IEC 62668-1

Edition 1.1 2024-09
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 62668-1:2019-09+AMD1:2024-09 CSV(en)

IEC Secretariat
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC 62668-1

Edition 1.1 2024-09
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 03.100.50, 31.020, 49.060

ISBN 978-2-8322-9708-7

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

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) IEC [draws/draw] attention to the possibility that the implementation of this document may involve the use of (a) patents(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch . IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62668-1 edition 1.1 contains the first edition (2019-09) [documents 107/335/CDV and 107/346A/RVC] and its amendment 1 (2024-09) [documents 107/416/FDIS and 107/421/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

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.

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 and its amendment will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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 (remarking 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.erai.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
IECQ	IEC quality assessment systems for electronic components
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~~ SAE AS5553D 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.

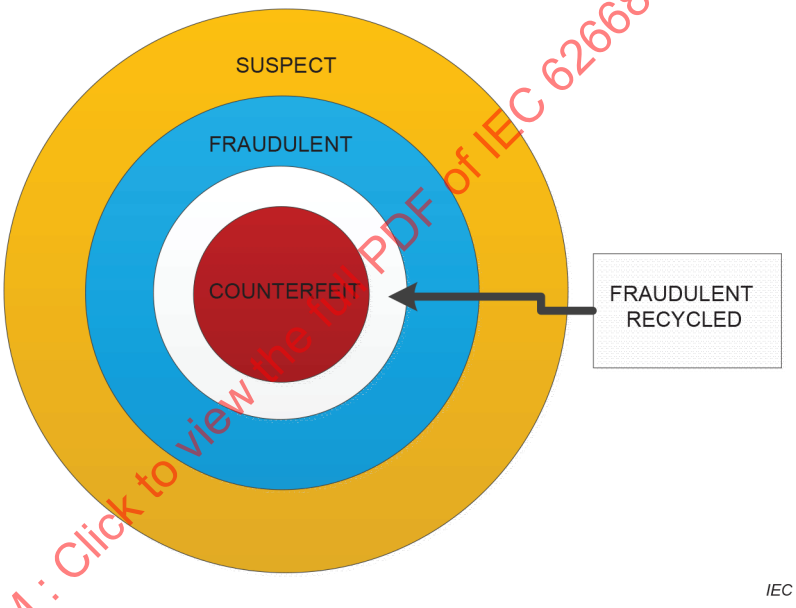


Figure 1 – Suspect components perimeter

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 (see Figure 2).

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.

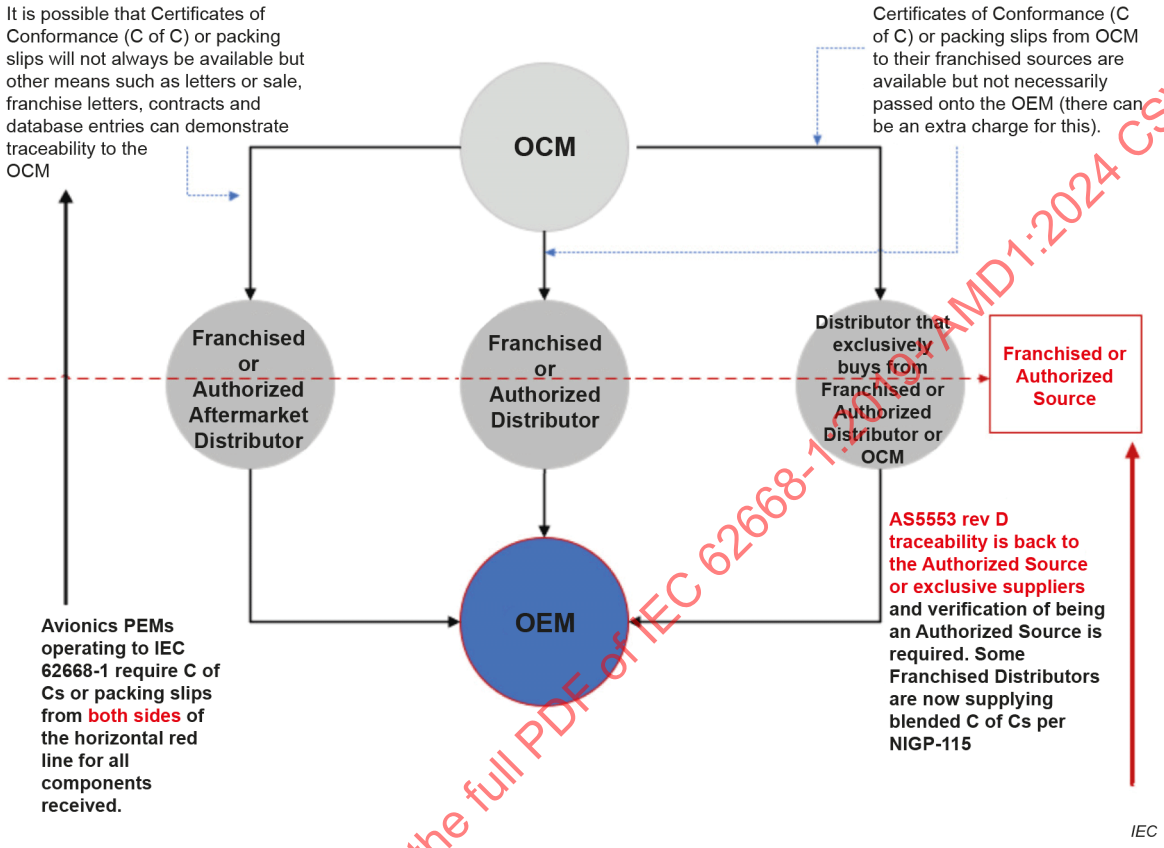


Figure 2 – Typical IEC 62668-1 and SAE AS5553 traceability requirements approach

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.

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.

1 Numbers in square brackets refer to the Bibliography.

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 tamper proof 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~~ AS5553 anti-counterfeit plan for electronic components may consider it in their IEC 62668-1 anti-counterfeit plans; ~~Table 2 and Table 3 identify~~ Table 3 identifies the IEC 62668-1 requirements which can be satisfied or not~~, respectively,~~ by SAE ~~AS5553A or AS5553B~~ AS5553D requirements.

SAE AS5553, currently at revision ~~B~~ D, ~~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~~16 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.~~ SAE AS5553D has traceability requirements which can be different from IEC 62668-1 requirements (see Figure 2), leading Table 3 to not be satisfactory without additional steps. 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.		

