IEC TS 62668-1

Edition 2.0 2014-07

TECHNICAL SPECIFICATION

colour inside

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

IEC TS 62668-1:2014-07(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

IEC TS 62668-1

Edition 2.0 2014-07

TECHNICAL SPECIFICATION

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XB

ICS 03.100.50; 31.020; 49.060

ISBN 978-2-8322-1679-8

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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC/TS 62668-1, which is a technical specification, has been prepared by IEC technical committee 107: Process management for avionics.

This second edition cancels and replaces the first edition, published in 2012. This edition constitutes a technical revision.

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

a) Update of “fraudulent component” definition, addition of “recycled component” and “suspect component” definitions, and updates of the concerned clauses accordingly.
b) Addition of counterfeit awareness training as a requirement.
c) Revision to update all references and web links in the annexes.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
107/226/DTS	107/235/RVC

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

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

A list of all the 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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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, which is a Technical Specification, 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/TS 62668-2. Although developed for the avionics industry, this specification may be applied by other high performance and high reliability industries at their discretion.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC/PAS 62435, *Electronic components – Long-duration storage of electronic components – Guidance for implementation*

IEC/TS 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 9110:2003, *Quality Maintenance Systems – Aerospace – Requirements for Maintenance Organizations*

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

GEIA-STD-0016, *Standard for Preparing a DMSMS Management Plan*

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

SAE AS5553A *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition*

SAE AS6081 *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition – Distributors Verification Criteria*

SAE AS6174, *Counterfeit Material: Detection, Mitigation and Disposition*[1]

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

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
commercial off-the-shelf products
one or more pieces, mechanical or electrical, developed for multiple commercial consumers, whose design and/or configuration is controlled by the supplier's specification or industry standard

Note 1 to entry: They can include electronic components, subassemblies, or top level assemblies. COTS subassemblies 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.

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.

---

1 Although published this is being revised for material component only.

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 technical specification, 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 organisation 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 direct 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 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
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.

3.1.12
non-franchised distributor
companies which do 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. However, some of them are able to purchase traceable components and/or to provide traceability paperwork and/or are able to return stock for investigation to the OCM.

3.1.13
OCM
original component manufacturer
company specifying and manufacturing the electronic component

3.1.14
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

3.1.15
piracy
willful copyright infringement

3.1.16
reseller
general supplier which offers a selection of electronic components to order from a catalog

3.1.17
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 or ESD damaged during the removal process.

3.1.18
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.

3.1.19
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).

3.1.20
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.

3.1.21
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.

3.1.22
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 datasheet, exhibiting the expected component life in the application for the OEM's reliability predictions and product warranty.

3.1.23
untraceable
property of electronic components which have lost their traceability (see 3.1.22)

3.2 Abbreviations

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
CATA	China Anti-counterfeit Technology Association
CB	Certifying Bodies (Third Party)
COTS	commercial off-the-shelf
CEM	contract electronic manufacturer
CEPA	Chinese Electronic Purchasing Association
CQAE	China Quality Management Association for Electronics Industry
CMOS	complementary metal oxide semiconductor
DFAR	Defense Federal Acquisition Regulation
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
EOS	electrical overstress
EU	European Union
FAA	Federal Aviation Administration
FAR	Federal Avionic Regulations
FFF	form, fit and function
FIT	failures in time
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
ID	independent distributors
IDEA	Independent Distributors of Electronics Association
IAQG	International Aerospace Quality Group – SAE
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
JIT	just in time
JPO	Japanese Patent Office
LTB	last time buy
LDC	lot date code
MBTF	mean time between failures
MOD	Ministry of Defence, UK
MTTF	mean time to failure

MSL	moisture sensitivity level
NDAA	National Defense Acquisition Act
NEDA	National Electronics Distributors Association
NOVRAM	non-volatile random access memory
OCM	original component manufacturer
OEM	original equipment manufacturer
OHIM	Office for Harmonisation in the Internal Market (EU)
PCB	printed circuit board
PCN	product change notice
PRC	People's Republic of China
RECS	Reliable Electronic Component Suppler
PUF	physical unclonable function
RFID	radio frequency identity detection
RAM	random access memory
ROM	read only memory
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 technical specification 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.

Subclauses 4.3 to 4.14.6 provide supporting information to 4.2.

Informative annexes are provided at the end of this specification and their content is subject to change. Users of this specification 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 organisations 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 and A.9.3);
- Annex D provides a flowchart of IEC/TS 62668-1 requirements and their relationship to external standards.

The key elements to control and understand are:

a) the definition of intellectual property (see 4.3);

b) the limitations of the term counterfeit (see 4.4);

c) the better term fraudulent (see 4.4.3);

d) what recycling is and why the avionics industry minimises recycling to in-house activities only (see 4.6);

e) the use of original component manufacturers (OCMs) which protect their intellectual property (see 4.7);

f) the use of approved franchised distributors or sources (see 4.10);

g) the use of risk management and component test processes when buying suspect untraceable components from non-franchised distributors in accordance with IEC/TS 62668-2 (see 4.12.6);

h) the protection of OEM intellectual property, throughout their product lifecycles including management of all spares;

i) the reporting of violations of intellectual property through local law enforcement (see 4.14, A.7.2, A.8 for useful contacts).

4.2 Minimum avionics OEM requirements

The avionics OEM 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).

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 specification which can be based on plans such as SAE-AS5553A or others similar (see 4.12.13) and shall flow this requirement down to lower level suppliers (see 4.12.13.3).

d) Have an AS/EN/JISQ 9100 process (see 4.12) to audit all sources of supply of components.

e) Have a process only allowing the purchase of traceable components (see 4.12.3) using the AS/EN/JISQ 9100 procedures, from:

   1) Reliable Electronic Component Supplier (RECS) approved original component manufacturers (OCM) (see 4.7.2) and franchised distributors (see 4.10) where the RECS scheme operates, e.g. China and the Far East. See Annex C for a typical RECS certificate.

