contrats et sollicitations afférents aux microcircuits électroniques de type Federal Supply Class (FSC) 5962, lorsque la description des microcircuits stipule une exigence de marquage à l'ADN pour ces derniers. Les contractants, aux termes de cet article, sont soumis à l'exigence de fournir des microcircuits marqués à l'aide d'un ADN d'origine végétale produit par Applied DNA Sciences Inc. ou ses détenteurs de licence agréés, le cas échéant; voir A.8.9.

¹ Les chiffres entre crochets se réfèrent à la Bibliographie.

Cette exigence de marquage est toutefois impopulaire au sein de l'Association de l'industrie des semiconducteurs (SIA) et bon nombre de ses membres refusent de soumissionner lorsqu'il s'agit de travailler avec la DLA. Cette dernière a par conséquent mis en place un plan de remboursement à destination des fournisseurs de confiance ayant fait appel à Applied DNA Science (voir Article A.20). Ce plan, initialement obligatoire, a été suspendu en décembre 2016 en raison du coût élevé des droits de licence et des charges exceptionnelles demandées pour la création de la séquence d'ADN. La DLA a toutefois obtenu le budget nécessaire à la poursuite de ce plan avec d'autres types de composants.

4.5.4.5 Système de contrôle des acquisitions fédérales pour la défense (DFARS) et système de contrôle des acquisitions fédérales (FARS) lié pour la chaîne d'approvisionnement américaine

Le 31 décembre 2012, le Président des Etats-Unis a signé l'Acte d'acquisition de la défense nationale (NDAA), comprenant l'article 818 relatif aux mesures de lutte contre la contrefaçon. Cet article traite de la manière de réduire le plus possible la présence de composants contrefaits au sein de la chaîne d'approvisionnement de la Défense américaine. De lourdes sanctions financières et pénales sont appliquées aux entreprises et aux individus impliqués dans la fourniture délibérée de composants frauduleux ou contrefaits aux organismes de la Défense américaine. Cette disposition s'applique à tous les acteurs de la chaîne d'approvisionnement, y compris les courtiers, les distributeurs, les fabricants d'équipements d'origine et les organismes chargés de la maintenance, des réparations et des révisions. Elle a été transformée en une politique de prévention destinée à la lutte contre la contrefaçon (numéro DoDI 4140.67), ainsi qu'en un nouveau DFARS (numéro 252.246 7007) destiné à être utilisé dans les contrats (voir A.8.10). Ce dernier est complété par le DFARS 252.246.7008 relatif aux fournisseurs de confiance, publié en 2016. Un amendement au DFARS 252.246 7008 devrait bientôt être publié.

Aucun fournisseur n'est soumis à l'exigence de se conformer à la SAE AS5553 afin de satisfaire aux exigences des DFARS 252.246 7007 et 252,246 7008.

NOTE 1 La SAE AS5553 est de nouveau en révision (révision C), aux termes de laquelle le comité de la Société des ingénieurs automobiles (SAE) cherche à inclure autant d'exigences relatives aux DFARS que possible, mais un compromis sera trouvé, étant donné que la SAE AS5553 est destinée à servir de référentiel concernant les bonnes pratiques pour toute l'industrie, et pas uniquement pour les chaînes d'approvisionnement de la Défense américaine. Le comité prévoit également de publier le document AIR 6860, afin d'expliquer l'extension de la conformité de la révision C de la SAE AS5553 aux exigences des DFARS.

Il existe également la possibilité qu'une institution publique américaine contrôle le respect des exigences des DFARS par les fournisseurs.

La totalité des sanctions est allégée dès lors que le fabricant d'équipements d'origine ou le distributeur publie un plan de gestion de la lutte contre la contrefaçon.

Toute présence de composants suspects doit être signalée dans la GIDEP, une base de données américaine utilisée aux Etats-Unis et au Canada (voir A.8.12). Les autres fournisseurs internationaux, du fait qu'ils ne peuvent accéder à la GIDEP, se trouvent en difficulté. La plupart de ces fournisseurs s'opposent aux articles du DFARS relatifs à la GIDEP.

NOTE 2 La GIDEP est en cours de modification (2017). Il est prévu que les données relatives aux composants suspects et contrefaits soient réparties en trois niveaux de sensibilité. Il est à espérer que les deux premiers seront consultables dans le monde entier.

De plus, la DoDI 7050.05 concernant les voies de recours relatives aux activités de fourniture en lien avec la fraude et la corruption a déjà été publiée.

4.5.4.6 Recommandations du Ministère de la Défense britannique en matière de lutte contre la contrefaçon

Le Ministère de la Défense britannique a créé une page web interactive (voir A.6.7), afin de fournir des recommandations concernant sa chaîne d'approvisionnement. Il a également publié le "Counterfeit Avoidance Maturity Model", qui comprend la norme Defence Standard 05-135, réactualisée en version 2.0 (elle comprend l'exigence de la gestion de l'obsolescence). La norme Defence Standard 05-135, ainsi que les lignes directrices associées concernant la sensibilisation à la vérification et à l'évaluation fournissent des exigences de haut niveau afin d'éviter la contrefaçon. Elles sont destinées à la gestion des chaînes d'approvisionnement complexes permettant aux forces armées de s'approvisionner en missiles, munitions, navires, chars, avions, mais aussi en pansements, nourriture, habillement et médicaments.

4.5.4.7 Organisation du traité de l'Atlantique nord (OTAN)

L'OTAN a désormais reconnu le risque d'existence de matériel contrefait au sein de sa chaîne d'approvisionnement et travaille à l'évaluation des problèmes relatifs à la contrefaçon.

4.5.5 Groupes d'intervention directe contre la contrefaçon de composants électroniques

Plusieurs fabricants de composants électroniques sont intervenus directement pour saisir des composants contrefaits imitant les leurs ainsi que l'outillage associé, en coopération avec les forces de l'ordre locales. L'ONG BEAMA, qui représente l'industrie électrotechnique au Royaume-Uni et en Europe, soit plus de 300 fabricants, mène par exemple des perquisitions dans des usines suspectes et chez des distributeurs écoulant des composants contrefaits (voir A.7.7). De plus, le groupe de travail anticontrefaçon du Conseil mondial des semi-conducteurs (voir Article A.3) travaille de concert avec les douanes et les forces de l'ordre, afin d'éliminer toute contrefaçon de la chaîne d'approvisionnement.

4.6 Composants recyclés

4.6.1 Généralités

Voir 3.1.20 pour la définition d'un "composant recyclé".

La vente de composants recyclés constitue une activité légale lorsque ces derniers sont présentés pour ce qu'ils sont. Cette pratique de récupération des jeux de composants les plus chers est courante dans beaucoup de secteurs, par exemple celui des télécommunications, où les composants des circuits intégrés spécifiques provenant des combinés de téléphones portables sont recyclés. Le recyclage en soi n'a rien d'illégal, du moment que l'ensemble des parties prenantes comprend bien que les composants sont recyclés.

NOTE Le secteur du recyclage de l'électronique se développe massivement, en raison d'une demande mondiale de produits de consommation à la hausse, généralement remplacés par des modèles plus évolués après quelques années. Les produits de consommation abandonnés sont envoyés dans des centres de recyclage internationaux, qui pour beaucoup recyclent les composants par le biais de processus non contrôlés. Il en résulte potentiellement des décharges électrostatiques ainsi que des dommages physiques, rendant les composants inutilisables par les fabricants d'équipements d'origine à haute performance pour la défense et l'aérospatiale.

4.6.2 Pourquoi l'industrie avionique n'utilise pas de composants recyclés

L'industrie avionique doit s'assurer que l'ensemble des équipements de vol qu'elle produit dispose d'une durée de vie prévue tenant compte de la durée de vie en service et de réparation prévues, afin de s'assurer que la population ne court aucun risque. Généralement un fabricant d'équipements d'origine calcule un temps moyen entre pannes (MTBF) et peut-être une durée moyenne avant défaillance (MTTF) afin de définir les interventions de maintenance. Ces calculs admettent par hypothèse que l'ensemble des composants est neuf ou estimé être "inutilisé" au moment de l'introduction de l'utilisation en vol, et qu'aucune durée de vie utile des composants n'a été entamée et/ou qu'aucun composant considéré comme "dangereux" n'a été utilisé.

Généralement, les composants recyclés ne donnent pas la possibilité aux utilisateurs de mesurer et déterminer dans quelle mesure leur durée de vie utile a déjà été entamée avant le recyclage. La durée de vie restante prévue, dans l'optique des interventions de maintenance définies par le fabricant d'équipements d'origine, ne peut donc pas être calculée avec précision. Le recyclage lui-même, s'il est réalisé par le biais d'un processus non contrôlé, peut causer des dommages aux composants, comme des décharges électrostatiques ou des dommages latents liés à une surtension, qui ne peuvent pas être immédiatement détectés, mais qui constituent un mécanisme de défaillance à long terme et qui peuvent affecter la fiabilité résiduelle des composants.

4.6.3 De quelle manière les composants recyclés deviennent suspects et potentiellement frauduleux

Les fabricants d'équipements d'origine à haute performance pour la défense et l'aérospatiale (ADHP) achètent généralement des composants inutilisés destinés à la fabrication de leurs produits et leurs bons de commande comprennent des termes et conditions excluant la livraison et l'acceptation de composants recyclés. Les composants ou produits livrés aux fabricants d'équipements d'origine à haute performance pour la défense et l'aérospatiale sont donc vus comme des "composants suspects recyclés frauduleusement" lorsque des preuves d'utilisation antérieure sont observées sur l'emballage du composant ou ses terminaisons. Cela arrive par exemple lorsqu'il existe des preuves que des soudures ont été effectuées sur les terminaisons ou que celles-ci ont été ressoudées ou réassemblées sur plaque. Généralement, dans ce type de situation, la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant de composants d'origine (voir 3.1.25) n'est plus assurée et les composants recyclés ont été introduits frauduleusement dans la chaîne d'approvisionnement des fabricants d'équipements d'origine à haute performance pour la défense et l'aérospatiale, et présentés comme "neufs" ou "inutilisés". Pour plus d'informations sur les composants frauduleux, voir 4.4.3. Les forces de l'ordre estiment généralement que cette activité relève de la "fraude" plutôt que de la "contrefaçon", la fraude se définissant par la vente de composants recyclés présentés comme neufs ou inutilisés.

NOTE Cette pratique se généralise, en particulier pour les composants obsolètes, difficiles à trouver et chers, étant donné que le secteur du recyclage des composants électroniques se développe, en raison du remplacement des produits de consommation par des modèles plus évolués.

Les fabricants d'équipements d'origine à haute performance pour la défense et l'aérospatiale peuvent mettre en place leurs propres procédures de recyclage lors de la réparation de leurs montages en interne, en utilisant leurs propres conditions de réparation, qui comprennent la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant de composants d'origine, de la manière définie dans l'IEC 62239-1 ECMP. Cette pratique est validée par le client.

4.7 Lignes directrices des fabricants de composants d'origine (OCM) en matière de lutte contre la contrefaçon

4.7.1 Généralités

Il est important que les fabricants de composants d'origine mettent en place des mesures de lutte contre la contrefaçon lors de la fabrication, de la production et de la vente de leurs composants. Les mesures suivantes constituent les pratiques habituelles qu'il convient d'utiliser sur le plan international, sauf s'il s'agit d'un mécanisme spécifique à une région ou à un pays, comme indiqué dans les alinéas respectifs du 4.7.2 au 4.7.11.

4.7.2 "Fournisseur fiable de composants électroniques" (RECS): le mécanisme de vérification chinois

Ce mécanisme de vérification était en vigueur en Chine. La Réunion des gouvernements et des autorités sur les semiconducteurs (GAMS 2009) et le Conseil mondial des semiconducteurs (WSC) en effectuaient la promotion. En janvier 2008, les premières entreprises certifiées au titre du RECS étaient au nombre de treize. Il a malheureusement été abandonné et ne présente dorénavant qu'un intérêt historique.

4.7.3 Certification tierce des fabricants de composants d'origine au titre de l'ISO 9001 et de l'AS/EN/JISQ 9100

Lorsque les fabricants de composants d'origine font l'objet d'un contrôle tiers de la part d'agents accrédités, les fabricants ainsi que leurs usines et leurs gammes de produits sont également certifiés. De même, les agents de vérification tiers sont tenus de se rendre à toutes les adresses indiquées sur les certificats et d'y effectuer leurs contrôles. Il est donc fortement recommandé d'acheter la totalité des composants auprès de fabricants bénéficiant d'une certification tierce, au minimum au titre de l'ISO 9001, ou au titre de l'AS/EN/JISQ 9100 (voir 4.2). Noter que l'ISO 9001 ne dispose pas de normes minimales de référencement pour la qualité d'exécution et ne garantit donc pas la qualité des composants.

La base de données en ligne Oasis, mise en place par le Groupe international de qualité en aérospace (IAQG) (voir A.8.11), peut être utilisée pour vérifier les certificats émis au titre de l'AS/EN/JISQ 9100, l'AS/EN/JISQ 9110 et l'AS/EN/JISQ 9120.

4.7.4 Marques déposées des fabricants de composants d'origine

Tous les fabricants de composants d'origine doivent protéger leur propriété intellectuelle et disposer d'une marque déposée ou d'un logo enregistré(e) auprès de l'Organisation mondiale de la propriété intellectuelle, etc. L'Association de l'industrie des semiconducteurs recommande d'enregistrer les marques déposées dans tous les pays intégrés à une zone franche, afin de s'assurer que les contrefacteurs n'importent pas leurs composants par le pays membre où la marque déposée n'est pas enregistrée. En Europe les marques déposées peuvent être enregistrées auprès de l'EUIPO (voir A.7.4), afin d'obtenir une "marque communautaire" valable dans la totalité des Etats membres de l'U.E. L'atteinte aux marques déposées des composants constitue la source de contrefaçon la plus répandue.