Table 3 – IEC 62668-1 requirements satisfied or not if OEM has an approved SAE ~~AS5553B~~ AS5553D 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 OCMs 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.~~	

IEC 62668-1 requirement	Satisfied by SAE AS5553D requirement See Note 1	Comments	Notes for avionics OEMs when writing an SAE AS5553D plan as a basis for an IEC 62668-1 plan
4.2 a)	No.		
4.2 b)	No.	SAE AS5553D 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 AS5553D plan only satisfies how individual components are purchased and brought into an OEM or MRO business with traceability back to the "authorized source or exclusive supplier" as well as requiring verification of that authorization by the OCM. The IEC 62668-1 process or 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 with traceability back to the OCM.	IEC 62668-1 requires that the organization has anti-counterfeit procedures for all requirements. These procedures can include an anti-counterfeit plan.	Issue a cross reference matrix based on Table 3 to show how the SAE AS5553D plan satisfies the IEC 62668-1 requirements. Manage traceability back to the OCM and not just the AS5553D "authorised source or exclusive supplier"
4.2 d)	No – not unless AS/EN/JISQ 9100 is invoked.	SAE AS5553D is written for both general industry and high reliability industries where the use of AS/EN/JISQ 9100 is optional.	Base your SAE AS5553D plan on your AS/EN/JISQ 9100 procedures.

IEC 62668-1 requirement	Satisfied by SAE AS5553D requirement See Note 1	Comments	Notes for avionics OEMs when writing an SAE AS5553D plan as a basis for an IEC 62668-1 plan
4.2 e)	Partially.		Base your SAE AS5553D plan on traceability through the supply chain back to the OCM and not just the "authorized source or exclusive supplier".
4.2 e) 1)	Partially.		Base your SAE AS5553D plan on traceability through the supply chain.
4.2e) 2)	Optional requirement depending on customer contract. No.	SAE AS5553D does not acknowledge this optional contract requirement using USA trusted sources.	Allow your SAE AS5553D plan to be customised using USA trusted suppliers where required by contract if you have USA customers.
4.2 e) 3)	Partially.		Base your SAE AS5553D plan on using franchised aftermarket sources when the part is obsolete with traceability through the supply chain to the OCM and not just the authorized source.
4.2 e) 4)	Partially.	IEC 62668-1 requires all franchised distributors to comply with SAE AS6496 (AS 5553D only refers to AS6496 in a note for guidance). IEC 62668-1 refers to IEC 62668-2 for non-franchised distributor purchases whereas AS5553D refers to ARP 6328.	Use franchised distributors that comply with AS6496. Use IEC 62668-2 for non-franchised distributors purchases Base your SAE AS5553D plan on traceability through the supply chain to the OCM and not just the authorized source or exclusive supplier.
4.2 f)	Yes.		
4.2 g) 1)	Partially.	SAE AS5553D 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.
4.2 g) 2)	Partially.	IEC 62668-1 refers to IEC 62668-2 for a risk assessment process. SAE AS5553D minimum requirements do not refer to IEC 62668-2 but refer to similar testing 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 to AS/EN/JISQ9120.
4.2 h)	Yes.	SAE AS5553D also applies to MRO organizations.	
4.2 i)	Yes.		
4.2 j)	Yes.		
4.2 k)	Partially.	An AS/EN/JISQ9100 Quality Management System can provide this assurance better than ISO 9001.	Base your anti-counterfeit plan on AS/EN/JISQ 9100.
4.2 l)	Yes.		

IEC 62668-1 requirement	Satisfied by SAE AS5553D requirement See Note 1	Comments	Notes for avionics OEMs when writing an SAE AS5553D plan as a basis for an IEC 62668-1 plan
4.2.m)	Yes.	SAE AS5553D is written for both general industry and high reliability industries where the use of AS/EN/JISQ 9110 is optional.	Base your anti-counterfeit plan on AS/EN/JISQ9110 with traceability back to the OCM.
NOTE 1 SAE AS5553D defines "authorized sourced" as: "AUTHORIZED SOURCE: Original component manufacturers and OCM-authorized sources of supply for an EEE part (i.e., franchised distributors, authorized distributors), and authorized aftermarket manufacturers" NOTE 2 The SAE AS5553D defines "exclusive supplier" as: "EXCLUSIVE SUPPLIER: Supplier who provides EEE parts it obtains directly from Authorized Sources but the Exclusive Supplier may not itself be authorized for those parts. "			

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 (0-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.13). 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.

Annex A
(informative)

Useful contacts[2]

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 Mocscow 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 (**R**ead-**O**nly-**M**emory of **M**adrid **A**ctive **R**egistry 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, expediated 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 6*ter* (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 though 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 (USPTP) 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 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.chinatrademarkoffice.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 Dongsi 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.chinatrademarkoffice.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 AS5553B**[3], 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 AS5553D**[4], *Counterfeit Electrical, Electronic and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation and Disposition*

  The scope is as follows:

  This standard is for use by organisations that procure and integrate EEE parts. These organisations may provide EEE parts that are not integrated into assemblies (e.g. pares and/or repair EEE parts. Examples of such organisations include but are not limited to: original equipment manufacturers; contract assembly manufacturers; maintenance, repair, and overhaul organisations; value-added resellers; and suppliers that provide EEE parts or assemblies as part of a service. The requirements of this standard are generic. These requirements are intended to be applied (or flowed down as applicable) through the supply chain to all organisations that procure EEE arts and/or systems, subsystems, 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 criticality of the application, desired performance and reliability of the equipment/hardware.

  The requirements of this document are intended to be used in conjunction with a higher-level quality standard (e.g. AS/EN/JISQ9100, ISO-9001, ANSI/ASQC E4, ASME NQA-1, AS9120, AS9003 or equivalent) and other quality management systems 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 authorised exemption/variance has been obtained. This document is not intended to make legal determination of fraud and appropriate legal counsel should be consulted for further action.

- **SAE AS6081**[5], 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

---

~~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 AS5553D ©2022 SAE International.

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

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 AS6171**[6], 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, 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;

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

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) for electromechanical parts, 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 6178**[7], 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 AS6174A**[8], 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.

---

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

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

- **SAE AS6496**[9], 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 AIR6273**[10] ~~**(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.~~

  The SAE Aerospace Information Report (AIR) provides standardized terms, definitions, and acronyms that may be used in the G-19 and G-21 documents, unless otherwise specified in those documents. The SAE International series of documents that address the mitigation of suspect and counterfeit parts will reference this document in their respective Applicable Documents sections.

  This AIR is for use by organizations that procure and/or use materiel or EEE parts. The terms and definitions of this AIR are intended to be used in conjunction with other G-19 and G-21 standards.

- **SAE AS6301**[11], 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; 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**[12] , 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**[13], 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.~~

---

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

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

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

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

~~13 Reprinted with permission from the published version of SAE document AS6462 ©2018 SAE International.~~

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:xzeadub0b0a&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).

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 DON[14] 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);
- 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=4ZIwOoaCPxI "Combatting the Counterfeit Drug Trade: Ashifi Gogo at TEDxBoston"

[14] DON : Department of Navy

Annex B
(informative)

Examples of aftermarket sources[15]

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.

15 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.