   2) Where the RECS scheme does not operate, purchase traceable components:

      i) direct 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), as considered necessary;

      ii) direct from 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;

      iii) in situations where the component is obsolete, purchase direct from the franchised aftermarket manufacturer (see 4.12.9 and Annex B);

      iv) from franchised distributors (see 4.10)

– which are preferably AS/EN/JISQ 9120 approved (see 4.9);

– which are also ISO9001 approved as a minimum requirement (see 4.8);

v) from non-franchised distributors (see 4.11) using IEC/TS 62668-2.

f) Have an AS/EN/JISQ 9100 process which avoids the use of unapproved brokers (see 4.11.5).

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

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/TS 62668-2. This risk management process will include conformity, quality, reliability and maintenance performances aspects.

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).

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. In the case of newly hired personnel, initiate immediate training for the specific discipline or department.

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.	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.	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 Healthcheck 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:

a) 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.

b) 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).

c) The International Trade Administration, U.S. Department of Commerce Stopfakes webpage (see A.8.2) has links to Intellectual Property Toolkits for other countries.

d) 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) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. This is property created through intellectual or creative activity. It includes patents, trademarks, copyright and designs. It can be owned, rented out, licensed, sold or given away.

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:

a) WIPO (see A.1.3); or

b) the European Patent Office (see A.7.3.);

c) the Chinese Patent and Trademark Office (see A.9.2);

d) the Japanese Patent Office (see A.10.1).

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.

These 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
- OHIM 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 b)).

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 OHIM (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/WD 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 3.1.21 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.

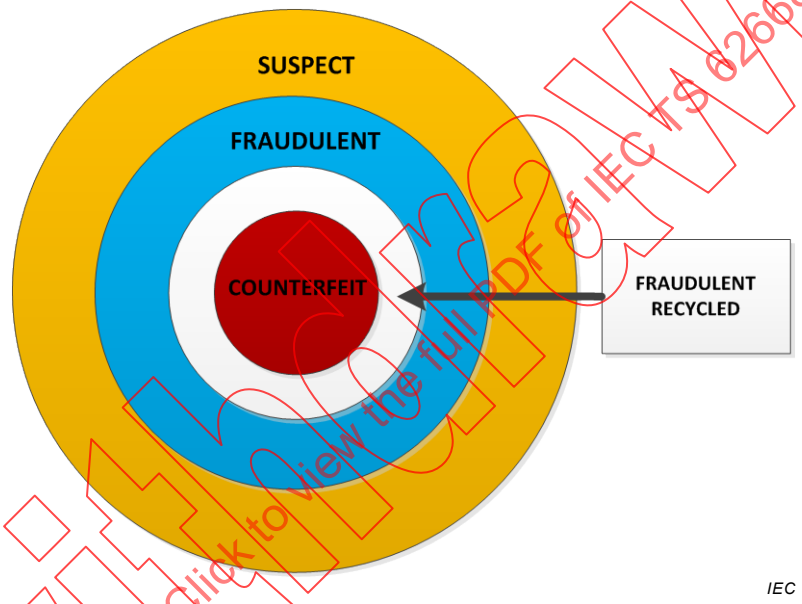

Figure 1 – Suspect components perimeter

4.4.4 How to establish traceability

See 3.1.22 for the definition of "traceability".

4.4.5 Reasons for the loss of component traceability

Many components lose their traceability (see 3.1.23 for the definition of "untraceable") back to the original manufacturer. This can be caused by:

a) 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.

b) 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.

c) 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.

d) Using inappropriate distributors, which are not AS/EN/JISQ 9120 certified, which although they may typically supply direct from manufacturers, 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.

e) Commercial grade components which are not supplied with full traceability back to the OEM.

4.5 Why is counterfeit a problem?

4.5.1 General

The recent USA report GAO-10-423, published by the US Government Accountability Office, details the extent to which counterfeiting activity affects the US economy.

The Japanese Patent Office also includes a 'FY2004 Survey Reports on Losses Caused by Counterfeiting' (see A.10.1).

4.5.2 General worldwide activities combating counterfeit issues

4.5.2.1 General

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

4.5.2.2 Anti-Counterfeiting Trade Agreement (ACTA)

ACTA establishes a new international legal framework that countries can join on a voluntary basis and will create its own governing body outside existing international institutions such as the World Trade Organization (WTO), the World Intellectual Property Organization (WIPO) or the United Nations.

The 11th and final round of the negotiations for the Anti-Counterfeiting Trade Agreement (ACTA) was concluded successfully in Tokyo, Japan, on 2 October 2010 (see Clause A.2).

Participants in the negotiations included Australia, Canada, the European Union (EU) represented by the European Commission and the EU Presidency (Belgium) and the EU Member States, Japan, Korea, Mexico, Morocco, New Zealand, Singapore, Switzerland and the United States of America.

ACTA aims to establish a comprehensive, first-time, international framework that will assist parties to the agreement in their efforts to effectively combat the infringement of intellectual property rights, in particular the proliferation of counterfeiting and piracy, which undermines legitimate trade and the sustainable development of the world economy. It will include state-of-the-art provisions on the enforcement of intellectual property rights, including provisions on civil, criminal, and border enforcement measures, robust cooperation mechanisms among ACTA Parties to assist in their enforcement efforts, and establishment of best practices for effective IPR enforcement.

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. It now 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) (see Clause A.3). 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).

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 organisations 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 source from franchised distributors or the OCM, which may have ceased trading.
- Long deliveries e.g. > 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. Also 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.