4.7.5 Contrôle de la propriété intellectuelle des fabricants de composants d'origine

Le contrôle de la propriété intellectuelle du fabricant est généralement la combinaison du contrôle des brevets et de la conception, ainsi que l'utilisation de marques déposées et de logos. Une partie cruciale du contrôle de la conception est constituée par le contrôle du programme d'essais d'acceptation finale (logiciel d'essai et postes d'essai relatifs au programme) et le contrôle des fiches techniques publiées. Il convient que le logiciel d'essai et les postes d'essai relatifs au programme d'essais d'acceptation soient numérotés et fassent l'objet de contrôles essentiels. Il convient que les fiches techniques (voir 3.1.8) soient publiées en lecture seule afin de ne pas pouvoir être modifiées et qu'elles contiennent également le logo ou la marque déposée du fabricant. En ce qui concerne les pièces disponibles dans le commerce, seules les données publiées dans la fiche technique du fabricant de composants d'origine constituent les informations relatives à la conception. Elles sont contrôlées par ses droits de propriété intellectuelle.

4.7.6 Marquage physique des pièces et des emballages des fabricants de composants d'origine

Les fabricants de composants d'origine effectuent des contrôles secrets de leurs activités finales de marquage de pièces, généralement par le biais d'actions en interne. Il est cependant essentiel que la marque déposée du fabricant de composants d'origine, qui apparaît physiquement sur les composants, soit la même que la marque déposée enregistrée auprès de l'Organisation mondiale de la propriété intellectuelle (voir Article A.1) et soit conforme aux informations fournies par le fabricant de composants d'origine. Les fabricants de composants d'origine, pour authentifier leurs produits, y apposent des marquages physiques, en utilisant une taille de police, un espacement entre les caractères, un placement des chiffres et des lettres, des marquages laser ou à l'encre spéciaux, etc., pour:

- les marques déposées;
- les codes de date de lot;
- les codes d'emplacement unique;
- les codes de date de tranche de lot;

- les marquages extérieurs spéciaux de l'emballage;
- les autres codes propriétaires destinés à la traçabilité.

Les fabricants de composants d'origine peuvent aider les fabricants d'équipements d'origine à valider le marquage de leurs pièces si nécessaire. Il existe cependant une limite au contrôle qui peut être exercé en employant seulement cette méthode. La plupart des fabricants de composants d'origine utilisent également des techniques propriétaires de marquage des puces et des emballages (voir 4.7.9, 4.7.10, 4.7.11). Noter que:

- l'ISO 12931 a été publiée dans le but d'apporter une aide quant aux méthodes d'authentification exigées pour lutter contre les risques de contrefaçon;
- l'ISO 16678 a été développée dans un but de suivi des méthodes d'expédition;
- les composants destinés aux organismes de la Défense américaine peuvent uniquement être identifiés en utilisant les méthodes d'identification d'élément unique (IUID) DoDI 8320.04.

4.7.7 Groupe de travail anticontrefaçon (ACTF) de l'Association de l'industrie des semiconducteurs

L'Association de l'industrie des semiconducteurs (SEMI) est une association mondiale des acteurs du secteur (voir Article A.4) qui fournit des recommandations sur les mesures pratiques pouvant être mises en place pour éviter les problèmes de contrefaçon.

La traçabilité des puces constitue une activité émergente pour les fonderies de plaquettes. Les nouveaux documents suivants ont été publiés avec pour préoccupation la contrefaçon des circuits intégrés des puces:

- SEMI T18-1106 (reapproved 0812), *Specification of Parts and Components Traceability* (disponible en anglais seulement);
- SEMI T20-0710, *Specification for authentication of semiconductors and related products* (disponible en anglais seulement);
- SEMI T20.1, *Specification for object labelling to authenticate semiconductors and related products in an open market* (disponible en anglais seulement);
- SEMI T20.2, *Guide for qualifications of authentication service bodies for detecting and preventing counterfeiting of semiconductors and related products* (disponible en anglais seulement);
- SEMI T21-0314, *Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain* (disponible en anglais seulement);
- SEMI T22-0212, *Specification for Traceability by Self Authentication Service Body and Authentication Service Body* (disponible en anglais seulement).

Ces nouveaux documents aident les fabricants de confiance de produits authentiques et utilisent des numéros de lots à chiffrement fort. L'utilisation d'un service d'authentification gratuit permet à quiconque envisageant l'achat d'un lot de produits de pouvoir utiliser le numéro de lot chiffré comme base de vérification pour la validation. La sérialisation sécurisée constitue un moyen crucial de dissuasion de la contrefaçon. Bien que les systèmes de sérialisation sécurisée n'empêchent pas à eux seuls la copie ou le vol des codes, ils peuvent se révéler efficaces pour détecter la survenue d'une telle fraude. La sérialisation sécurisée sert donc de moyen de dissuasion et de système d'alerte avancé. Développées pour être utilisées avec des circuits et dispositifs à semiconducteurs, ces procédures peuvent également être étendues aux autres pièces électroniques et aux autres types de produits.

L'Association de l'industrie des semiconducteurs a publié en 2013 un livre blanc où sont exposées ses activités récentes en matière de lutte contre les composants contrefaits (voir Article A.3). Ce document conclut que la meilleure stratégie consiste à acheter les composants aux fabricants de composants d'origine et à leurs distributeurs franchisés, y compris les distributeurs franchisés du marché secondaire, et d'éviter d'acheter à des distributeurs non franchisés ou sur le marché libre.

4.7.8 Les fonderies de confiance: le programme américain

En réaction à plusieurs problèmes de contrefaçon, le Ministère de la Défense américain a mis en place de nouvelles politiques, dont le Trusted Access Program Office (TAPO) (voir A.8.5), dont la responsabilité est de trouver et de conserver des fournisseurs de pièces microélectroniques de confiance, au titre de la DODI 5200.44.

La gestion des fournisseurs de confiance dépend à présent de la Defence Micro Electronics Activity (DMEA) (voir A.8.5), qui tient à jour la liste des fournisseurs accrédités:

La protection des composants de circuits intégrés spécifiques personnalisés utilisés dans des applications américaines essentielles est ainsi assurée. Ces éléments sont généralement désignés sous le nom de composants visés par la réglementation sur le commerce international des armes (ITAR). Il convient que les utilisateurs vérifient le statut ITAR des composants provenant des fabricants participant au programme des fonderies de confiance.

4.7.9 Programme américain d'accréditation des fournisseurs de confiance de circuits intégrés

Les fournisseurs américains de confiance, en plus de ceux figurant en 4.7.8, dont la gestion incombe maintenant à la DMEA (voir A.8.5), comprennent également les laboratoires d'essais de confiance, les courtiers, les installations de post-traitement, les installations d'emballage/d'assemblage/d'essai, etc. Les fournisseurs de confiance accrédités reçoivent un certificat de fournisseur de confiance, valable pour un temps donné (la date d'expiration étant indiquée sur le document) et pouvant être consulté sur le site web de l'entreprise concernée.

4.7.10 Fonction physique non clonable (PUF)

Pour une bonne définition de la PUF, qui est un terme de cryptographie, voir Article A.11, où de nombreux exemples de fonctions physiques non clonables magnétiques et d'autres relatives au revêtement du silicium, des mémoires vives statiques et des circuits intégrés sont donnés. Il s'agit d'une technologie émergente comprenant des applications immédiates de prévention des activités de contrefaçon, par exemple les étiquettes RFID et les applications militaires.

NOTE L'ISO 17367, l'ISO/IEC 20243 (toutes les parties) et l'ISO/IEC TR 24729-1 peuvent aider à appréhender les questions liées aux étiquettes RFID.

Les chercheurs s'inquiètent cependant du fait que cette technologie puisse être détournée et suggèrent qu'il convient de l'utiliser prudemment (voir Article A.11).

Les organismes et produits pouvant apporter une aide concernant l'utilisation de cette technologie comprennent l'Initiative pour une sécurité intrinsèque du matériel (HIS), lancée en mai 2010 (voir Article A.12). Cette technologie exploite l'"empreinte électronique" unique propre à chaque semiconducteur (voir 3.1.21), la fonction physique non clonable (PUF). Les composants à base de semiconducteurs sont maintenant fabriqués en y intégrant la PUF, qui représente une partie de leur système de gestion des dispositifs sécurisés.

4.7.11 Meilleures pratiques des fabricants de composants d'origine

Il convient que les fabricants de composants d'origine exercent un contrôle rigoureux sur leurs sous-traitants, y compris les fabricants contractuels de matériel électronique ou les systèmes de management environnemental, afin de s'assurer que les rebuts, les composants après des essais en conditions réelles et les composants présentant un mauvais rendement ne soient pas réutilisables. Cela permettra de s'assurer que ces composants ne sont pas vendus sur le marché libre aux fabricants d'équipements électroniques par le biais de fournisseurs non franchisés. Il convient également que les fabricants de composants d'origine aident leurs distributeurs et les fabricants d'équipements d'origine en indiquant sur leur documentation lorsque les composants ont été légitimement re-marqués. Il convient également que les fabricants de composants d'origine partagent une partie de leurs processus de vérification du marquage, par exemple en mettant en place des sites web où les fabricants d'équipements d'origine ainsi que les autres utilisateurs disposent d'informations leur permettant de rechercher et de vérifier le marquage physique des composants, ainsi que les étiquettes inviolables (voir Article A.13).

4.8 Accréditations minimales des distributeurs

Il convient, à titre de recommandation, que la totalité des distributeurs possède au minimum les accréditations tierces suivantes:

- l'Organisation Internationale de Normalisation (ISO) 9001: une norme concernant les systèmes de management de la qualité;
- l'ISO 14001: un système de gestion environnemental;
- la série concernant l'évaluation de la santé et de la sécurité au travail (OHSAS) 18001: une spécification de système de gestion de la santé et de la sécurité au travail ou toute autre procédure équivalente;
- l'American National Standards Institute/Electrostatic Discharge ANSI/ESD S20.20: une norme concernant les programmes de contrôle des décharges électrostatiques ou l'IEC 61340-5-1, ou toute autre procédure équivalente.

4.9 Certification tierce AS/EN/JISQ 9120 des distributeurs

L'AS/EN/JISQ 9120 est une sous-section de l'ISO 9001 et constitue la norme aéronautique complémentaire destinée aux négociants/distributeurs. Elle gère les exigences de la distribution avionique et est conforme aux exigences de l'AS/EN/JISQ 9100 relative aux fabricants d'équipements d'origine. L'achat de composants d'origine certifiée, dont la traçabilité jusqu'au fabricant d'origine est garantie, constitue un aspect essentiel du processus de certification de l'AS/EN/JISQ 9120. La section relative aux révisions de contrats de l'audit de l'AS/EN/JISQ 9120 pose comme exigence que la totalité des distributeurs impliqués lors de l'établissement d'un devis indique clairement si celui-ci concerne des composants avec une traçabilité jusqu'au fabricant d'origine ou d'origine inconnue. Le distributeur perd sa certification AS/EN/JISQ 9120 s'il fournit des composants d'origine inconnue alors que la commande concerne des composants avec une traçabilité jusqu'au fabricant d'origine.

Les distributeurs franchisés ainsi que les autres peuvent être certifiés au titre de l'AS/EN/JISQ 9120.

Il est recommandé que l'ensemble des distributeurs, en particulier les distributeurs non franchisés utilisés par les fabricants d'équipements avioniques d'origine, soient soumis à un contrôle tiers au titre de l'AS/EN/JISQ 9120:2016. La base de données en ligne Oasis, mise en place par le Groupe international de qualité en aéronautique ou IAQG (voir A.8.11), peut être utilisée pour vérifier les certificats émis au titre de l'AS/EN/JISQ 9100, l'AS/EN/JISQ 9110 et l'AS/EN/JISQ 9120.

4.10 Réseau de distributeurs franchisés

4.10.1 Généralités

Les fabricants peuvent vendre leurs composants par le biais de réseaux de distributeurs franchisés agréés (voir 3.1.9 pour la définition d'un "distributeur franchisé").

Ces distributeurs franchisés sont agréés pour une période déterminée par le fabricant de composants d'origine, par exemple annuellement ou tous les 2 ans. De plus, un distributeur peut n'être franchisé que pour un fabricant et non pour tous les fabricants de sa gamme. Il n'existe aucune base de données centralisée où il soit possible de trouver l'ensemble des distributeurs franchisés et où l'attribution de leur agrément soit chronologiquement recensée. Il est conseillé aux fabricants d'équipements d'origine d'établir leurs propres archives, afin de savoir à quel moment un distributeur est franchisé pour un fabricant donné et à quel moment cette franchise prend fin.

Les informations concernant les distributeurs franchisés de semiconducteurs sont disponibles auprès de l'entité suivante:

- L'Electronics Authorized Directory (voir Article A.5), qui a été mis en place par Rochester Electronics pour le compte de l'Association de l'industrie des semiconducteurs (SIA) et qui a été créé par celle-ci en tant que mesure de lutte contre la contrefaçon.

Il convient cependant de vérifier l'information la plus récente sur le site web du fabricant de composants d'origine, en particulier les pages consacrées aux revendeurs locaux, ainsi qu'aux bureaux gérant la distribution, les ventes et les distributeurs.

Les associations de distributeurs franchisés deviennent de plus en plus strictes quant à leurs critères d'appartenance. Simples associations de réseautage à l'origine, elles se transforment en porte-étendards des bonnes pratiques.