Annex C
(informative)

Typical example of a RECS certificate[16]

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

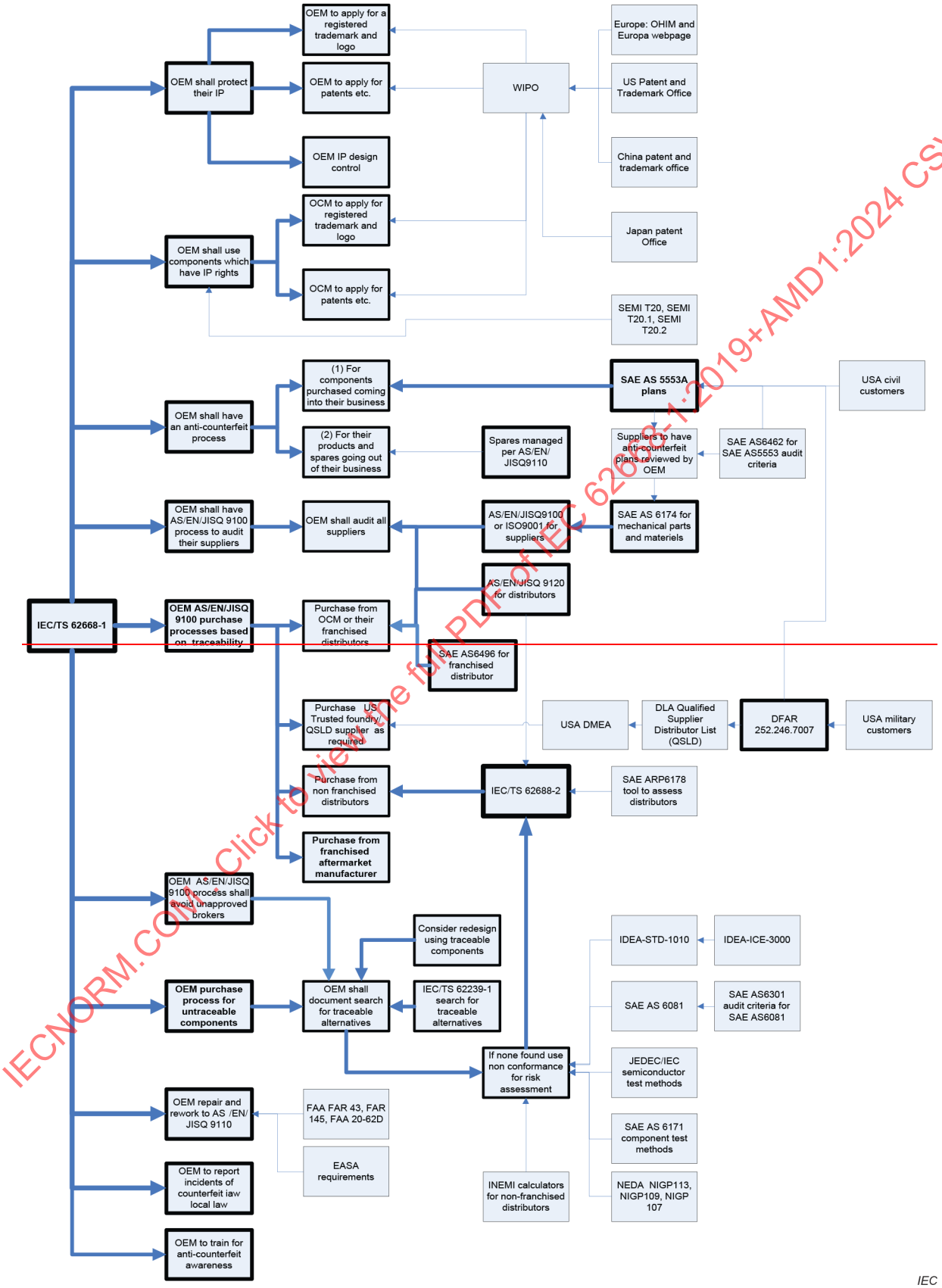
IEC

16 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

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



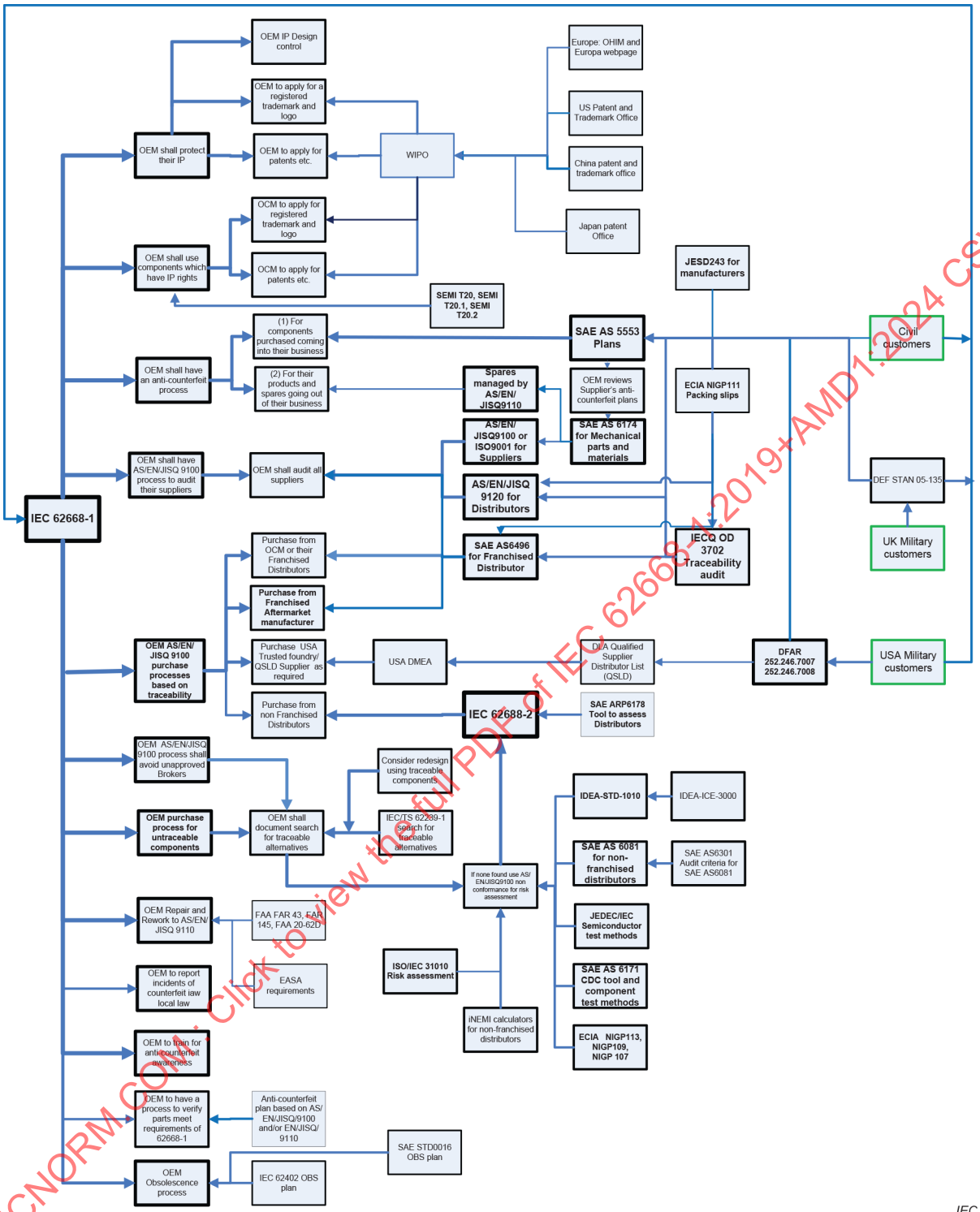


Figure D.1 – Flowchart of IEC 62668-1 requirements and their relationship to external standards

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.