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

a) Buy components directly from the original component manufacturer or the approved franchised distributor.

b) Maintain component traceability back to the original manufacturer, typically through the use of certificates of conformance or test certifications.

c) Maintain approved supplier lists and criteria of supplier approval.

d) Ensure supply chain anti-counterfeit procedures are established and are maintained.

e) Use escrow accounts operated by ERAI when purchasing potentially suspect components.

f) Use IDEA-STD-1010B type visual inspection regimes and test suspect components, e.g. X-ray, electrical test, as required.

g) Use of databases to track suspect or counterfeit components, using GIDEP.

h) DOD entities should use Product Quality Deficiency Reports (PQDRs) to report non-working electronic components.

i) Proposing that FAR regulations are changed for the procurement of components for mission critical applications.

j) That a centralised US federal reporting mechanism and database be set up for collecting counterfeit data with close ties to law enforcement. [10][2]

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.

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 datasheets, exhibiting the expected component life in the application for the OEM’s reliability predictions and product warranty.

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

4.5.4.4 Defense Logistics Agency (DLA)

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

---

[2] Numbers in square brackets refer to the Bibliography.

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.8.13; see A.8.13 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, 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.8.13.

However this marking requirement is unpopular with the Semiconductor Industry Association (SIA) many of whose members are refusing to bid for working with the DLA.

The recent 2013 appraisal of the US FY2013 National Defence Authorisation Act acknowledges this (see A.8.13).

4.5.4.5 USA NDAA section 818 anti-counterfeit legislation

The USA President signed the National Defence Acquisition Act (NDAA), which included section 818 on anti-counterfeit measures, on December 31st 2012. The section 818 addresses how to minimise counterfeit components in the US defence supply chain. Severe penal and financial penalties will be levied on organisations and individual personal found to be involved in deliberately supplying counterfeit or fraudulent components to the US defence organisations. This applies to all parts of the supply chain including brokers, distributors and OEMs. These penalties are alleviated if the OEM or distributor publishes an anti-counterfeit management plan using for example SAE AS5553A or this specification.

The DOD has published its anti-counterfeit Prevention Policy, number DoDI 4140.67 and is preparing a DFAR for use in contracts. The status of the DFAR can be tracked on the webpage, see A.8.14. The draft DFAR was recently circulated for public consultation using the term ‘trusted supplier’ which has caused confusion as this term is already in use (see 4.7.8 and 4.7.9) and is available from only US based manufacturers. However, it appears that this term ‘trusted supplier’ will be enhanced and be further defined in the near future. International members of the US defence supply chains hope that the term ‘trusted supplier’ takes account of international supply chain requirements.

This NDAA section 818 anti-counterfeit activity is in addition to DoDI 7050.05 concerning remedies for fraud and corruption-related procurement activities which are already published.

4.5.4.6 UK MOD anti-counterfeit guidance

The UK DOD has created an interactive webpage (see A.6.7), to provide guidance for their supply chain.

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 organisation BEAMA for the electrotechnical 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 3.1.17 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, e.g. 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 does the avionics industry 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 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 When do 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, e.g. where typically 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 3.1.22) 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/TS 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 paragraph.

4.7.2 Chinese Reliable Electronic Component Supplier (RECS) audit scheme

This auditing scheme operates in China and was promoted by GAMS 2009 and by the WSC. The RECS scheme announced the first thirteen qualified enterprises in January 2008 (see A.9.3).

The RECS system certifies and authenticates electronic component manufacturers and authorized distributors which provide products from legal and reliable sources. RECS was established in response to a growing trend of counterfeit products in China and is designed to promote legitimate product sources and educate China electronic purchasers to buy from reliable sources of electronics components while ensuring the reliability and traceability of product sources. RECS is identified by the China Quality Management Association and the China Electronics Enterprises Association Procurement Branch, in support of the Ministry of Information Industry which jointly organized and implemented industry activities.

NOTE However, there is concern that this is not being maintained and there appears to have been no activity in the last few years.

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 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.8.15), can be used to verify AS/EN/JISQ 9100/9110/9120 certificates.

4.7.4 Original component manufacturer (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 OHIM (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 (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 datasheets. ATP test software and test stations should be numbered and critically controlled. Datasheets (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 datasheet is the OCM's design information which is controlled by their intellectual property rights.

4.7.6 Original component manufacturer (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/WD 16678 was developed for tracking and trace methods for shipment.
- ISO/IEC 15459-8 is 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.
- 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). The SEMI intellectual property webpage (see Clause A.4) 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 standards have been published focusing on IC chip counterfeiting:

- 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.

These new standards 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.8.8), which are responsible for finding and maintaining suppliers of trusted microelectronic parts for USA Military and USA Mission Assurance Category I systems (DoDI 8500.2) critical programs.

Trusted suppliers are now managed by the Defence Micro Electronics Activity (DMEA) (see A.8.9) 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.

For an example see A.8.9, where the manufacturer provides custom components, with a Unique Number Generator (UNG) which is a die specific identification in a 256 × 1 bit serial access 'self-programming' ROM. This ROM can be read electrically at wafer level test, after package assembly and in the field and is operable from –40 °C to +125 °C. These ROMs can be placed in several locations on a die within different circuit elements. This prevents re-engineering and acts as a counterfeit deterrent.

4.7.9 USA Trusted IC Supplier Accreditation Program

USA trusted suppliers in addition to those listed in 4.7.8 above, which are now managed by DMEA (see A.8.9) 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 described. This is a new emerging technology with immediate applications for preventing counterfeit activities for example RFID tags and military applications.

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

Organisations 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 3.1.18), the physical unclonable function (PUF).

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, e.g. websites with look-up

information for OEMs and other users to verify physical component markings and tamperproof labels or tags (see Clause A.13).