Quelques exemples d'associations de distributeurs:

- 1) L'Electronics Components Industry Association (ECIA), une ONG nord-américaine (voir A.8.7) qui élabore des lignes directrices comprenant:
 - NIGP 113: *NEDA Guidelines for Product Returns* (disponible en anglais seulement);
 - NIGP 109: *Guidelines for Distributor Assessment of Manufacturer Performance* (disponible en anglais seulement);
 - NIGP 107: *Guidelines for the format of Military Certificates of Conformance* (disponible en anglais seulement);
 - NIGP 111: *Guidelines for the format of Packing Slips* (disponible en anglais seulement);
 - NIGP 115: *Guidelines for Certificates of Conformance for Commercial Electronic Parts* (disponible en anglais seulement);
 - NIGP 116: *ECIA Guidelines for Disposition of Excess Inventory* (disponible en anglais seulement);
 - un nouveau site qui propose un répertoire des distributeurs autorisés, destiné à soutenir les professionnels du secteur.
- 2) L'Electronic Component Supplier Network (ECSN), une association professionnelle britannique à but non lucratif (voir A.6.6), qui publie plusieurs guides et peut servir d'arbitre dans le domaine des accords de franchise.
- 3) L'International Independent Distributors of Electronics Association (IDEA) (voir A.8.6), à l'origine de la norme IDEA-STD-1010, qui couvre la lutte contre la contrefaçon sous l'angle de l'inspection visuelle, et qui dispense des formations certifiées au titre de l'IDEA-ICE-3000. En outre, l'IDEA publie des livres blancs, gère des listes de pièces suspectes et contrefaites ainsi que des lignes directrices destinées aux distributeurs indépendants non franchisés.

Les distributeurs franchisés présentent d'énormes avantages pour l'industrie avionique, car ils peuvent apporter une aide précieuse concernant les informations relatives à la traçabilité des composants et ils peuvent également fournir des informations et recommandations considérables concernant les questions d'obsolescence.

Les distributeurs franchisés peuvent également vendre à d'autres distributeurs franchisés. Il est fortement recommandé que les fabricants d'équipements d'origine ainsi que les clients de distributeurs demandent que la totalité du stock franchisé provienne directement du fabricant de composants d'origine et non du stock acquis auprès d'un autre distributeur franchisé, qui pourrait contenir des stocks renvoyés par les clients, avec le risque associé de contamination des composants. Il y a dans ce cas violation, par exemple, des exigences du DFARS 252.246-7007 et du DFARS 252-246-7008, stipulant de ne pas utiliser les stocks "contaminés" pour l'approvisionnement du matériel destiné à la Défense américaine.

Il existe beaucoup de distributeurs franchisés qui font également office de distributeurs non franchisés. Ce type de distributeurs, généralement appelés distributeurs "mixtes", est souvent difficile à gérer, en particulier si le fabricant d'équipements d'origine est partie prenante de la chaîne d'approvisionnement au titre du DFARS 252.246.7007 ou du DFARS 252-246-7008. Le problème réside dans le fait que leur stock peut être mélangé ou contaminé.

Il est fortement recommandé que les fabricants d'équipements d'origine ainsi que les clients de distributeurs insèrent des articles dans leurs contrats aux termes desquels l'achat de stocks renvoyés ou "contaminés" est interdit, tout en insistant sur la fourniture exclusive de nouveaux stocks directement par le fabricant de composants d'origine.

NOTE 1 La "contamination" désigne le fait que le stock renvoyé soit mélangé au nouveau stock, reçu directement du fabricant de composants d'origine. Le stock résultant est ainsi déclaré "contaminé".

NOTE 2 Les distributeurs franchisés font preuve d'une préoccupation grandissante quant à la progression de la distribution à très grande échelle par Internet, qui peut en fin de compte devenir le circuit dominant pour l'industrie générale.

4.10.2 SAE AS6496

Une nouvelle spécification relative aux distributeurs franchisés, la SAE AS6496 (voir Article A.16), a été publiée par le comité SAE G-19 afin d'aborder la manière dont la chaîne d'approvisionnement de la distribution franchisée limite le risque d'apparition de composants contrefaits. Un de ses points essentiels réside dans le fait que les distributeurs franchisés doivent réinspecter tout stock renvoyé, afin de s'assurer qu'il ne contient aucun composant contrefait ou recyclé.

4.10.3 Contrôle des stocks par le biais de mécanismes de suivi

Les distributeurs franchisés contrôlent les stocks du fabricant par le biais de mécanismes de suivi appropriés et peuvent accepter que les fabricants d'équipements d'origine et les organismes chargés de la maintenance, des réparations et des révisions leur vendent des stocks inutilisés, qu'ils revendent ensuite à d'autres clients en fournissant la traçabilité exigée (voir 4.10.1 pour la NGIP 113 et 4.10.2 pour la SAE AS6496).

Les composants destinés aux organismes de la Défense américaine peuvent être suivis en utilisant les normes de suivi stipulées dans la DoDI 8320.04 IUID.

Il existe de nombreux autres mécanismes de suivi, tels que le mécanisme de marquage à l'"ADN numérique" (voir Article A.20), ainsi que des sociétés de conception de solutions inviolables (voir Article A.13).

Se reporter au 4.13.8 pour le contrôle des produits dans la chaîne d'approvisionnement.

4.10.4 Contrôle des rebuts

Les distributeurs franchisés contrôlent également les rebuts des fabricants de composants d'origine et ont légalement le droit de mettre au rebut et de détruire un stock "suspecté" d'être contrefait ou frauduleux au nom de l'OCM (voir 4.10.2 pour la SAE AS6496).

4.10.5 Fournisseur fiable de composants électroniques (RECS)

Il y a quelques années, il a été recommandé à la totalité des distributeurs franchisés d'Extrême-Orient de se soumettre à un contrôle RECS (voir 4.7.2). Ce mécanisme n'existe toutefois plus et la validité ainsi que la pertinence des certificats RECS ne sont à présent plus prises en compte dans la gestion de la chaîne d'approvisionnement.

4.11 Lignes directrices des distributeurs non franchisés en matière de lutte contre la contrefaçon

4.11.1 Généralités

Se reporter au 3.1.14 pour la définition d'un "distributeur non franchisé".

La chaîne d'approvisionnement des composants achetés par le biais de distributeurs non franchisés peut être très longue. Il est possible que plusieurs distributeurs et courtiers soient impliqués. Les distributeurs non franchisés ne connaissent pas toujours les autres sources d'une chaîne d'approvisionnement aussi longue et les composants y circulant peuvent à un moment ou à un autre devenir "suspects".

Il est recommandé que les fabricants d'équipements d'origine adoptent une gestion des distributeurs non franchisés conforme au 4.11.4.

Les distributeurs non franchisés peuvent également faire l'objet d'une certification tierce au titre de l'AS/EN/JISQ 9120. La base de données en ligne Oasis, mise en place par le Groupe international de qualité en aérospace ou IAQG (voir A.8.11), peut être utilisée pour vérifier les certificats émis au titre de l'AS/EN/JISQ 9100, l'AS/EN/JISQ 9110 et l'AS/EN/JISQ 9120.

Les distributeurs non franchisés ont également besoin de mettre en place une procédure relative à la manière de traiter les composants suspects, étant donné qu'ils ne peuvent les renvoyer dans la chaîne d'approvisionnement sans être légalement tenus pour responsables de détention de composants contrefaits et sans être accusés de fraude.

La SAE ARP 6178, qui est une liste de contrôle utilisée lors des audits, constitue un outil utile pour l'évaluation des sources d'approvisionnement (voir Article A.16), et lorsqu'elle est complétée, elle peut devenir une partie du plan de gestion de la lutte contre la contrefaçon des distributeurs non franchisés.

Voir l'IEC 62668-2 pour plus d'informations.

4.11.2 Programme certifié CCAP-101 destiné aux distributeurs indépendants

Le Components Technology Institute Inc. (CTI), situé aux Etats-Unis, a créé le programme certifié CCAP-101 destiné aux distributeurs indépendants (voir A.8.8), afin de définir les pratiques obligatoires visant à détecter les composants électroniques contrefaits et à en éviter la livraison à leurs clients. Il existe environ dix distributeurs certifiés, principalement aux Etats-Unis.

4.11.3 SAE AS6081

La SAE AS6081 a été publiée à l'intention des distributeurs non franchisés qui proposent des composants à la vente. Ce document décrit les essais à effectuer pour éviter que des composants contrefaits, frauduleux ou recyclés ne se retrouvent dans la chaîne d'approvisionnement. La SAE AS6301 constitue la norme de vérification. La traçabilité de ce type de composants jusqu'au fabricant d'origine (OCM) peut ne pas être garantie.

L'IECQ a créé un programme de vérification destiné aux distributeurs non franchisés utilisant la SAE AS6081 (voir A.7.6).

La DLA a adopté la SAE AS6081 le 10 juin 2013, afin que le Ministère de la Défense l'utilise. La DLA contrôle le distributeur qui soumet à essai les composants au titre de la SAE AS6081, et qui est inscrit sur la liste des fournisseurs d'essai certifiés (QTSL) lorsque le contrôle s'avère satisfaisant (voir A.8.9).

Il est cependant nécessaire que les fabricants d'équipements d'origine prennent des précautions lorsqu'ils utilisent des composants soumis à essai au titre de la SAE AS6081, étant donné que la traçabilité jusqu'au fabricant d'origine peut ne pas être garantie. Selon les termes de la SAE AS6081, la mise à l'essai peut être personnalisée, et les pièces ne font pas l'objet d'une évaluation du risque pour l'application prévue, étant donné que les distributeurs non franchisés ne la connaissent pas. Les fabricants d'équipements avioniques d'origine peuvent préférer intervenir directement et gérer la totalité de la chaîne d'approvisionnement et choisir les essais appropriés en utilisant l'IEC 62668-2 (voir 4.11.4).

4.11.4 Distributeurs non franchisés gérés par les fabricants d'équipements d'origine

La plupart des fabricants d'équipement d'origine ont besoin de faire occasionnellement appel à des distributeurs non franchisés afin de se fournir en composants d'origine certifiée étant donné qu'il est impossible, avec les programmes de réduction des fournisseurs (fabricants de composants d'origine ou distributeurs franchisés) en vigueur aujourd'hui, de fournir la totalité des composants nécessaires en faisant uniquement appel aux distributeurs franchisés.

Il existe un petit groupe de distributeurs non franchisés qui n'achètent qu'aux fabricants de composants d'origine ou à leurs distributeurs franchisés spécialisés dans le marché avionique. Ces distributeurs disposent généralement d'une certification tierce au titre de l'AS/EN/JISQ9120 ou de la SAE AS6081. Ils font généralement preuve d'une traçabilité totale et peuvent être de bons fournisseurs de l'industrie avionique. Ils peuvent également satisfaire aux exigences du DFARS 252.246-7007 et du DFARS 252-246-7008. Ces distributeurs sont parfois appelés des fournisseurs "transitaires".

Voir l'IEC 62668-2 pour plus d'informations.

4.11.5 Courtiers

Faire appel à des courtiers (voir 3.1.2) pour l'achat de composants avioniques n'est pas recommandé.

Voir l'IEC 62668-2 pour plus d'informations.

4.12 Lignes directrices des fabricants d'équipements avioniques d'origine en matière de lutte contre la contrefaçon lors de l'achat de composants

4.12.1 Approche générale de la lutte contre la contrefaçon

Les fabricants d'équipements d'origine doivent disposer de leurs propres plans de gestion de la lutte contre la contrefaçon, qui s'appuient sur:

- les procédures de l'AS/EN/JISQ 9100 (voir 4.2);

- l'IEC 62239-1 (ECMP), qui comprend la gestion de l'obsolescence.

NOTE La gestion de l'obsolescence contribue grandement à la prévention de la contrefaçon. L'IEC 62402 et la SAE STD-0016 fournissent des lignes directrices concernant la gestion de l'obsolescence des composants.

4.12.2 Achat auprès de sources agréées

Il convient que la totalité des composants soit choisie chez des fabricants agréés ayant mis en place des contrôles relatifs aux marques déposées, aux logos et à tout autre type de propriété intellectuelle, mais également qu'ils soient achetés à des sources autorisées dont la traçabilité jusqu'au fabricant d'origine est garantie, en utilisant les processus agréés des fabricants d'équipements d'origine au titre de l'AS/EN/JISQ 9100. Il convient que les sources autorisées disposent d'un agrément ISO 9001 ou mieux encore AS/EN/JISQ 9100 ou AS/EN/JISQ 9120 et soient les fabricants de composants d'origine ou leurs distributeurs franchisés agréés (voir 4.10). La base de données en ligne Oasis, mise en place par le Groupe international de qualité en aérospatiale ou IAQG (voir A.8.11), peut être utilisée pour vérifier les certificats émis au titre de l'AS/EN/JISQ 9100, l'AS/EN/JISQ 9110 et l'AS/EN/JISQ 9120.

La SAE ARP 6178, qui est une liste de contrôle utilisée lors des audits, peut constituer un outil utile pour l'évaluation des sources d'approvisionnement (voir Article A.16), et elle peut constituer une partie du processus d'agrément des fournisseurs des fabricants d'équipements d'origine, au titre de l'AS/EN/JISQ 9100.

NOTE l'ISO 22380, en cours de rédaction, peut apporter une aide pour la gestion du risque de fraude produit.

4.12.3 Composants avec une traçabilité jusqu'au fabricant d'origine

L'AS/EN/JISQ 9100 exige une démonstration de conformité à la définition du produit. En ce qui concerne les composants électroniques, cela peut être attesté en garantissant leur traçabilité jusqu'au fabricant d'origine, afin de valider leur authenticité et leur conformité aux spécifications indiquées/aux fiches techniques.