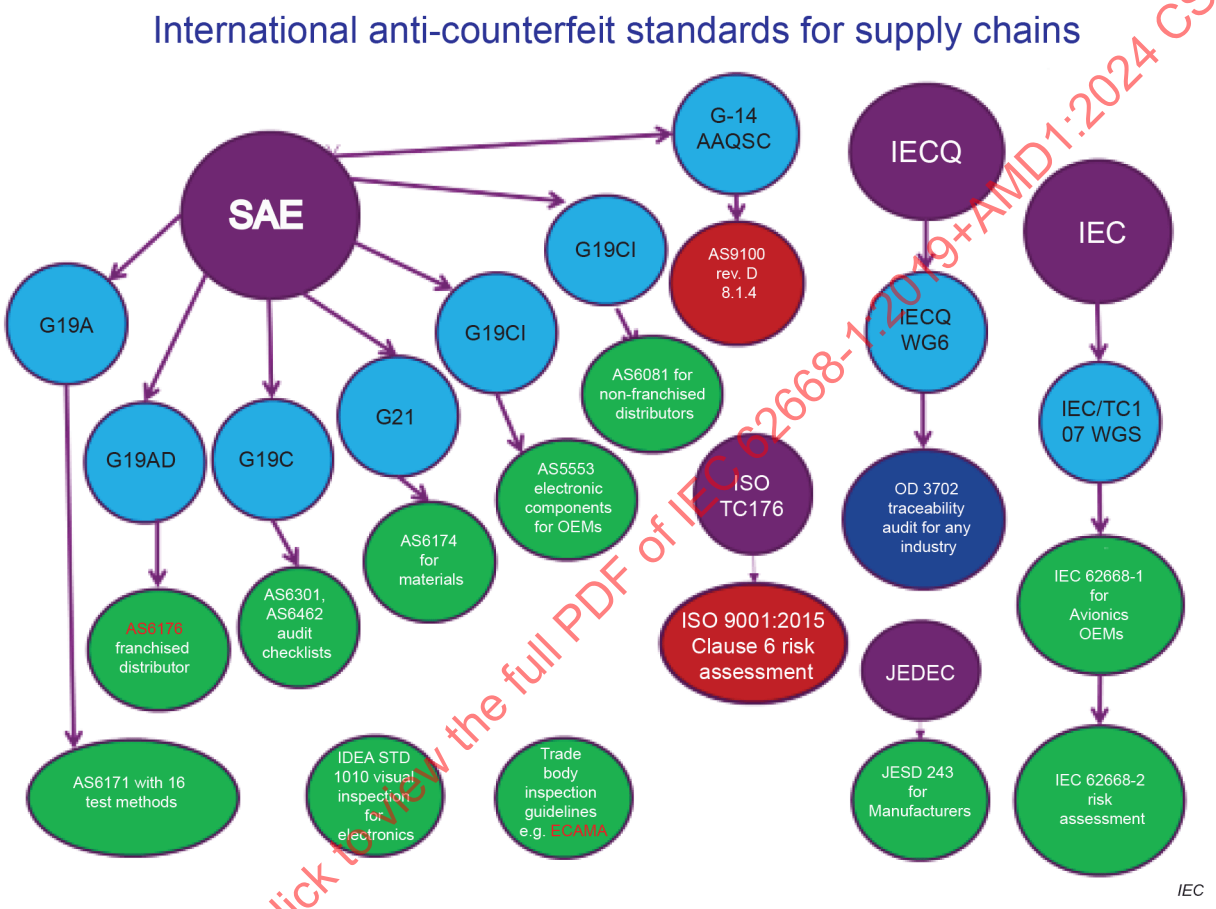


Figure E.1 – Available anti-counterfeit standards for supply chains

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 material. 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*~~ *Counterfeit Electronics Parts 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~~ Test Laboratory Standards Development Committee
    i) 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~~

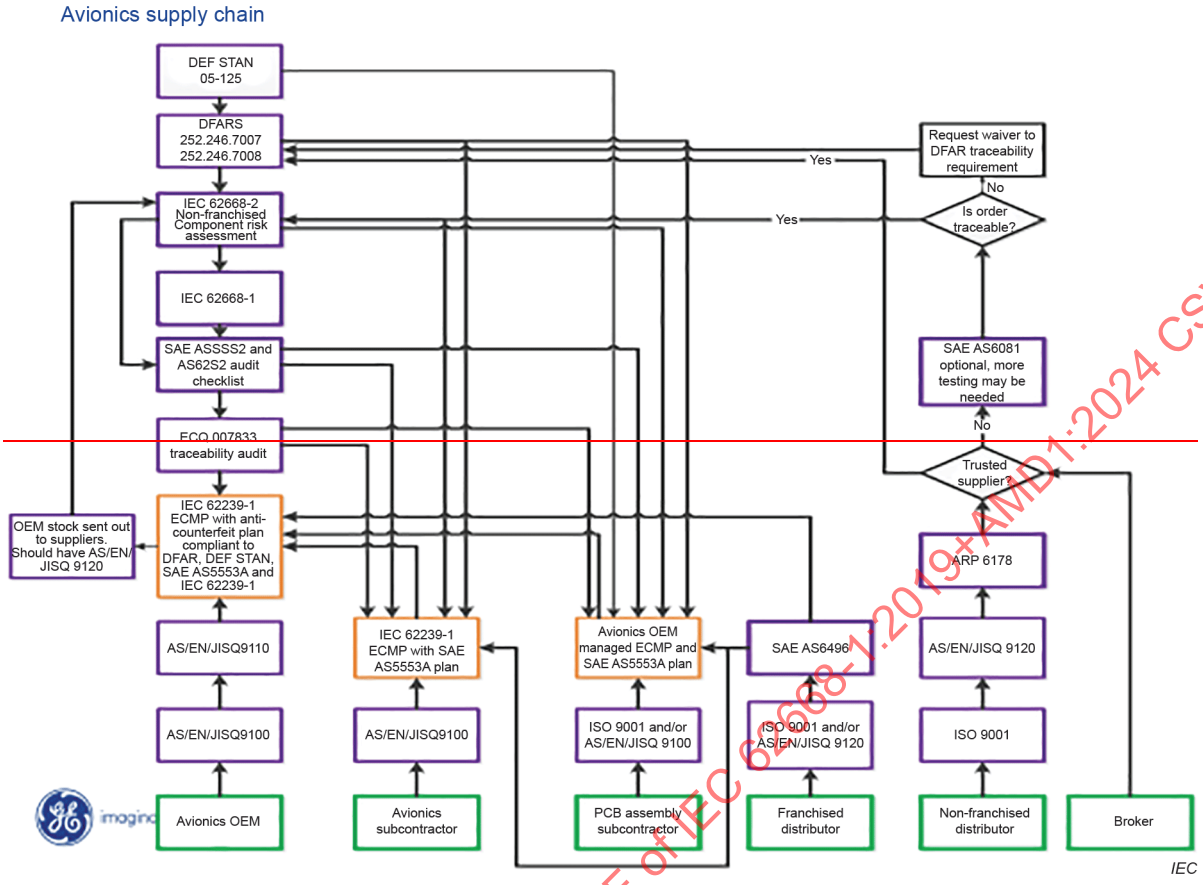
  For additional information on this SAE Technical Standards Committee, please visit:
  ~~http://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG19~~
  https://standardsworks.sae.org/standards-committees/g-19-counterfeit-electronic-parts-committee