4.8 Distributor minimum accreditations

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

- International Organization for Standardization (ISO) 9001: a quality management system standard.
- ISO 14001: an environmental management system.
- Standard Occupational Health and Safety Assessment Series (OHSAS) 18001: an occupational health and safety management system specification or equivalent procedure.
- American National Standards Institute/Electrostatic Discharge (ANSI/ESD) S20.20: an ESD control program standard or 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 distributor 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.8.15), can be used to verify AS/EN/JISQ 9100/9110/9120 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, e.g. annually or every 2 years. Also 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 Electronic 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:

a) ECIA, the Electronics Components Industry Association, a non-profit organisation in North America (see A.8.11) 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.
   - A new authorised inventory search site that supports authorised distribution.
b) ECSN, the Electronic Component Supplier Network, is a non- profit UK trade association (see A.6.6), which publishes several guides and can act as an arbitrator for franchise agreements
c) IDEA, the Independent Distributors of Electronics Association (IDEA) (see A.8.10).

A new franchised distributor specification is being created by the SAE G-19AD committee, SAE AS 6496[3] (see Clause A.17), to address how the franchised distribution supply chain mitigates the risk of counterfeit components.

4.10.2 Control stock through tracking schemes

Franchised distributors control manufacturers stock through relevant tracking schemes and can accept back unused stock from the OEMs and resell onto other customers with the required traceability (see the NIGP 113 NEDA Guidelines for Product Returns).

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

4.10.3 Control 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.

4.10.4 RECS

All franchised distributors in the Far East are recommended to be RECS audited (see 4.7.2).

4.11 Non- franchised distributor anti-counterfeit guidelines

4.11.1 General

See 3.1.12 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.

[3] Under consideration.

Non-franchised distributors can also be AS/EN/JISQ 9120 Third Party Certified. The IAQG online Oasis database (see A.8.15), can be used to verify AS/EN/JISQ 9100/9110/9120 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.

For more information, see IEC/TS 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.8.12), to define mandatory practices to detect and avoid the delivery of counterfeit electronic components to their customers.

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. 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.8.13.

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/TS 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.

For more information, see IEC/TS 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/TS 62668-2.

4.12 Avionics OEM anti-counterfeit guidelines when procuring components

4.12.1 General

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

- AS/EN/JISQ 9100 procedures; and

- IEC/TS 62239-1 ECMP which includes 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.8.15), can be used to verify AS/EN/JISQ 9100/9110/9120 certificates.

SAE ARP 6178, which is an audit checklist, may be a useful tool in assessing sources of supply (see Clause A.17) and could become part of the OEM AS/EN/JISQ 9100 approved supplier process.

4.12.3 Traceable components

AS/EN/JISQ 9100 requires demonstration of conformity to 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/datasheets.

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 KANBAN 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 can be requested confirming this traceability (see 3.1.22 and 4.12.4).

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 9100 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 Certificates of conformance

This is the traditional way of checking traceability back to the original 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.

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.

4.12.5 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 their IEC/TS 62239-1 ECMP or their GEIA-STD-0016 DMSMS management plan and monitors component requirements throughout the lifecycle of their product.

OEMs JIT policies need 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/PAS 62435).

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.17)
2) iNEMI anti-counterfeit risk assessment calculators (see Clause A.18)

When non-franchised distributors are shipping untraceable components, the OEM shall follow the requirements of IEC/TS 62668-2 for more information, which requires that all purchased components be tested prior to use. Prior approval by the customer, generally the OEM (see 3.1.14), 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/TS 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 needed 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 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 monitor 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) shall be used before sourcing untraceable components. See Annex B for examples of aftermarket sources.

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

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/TS 62239-1 ECMP or GEIA-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/TS 62239-1,
- GEIA-STD-0016,
- IEC/TS 62402,
- SD-22.

4.12.10 IEC/TS 62239-1 approved alternatives

Where no traceable or aftermarket components can be found, the OEMs should consider using their IEC/TS 62239-1 Electronic Component Management Plan (ECMP) process to find traceable IEC/TS 62239-1 approved components which are form, fit and function alternatives suitable for the application.

4.12.11 Product redesign

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

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 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 should be managed within an OEM anti-counterfeit management plan (see 4.12.13).

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 specification, see 4.2 in particular 4.2 c).

The OEMs which do not have an SAE AS5553A plan shall meet the requirements specified in 4.2 c).

The OEMs that have an SAE AS5553A anti-counterfeit plan for electronic components may include it in lieu of the requirements listed in Table 2 in their IEC/TS 62668-1 anti-counterfeit plans.

SAE AS5553A is a very comprehensive document targeted at general industry and written for USA users (see Clause A.17 for further information), but only applies to electronic components coming into a business.

In addition to the management of electronic components coming into a business, IEC/TS 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/TS 62668-1 requirements waived if OEM has an approved SAE AS5553A plan

IEC/TS 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/TS 62668-1 plan
4.2 a)	No.		
4.2 b)	No.	SAE AS5553A has no minimum specific component selection rules, only rules for maximizing the availability of parts with an obsolescence management plan and rules for sourcing or buying components.	Refer to an IEC/TS 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/TS 62668-1 plan also has to address all the 4.2 requirements including how they 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/TS 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.
4.2e) 1)	No.	The Chinese RECS scheme is not acknowledged by the SAE.	Include the Chinese RECS scheme if your company buys components from China.
4.2 e) 2) i)	Yes.		Base your SAE AS5553A plan on traceability through the supply chain.

IEC/TS 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/TS 62668-1 plan
4.2e) 2) ii)	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) 2) iii)	Yes.		Base your SAE AS5553A plan on using franchised aftermarket sources when the part is obsolete.
4.2 e) 2) iv)	Yes.		Base your SAE AS5553A plan on traceability through the supply chain.
4.2e) 2) v)	No.	SAE AS5553A does not refer to IEC/TS 62668-2.	Base your anti-counterfeit plan on using IEC/TS 62668-2 for managing non-franchised distributors.
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/TS 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 AS5553A minimum requirements do not refer to IEC/TS 62668-2 and do not mandate the use of AS/EN/JISQ 9100 non-conformance procedures.	Base your anti-counterfeit plan on using IEC/TS 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.		