La plupart des fabricants d'équipements avioniques d'origine exigent donc que la traçabilité jusqu'au fabricant d'origine de la totalité des composants achetés soit garantie, étant donné qu'ils utilisent des procédures de stock unique pour l'ensemble de leurs programmes et que leurs acheteurs, au moment de la commande, ne savent pas où les composants seront utilisés et si l'application à laquelle ils sont destinés est essentielle au vol ou non. Les acheteurs des fabricants d'équipements d'origine doivent s'assurer de la traçabilité totale de l'ensemble du stock commandé, et formuler une requête spéciale d'achat en non-conformité lorsqu'ils ne peuvent se procurer que des composants d'origine inconnue. Cette procédure doit s'appliquer à tout processus d'approvisionnement comprenant des opérations d'approvisionnement en ligne directe (DLF) à travers un système de remplacement type et/ou tout type d'entrepôt traditionnel.

La traçabilité des composants est pleinement garantie lorsqu'ils sont achetés au fabricant d'origine, à ses distributeurs franchisés ou à ses fournisseurs franchisés du marché secondaire du produit final en boîtier ou des puces ou des tranches, ou encore à ses distributeurs non franchisés gérés par les fabricants d'équipements d'origine (voir 4.11.4). Les composants avec une traçabilité jusqu'au fabricant d'origine sont également disponibles auprès des distributeurs certifiés au titre de l'AS/EN/JISQ 9120 qui peuvent être franchisés ou non. Un certificat de conformité et/ou une copie du bordereau d'expédition du fabricant de composants d'origine peuvent être demandés, afin de confirmer la traçabilité (voir 3.1.25 et 4.12.4). La lettre concluant un accord de franchise ou le contrat passé avec le fabricant de composants d'origine, accompagnés des entrées d'une base de données de système commercial relatives au fournisseur, indiquant les dates de réception, les quantités ainsi que les codes de date de lot, etc. peuvent satisfaire aux exigences de traçabilité jusqu'au fabricant de composants d'origine.

Il est conseillé de contrôler périodiquement ces fournisseurs, par exemple en utilisant les listes de contrôle de vérification de la traçabilité de l'IECQ OD 3407-1.

Les distributeurs franchisés du marché secondaire luttent souvent pour fournir suffisamment de documents attestant de la traçabilité jusqu'au fabricant de composants d'origine, étant donné qu'ils peuvent avoir acquis les composants de nombreuses années avant que la traçabilité tout le long de la chaîne d'approvisionnement ait dû être contrôlée et attestée.

Il peut se révéler nécessaire pour les fabricants d'équipements d'origine de mettre en place des accords contractuels spéciaux avec les distributeurs, afin de s'assurer que leurs commandes font preuve d'une traçabilité totale jusqu'au fabricant de composants d'origine avant que celles-ci ne soient émises. Il convient que cet accord contractuel constitue une partie du processus d'évaluation et d'agrément du distributeur aux termes de l'OEM AS/EN/JISQ 9120 (voir 4.12.2).

Il convient que l'ensemble des fabricants d'équipements d'origine commande des composants dont la traçabilité est garantie, étant donné que la sécurité est une priorité cruciale.

Les mécanismes de suivi de la chaîne d'approvisionnement, par exemple les méthodes d'identification d'élément unique (IUID) DoDI 8320.04, peuvent être utiles dans ce processus.

4.12.4 Certificat de conformité et bordereau d'expédition

4.12.4.1 Certificat de conformité

Un certificat de conformité constitue la manière traditionnelle de garantir la traçabilité jusqu'au fabricant de composants d'origine. Un certificat de conformité signé par le fabricant de composants d'origine ne garantit pas seulement la traçabilité, mais aussi la conformité à la conception du produit. Les certificats de conformité des fabricants de composants d'origine sont régulièrement utilisés par les fabricants d'équipements avioniques d'origine pour garantir leurs certificats de navigabilité, étant donné que les certificats de conformité fournissent la preuve que les produits ont été validés comme conformes à leurs caractéristiques de conception. Il s'agit généralement d'une déclaration écrite signée par le gestionnaire qualité du distributeur ou de la société vendant les composants, comprenant une garantie écrite que ceux-ci sont neufs, inutilisés et que leur traçabilité jusqu'au fabricant d'origine est garantie. Ces informations peuvent être conservées sous forme électronique dans une base de données ou sous forme papier.

Aux Etats-Unis, les certificats de conformité relatifs aux composants destinés aux organismes de la Défense américaine suivent les exigences de la JESD31.

Noter que les certificats de conformité peuvent seulement être ceux du fournisseur et non ceux du fabricant de composants d'origine. Ils peuvent également être contrefaits.

4.12.4.2 Bordereau d'expédition

S'agissant de composants non destinés aux organismes de la Défense, la traçabilité peut être attestée par les "bordereaux d'expédition" du distributeur, suivant généralement les publications de l'ECIA (voir A.8.7):

- la NIGP 111, *Guidelines for the Format of Packing Slips* (disponible en anglais seulement), qui admet l'impression du certificat de conformité directement au recto du bordereau d'expédition ou en tant que document à part entière accompagnant la liste de colisage;
- la NIGP 115, *Certificates of Conformance for Commercial Electronic Parts* (disponible en anglais seulement).

Dans ce cas, étant donné qu'il y a transfert de l'information, les fabricants d'équipements d'origine doivent vérifier auprès des distributeurs que la traçabilité jusqu'aux fabricants de composants d'origine est garantie.

4.12.5 Planification et achat de quantités suffisantes

Les fabricants d'équipements d'origine n'achètent souvent les composants qu'avec une marge de deux ans, étant donné qu'il s'agit là du délai de couverture des commandes qu'ils proposent à leurs clients pour les produits qu'ils leur livrent, même si ceux-ci présentent une durée de vie de 15 ans, sans compter la durée de maintenance. Les fabricants d'équipements d'origine utilisent souvent des procédures de commande en "juste à temps" (JIT). En conséquence, ils n'achètent généralement pas assez de composants voire ratent les occasions se présentant lors des annonces de dernier achat (LTB). Il est essentiel que chaque fabricant d'équipements d'origine utilise un processus de gestion de l'obsolescence pouvant être en conformité avec son plan de gestion mis en place au titre de l'IEC 62239-1 ECMP ou de la SAE STD-0016 DMSMS, et contrôle les exigences des composants tout au long du cycle de vie de son produit.

Les politiques JIT des fabricants d'équipements d'origine doivent être alignées sur leurs politiques de gestion de l'obsolescence. La gestion du risque pourrait être meilleure en mettant en place davantage d'"achats uniques" en fonction de l'application concernée, ou en effectuant des commandes périodiques afin de préserver le lien avec le fabricant de composants d'origine, pour les composants presque obsolètes, plutôt que d'attendre le moment des annonces de dernier achat (LTB). De plus, les composants destinés aux annonces de dernier achat exigent une gestion et une conservation soigneuses (voir les lignes directrices de l'IEC 62435-1).

4.12.6 Recours à des distributeurs non franchisés

Il convient de faire appel à des distributeurs non franchisés (voir 4.11) le moins souvent possible, étant donné qu'ils exigent une gestion directe. Ils représentent un risque inhérent de fourniture de composants contrefaits. Les fabricants d'équipements d'origine doivent faire preuve d'une gestion rigoureuse à leur égard, afin de savoir à quel moment ils expédient des composants avec une traçabilité complète jusqu'au fabricant d'origine et à quel moment ils expédient des composants d'origine inconnue. Il est fortement recommandé que l'ensemble des distributeurs non franchisés soient certifiés au titre de l'AS/EN/JISQ 9120, étant donné que cette caractéristique est clairement indiquée sur tous les devis établis pour les fabricants d'équipements d'origine. Les fabricants d'équipements d'origine peuvent également envisager l'utilisation de nombreux outils existants, destinés à l'évaluation des risques encourus en faisant appel à des distributeurs non franchisés, notamment:

- 1) la SAE ARP 6178 (voir Article A.16);
- 2) les calculateurs de l'INEMI, permettant d'évaluer les risques liés à la lutte contre la contrefaçon (voir Article A.17);
- 3) la SAE AS6171, qui comprend l'utilisation d'un outil en ligne de couverture des défauts et contrefaçons (voir Article A.16).

Lorsque les distributeurs non franchisés expédient des composants d'origine inconnue, le fabricant d'équipements d'origine doit suivre les exigences de l'IEC 62668-2 afin d'obtenir de plus amples informations. Ces exigences imposent de soumettre la totalité des composants achetés à une analyse de risque et de soumettre à essai l'atténuation des risques avant l'utilisation des composants. Une approbation préalable est généralement exigée de la part du client, le plus souvent un fabricant d'équipements d'origine (voir 3.1.15).

4.12.7 Courtiers

Faire appel à des courtiers non approuvés (voir 3.1.2) pour l'achat de composants avioniques n'est pas recommandé, en particulier lorsqu'ils travaillent par le biais d'Internet (voir l'IEC 62668-2 pour de plus amples informations).

4.12.8 Recours au fabricant d'origine

Le fabricant de composants d'origine peut relancer la production d'un produit obsolète ou très peu fabriqué, s'il reste suffisamment de puces dans le stock de plaquettes. Le site web du fabricant peut ne pas mentionner cette information. Il est alors nécessaire de contacter directement le fabricant de composants d'origine pour déterminer si cela est possible.

4.12.9 Composants obsolètes et sources franchisées du marché secondaire

Les composants obsolètes représentent souvent la plus grande source de composants contrefaits ou recyclés au sein de la chaîne d'approvisionnement. Les composants obsolètes peuvent encore être vendus par les distributeurs franchisés longtemps après les annonces de dernier achat (LTB). Il convient de prendre soin de contrôler les codes de date de lot (LDC) lors des annonces de dernier achat, afin de s'assurer de l'authenticité des pièces mises en vente. Les fabricants de composants d'origine peuvent contribuer à la vérification des codes de date de lot. De plus, de nombreux outils de contrôle actif de l'obsolescence et de la contrefaçon existent pour aider les fabricants d'équipements d'origine à contrôler les annonces de dernier achat, les avis de modification de produit (PCN) et les rapports de contrefaçon. Il peut ainsi être procédé à une vérification rapide des codes de date de lot.

Les composants obsolètes toujours disponibles auprès de distributeurs franchisés "en sommeil" ou de sources du "marché secondaire" agréées par le fabricant (voir 3.1.1) doivent être utilisés avant de s'approvisionner en composants d'origine inconnue. Se reporter à l'Annexe B pour les exemples de sources du marché secondaire.

Il peut être nécessaire de vérifier le contrat de franchise conclu entre le fabricant franchisé "en sommeil" ou du "marché secondaire" et le fabricant d'origine, par exemple en demandant au franchisé les contrats et lettres afférents, en recherchant les communiqués de presse et les déclarations publiées appropriés, etc.

Le distributeur ou fabricant franchisé du marché secondaire peut ne pas toujours être en possession du certificat original de conformité ou du bordereau d'expédition fournis par le fabricant de composants d'origine, mais figurera dans les entrées d'une base de données de système commercial, qui confirment la date de réception des marchandises expédiées par le fournisseur (dont il convient qu'il s'agisse du fabricant de composants d'origine ou d'un de ses distributeurs franchisés), la quantité ainsi que le code de date de lot. Il convient que cette information issue du système commercial, accompagnée d'une copie du contrat de franchise fournisse suffisamment d'informations pour satisfaire aux exigences de traçabilité jusqu'au fabricant de composants d'origine (voir également 4.12.3).

Lorsque seules les puces provenant de sources franchisées sont disponibles, elles peuvent être emballées par des sociétés tierces spécialisées (voir Article B.3) et agréées conformément aux termes de l'IEC 62239-1 ECMP ou de la SAE STD-0016 du fabricant d'équipements d'origine.

Il convient que les composants obsolètes ou en passe de l'être soient identifiés assez tôt, par l'utilisation de procédures proactives de détection de l'obsolescence, reposant sur au moins l'un des documents suivants:

- IEC 62239-1;
- SAE STD-0016;
- IEC 62402;
- SD-22.

4.12.10 Substituts agréés au titre de l'IEC 62239-1

Lorsque des composants d'origine avec une traçabilité jusqu'au fabricant d'origine ou provenant du marché secondaire ne peuvent être obtenus, il convient que les fabricants d'équipements d'origine envisagent de mettre en action leur plan de gestion des composants électroniques au titre de l'IEC 62239-1, afin de trouver des composants d'origine certifiée agréés au titre de l'IEC 62239-1 qui soient des substituts satisfaisants sur le plan de la forme, de la compatibilité et de la fonction et adaptés à l'application.

4.12.11 Reconception produit

Il convient, lorsqu'il n'existe aucun substitut disponible sur le marché secondaire franchisé ou au titre de l'IEC 62239-1, que les fabricants d'équipements d'origine envisagent une reconception, afin que des composants avec une traçabilité jusqu'au fabricant d'origine puissent être utilisés. La reconception peut se limiter au développement d'un petit "intermédiaire électronique" ou d'une "carte-fille" plutôt qu'à la reconception de l'ensemble du circuit.

4.12.12 Composants d'origine inconnue

Lorsque toutes les autres sources d'approvisionnement sont épuisées et qu'il n'existe aucune possibilité de reconception produit, les composants d'origine inconnue sont souvent vus comme étant la seule solution. L'approvisionnement en composants d'origine inconnue est un processus à haut risque, sans aucune garantie de réussite, étant donné qu'il est fortement probable d'être fourni en composants contrefaits ou recyclés. Les implications légales de ce qu'il faut faire si les composants s'avèrent être contrefaits doivent être prises en compte, étant donné qu'ils ne peuvent être mélangés à des composants avec une traçabilité jusqu'au fabricant d'origine et ne peuvent être renvoyés dans la chaîne d'approvisionnement. Le renvoi de ces composants dans la chaîne d'approvisionnement constitue une forme de commerce illégal qui peut entraîner des poursuites. Il convient d'isoler et de conserver les composants qui s'avèrent contrefaits comme preuve et de signaler les faits aux forces de l'ordre (voir 4.14, A.7.2. et Article A.8 pour les contacts utiles). Les composants d'origine inconnue doivent être gérés dans le cadre d'un plan de gestion de la lutte contre la contrefaçon des fabricants d'équipements d'origine (voir 4.12.13) dans le cadre de l'IEC TS 62668-2.