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.



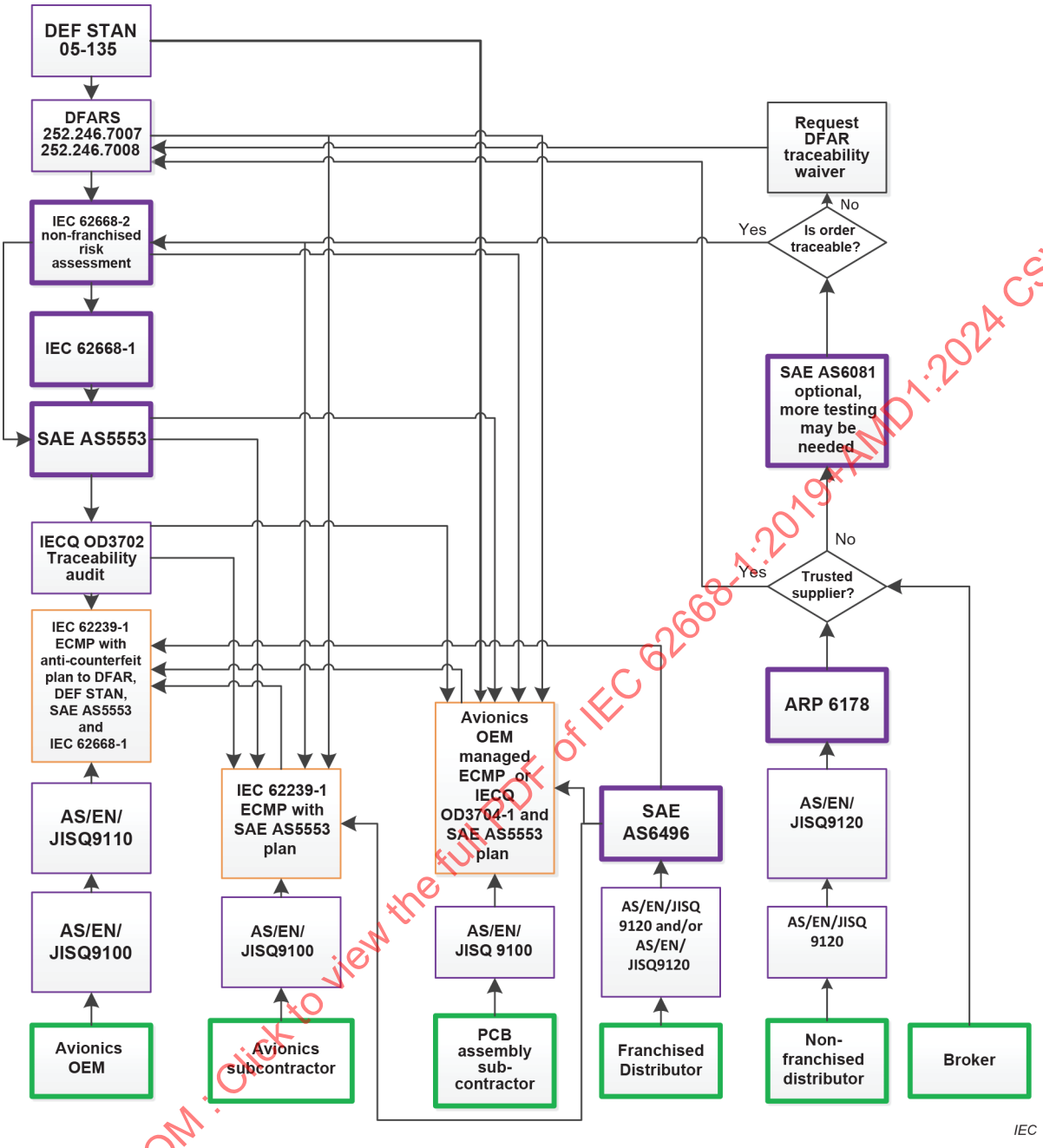


Figure E.2 – Overview of typical relationships for anti-counterfeit standards in an avionics supply chain