NOTE SAE AS6174 for mechanical components has been published but is being revised (see Clause A.17) and can be used as a basis for material anti-counterfeit plans.

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 will be adopted and modified to be published as IEC/TS 62668-2 in the near future.

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.

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.14 for examples).

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

Recent tamperproof 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 board 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. Antifused 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.15 for examples).

4.13.4.4 NOVRAM

Some NOVRAMs contain an internal microprocessor, which can be factory programmed to destroy the internal code (see Clause A.16).

4.13.5 Control the final OEM product marking

The OEM shall ensure that the equipment supplied shall be marked in accordance with the regulatory requirements and provide full traceability. Note that radio frequency ID tags are becoming common in the automotive world in order to distinguish genuine components from counterfeit ones (see Clause A.13).

The user can note the following:

- ISO 12931 has been issued to assist with the authentication methods required to combat counterfeit risks;
- ISO/WD 16678 is being developed for tracking and trace methods for shipment;
- 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;
- 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 using DoD 4160.21-M.

4.13.7 OEM trademarks and logos

All trademarks should be registered. 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.8.5.

The FAA has webpages for engine identification and registration marking requirements (see A.8.6).

4.13.9 Repairs to OEM products

Most civil OEMs repair their equipment internally, in their own approved 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.

However, military customers typically use their approved military repair centres and order replacement components for repairs. This ordering activity is beyond the control of the OEM which supplied the equipment and the OEM cannot be held responsible for this procurement activity.

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 9110:2003 has a specific clause in 7.4.1 f) requiring that appropriate measures are taken to prevent purchase of counterfeit/unapproved products.

Civil air framers also carry out repairs and use FAA approved facilities as follows:

- FAR Part 43 describes the rules for any aircraft having a US air-worthiness certificate.
- FAA advisory circular 20-62E, dated December 23rd 2010, defines the quality, eligibility and traceability of aeronautical parts and materials intended for installation on US type certified products.
- FAR Part 145 describes the certification, training, facility requirements and operating rules for Aeronautics and Space repair stations.

EASA, The European Aviation Safety Agency (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 on approved maintenance organisations

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.

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.8.7).

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 Standard 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 b)) 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.

Annex A
(informative)

Useful contacts[4]

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 as follows:

- WIPO Brazil Office, Rua Farme de Amoedo, 56-7th Floor, Ipanema-CEP22420020, Rio de Janeiro-RJ, Brazil, tel: (+5521) 2103-4625, see webpage: http://www.wipo.int/contact/en/area.jsp?area=wbo
- WIPO Japan Office UNU Building, 6F 5-53-70 Jingumae, Shibuya-Ku, Tokyo 150-0001, Japan, tel: (+81) 3 5467 1216
- WIPO New York Office, WIPO Coordination Office, 2 UN Plaza, Suite 2525, New York, NY 10017, tel:(+1) 212-963-6813
- WIPO Singapore Office, 29 Heng Mui King Terrace, #06-16, Singapore, 119620, Singapore, tel:(+65) 6774 7712

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.

A.1.3 WIPO Intellectual Property Services

a) 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 in a large number of countries 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.

b) International trademark registration (Madrid System)

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

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 multiple 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.

The Madrid Express database is discontinued as of 1 January 2011.

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 over 80 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 **In**formation) database at webpage http://www.wipo.int/madrid/en/romarin/

c) International design registration (Hague System)

The Hague System (see webpage http://www.wipo.int/hague/en/) allows applicants to register an industrial design in multiple 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.

d) 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.

e) 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 arbitration, 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.

f) 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.

g) 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.

h) Protection of State emblems (Article 6*ter* 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:

This web page has been launched in order to support the work and sharing of resources, including training programs, of the Global Network of IP Academies and to provide an effective forum for exchanging of views and experiences among the members of the network.

The contents of the webpage are the following:

- Secretariat;
- Global Intellectual Property Academy, United States Patent and Trademark Office (USPTO);
- International Intellectual Property Training Institute (IIPTI) of the Korean Intellectual Property Office (KIPO);
- WIPO Academy;
- Present Members.

List of present members:

Country / Organization	Institution
ARIPO	African Regional Intellectual Property Organization
Australia	Intellectual Property Research Institute of Australia
Azerbaijan	Copyright Agency of the Republic of Azerbaijan through its Enforcement of IPR Center
Brazil	National Institute of Industrial Property of Brazil (INPI)
Bulgaria	Centre for Intellectual Property of the University of National and World Economy
China	State Intellectual Property Office of China (SIPO)

Country / Organization	Institution
Colombia	Superintendence of Industry and Commerce
Costa Rica	Registro de la Propiedad Industrial, Registro Nacional, Ministerio de Justicia y Paz
Croatia	State Intellectual Property Office of Croatia (SIPO)
Cuba	Industrial Property Office of Cuba (OCPI)
Dominican Republic	Oficina Nacional de la Propiedad Industrial (ONAPI)
EPO	European Patent Academy
India	Global Institute of Intellectual Property
Indonesia	Indonesian IP Academy (IIPA)
Japan	National Center for Industrial Property Information and Training
Kenya	Kenya Industrial Property Institute (KIPI)
Mexico	Mexican Institute of Industrial Property (IMPI)
Morocco	Moroccan Industrial and Commercial Property Office
Nigeria	Nigerian Copyright Institute Nigerian Copyright Commission (NCC)
OAPI	Organisation Africaine de la Propriété Intellectuelle – Intellectual Property Training Center Denis Ekani
OHIM	Office for Harmonization in the Internal Market (Trade Marks and Designs)
Pakistan	Intellectual Property Office (IPO-Pakistan) – Intellectual Property Academy
Peru	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
Philippines	Intellectual Property Office of the Philippines (IPOPHIL) – Intellectual Property Research Training Institute of the Philippines (IPRTI)
Poland	The Patent Office of the Republic of Poland
Portugal	National Institute of Industrial Property of Portugal (INPI)
Republic of Korea	International Intellectual Property Training Institute of the Republic of Korea Korea Copyright Commission
Russian Federation	Russian State Institute of Intellectual Property (RGIIS)
Singapore	IP Academy
Switzerland	Swiss Federal Institute of Intellectual Property (IPI)
The former Yugoslav Republic of Macedonia	Center for Intellectual Property Education of the Republic of Macedonia (CIPE)
Ukraine	State Institute of Intellectual Property of Ukraine
United States of America	United States Patent and Trademark Office Global Intellectual Property Academy
Vietnam	The Vietnam Intellectual Property Research Institute
WIPO	WIPO Academy