4.12.13 Plans de lutte contre la contrefaçon des OEM comprenant la SAE AS5553 et la SAE AS6174

4.12.13.1 Généralités

Les fabricants d'équipements d'origine doivent disposer d'un plan destiné au recyclage et à la lutte contre la fraude et la contrefaçon, conformément au présent document (voir 4.2 et plus particulièrement 4.2 c)).

Les fabricants d'équipements d'origine ne disposant pas d'un plan au titre de la SAE AS5553 doivent satisfaire aux exigences spécifiées en 4.2 c)).

Les fabricants d'équipements d'origine disposant d'un plan de lutte contre la contrefaçon des composants électroniques au titre de la SAE AS5553A ou de la SAE AS5553B peuvent en tenir compte dans la définition de leur plan de lutte contre la contrefaçon au titre de l'IEC 62668-1. Les Tableaux 2 et 3 font l'inventaire des exigences de l'IEC 62668-1 qui peuvent être respectées ou non par les exigences de la SAE AS5553A ou de la SAE AS5553B, respectivement.

La révision de la SAE AS5553 actuellement en vigueur est la B, la C étant en cours de rédaction. Ce document, très complet, est destiné à l'industrie générale ainsi qu'à l'industrie à grande sécurité et est principalement rédigé à l'intention des utilisateurs américains (voir Article A.17 pour de plus amples informations). Il n'est valable que pour les composants électroniques destinés à la mise en vente.

Noter que la SAE AS5553 révision C en cours de rédaction peut, à sa publication, présenter des exigences de traçabilité différentes au regard des révisions précédentes et peut donc répondre différemment aux exigences de l'IEC 62668-1. Il est donc possible que les Tableaux 2 et 3 ne soient pas totalement satisfaisants en la matière. En plus de la gestion des composants électroniques destinés à la mise en vente, l'IEC 62668-1 comprend également la gestion de la propriété intellectuelle de tous les produits du fabricant d'équipements d'origine vendus à part, y compris la gestion des pièces détachées (qu'elles soient vendues en tant que composants individuels ou dans un montage) et des réparations.

Tableau 2 – Respect ou non des exigences de l'IEC 62668-1 en fonction de la présence d'un plan agréé au titre de la SAE AS5553A chez le fabricant d'équipements d'origine

Exigences de l'IEC 62668-1	Respectées par les exigences de la SAE AS5553A	Commentaires	Notes destinées aux fabricants d'équipements avioniques d'origine lors de la rédaction d'un plan au titre de la SAE AS5553A servant de base à un plan au titre de l'IEC 62668-1
4.2 a)	Non.		
4.2 b)	Non.	La SAE AS5553A ne dispose pas de règles minimales de choix spécifiques de composants prenant en compte la propriété intellectuelle, mais uniquement de règles destinées à maximiser la disponibilité des pièces au moyen d'un plan de gestion de l'obsolescence, ainsi que de règles destinées à l'approvisionnement en composants et à leur gestion.	Pour les fabricants d'équipements avioniques d'origine, se reporter au plan établi au titre de l'IEC 62239-1 ECMP, qui traite des règles relatives à la gestion de l'obsolescence ainsi que des règles de choix et de qualification des composants.
4.2 c)	Un plan établi au titre de la SAE AS5553A ne couvre que les exigences relatives à l'achat et à la mise en vente des composants. Le plan établi au titre de l'IEC 62668-1 doit également prendre en compte les exigences du 4.2, y compris la manière dont les propriétaires du plan gèrent leur propriété intellectuelle, leurs pièces détachées, leurs réparations et la mise sur le marché de pièces détachées individuelles.		Afin de montrer de quelle manière le plan établi au titre de la SAE AS5553A satisfait aux exigences de l'IEC 62668-1, fournir une matrice de renvoi fondée sur le Tableau 2.
4.2 d)	Non – à moins que l'AS/EN/JISQ 9100 ne soit invoquée.	La SAE AS5553A a été rédigée à l'intention de l'industrie générale et ne rend pas obligatoire l'utilisation de l'AS/EN/JISQ 9100.	Fonder le plan établi au titre de la SAE AS5553A sur les procédures issues de l'AS/EN/JISQ 9100.
4.2 e)	Oui.		Fonder le plan établi au titre de la SAE AS5553A sur la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant d'origine.
4.2 e) 1)	Oui.		Fonder le plan établi au titre de la SAE AS5553A sur la traçabilité de la chaîne d'approvisionnement.

Exigences de l'IEC 62668-1	Respectées par les exigences de la SAE AS5553A	Commentaires	Notes destinées aux fabricants d'équipements avioniques d'origine lors de la rédaction d'un plan au titre de la SAE AS5553A servant de base à un plan au titre de l'IEC 62668-1
4.2 e) 2)	Exigence optionnelle liée au contrat passé avec le client. Non.	La SAE AS5553A ne reconnaît pas cette exigence contractuelle optionnelle faisant appel à des sources américaines de confiance.	Permettre l'adaptation du plan établi au titre de la SAE AS5553A en faisant appel à des fournisseurs américains de confiance lorsque des clients américains l'exigent par contrat.
4.2 e) 3)	Oui.		Fonder le plan établi au titre de la SAE AS5553A sur le recours aux sources franchisées du marché secondaire lorsque les pièces sont obsolètes.
4.2 e) 4)	Oui.		Fonder le plan établi au titre de la SAE AS5553A sur la traçabilité de la chaîne d'approvisionnement.
4.2 f)	En partie.	La SAE AS5553A a été rédigée à l'intention de l'industrie générale et ne rend pas obligatoire l'utilisation de l'AS/EN/JISQ 9100.	Fonder le plan de lutte contre la contrefaçon sur les procédures issues de l'AS/EN/JISQ 9100.
4.2 g) 1)	En partie.	La SAE AS5553A n'impose pas l'exhaustivité de la recherche, pas plus qu'elle ne stipule qu'il convient d'envisager des solutions de substitution avant de se fournir en pièces d'origine inconnue achetées à une source non franchisée.	Fonder le plan de lutte contre la contrefaçon sur l'utilisation de l'IEC TS 62239-1, destinée à l'évaluation des risques et à la prise en compte de solutions de substitution reposant sur les pièces avec une traçabilité jusqu'au fabricant d'origine, avant d'y déroger et de se fournir en pièces d'origine inconnue en dehors du réseau des fabricants de composants d'origine et des distributeurs franchisés.
4.2 g) 2)	Non.	Les exigences minimales de la SAE AS5553A ne font pas référence à l'IEC 62668-2 et ne rendent pas obligatoire l'utilisation des procédures de non-conformité de l'AS/EN/JISQ 9100.	Fonder le plan de lutte contre la contrefaçon sur l'utilisation de l'IEC 62668-2, destinée à la gestion des distributeurs non franchisés.
4.2 h)	Non.	La SAE AS5553A ne s'applique pas aux produits ou aux pièces n'étant plus rattachées aux fabricants d'équipement d'origine.	
4.2 i)	Oui.		
4.2 j)	Oui.		
4.2 k)			
4.2 l)	Oui.		

Tableau 3 – Respect ou non des exigences de l'IEC 62668-1 en fonction de la présence d'un plan agréé au titre de la SAE AS5553B chez le fabricant d'équipements d'origine

Exigences de l'IEC 62668-1	Respectées par les exigences de la SAE AS5553B	Commentaires	Notes destinées aux fabricants d'équipements avioniques d'origine lors de la rédaction d'un plan au titre de la SAE AS5553B servant de base à un plan au titre de l'IEC 62668-1
4.2 a)	Non.		
4.2 b)	Non.	La SAE AS5553B ne dispose pas de règles minimales de choix spécifiques de composants prenant en compte la propriété intellectuelle, mais uniquement de règles destinées à maximiser la disponibilité des pièces au moyen d'un plan de gestion de l'obsolescence, ainsi que de règles destinées à l'approvisionnement en composants et à leur gestion.	Pour les fabricants d'équipements avioniques d'origine, se reporter au plan établi au titre de l'IEC 62239-1 ECMP, qui traite des règles relatives à la gestion de l'obsolescence ainsi que des règles de choix et de qualification des composants.
4.2 c)	Un plan établi au titre de la SAE AS5553B ne couvre que les exigences relatives à l'achat et à la mise en vente des composants. Le plan établi au titre de l'IEC 62668-1 doit également prendre en compte les exigences du 4.2, y compris la manière dont les propriétaires du plan gèrent leur propriété intellectuelle, leurs pièces détachées, leurs réparations et la mise sur le marché de pièces détachées individuelles.		Afin de montrer de quelle manière le plan établi au titre de la SAE AS5553B satisfait aux exigences de l'IEC 62668-1, fournir une matrice de renvoi fondée sur le Tableau 2.
4.2 d)	Non – à moins que l'AS/EN/JISQ 9100 ne soit invoquée	La SAE AS5553B a été rédigée à l'intention de l'industrie générale et ne rend pas obligatoire l'utilisation de l'AS/EN/JISQ 9100.	Fonder le plan établi au titre de la SAE AS5553B sur les procédures issues de l'AS/EN/JISQ 9100.
4.2 e)	Oui.		Fonder le plan établi au titre de la SAE AS5553B sur la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant d'origine, en utilisant le plan de management de la qualité établi au titre de l'AS/EN/JISQ.
4.2 e) 1)	Oui.		Fonder le plan établi au titre de la SAE AS5553B sur la traçabilité de la chaîne d'approvisionnement jusqu'au fabricant d'origine.
4.2 e) 2)	Exigence optionnelle liée au contrat passé avec le client.	La SAE AS5553B ne reconnaît pas cette exigence contractuelle optionnelle faisant appel à des sources américaines de confiance.	Permettre l'adaptation du plan établi au titre de la SAE AS5553B en faisant appel à des fournisseurs américains de confiance lorsque des clients américains l'exigent par contrat.

Exigences de l'IEC 62668-1	Respectées par les exigences de la SAE AS5553B	Commentaires	Notes destinées aux fabricants d'équipements avioniques d'origine lors de la rédaction d'un plan au titre de la SAE AS5553B servant de base à un plan au titre de l'IEC 62668-1
4.2 e) 3)	Oui.		Fonder le plan établi au titre de la SAE AS5553B sur le recours aux sources franchisées du marché secondaire lorsque les pièces sont obsolètes, en garantissant la traçabilité jusqu'au fabricant d'origine.
4.2 e) 4)	Oui.		Fonder le plan établi au titre de la SAE AS5553B sur la traçabilité de la chaîne d'approvisionnement.
4.2 f)	En partie.	La SAE AS5553B a été rédigée à l'intention de l'industrie générale et ne rend pas obligatoire l'utilisation de l'AS/EN/JISQ 9100.	Fonder le plan de lutte contre la contrefaçon sur les procédures issues de l'AS/EN/JISQ 9100.
4.2 g) 1)	En partie.	La SAE AS5553B n'impose pas l'exhaustivité de la recherche, pas plus qu'elle ne stipule qu'il convient d'envisager des solutions de substitution avant de se fournir en pièces d'origine inconnue achetées à une source non franchisée.	Fonder le plan de lutte contre la contrefaçon sur l'utilisation de l'IEC 62239-1, destinée à l'évaluation des risques et à la prise en compte de solutions de substitution reposant sur les pièces avec une traçabilité jusqu'au fabricant d'origine, avant d'y déroger et de se fournir en pièces d'origine inconnue en dehors du réseau des fabricants de composants d'origine et des distributeurs franchisés.
4.2 g) 2)	Non.	Les exigences minimales de la SAE AS5553B ne font pas référence à l'IEC 62668-2 et ne rendent pas obligatoire l'utilisation des procédures de non-conformité de l'AS/EN/JISQ 9100.	Fonder le plan de lutte contre la contrefaçon sur l'utilisation de l'IEC 62668-2, destinée à la gestion des distributeurs non franchisés (qui comprend la référence à la SAE AS6171).
4.2 h)	Non.	La SAE AS5553B ne s'applique pas aux produits ou aux pièces n'étant plus rattachées aux fabricants d'équipement d'origine.	
4.2 i)	Oui.		
4.2 j)	Oui.		
4.2 k)	Non.		La SAE AS5553B ne traite pas de l'inspection des composants ou produits renvoyés.
4.2 l)	Oui.	La SAE AS5553B exige un processus de gestion de l'obsolescence.	

4.12.13.2 Guide du Groupement des Industries Françaises Aéronautiques et Spatiales (GIFAS) destiné aux fabricants d'équipements d'origine faisant appel aux distributeurs non franchisés

Le guide GIFAS 5052 est publié par le Comité national français du GIFAS. Il a été adopté et modifié afin d'être publié en tant qu'IEC 62668-2.

4.12.13.3 Implication des sous-traitants de niveau inférieur

Les fabricants d'équipements d'origine doivent transmettre les exigences d'un plan de lutte contre la contrefaçon aux sous-traitants de niveau inférieur ou doivent les gérer efficacement; cela comprend les opérations de maintenance, de réparation et de révision effectuées sous la responsabilité des fabricants d'équipements d'origine.

NOTE Les Figures E.1, E.2, E.3, E.4 et E.5 peuvent aider à la mise en place des normes de lutte contre la contrefaçon.

Les fabricants d'électronique sous contrat (CEM), qui effectuent des opérations de fabrication en sous-traitance pour les fabricants d'équipements d'origine et qui disposent de plans de lutte contre la contrefaçon au titre de la SAE AS5553, peuvent également être soumis à des contrôles de traçabilité seconds ou tiers au titre de l'IEC OD 3702.