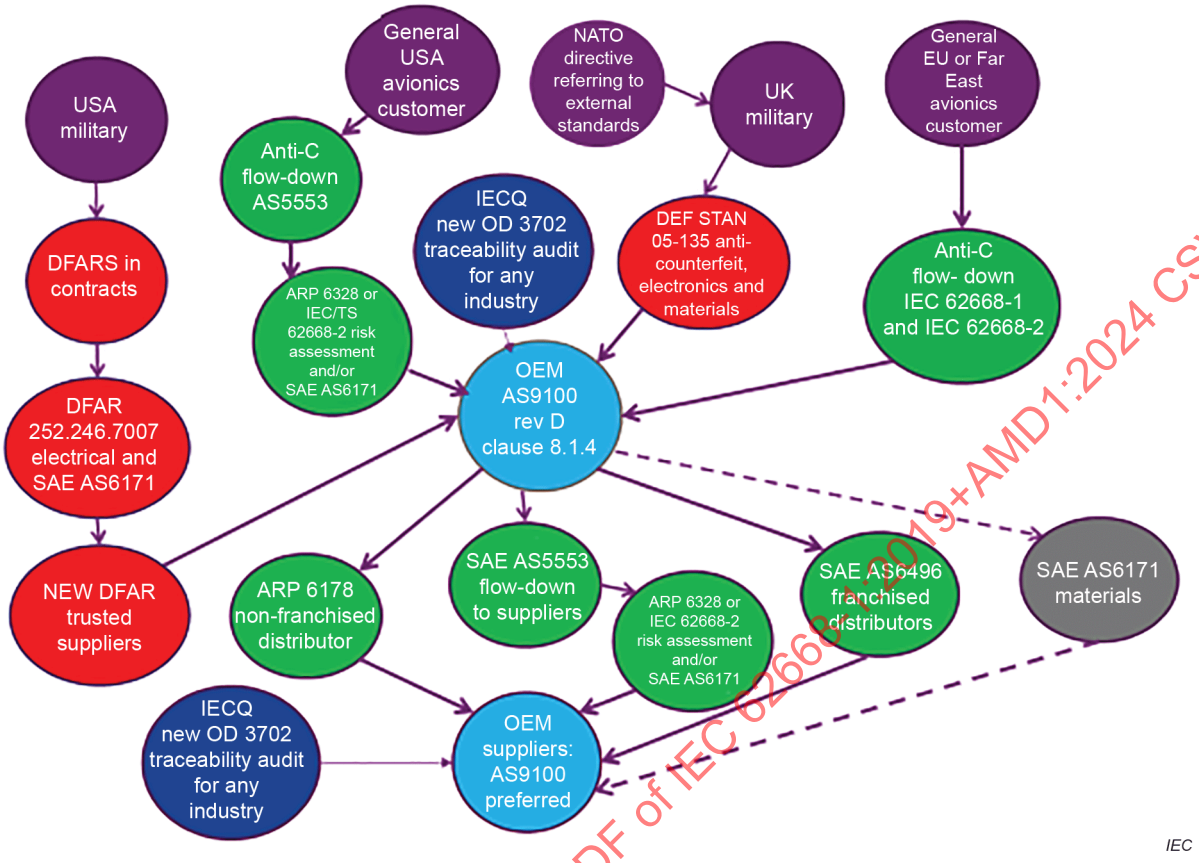


Figure E.3 – Overview of typical anti-counterfeit standards in an avionics OEM supply chain