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

This agreement was concluded successfully in Tokyo, Japan, on 2 October 2010.

For the joint statement from all the negotiating parties see the webpage http://trade.ec.europa.eu/doclib/press/index.cfm?id=623 where the following information can be found:

“The 11th and final round of the negotiations for the Anti-Counterfeiting Trade Agreement (ACTA) was concluded successfully in Tokyo, Japan, on 2 October 2010. The Government of Japan hosted the negotiations.

Participants in the negotiations included Australia, Canada, the European Union (EU) represented by the European Commission and the EU Presidency (Belgium) and the EU Member States, Japan, Korea, Mexico, Morocco, New Zealand, Singapore, Switzerland and the United States of America.

ACTA aims to establish a comprehensive, first-time, international framework that will assist Parties to the agreement in their efforts to effectively combat the infringement of intellectual property rights, in particular the proliferation of counterfeiting and piracy, which undermines legitimate trade and the sustainable development of the world economy. It will include state-of-the-art provisions on the enforcement of intellectual property rights, including provisions on civil, criminal, and border enforcement measures, robust cooperation mechanisms among ACTA Parties to assist in their enforcement efforts, and establishment of best practices for effective IPR enforcement.”

The Europa webpage (A.7.1.c)) contains a copy of the final ACTA agreement with further information.

The ACTA treaty was signed on February 4th 2013 by 31 states (USA, Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea, as well as the EU). See webpage https://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement#Signatures_and_ratifications for more information.

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 22 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/Home/About).

A.3 World Semiconductor Council (WSC)

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

"The purpose (of the World Semiconductor Council) is to promote cooperative semiconductor industry activities, to expand international cooperation in the semiconductor sector in order to facilitate the healthy growth of the industry from a long-term, global perspective.

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.

The webpage provides links to the Semiconductor Industry Associations from China, Chinese Taipei, Europe, Japan, Korea and the United States which are all members of the World Semiconductor Council.

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

The European Semiconductor Industry Association webpage is chair of the counterfeit committee (see webpage http://www.eeca.eu/esia/). Their counterfeit webpage is http://www.eeca.eu/esia/public-policy/anti-counterfeiting which contains details of how to file for action for trademark infringement.

A.4 SEMI

SEMI Global headquarters are located at 3081 Zanker Road, San Jose, CA 95134, 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/index.htm 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;
- Photovoltaics (PV);
- LED;
- Flat Panel Display (FPD);
- Micro-electromechanical systems (MEMS);
- Printed and flexible electronics;
- 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 has a website www.authorizeddirectory.com which has the following information and search capabilities:

"Welcome to the only comprehensive worldwide directory for AUTHORIZED distributors of semiconductors. With our quick, up to date search tool, you can search by semiconductor manufacturer, by country to find authorized distributors worldwide. If you are not purchasing your semiconductors from the original manufacturer, Authorized Directory is your #1 trusted source for AUTHORIZED semiconductor distributors.

Having difficulty finding a genuine semiconductor device?

Don't compromise, buy from an authorized semiconductor distributor or manufacturer:

- find the semiconductor manufacturer;
- search for manufacturer headquarters and sales offices;
- find the authorized semiconductor distributor;
- check worldwide inventory of authorized devices ".

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:

a) Patents (see webpage http://www.ipo.gov.uk/types/patent.htm) 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.

b) Trademarks (see webpage http://www.ipo.gov.uk/types/tm.htm) which are discussed with details of how to apply and manage these. Details are also provided for other people's trademarks and trademark infringement.

c) Designs (see webpage http://www.ipo.gov.uk/types/design.htm) which are discussed with details of how to apply to register a design.

d) Copyright (see webpage http://www.ipo.gov.uk/types/copy.htm) 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 the 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 information@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, tel + 44 020 7803 1319, see webpage www.allianceagainstiptheft.co.uk where the following information is found:

"Established in 1998, the Alliance Against Intellectual Property (IP) Theft is a UK-based coalition of 23 associations and enforcement organisations with an interest in ensuring intellectual property rights receive the protection they need and deserve. With a combined turnover of over £250 billion, 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 Trading Standards Institute

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

"Trading standards professionals act on behalf of consumers and business. They advise on and enforce laws that govern the way we buy, sell, rent and hire goods and services.

Trading standards officers (TSOs) work for local councils advising on consumer law, investigating complaints and, if all else fails, prosecuting traders which break the law.

These laws cover a wide area, which includes:

- counterfeit goods, product labelling, weights and measures, under-age sales, animal welfare;
- checking that food labelling is correct and advertising is not misleading;
- advising consumers and businesses about the law;
- investigating suspected offences, which could include undercover or surveillance work;
- preparing evidence and prosecuting cases in court;
- inevitably, writing reports and keeping records."

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 http://www.hmrc.gov.uk/reportingfraud/help.htm .

The UK customs hotline for reporting counterfeit items is: 0800 59 5000.