4.12.13.4 Composants refabriqués

Voir 3.1.18 pour la définition d'un "composant refabrique". Ces composants peuvent être fabriqués afin de satisfaire aux besoins du marché en composants emballés différemment ou présentant différents indices de température ou destinés à résoudre des problèmes d'obsolescence, etc. Les techniques d'extraction des puces sont vues comme potentiellement destructrices, étant donné que le processus d'extraction peut être non contrôlé et peut provoquer des décharges électrostatiques, ainsi que des dommages mécaniques et thermiques. Les puces peuvent également avoir été précédemment utilisées dans une application, et donc être recyclées. Leur durée de vie ainsi que leur fiabilité à long terme au sein d'une nouvelle application sont inconnues.

Les composants refabriqués ne sont pas vus comme étant contrefaits ou frauduleux si les refabricants utilisent leur logo, leur nom et leurs numéros de pièces pour les décrire et indiquent sur leurs fiches techniques toutes les informations techniques nécessaires, comme les caractéristiques électriques, fonctionnelles et physiques, ainsi que le processus de refabrication.

Ces composants refabriqués ne présentent pas la même fiabilité à long terme que les composants produits par les fabricants de composants d'origine. Les composants refabriqués ne sont donc pas traités dans le présent document, et il est recommandé d'éviter de les utiliser en avionique civile, étant donné qu'ils peuvent présenter un risque inacceptable de réduction du temps moyen entre pannes.

4.13 Lignes directrices des fabricants d'équipements d'origine en matière de lutte contre la contrefaçon concernant leurs produits

4.13.1 Contrôle de la propriété intellectuelle

Il convient que les fabricants d'équipements d'origine contrôlent leurs conceptions, par le biais d'une combinaison de brevets, contrats de franchises, contrôles de la conception, des marques déposées et des logos. Il convient que les fabricants d'équipements d'origine contrôlent également, de manière sécurisée, leur programme d'acceptation finale ainsi que leurs postes d'essai, leurs nomenclatures des matériels (BoM), leurs dessins et leurs spécifications.

4.13.2 Rendre les conceptions des fabricants d'équipements d'origine inviolables

Il existe de nombreuses manières de configurer les conceptions des fabricants d'équipement d'origine par le biais de fonctionnalités inviolables, qu'elles soient matérielles ou logicielles.

Il existe de nombreux sous-traitants spécialisés proposant des services complets de garantie d'inviolabilité destinés à des conceptions complètes (voir Article A. 13 pour des exemples).

En variante, des circuits intégrés spécifiques et des réseaux de portes programmables in situ personnalisés peuvent être conçus en utilisant la technologie de la fonction physique non clonable ou PUF (voir 4.7.10), ou d'autres technologies semblables.

Parmi les articles récents traitant de l'inviolabilité:

- Adam Waksman, Simha Sethumadhavan, "Tamper Evident Microprocessors", faculté d'informatique, université Columbia, New-York. [11]

4.13.3 Etiquettes inviolables

Il existe plusieurs types d'étiquettes inviolables. Elles peuvent être apposées au cours de l'assemblage, afin d'indiquer si un démontage ou une réparation non autorisés ont été effectués. Les unités peuvent être plombées de l'extérieur à l'aide de matériel ou d'étiquettes inviolables (voir Article A.13).

4.13.4 Utilisation de circuits intégrés spécifiques et de réseaux de portes programmables in situ disposant de fonctions de protection de la propriété intellectuelle

4.13.4.1 Généralités

Les circuits intégrés spécifiques et les réseaux de portes programmables in situ sont des microcircuits complexes contenant un code logiciel propriétaire, qui constitue généralement la propriété intellectuelle des fabricants d'équipements d'origine. Ce code exige la protection de la propriété intellectuelle.

4.13.4.2 Réseaux de portes programmables in situ et microcircuit intégré

Certains réseaux de portes programmables in situ (fondés sur la mémoire vive) ont été fabriqués sous la forme d'un microcircuit unique, assemblé sur un circuit imprimé (PCB). Des traces de ce PCB se trouvent entre le microcircuit et les mémoires à semiconducteur adjacentes, assemblées et emballées séparément. Ces traces de PCB peuvent être interceptées par les contrefacteurs, qui peuvent alors lire les signaux passant à travers. Les réseaux de portes programmables in situ équipés de dispositifs antiperturbation ou ceux équipés d'une mémoire à semiconducteur insérée dans un microcircuit intégré sont des produits protégeant mieux la propriété intellectuelle, étant donné qu'aucune mémoire externe n'est exigée. Les fabricants de réseaux de portes programmables in situ intègrent également à présent des microcircuits périphériques supplémentaires à leurs produits, au sein d'un microcircuit hautement complexe, fournissant par là même un produit intégré dans un microcircuit, destiné à être assemblé sur une couche de PCB.

4.13.4.3 Sérialisation des puces des réseaux de portes programmables in situ

La sérialisation confidentielle de puce unique générée aléatoirement, destinée aux réseaux de portes programmables in situ, est à présent proposée par certains fabricants (voir Article A.14 pour des exemples).

4.13.4.4 Mémoire RAM non volatile (NVRAM)

Certaines mémoires vives non volatiles contiennent un microprocesseur interne, qui peut être programmé en usine pour détruire le code interne (voir Article A.15).

4.13.5 Contrôle du marquage final du produit du fabricant d'équipements d'origine

Les fabricants d'équipements d'origine doivent s'assurer que l'équipement fourni est marqué conformément aux exigences réglementaires et que sa traçabilité est pleinement garantie. Noter que les étiquettes d'identification par radiofréquence se répandent, pour permettre de distinguer les composants authentiques de ceux qui sont contrefaits (voir Article A.12).

L'utilisateur peut prendre note des informations suivantes:

- l'ISO 12931 a été publiée dans le but d'apporter une aide quant aux méthodes d'authentification exigées pour lutter contre les risques de contrefaçon;
- l'ISO 16678 est utile pour la mise en place de méthodes de suivi et de traçage des expéditions, destinées à empêcher la contrefaçon et le commerce illicite;
- l'ISO/IEC 15459-8 a été publiée afin de faciliter la définition d'une chaîne de caractères unique et sans signification, destinée à servir d'identifiant unique pour le groupage d'unités de transport. Cet identifiant peut être représenté sous la forme d'une étiquette portant un code-barres ou de tout autre support matérialisant le groupage, afin de satisfaire aux besoins réglementaires et à ceux de la chaîne d'approvisionnement;
- l'ISO 17367 a été publiée afin de définir les fonctionnalités de base du RFID en vue de son utilisation dans la chaîne d'approvisionnement et peut servir d'aide dans la définition de la traçabilité des produits à chaque étape du processus de production;
- l'ISO/IEC 20243 (toutes les parties) a été publiée afin de constituer l'Open Trusted Technology Provider Standard (O-TTPS), destinée à réduire le risque d'apparition de produits contrefaits et délibérément corrompus;
- l'ISO/IEC TR 24729-1 a été publiée afin de fournir des recommandations relatives à l'utilisation des étiquettes RFID et à l'emballage dans la chaîne d'approvisionnement;
- la MIL-STD-130 spécifie les marquages d'identification du matériel appartenant aux organismes de la Défense américaine;
- la MIL-STD-129 définit les pratiques de marquage des organismes de la Défense américaine en matière d'expédition et de conservation.

4.13.6 Contrôle des rebuts des fabricants d'équipements d'origine

Il convient de détruire physiquement la totalité des rebuts internes, afin de s'assurer que les contrefacteurs potentiels ne puissent pas les réassembler et les revendre frauduleusement comme des composants ou unités d'origine. Il convient d'éliminer le matériel destiné aux organismes de la Défense américaine en respectant les dispositions de la DoD 4160.21-M.

4.13.7 Logos et marques déposées des fabricants d'équipements d'origine

Il convient que l'ensemble des marques déposées soit enregistré (voir A.1.3). Il convient que les fabricants d'équipements d'origine prennent autant de précautions que possible pour protéger leurs produits de l'utilisation frauduleuse des numéros de série spéciaux, des marquages des codes de date de lot, des marquages extérieurs, des marquages d'emballages ainsi que des processus d'expédition des produits.

4.13.8 Contrôle des livraisons des produits et pièces détachées des fabricants d'équipements d'origine et de leur durée de vie utile

Il convient que les fabricants d'équipements d'origine étudient l'utilisation de mécanismes spéciaux de suivi pour les composants essentiels aux missions entreprises tels que les moteurs, qui sont des produits FAA de classe I.

Pour de plus amples informations sur l'Administration fédérale de l'aviation (FAA) et sa classification des produits, voir A.8.4.

La FAA dispose de pages web destinées à l'identification des moteurs et aux exigences en ce qui concerne la marque d'immatriculation (voir A.8.4.2).

Elle a récemment publié la circulaire consultative AC 00-56B concernant son "programme d'accréditation des distributeurs volontaires de l'industrie", créé pour accréditer les distributeurs de composants électroniques destinés aux aéronefs civils, sur la base de la surveillance volontaire.

Voir également la DI-LISC-81356 concernant les certificats de conformité délivrés lors de la livraison d'équipement aux clients faisant partie des organismes de la Défense américaine.

4.13.9 Activités MRO

4.13.9.1 Généralités

Voir 3.1.13 pour la définition de "MRO". Il est recommandé que toutes les organisations de maintenance soient certifiées par une tierce partie auprès du système de management de la qualité AS/EN/JISQ 9110, afin d'assurer la totale traçabilité de tous les composants et unités réparés. De plus, l'AS/EN/JISQ 9110 dispose d'un article particulier exigeant de prendre des mesures appropriées pour empêcher l'achat de produits contrefaits/non approuvés. Voir 4.4.4 pour la traçabilité dans les activités MRO.

4.13.9.2 Réparations d'équipements avioniques civils en fonction des produits OEM

La plupart des OEM civils réparent leurs équipements en interne, dans leurs centres de réparation MRO homologués, afin d'être sûrs d'utiliser des composants authentiques et de contrôler les réparations. Les OEM génèrent également des manuels de maintenance des composants (CMM) pour leurs produits, qui donnent des informations détaillées sur la conception et les composants de remplacement. Souvent, le composant de remplacement peut uniquement être acheté auprès de l'OEM, ce qui est encore une fois une mesure de prévention de la contrefaçon.

Certains constructeurs aéronautiques civils procèdent également aux réparations. Certains d'entre eux utilisent des installations approuvées par la FAA, par exemple:

- la FAR Partie 43 décrit les règles relatives aux avions disposant d'un certificat de navigabilité américain;
- la FAA AC (circulaire d'information) 20-62 définit la qualité, l'admissibilité et la traçabilité des pièces et matériaux aéronautiques destinés à être installés sur des produits certifiés aux Etats-Unis;
- la FAR Partie 145 décrit les exigences de certification, de formation et d'installation, ainsi que les règles de fonctionnement des centres de réparation aéronautiques et spatiaux.

L'AESA (voir A.7.5) certifie les avions civils en Europe et les installations de réparation:

- la réglementation AESA Partie M établit les exigences techniques communes et les procédures administratives visant à assurer la navigabilité permanente des avions;
- l'AESA Partie 145 concerne les organisations de maintenance approuvées.

Certains fabricants de moteurs d'avion utilisent des plans de suivi en temps réel pour la gestion de l'état des moteurs, assurant une traçabilité complète au moyen de plans de suivi par satellite prévus sur leurs moteurs tout au long de leur durée de vie opérationnelle. Les processus utilisant ce concept sont vivement recommandés.

La CAAC certifie les avions civils en Chine, ainsi que les installations de réparation (voir A.9.5):

- la CAAC CCAR 145 établit les règlements de maintenance des avions civils conjointement avec la circulaire d'information CAAC AC-145-06R1.

4.13.9.3 Réparations d'équipements avioniques de défense provenant d'OEM

Les clients du secteur de la défense utilisent en règle générale leurs centres de réparation MRO de défense homologués et commandent les composants de rechange pour procéder aux réparations. Dans l'armée américaine, les réparations sont réalisées conformément au DFARS 242.256.7007 et au DFARS 242-256-7008 pour la prévention de la contrefaçon (voir 4.5.4.5). Si les composants sont obsolètes et ont un impact sur la réparation d'un produit, il est recommandé au client de rechercher des alternatives fiables (y compris une éventuelle reconception de l'équipement) plutôt que d'utiliser, par exemple, des composants refabriqués ne présentant aucune fiabilité prévisible.

4.14 Déclaration de contrefaçon, de fraude et de recyclage de composants

4.14.1 Généralités

Il est recommandé de transmettre dans les plus brefs délais la preuve de contrefaçon, d'acte frauduleux et d'activités de recyclage de composants électroniques aux autorités de police locales compétentes, de préférence avant que le composant suspect ne passe le contrôle aux frontières.

4.14.2 Programme relatif aux pièces non approuvées suspectes de la FAA aux Etats-Unis

Les questions relatives aux composants contrefaits suspects peuvent être envoyées par courrier électronique au service d'assistance téléphonique de la sécurité aérienne (voir A.8.4.3).

4.14.3 AESA

L'AESA publie des bulletins d'informations de sécurité (BIS) relatifs aux éventuels risques pouvant inclure la déclaration de composants contrefaits ou frauduleux (voir A.7.5).

4.14.4 Déclaration de contrefaçon au Royaume-Uni

La page web UK Revenue and Customs (administration fiscale et douanière du Royaume-Uni) (voir A.6.4) propose un système de déclaration des composants contrefaits suspects. De plus, le Trading Standards Office (service des normes de commercialisation) (voir A.6.3) propose un système de déclaration des marchandises de contrefaçon.

4.14.5 Déclaration de contrefaçon dans l'Union européenne

Dans l'Union européenne, il convient de déclarer les contrefaçons au niveau local. La page web Europa (voir A.7.1, deuxième point) contient des formulaires et des détails quant à la manière de traiter les demandes au niveau national et européen pour l'action sur la propriété intellectuelle menée par les autorités douanières.