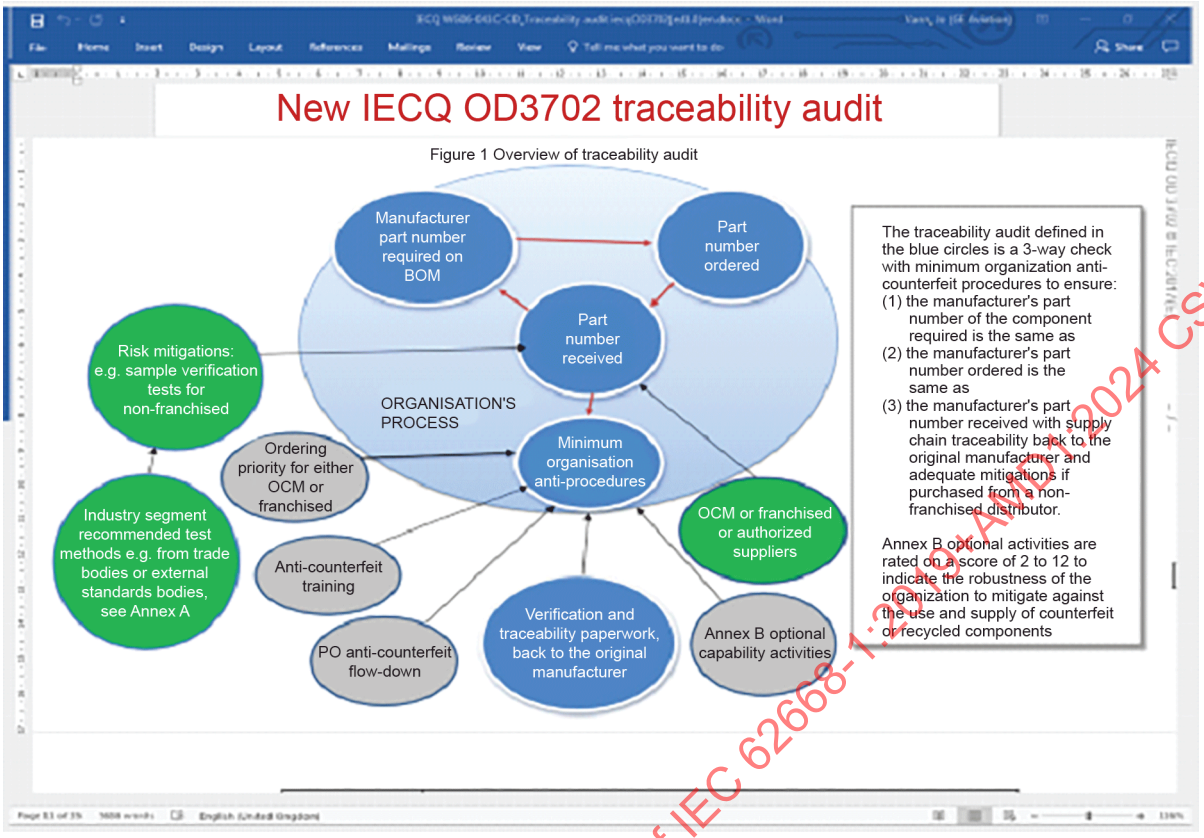


Figure E.4 – IECQ OD 3702 traceability audit

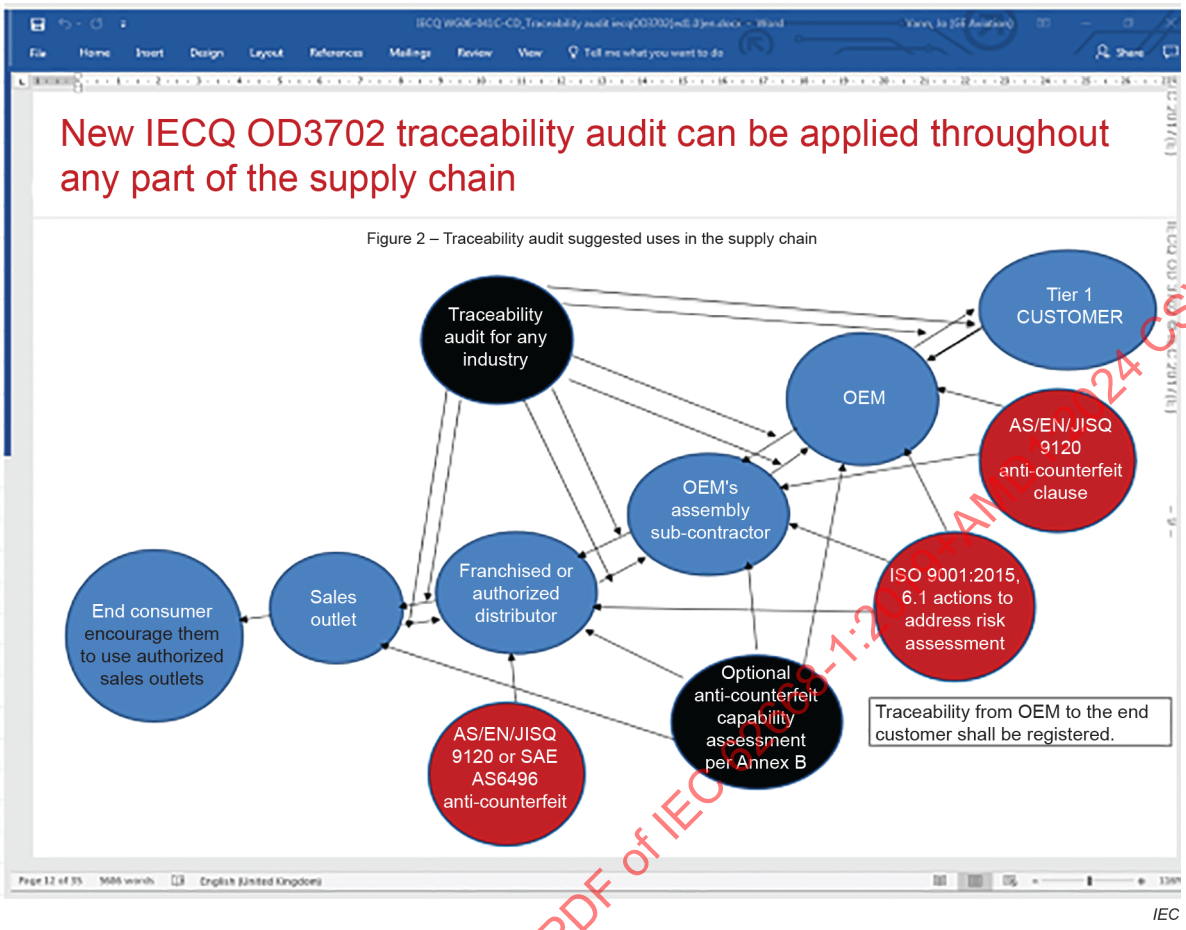


Figure E.5 – Typical IECQ OD 3702 coverage in any supply chain

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 ProviderTM 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 RiskGIFAS 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 AIR6273[17], *Terms and Definitions – Fraudulent/Counterfeit Electronic Parts*

SAE ARP 6178[18], *Fraudulent/Counterfeit Electronic – Parts: Tool for Risk Assessment of Distributors*

SAE ARP 6328[19], *Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems*

~~SAE AS5553A[20], *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition*~~

SAE AS5553[21], *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition*

SAE AS6081[22], *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition – Distributors Counterfeit Electronic parts; Avoidance Protocol, Distributors*

SAE AS6171[23], *Test Methods Standard: Counterfeit Electronic Parts*

SAE AS6174[24], *Counterfeit Material: Detection, Mitigation and Disposition*

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

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

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

~~20 Reprinted with permission from the published version of SAE document AS5553 (c) 2018 SAE international.~~

21 Reprinted with permission from the published version of SAE document AS5553 (c) 2022 SAE international.

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

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

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

SAE AS6301[25], *Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors*

~~SAE AS6462[26], *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria*~~

SAE AS6496[27], *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution*

SAE STD-0016[28], *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 Compinents 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*

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

~~26 Reprinted with permission from the published version of SAE document AS6462 (c) 2018 SAE International.~~

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

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

CONTENTS

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) IEC [draws/draw] attention to the possibility that the implementation of this document may involve the use of (a) patents(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch . IEC shall not be held responsible for identifying any or all such patent rights.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62668-1 edition 1.1 contains the first edition (2019-09) [documents 107/335/CDV and 107/346A/RVC] and its amendment 1 (2024-09) [documents 107/416/FDIS and 107/421/RVD].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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.

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 and its amendment will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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 (remarking 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.erai.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
IECQ	IEC quality assessment systems for electronic components
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 AS5553D 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.

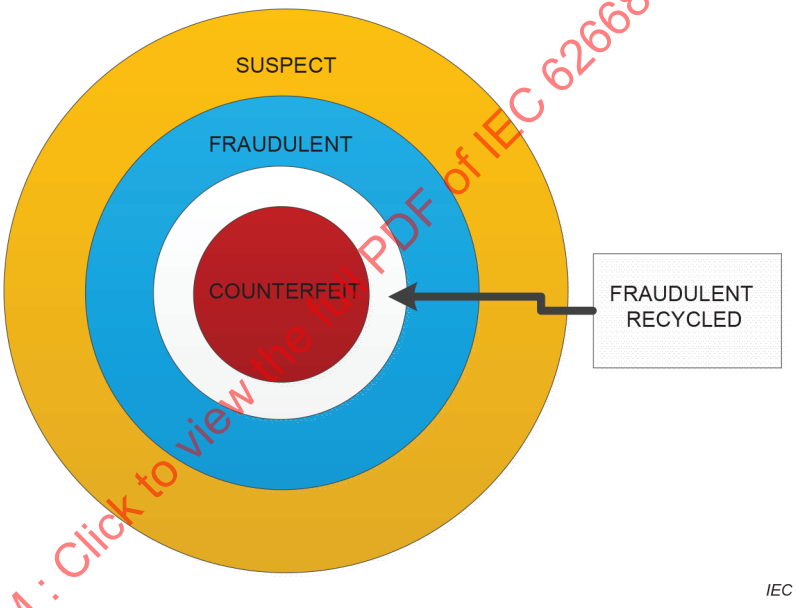


Figure 1 – Suspect components perimeter

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 (see Figure 2).

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.