A.6.5 ESCO Anti-counterfeiting Forum (formerly UKEA Anti-Counterfeiting Forum)

The ESCO Anti-Counterfeiting Forum, see webpage http://www.anticounterfeitingforum.org.uk/counterfeiting.aspx, is now part of the Electronic Systems Community (ESCO, see website http://www.esco.org.uk/) 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 as: 0800 59 5000.

A.6.6 Electronic Component Supplier Network (ESCN)

The Electronic Component Supplier Network (see webpage 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.7 Europe

A.7.1 Europa Summaries of EU Legislation

a) The Intellectual Property interactive webpage is http://europa.eu/legislation_summaries/internal_market/businesses/intellectual_property/index_en.htm which has the following information:

   Intellectual property

   "A uniform system of protection of intellectual property rights, ranging from industrial property to copyright and related rights, constitutes the foundation for creativeness and innovation within the European Union. Respect of the basic principles of the internal market (the free movement of goods and services and free competition) is based on standardization of intellectual property at European level. Protection of intellectual property is covered by many international conventions, most of which are implemented by the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO). The European Union possesses two important bodies to carry out its mission: the Office for Harmonization in the Internal Market (OHIM), which is responsible for the registration of Community trademarks and designs, and the European Patent Office (EPO). The Commission is currently campaigning for the effective introduction of a Community patent system, which would be less costly and more legally effective, as a guarantee of competitiveness for European industry. Finally, the protection of these rights also entails protecting them against piracy, illegal trade and counterfeiting."

b) 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

c) 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 http://www.europol.europa.eu/

A.7.3 European Patent Office

See the interactive webpage www.epo.org/ (telephone +0049 89 2399 4636), where a search or application can be made.

A.7.4 Europe at OHIM

See webpage https://oami.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://oami.europa.eu/ohimportal/en/trade-mark-definition which contains the following information:

"Legally speaking, a trade mark is a sign which serves to distinguish the goods and services of one organization from those of another.

Trademarks are words, logos, devices or other distinctive features which can be represented graphically. They can consist of, for example, the shape of goods, their packaging, sounds and smells.

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://easa.europa.eu/home.php. 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/TS 62668-1 for avionics OEMs in the near future.

A.7.7 BEAMA

BEAMA is the independent expert knowledge base and forum for the electrotechnical industry for the UK and across Europe. Representing over 300 manufacturing companies in the electrotechnical sector, the organisation has significant influence over UK and international political, standardisation and commercial policy, see webpage http://www.beama.org.uk/ and webpage http://www.beama.org.uk/en/what-we-do/services/anti--counterfeiting/index.cfm 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, tel: 1-800-786-9199. The USPTO has many customer support centres which can be found on their webpage.

The USPTP website is http://www.uspto.gov/ which contains the following information:

a) "What is a patent?

   A patent is an intellectual property right granted by the Government of the United States of America to an inventor "to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States" for a limited time in exchange for public disclosure of the invention when the patent is granted.

   This right was established over 200 years ago in Article 1, Section 8 of the United States Constitution: "To promote the Progress of Science and useful Arts, by securing for limited

Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

General Information Concerning Patents

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. The webpage has a Process for Obtaining a Utility Patent
- 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."

b) Trademarks Home, see Trademarks Home at webpage: http://www.uspto.gov/trademarks/index.jsp

A.8.2 The International Trade Administration, U.S. Department of Commerce

The International Trade Administration, U.S. Department of Commerce Stopfakes.gov has a webpage http://www.stopfakes.gov/sf_how.asp which contains very useful information for protecting IP.

A.8.3 USA Embassy in China information

The USA Embassy in China webpage (see webpage http://beijing.usembassy-china.org.cn/ipr.html) has extremely useful information for protecting IP and provides hyperlinks to the following and frequently asked questions.

General websites:

State Intellectual Property Rights Office http://www.cpo.cn.net/

Judicial Protection of IPR in China http://www.chinaipr.gov.cn/

Judicial Interpretation on the Application of Law to the Trial of Trademark Dispute Cases Issued (http://www.ccpit-patent.com.cn/News/2003021902.htm)

"Frequently Asked Questions

Q: What must a foreign trademark holder do to become eligible for trademark protection in China?

A: The registration system is voluntary. However, protection is not offered to a company that claims "first use" in China. China has a "first to file" system that grants trademark rights based on the time of trademark registration. Trademark applications must be filed at the SAIC's Trademark Office. See above for more details on registration and mandatory use of certified trademark registration agents by some types of foreign companies.

Q: What is the duration of trademark protection in China?

A: A registered trademark is valid for a period of ten years, calculated from the time on which the registration is approved.

Q: Where should a trademark owner file a complaint alleging trademark infringement?

A: File the complaint with the local AIC Trademark Division, usually in the place where trademark infringement occurred.

Q: If a trademark owner selects the administrative channel, can the owner obtain compensatory damages?

A: No. A registered trademark holder may only seek compensatory damages through civil litigation.

Q: What administrative corrective measures may be imposed against the infringer by the local AIC trademark division?

A: The Trademark Division may issue a cease and desist order, confiscate and destroy goods to which are attached illegal representations, confiscate materials, tools and equipment used to produce counterfeit goods, impose fines up to the maximum of three times the illegal gain or in cases where it is difficult to determine the illegal gain, administrative authorities may impose a maximum fine of RMB100 000 (US$12 000). A complainant is entitled to a written decision regarding the corrective measure taken.

Q: What is the criterion for criminal prosecution?

A: In practice, it appears to be RMB50 000 (US$6 000) in illegal gain. However, the "Provisions on Standards for Prosecution of Economic Crimes," issued by the Supreme People's Court in I993, provide for lower thresholds.

Q: What are the minimum and maximum criminal punishments?

A: If the circumstances are "serious" or if the amount of illegal gain is "huge," the defendant may be sentenced to imprisonment a minimum of three years, maximum seven years, and may also be fined.