4.14.6 Forum de l'UKEA contre la contrefaçon

Voir A.6.5; forum géré par l'UK Electronic Alliance (UKEA).

Leur site web contient des informations utiles et des liens permettant aux industriels de lutter contre la présence de composants de contrefaçon dans leurs chaînes d'approvisionnement. Il contient un répertoire en ligne d'informations pertinentes en accès libre comprenant des articles, les meilleures pratiques, les événements, des présentations, les sources de composants fiables, des rapports et des fournisseurs de solutions. Les visiteurs peuvent s'enregistrer gratuitement pour alimenter une base de données et y rechercher des composants de contrefaçon suspects.

4.15 Formation de sensibilisation à la prévention de la contrefaçon

Une formation de sensibilisation à la prévention de la contrefaçon est essentielle à l'identification et la gestion des composants contrefaits et frauduleux. Différentes vidéos et différents modules de formation à la prévention de la contrefaçon sont disponibles dans le domaine public, et incluent les exemples suivants:

- le Nuclear Industry Safety Directors Forum (forum des directeurs de la sécurité dans l'industrie nucléaire) dont une vidéo en ligne a récemment été publiée (voir Article A.21);
- l'association mondiale du roulement (World Bearing Association - WBA) publie une excellente page web et une vidéo de formation de sensibilisation en ligne intitulée "Stop Fake Bearings" (Halte aux roulements contrefaits) (voir Article A.22);
- des vidéos en ligne de sensibilisation à la contrefaçon publiées par des sociétés industrielles sont disponibles et ciblent des secteurs industriels particuliers (voir Article A.23 pour un exemple);
- des modules de formation reposant sur un abonnement, par exemple le programme de l'ERAI (voir Article A.24);
- des publications du gouvernement américain (voir Article A.25);
- la page web de prévention de la contrefaçon IECQ WG6 (voir Article A.26);
- différentes vidéos sur Internet expliquant le lien entre crime organisé et le monde de la contrefaçon.

4.16 Informations pour la prise en charge de la gestion de la chaîne d'approvisionnement

Certains documents comme l'ISO 28000, l'ISO 28001, l'ISO 28002, l'ISO 28003 et l'ISO 28004 (toutes les parties) peuvent aider à gérer et sécuriser la chaîne d'approvisionnement concernant la réduction des risques liés aux actes de piratage et de fraude.

Annexe A (informative)

Contacts utiles²

A.1 Organisation mondiale de la propriété intellectuelle (OMPI)

A.1.1 Généralités

Le siège de l'OMPI se trouve à Genève: 34, Chemin des Colombettes, 1211 Genève 20, Suisse, tél: (+41-22) 338 9111, et ses bureaux régionaux sont les suivants:

- OMPI Brésil, Avenida Atlântica, N° 1130, 5th Floor - Part B, Copacabana, Rio de Janeiro, Brésil, Code postal: 22021-000 tél: (+5521) 2513-3506, voir la page web: <https://www3.wipo.int/contact/en/area.jsp?area=wbo>
- OMPI Chine, No.2 Dongkoudai Hutong, Xicheng District, Pékin 100009, Chine, tél: + 86 10 83 22 02 38 /+ 86 10 83 22 08 33, Fax: + 86 10 83 22 03 23, voir la page web <http://www.wipo.int/about-wipo/en/offices/china/>
- OMPI Japon Daido Seimei Kasumigaseki Bldg. 7F, 1-4-2 Kasumigaseki, Chiyoda-ku Tokyo 100-0013, Japon tél: (+81) 3 5532 5030, voir la page web <http://www.wipo.int/about-wipo/en/offices/japan/>
- OMPI Moscou, 5 Nobelya str. Skolkovo Innovation Center Moscow, 143026 Fédération de Russie, tél: +7 499 940 04 82, Fax: +7 499 940 04 83, voir la page web <http://www.wipo.int/about-wipo/en/offices/russia/>
- OMPI New York, WIPO Coordination Office, 2 UN Plaza, Suite 2525, New York, NY 10017, tél: (+1) 212-963-6813, voir http://www.wipo.int/about-wipo/en/new_york/
- OMPI Singapour, 29 Heng Mui King Terrace, #06-16, Singapore, 119620, Singapour, tél: (+65) 6774 6406 et voir (+65) 6774 4298, page web <http://www.wipo.int/about-wipo/en/offices/singapore/>

La page web de l'OMPI est disponible à l'adresse suivante: <https://www.wipo.int/portal/fr/>. Elle contient les informations suivantes.

A.1.2 Présentation de l'OMPI

L'Organisation Mondiale de la Propriété Intellectuelle (OMPI) est une agence spécialisée des Nations Unies. Elle se consacre au développement d'un système de propriété intellectuelle (PI) international équilibré et accessible, qui récompense la créativité, stimule l'innovation et contribue au développement économique tout en protégeant l'intérêt public.

L'OMPI a été créée par la Convention instituant l'OMPI en 1967 dans le cadre d'un mandat accordé par les Etats membres dans le but de promouvoir la protection de la PI à l'international par la coopération des Etats et en collaboration avec d'autres organisations internationales. Son siège social se trouve à Genève, en Suisse.

A.1.3 Services de la propriété intellectuelle de l'OMPI

- **Protection par brevet au niveau international – Traité de coopération en matière de brevets (PCT)**

Le Système PTC (voir la page web <http://www.wipo.int/pct/en/>) permet aux inventeurs et aux déposants d'obtenir une protection par brevet en déposant une seule demande

² Les informations de l'Annexe A sont données à l'intention des utilisateurs du présent document et ne signifient nullement que l'IEC approuve ou recommande les organismes ou logiciels mentionnés.

internationale auprès d'un seul bureau des brevets. Dépôt et traitement des demandes de brevet dans le cadre du PCT:

- rend le monde accessible;
- reporte les principaux coûts liés à la protection par brevet au niveau international;
- donne des informations utiles relatives à l'éventuelle brevetabilité de l'invention;
- est sûre et facile avec le logiciel de dépôt électronique de l'OMPI.

- **Registre international des marques (système de Madrid)**

Le Système de Madrid (voir la page web <https://www.wipo.int/madrid/fr/> ou <https://www.wipo.int/trademarks/fr/>) offre la possibilité aux propriétaires de marques de protéger une marque dans 115 pays en déposant une seule demande auprès d'un bureau national ou régional des marques. Les marques sont des signes distinctifs utilisés pour distinguer les biens identiques ou similaires proposés par différents producteurs ou fournisseurs de services. Les marques sont un type de propriété industrielle, protégé par des droits de propriété intellectuelle.

L'OMPI n'est pas en mesure d'offrir des conseils juridiques aux personnes ou aux entreprises concernant des questions particulières. Le bureau national de la propriété intellectuelle, un agent de propriété intellectuelle ou la législation nationale ou régionale pertinente (WIPO Lex) peuvent être consultés.

Le registre international des marques par le biais du système de Madrid présente les avantages suivants:

- évite de déposer plusieurs demandes auprès de différents bureaux;
- couvre 115 pays dans le monde;
- facilite la gestion de la marque, les modifications ou renouvellements pouvant être enregistrés en un seul acte de procédure;
- les propriétaires de marque ont simplement besoin de remplir un formulaire auprès de leur bureau national, dans une seule langue, payer un ensemble de frais, dans une seule monnaie, afin d'obtenir et de modifier le registre international;
- les propriétaires de marque disposent d'outils en ligne pour rechercher les marques existantes, consulter la gazette de l'OMPI, estimer les frais liés au dépôt, procéder à des paiements électroniques et à des renouvellements, et vérifier le statut de l'enregistrement;
- ce service unique offert par le Système de Madrid facilite l'enregistrement et la gestion d'une marque ou d'un portefeuille volumineux: il donne du pouvoir aux entreprises et les aide à trouver de nouveaux débouchés à l'étranger;
- l'OMPI travaille avec les Etats membres à développer les lois et Normes internationales pour les marques. Voir le Comité permanent du droit des marques, des dessins et modèles industriels et des indications géographiques (SCT - Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications);
- pour consulter les registres internationaux des marques, voir la base de données ROMARIN (Read-Only-Memory of Madrid Active Registry Information) sur la page web <https://www.wipo.int/madrid/fr/monitor/>

- **Système international des données de conception industrielles (Système de La Haye)**

Le Système de La Haye (voir la page web <https://www.wipo.int/hague/fr/>) permet aux déposants de faire enregistrer des données de conception industrielles dans 66 pays pour un minimum de formalités et de frais. Le choix du Système de La Haye pour protéger les données de conception industrielles au niveau international:

- évite de remplir plusieurs demandes auprès de différents bureaux;
- permet aux déposants d'enregistrer jusqu'à 100 données de conception industrielles avec un seul formulaire;

- facilite la gestion des données de conception enregistrées, les modifications ou renouvellements pouvant être enregistrés en un seul acte de procédure.

- **Système international des appellations d'origine (Système de Lisbonne)**

Le Système de Lisbonne (voir la page web <https://www.wipo.int/lisbon/fr/>) facilite la protection au niveau international des appellations d'origine au moyen d'une seule procédure d'enregistrement. Le Système de Lisbonne:

- évite de remplir plusieurs demandes auprès de différents bureaux;
- couvre jusqu'à deux douzaines de pays en Afrique, en Asie, en Europe et en Amérique Latine.

- **Règlement extrajudiciaire des litiges**

Le Centre d'arbitrage et de médiation de l'OMPI (voir la page web <https://www.wipo.int/amc/fr/>) est la ressource principale en matière de règlement en dehors des tribunaux des litiges relatifs à la propriété intellectuelle. Il offre des procédures spécialisées incluant un arbitrage neutre, une médiation expédiée et des procédures d'expertise pour le règlement de litiges commerciaux internationaux entre des parties privées. Les procédures du Centre sont conçues comme des alternatives efficaces et peu onéreuses aux procédures judiciaires, et peuvent se dérouler dans n'importe quel pays, dans n'importe quelle langue et en vertu de toute loi.

- **Règlement des litiges relatifs aux noms de domaine**

Le Centre d'arbitrage et de médiation de l'OMPI (voir la page web <https://www.wipo.int/amc/fr/>) est reconnu au niveau international comme étant le fournisseur de services de règlement de litiges de premier plan concernant l'enregistrement et l'utilisation abusifs des noms de domaine Internet, une pratique communément appelée "cybersquattage". Applicable à tous les domaines internationaux et à un nombre grandissant de domaines qui sont des codes de pays, la procédure de résolution est assurée au format électronique et donne lieu à une décision exécutoire dans les deux mois.

- **Classifications internationales**

Tout déposant qui demande la protection d'un actif de propriété intellectuelle au niveau national ou international est tenu d'établir si sa création est nouvelle ou si un tiers en a déjà obtenu ou revendiqué la propriété. Pour ce faire, une énorme quantité d'informations doivent être recherchées. Les Systèmes de classification internationale (voir la page web <https://www.wipo.int/classifications/fr/>) facilitent ces recherches en organisant les informations sur les inventions, les marques et les données de conception industrielles selon des structures indexées aisément utilisables à des fins d'extraction.

- **Protection des emblèmes d'Etat (Article 6ter de la Convention de Paris)**

La protection des emblèmes d'Etat, ainsi que des noms et des emblèmes d'organisations internationales intergouvernementales est régie par l'Article 6ter (voir la page web <https://www.wipo.int/article6ter/fr/>) de la Convention de Paris, administrée par l'OMPI.

A.1.4 Réseau mondial d'académies de la propriété intellectuelle de l'OMPI

Voir les pages web <https://www.wipo.int/academy/fr/> et https://www.wipo.int/academy/fr/training_institutions.html, qui contiennent les informations suivantes:

L'Académie de l'OMPI joue un rôle central en matière de formation et d'activités de renforcement des capacités humaines, en particulier pour les pays en développement, les pays les moins avancés (LDC) et les pays en transition.

Contactez l'Académie de l'OMPI sur la page web <https://www3.wipo.int/contact/fr/area.jsp?area=academy>

A.2 Accord commercial anticontrefaçon (ACAC)

A.2.1 ACAC

Pour plus d'informations, voir les informations sur le Bureau des représentants américains au commerce (Office of the US Trade Representatives) (voir la page web <https://ustr.gov/acta>) où le texte final de l'accord peut être consulté à l'adresse http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf.

L'accord vise à établir un cadre légal international pour cibler les biens contrefaits, les médicaments génériques et les atteintes au droit d'auteur sur Internet, et est à l'origine de la création d'un organe directeur hors des forums existants, comme l'Organisation mondiale du commerce, l'Organisation mondiale de la propriété intellectuelle et les Nations Unies.

L'accord a d'abord été signé en octobre 2011 par l'Australie, le Canada, le Japon, le Maroc, la Nouvelle-Zélande, Singapour, la Corée du Sud et les Etats-Unis. En 2012, le Mexique, l'Union européenne et 22 pays qui sont des Etats membres de l'Union européenne l'ont également signé. Un pays signataire (le Japon) a ratifié (formellement approuvé) l'accord, qui entre en vigueur dans les six pays qui l'ont ratifié (voir Article A.2). Toutefois, l'Union européenne s'est retirée de l'accord en juillet 2012.

A.2.2 Réseau mondial anticontrefaçon (GACG - Global Anti-Counterfeiting Network)

Le GACG est un réseau informel d'organismes nationaux et régionaux de protection et de mise en application de la loi qui ont une grande dimension internationale eu égard à leurs activités. Actuellement, 21 membres couvrent 40 pays, en plus des contacts informels directs avec d'autres associations nationales et industrielles. Il s'agit d'échanger et de partager les meilleures pratiques et des informations, et de participer aux activités communes appropriées afin de répondre aux défis liés à l'application de la loi en matière de droit de propriété intellectuelle (voir la page web <http://www.gacg.org/>).