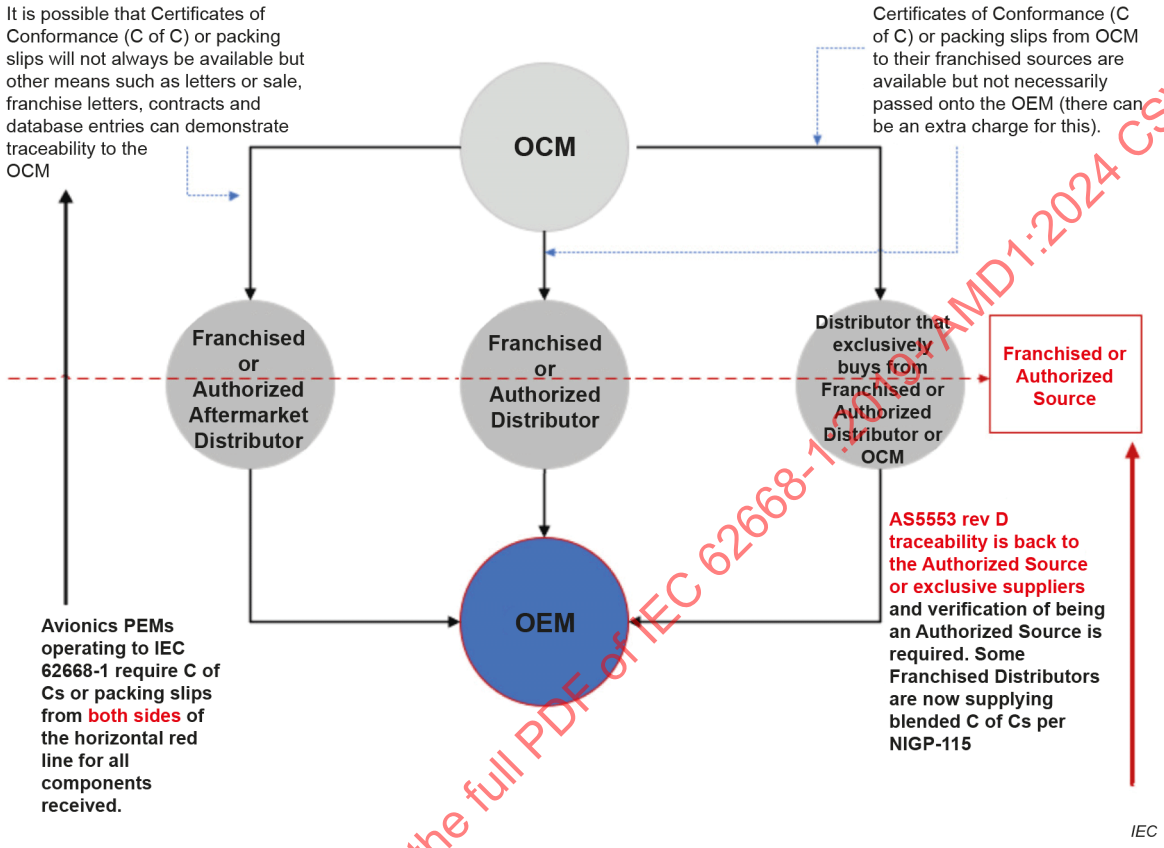


Figure 2 – Typical IEC 62668-1 and SAE AS5553 traceability requirements approach

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.

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.

1 Numbers in square brackets refer to the Bibliography.

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 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 tamper proof 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 AS5553 anti-counterfeit plan for electronic components may consider it in their IEC 62668-1 anti-counterfeit plans; Table 3 identifies the IEC 62668-1 requirements which can be satisfied or not by SAE AS5553D requirements.

SAE AS5553, currently at revision D, is a very comprehensive document targeted at the general and high reliability industry (see Clause A.16 for further information).

SAE AS5553D has traceability requirements which can be different from IEC 62668-1 requirements (see Figure 2), leading Table 3 to not be satisfactory without additional steps. 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 3 – IEC 62668-1 requirements satisfied or not if OEM has an approved SAE AS5553D plan

IEC 62668-1 requirement	Satisfied by SAE AS5553D requirement See Note 1	Comments	Notes for avionics OEMs when writing an SAE AS5553D plan as a basis for an IEC 62668-1 plan
4.2 a)	No.		
4.2 b)	No.	SAE AS5553D 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 AS5553D plan only satisfies how individual components are purchased and brought into an OEM or MRO business with traceability back to the "authorized source or exclusive supplier" as well as requiring verification of that authorization by the OCM. The IEC 62668-1 process or 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 with traceability back to the OCM.	IEC 62668-1 requires that the organization has anti-counterfeit procedures for all requirements. These procedures can include an anti-counterfeit plan.	Issue a cross reference matrix based on Table 3 to show how the SAE AS5553D plan satisfies the IEC 62668-1 requirements. Manage traceability back to the OCM and not just the AS5553D "authorised source or exclusive supplier"
4.2 d)	No – not unless AS/EN/JISQ 9100 is invoked.	SAE AS5553D is written for both general industry and high reliability industries where the use of AS/EN/JISQ 9100 is optional.	Base your SAE AS5553D plan on your AS/EN/JISQ 9100 procedures.
4.2 e)	Partially.		Base your SAE AS5553D plan on traceability through the supply chain back to the OCM and not just the "authorized source or exclusive supplier".
4.2 e) 1)	Partially.		Base your SAE AS5553D plan on traceability through the supply chain.
4.2e) 2)	Optional requirement depending on customer contract. No.	SAE AS5553D does not acknowledge this optional contract requirement using USA trusted sources.	Allow your SAE AS5553D plan to be customised using USA trusted suppliers where required by contract if you have USA customers.
4.2 e) 3)	Partially.		Base your SAE AS5553D plan on using franchised aftermarket sources when the part is obsolete with traceability through the supply chain to the OCM and not just the authorized source.

IEC 62668-1 requirement	Satisfied by SAE AS5553D requirement See Note 1	Comments	Notes for avionics OEMs when writing an SAE AS5553D plan as a basis for an IEC 62668-1 plan
4.2 e) 4)	Partially.	IEC 62668-1 requires all franchised distributors to comply with SAE AS6496 (AS 5553D only refers to AS6496 in a note for guidance). IEC 62668-1 refers to IEC 62668-2 for non-franchised distributor purchases whereas AS5553D refers to ARP 6328.	Use franchised distributors that comply with AS6496. Use IEC 62668-2 for non-franchised distributors purchases Base your SAE AS5553D plan on traceability through the supply chain to the OCM and not just the authorized source or exclusive supplier.
4.2 f)	Yes.		
4.2 g) 1)	Partially.	SAE AS5553D 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.
4.2 g) 2)	Partially.	IEC 62668-1 refers to IEC 62668-2 for a risk assessment process. SAE AS5553D minimum requirements do not refer to IEC 62668-2 but refer to similar testing 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 to AS/EN/JISQ9120.
4.2 h)	Yes.	SAE AS5553D also applies to MRO organizations.	
4.2 i)	Yes.		
4.2 j)	Yes.		
4.2 k)	Partially.	An AS/EN/JISQ9100 Quality Management System can provide this assurance better than ISO 9001.	Base your anti-counterfeit plan on AS/EN/JISQ 9100.
4.2 l)	Yes.		
4.2.m)	Yes.	SAE AS5553D is written for both general industry and high reliability industries where the use of AS/EN/JISQ 9110 is optional.	Base your anti-counterfeit plan on AS/EN/JISQ9110 with traceability back to the OCM.
NOTE 1 SAE AS5553D defines "authorized sourced" as: "AUTHORIZED SOURCE: Original component manufacturers and OCM-authorized sources of supply for an EEE part (i.e., franchised distributors, authorized distributors), and authorized aftermarket manufacturers" NOTE 2 The SAE AS5553D defines "exclusive supplier" as: "EXCLUSIVE SUPPLIER: Supplier who provides EEE parts it obtains directly from Authorized Sources but the Exclusive Supplier may not itself be authorized for those parts. "			

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 (0-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.

Annex A
(informative)

Useful contacts[2]

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 Mocscow 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 (**R**ead-**O**nly-**M**emory of **M**adrid **A**ctive **R**egistry 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, expediated 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 6*ter* (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 though 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.