Q: Is it possible to prevent the defendant from destroying evidence?

A: Yes. A trademark holder may seek a preliminary injunction from the court. The rights holder is required to post a bond."

A.8.4 International Intellectual Property Alliance

See webpage http://www.iipa.com/aboutiipa.html 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 seven member associations are: the Association of American Publishers (AAP), the Business Software Alliance (BSA), the Entertainment Software Association (ESA), the Independent Film & Television Alliance (IFTA), the Motion Picture Association of America (MPAA), the National Music Publishers' Association (NMPA) and the Recording Industry Association of America (RIAA). IIPA's seven member associations represent over 1,900 U.S. companies producing and distributing materials protected by copyright laws throughout the world—all types of computer software, including business applications software and entertainment software (such as videogame discs and cartridges, personal computer CD-ROMs, and multimedia products); theatrical films, television programs, DVDs and home video and digital representations of audio-visual works; music, records, CDs, and audiocassettes; and textbooks, trade books, reference and professional publications and journals (in both electronic and print media).

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 over 80 countries 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.8.5 The FAA

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

A.8.6 FAA Engine Approval

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.8.7 FAA Aviation Safety Hotline office

See webpage http://www.faa.gov/contact/safety_hotline/

A.8.8 Trusted Access Program Office (TAPO)

The Trusted Access Program Office (TAPO) webpage is https://www.tapoffice.org/ 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 IBM to produce advanced microelectronics parts in a trusted environment. IBM maintains domestic facilities, providing capabilities to the government with yearly options through fiscal year 2013. 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 ASIC trusted foundry contracts. Accredited suppliers are listed on the DMEA webpage, see A.8.9.

A.8.9 Defense Microelectronics Activity (DMEA)

The DMEA Trusted IC Supplier Accreditation Program webpage is: http://www.dmea.osd.mil/ where after entering the webpage and accepting the disclaimer notice, the Trusted IC webpage is found at webpage http://www.dmea.osd.mil/home.html where the following information is found:

"The Office of Secretary of Defense (OSD) issued the Defense Trusted Integrated Circuits Strategy (DTICS) that established "Trust" as a minimum need for DOD in October 2003. Interim Guidance from the Office of Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD/AT&L, dated 27 January 2004) initiated development of policy that requires all Mission Assurance Category I systems (DoDI 8500.2) to "employ only trusted foundry service(s) to fabricate their custom designed ICs". As a result, the new vendor criteria issued to DOD Program Managers has increased the need for trusted parts and the subsequent expansion of the Trusted Foundry Program. The OUSD/AT&L, through TAPO and DMEA, has implemented an accreditation plan for design, aggregator/broker, mask and wafer fabrication, packaging and test services across a broad technology range for specialized governmental applications both classified and unclassified. The Defense MicroElectronics Activity (DMEA) has been designated by the Department of Defense through the Trusted Access Program Office (TAPO) as the accrediting authority for this program."

For a current list of accredited suppliers, download the following PDF file at the following webpage: http://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf .

> The Defense MicroElectronics Activity (DMEA) 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.

Send an email to TrustedIC@dmea.osd.mil or call (916) 231-1514 for more information related to the accreditation of trusted IC suppliers.

A.8.10 Independent Distributors of Electronic Association (IDEA)

The Independent Distributors of Electronics Association (IDEA) organisation is located at 6312 Darlington Avenue, Buena Park, CA 90621, USA, tel 714-670-0200. See webpage http://www.idofea.org/ where the following information is available:

"The Independent Distributors of Electronics Association (IDEA) is a non-profit trade association representing quality and ethically oriented independent distributors of electronic components. The purpose of IDEA is to promote the independent distribution industry through a media advocacy campaign, to improve the quality of products and services through a quality certification program, educational seminars, and conferences, and to promote the study, development, and implementation of techniques and methods designed to improve the business of independent distributors."

A.8.11 ECIA formerly National Electronic Distributors Association (NEDA)

The Electronic Component Industry Association in North America is located at 111 Alderman Dr., Suite 400, Alpharetta, GA 30005, USA, tel: 678-393-9990. See webpage http://www.eciaauthorized.com/about-us which contains the following information:

“In January, 2011 the Electronic Components Association (ECA) and the National Electronic Distributors Association (NEDA) united to form the Electronic Components Industry Association (ECIA). ECIA supports the expanding needs and interests of the global supply chain. The association connects all facets of the electronic components industry in a way no association has in the past: manufacturers, authorized distributors and manufacturers’ representatives working together as a stronger voice for our entire industry. The Association’s mission is to promote and improve the business environment for the authorized sale of electronic components.”

Visit 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 threat of counterfeit products is a significant industry issue. Visit www.supplierauthorizeddistributor.com/ to learn more about this growing problem and the solution that sourcing electronic product through the authorized channel provides.

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.8.12 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/index.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:

Components Technology Institute, Inc.
904 Bob Wallace Avenue, Suite 117
Huntsville, AL 35801
Tel: 256-536-1304
Fax: 256-539-8477

A.8.13 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 http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/QTSL.aspx, where approximately 16 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 http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?Section=QSL

The DLA 2013 report at webpage http://www.landandmaritime.dla.mil/downloads/news/ElectricalElectronics.pdf contains information about all the DLA programs including reference to SAE AS6081 and the Deoxyribonucleic Acid (DNA) marking.

Webpage http://www.dla.mil/InformationOperations/sirc/Lists/News%20Feed/CustomDispForm.aspx?ID=43 provides general information related to the DLA policy to expand requirements for DNA authentication marking on items falling within FSC 5962, electronic microcircuits, which have been determined to be at high risk for counterfeiting.

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.

A.8.14 DFAR progress

The status of DFAR Case 2012-D055 can be tracked on US webpage http://www.acq.osd.mil/dpap/dars/case_status.html