A.3 Conseil mondial des semiconducteurs (WSC - World Semiconductor Council) et GAMS

La page web est <http://www.semiconductorcouncil.org/>, où les informations suivantes sont disponibles:

"Le Conseil mondial des semiconducteurs (WSC) est un forum international qui rassemble les leaders de l'industrie afin de répondre aux problèmes d'intérêt mondial de l'industrie des semiconducteurs. Composé des associations de l'industrie des semiconducteurs (SIA) des Etats-Unis, de la Corée, du Japon, de l'Europe, de la Chine et de Taïwan, le WSC a pour objectif de promouvoir la coopération internationale dans le secteur des semiconducteurs afin de faciliter la croissance saine du secteur d'un point de vue mondial et à long terme.

Il favorise également le développement du marché mondial des produits et services liés aux technologies informatiques, en appelant à la concurrence loyale, aux avancées technologiques et aux bonnes pratiques en matière d'environnement, de santé et de sécurité.

Les activités du WSC doivent être réalisées sur la base du volontariat et doivent être guidées par les principes de loyauté, de respect des principes du marché et de conformité aux règles de l'OMC et aux lois des pays ou régions respectifs de chaque Membre. Le WSC reconnaît qu'il est important de s'assurer que les marchés sont ouverts sans discrimination. Il convient que la compétitivité des compagnies et de leurs produits soit le principal facteur déterminant du succès industriel et des échanges commerciaux au niveau international."

Référence: "Agreement Establishing a New World Semiconductor Council", 10 juin 1999; Bruxelles, Belgique.

Le WSC se réunit tous les ans. Lors de la réunion du mois de mai 2017, le WSC a convenu d'intensifier les activités de lutte contre la contrefaçon par l'intermédiaire du groupe de travail anticontrefaçon. Lors de la réunion de Hangzhou (Chine) de mai 2015, le WSC a reconnu l'importance de la protection des secrets commerciaux. Les membres se sont mis d'accord sur un ensemble d'éléments "centraux" du modèle de législation relative aux secrets commerciaux et appellent les autorités gouvernementales (y compris le GAMS) à prendre en charge les éléments centraux.

Le GAMS est composé de membres des associations de l'industrie des semiconducteurs en Chine, à Taïwan, dans l'UE, au Japon, aux Etats-Unis et en Corée. La Déclaration commune est revue tous les cinq ans. La Déclaration commune permet à l'industrie de créer des rapports et de formuler des recommandations à l'attention des gouvernements concernant les politiques qui peuvent avoir un impact sur les perspectives et conditions de concurrence futures dans l'industrie mondiale des semiconducteurs, par l'intermédiaire d'un Conseil mondial des semiconducteurs (WSC) au niveau du directeur général. Les sujets abordés portent sur les questions de prévention de la contrefaçon. La réunion de 2009 a confirmé l'accord conclu entre les membres de prendre des mesures exécutoires contre la contrefaçon des semiconducteurs. L'Association européenne de l'industrie des semiconducteurs (ESIA) (voir Article A.3) est présidente du comité contre la contrefaçon. Ce comité a récemment publié un livre blanc sur les mesures de lutte contre la contrefaçon (voir 4.7.7 et Article A.3) et a exclu le marquage d'empreintes ADN des composants comme étant une technique viable d'atténuation de la contrefaçon (voir 4.5.4.4). La réunion d'octobre 2014 s'est tenue à Fukuoka, au Japon, et le GAMS poursuit sa collaboration avec le WSC pour éliminer les contrefaçons de la chaîne d'approvisionnement. Récemment, l'ESIA a saisi une grande quantité de composants contrefaits, en participant à des opérations douanières européennes et en collaborant avec 12 Etats membres de l'Union européenne en 2016.

Le groupe de travail anticontrefaçon du WSC (ACTF) travaille à éliminer les contrefaçons du marché des semiconducteurs et a publié, en mai 2014, un livre blanc intitulé "Winning the battle against counterfeit semiconductor products" (Remporter la bataille contre la contrefaçon de produits semiconducteurs).

La page web donne des liens vers les associations de l'industrie des semiconducteurs en Chine, à Taïwan, en Europe, au Japon, en Corée et aux Etats-Unis, qui sont toutes membres du Conseil mondial des semiconducteurs. La page web <http://www.semiconductorcouncil.org/about-wsc/members/> donne des informations relatives à l'appartenance au WSC.

La page web de l'association de l'industrie des semiconducteurs aux Etats-Unis, qui contient les déclarations en matière de contrefaçon, est disponible à l'adresse suivante: http://www.semiconductors.org/issues/anticounterfeiting/anti_counterfeiting/

L'Association européenne de l'industrie électronique des semiconducteurs (EECA) est présidente du comité contre la contrefaçon (voir la page web <http://www.eusemiconductors.eu/esia/home>). La page web relative aux contrefaçons est la suivante: <https://www.eusemiconductors.eu/esia/public-policy/anti-counterfeiting>

A.4 SEMI

Le siège social du SEMI se trouve au 673 South Milpitas Blvd. Milpitas, CA 95035, USA (tél: +1 408 943 6900) (voir la page web <http://www.semi.org/About/ContactUs>). Le SEMI est une association mondiale d'entreprises qui alimentent la chaîne logistique de fabrication des industries micro et nanoélectroniques, avec des bureaux présents dans le monde entier. Voir la page web <http://www.semi.org/en/About/> contenant les informations suivantes:

"Le SEMI est une association mondiale d'entreprises qui alimentent la chaîne logistique de fabrication des industries micro et nanoélectroniques, y compris:

- les semiconducteurs (les fabricants de dispositifs, les fournisseurs d'équipements, de matériaux et autres services);
- les éléments électroniques souples, hybrides et imprimés;
- les microsystèmes électromécaniques (MEMS);
- les capteurs;
- les LED à haute luminosité;
- les panneaux photovoltaïques (PV);
- les écrans plats (FPD);
- les éléments micro et nanoélectroniques connexes.

Les industries, compagnies et personnes que représente le SEMI sont les architectes de la révolution électronique. Les membres du SEMI sont responsables des innovations et des technologies permettant de créer des produits et appareils électroniques plus intelligents, plus rapides, plus puissants et plus abordables, et permettant au plus grand nombre de vivre à l'ère du numérique au quotidien.

Pendant plus de 40 ans, le SEMI a été au service de ses membres et des entreprises qu'il représente à travers des programmes, des initiatives et des actions visant à promouvoir l'activité et la croissance du marché dans le monde entier. Le SEMI soutient ses membres par le biais d'un réseau mondial de bureaux, d'activités et d'événements dans les principales régions de fabrication de produits électroniques dans le monde.

Notre objectif:

Les secteurs d'activité qui composent la chaîne d'approvisionnement microélectronique sont de plus en plus complexes, présentent une forte intensité de capital et sont interdépendants. La livraison de composants électroniques de pointe sur le marché exige:

- de construire de nouvelles installations de fabrication;
- de développer de nouveaux processus, outils et matériaux et de nouvelles normes de fabrication;
- de promouvoir l'adoption et l'application de politiques et de règlements qui encouragent la croissance de l'entreprise;
- d'investir dans des ressources organisationnelles et financières;
- de s'intégrer dans tous les segments de l'industrie dans le monde entier;
- répondre à ces besoins et relever les défis exige une action organisée et collective à l'échelle mondiale.

Le SEMI aide au développement et à la croissance de nos entreprises et de nos régions de fabrication en organisant des manifestations commerciales régionales (expositions), des missions commerciales et des conférences, en mobilisant les gouvernements et responsables politiques locaux et nationaux, en encourageant la collaboration, en menant des recherches industrielles et en consignant les données du marché, en soutenant d'autres initiatives en faveur de l'investissement, des échanges commerciaux et de l'innovation technologique.

Outre le fait de favoriser l'accès aux marchés régionaux, le SEMI aide ses membres à trouver des débouchés commerciaux diversifiés et contribue à la croissance et au développement de marchés des technologies émergents et connexes."

La page web SEMI Intellectual Property

<http://www.semi.org/en/Issues/IntellectualProperty/> donne des informations complémentaires.

De même, voir la page web

<http://ams.semi.org/ebusiness/standards/semistandard.aspx?volumeid=17> pour obtenir une liste des spécifications publiées.

A.5 Electronics Authorized Directory

L'Electronics Authorized Directory (répertoire agréé des produits électroniques) disposait d'un site web permettant de rechercher les distributeurs de composants agréés, mais cela est désormais géré par l'ECIA (voir A.8.7).

A.6 Royaume-Uni

A.6.1 Bureau de la propriété intellectuelle du Royaume-Uni

La page web interactive est la suivante: <http://www.ipo.gov.uk/>.

Ce site web contient des informations permettant de choisir le type exigé de protection de la propriété intellectuelle:

- brevets (voir la page web <https://www.gov.uk/intellectual-property/patents>), qui sont présentés avec des détails sur la manière de les appliquer et de les gérer. Des détails sont également fournis sur l'utilisation des brevets d'autres personnes et sur la contrefaçon de brevet;
- marques (voir la page web <https://www.gov.uk/intellectual-property/trade-marks>), qui sont présentées avec des détails sur la manière de les appliquer et de les gérer. Des détails sont également fournis sur les marques d'autres personnes et sur la contrefaçon de marque;
- dessins et modèles (voir la page web <https://www.gov.uk/intellectual-property/designs>), qui sont présentés avec des détails sur la manière de les appliquer et de les enregistrer;
- droits d'auteur (voir la page web <https://www.gov.uk/intellectual-property/copyright>) qui sont présentés avec les détails de la propriété et des détails sur la manière de l'appliquer légalement pour utiliser les œuvres protégées par droit d'auteur d'autres personnes.

De même, voir l'outil en ligne sur la page web www.ipo.gov.uk/iphealthcheck. Cet outil donne des informations relatives à l'utilisation de la propriété intellectuelle pour protéger l'entreprise, et répond aux questions classiques en matière de propriété intellectuelle.

L'UK Information Centre est également en mesure d'apporter son aide, tél: 0300 300 2000 au Royaume-Uni ou 44 (0)1633 814000 hors du Royaume-Uni ou par e-mail enquiries@ipo.gov.uk

A.6.2 Alliance for IP

L'Alliance for Intellectual Property (alliance pour la propriété intellectuelle) se trouve au deuxième étage du Riverside Building, County Hall, Westminster Bridge Road, Londres, SE1 7JA, tél: +44 020 7803 1319. Voir la page web <http://www.allianceforip.co.uk/>, où les informations suivantes sont disponibles:

"Créée en 1998, l'Alliance Against Intellectual Property (IP) (alliance contre le vol de propriété intellectuelle) est une coalition, domiciliée au Royaume-Uni, de 20 associations et organismes de mise en application de la loi, qui veille à ce que les droits de propriété intellectuelle disposent de la protection dont ils ont besoin et qu'ils méritent. Nos membres sont des représentants du monde de l'audiovisuel, de la musique, des jeux vidéo et des logiciels de gestion, de l'industrie du sport, des produits manufacturés de marque, des éditeurs, des auteurs, des détaillants et des concepteurs."

A.6.3 UK Chartered Trading Standards Institute

Le Chartered Trading Standards Institute (institut des normes de commercialisation) (voir la page web <http://www.tradingstandards.uk/>) dispose des informations suivantes:

"Le CTSI représente les professionnels des normes de commercialisation qui travaillent au Royaume-Uni et à l'étranger, dans les collectivités locales, dans le secteur privé et des biens de consommation, ainsi qu'au gouvernement central.

Le CTSI est là pour:

- favoriser et protéger la réussite d'une économie moderne dynamique; et
- protéger la santé, la sécurité et le bien-être des citoyens en renforçant le professionnalisme de ses membres."

A.6.4 UK HM Revenue and Customs

Le HM Revenue and Customs (administration fiscale et douanière) tient une page web: www.hmrc.gov.uk. Pour les droits de la propriété intellectuelle, voir les pages web http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageLibrary_ShowContent&id=HMCE_CL_000244&propertyType=document et <https://www.gov.uk/fraud-and-international-trade>.

Les moyens suivants permettent de signaler une fraude, y compris les contrefaçons:

- assistance téléphonique au Royaume-Uni: 0800 788 887;
- page web: <https://www.gov.uk/government/news/hmrc-launches-new-fraud-hotline>; ou
- formulaire numérique en ligne sur la page web <https://www.gov.uk/report-an-unregistered-trader-or-business>.

A.6.5 Anti-Counterfeiting Forum

L'ESCO Anti-Counterfeiting Forum (Forum de lutte contre la contrefaçon ESCO) est désormais l'Anti-counterfeiting Forum (voir la page web <http://www.anticounterfeitingforum.org.uk/counterfeiting.aspx>) et donne des recommandations quant à la manière d'éviter les composants contrefaits.

Les contrefaçons suspectes peuvent être signalées sur cette page web, accessible à tous les membres. Cette page web donne le numéro de téléphone de l'assistance au Royaume-Uni pour signaler les contrefaçons: 0800 788 887

A.6.6 Electronic Component Supplier Network (ESCN)

L'Electronic Component Supplier Network (réseau de fournisseurs de composants électroniques) (voir la page web <http://www.ecsn-uk.org/>) est une association commerciale à but non lucratif gérée par ses membres, domiciliée au Royaume-Uni, et qui soutient des mesures permettant d'éviter les contrefaçons.

A.6.7 Ministère de la Défense britannique

Des recommandations à l'intention des équipes de livraison du Ministère de la Défense concernant les moyens permettant d'éviter les produits frauduleux et de contrefaçon sont disponibles sur la page web interactive:

https://www.aof.mod.uk/aofcontent/tactical/quality/content/counterfeitavoid/counterfeit.htm?zoom_highlight=Counterfeit.

NOTE L'enregistrement (en tant que "civil" dans le "cadre opérationnel d'acquisition" (AOF – Acquisition Operating Framework)) est nécessaire pour accéder au site web.