IEC TS 62668-2

Edition 2.0 2016-08

TECHNICAL SPECIFICATION

colour inside

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

IEC TS 62668-2:2016-08(en)

International Electrotechnical Commission

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 It also gives information on projects, replaced and withdrawn publications.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 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 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 62668-2

Edition 2.0 2016-08

TECHNICAL SPECIFICATION

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 03.100.50; 31.020; 49.060

ISBN 978-2-8322-3573-7

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

PROCESS MANAGEMENT FOR AVIONICS – COUNTERFEIT PREVENTION –

Part 2: Managing electronic components from non-franchised sources

FOREWORD

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 62668-2, 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 2014. This edition constitutes a technical revision.

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

a) Updates to the risk assessment process.
b) Updates to the test methods including reference to the SAE AS6171 test methods in development.
c) Updates in line with IEC TS 62668-1 for definitions and references to DFARS and removal of reference to RECS.

This technical specification is to be used in conjunction with IEC TS 62239-1 and IEC TS 62668-1.

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

Enquiry draft	Report on voting
107/280/DTS	107/286/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 document 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 document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- 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.

INTRODUCTION

The avionics industry has a responsibility to ensure that all flight equipment produced has a predicted product life which correlates to the predicted repair and service life to ensure the public is not endangered. Typically an original equipment manufacturer (OEM) calculates a mean time between failure (MTBF) and possibly a mean time to failure (MTTF) prediction. 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. For example it is therefore essential that counterfeit, recycled and fraudulent components which have had potentially some of their ”useful life” consumed and which may also be malfunctioning are not purchased for use in aerospace, defence and high performance (ADHP) industries.

PROCESS MANAGEMENT FOR AVIONICS – COUNTERFEIT PREVENTION –

Part 2: Managing electronic components from non-franchised sources

1 Scope

This part of IEC 62668, which is a technical specification, defines requirements for avoiding the use of counterfeit, recycled and fraudulent components when these components are not purchased from the original component manufacturer (OCM) or are purchased from outside of franchised distributor networks for use in the aerospace, defence and high performance (ADHP) industries. This practice is used, as derogation, only when there are no reasonable or practical alternatives.

NOTE Typically this technical specification is used in conjunction with IEC TS 62239-1 and IEC TS 62668-1, enabling ADHP industries to manage and avoid the use of counterfeit, recycled and fraudulent components in their supply chains.

Although developed for the ADHP industry, this document may be used by other high-performance and high-reliability industries, at their discretion.

2 Normative references

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

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

IEC TS 62668-1:2016, *Process management for avionics – Counterfeit prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

3.1.1
aftermarket source
reseller which may or may not be under contract with the original component manufacturer (OCM) or is sometimes a component "re-manufacturer", under contract with the OCM

Note 1 to entry: The reseller accumulates inventories of encapsulated or non-encapsulated components (wafer and/or die) 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.

[SOURCE: IEC TS 62668-1:2016, 3.1.1]

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 another. The broker operates within a worldwide component exchange network.

[SOURCE: IEC TS 62668-1:2016, 3.1.2]

3.1.3
COTS product
commercial off-the-shelf product
one or more components, assembled and developed for multiple commercial consumers, whose design and/or configuration is controlled by the manufacturer's specification or industry standard

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

[SOURCE: IEC TS 62668-1:2016, 3.1.3]

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 willful trademark infringement.

[SOURCE: IEC TS 62668-1:2016, 3.1.4]

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.

[SOURCE: IEC TS 62668-1:2016, 3.1.5]

3.1.6
customer device specification
device specification written by a user and agreed by the supplier

[SOURCE: IEC TS 62668-1:2016, 3.1.6]

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

[SOURCE: IEC TS 62668-1:2016, 3.1.7]

3.1.8
data sheet
document prepared by the manufacturer that describes the electrical, mechanical, and environmental characteristics of the component

[SOURCE: IEC TS 62668-1:2016, 3.1.8]

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 dispatched 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.

[SOURCE: IEC TS 62668-1:2016, 3.1.9]

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 (for example 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.

[SOURCE: IEC TS 62668-1:2016, 3.1.10]

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).

[SOURCE: IEC TS 62668-1:2016, 3.1.11]

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.

[SOURCE: IEC TS 62668-1:2016, 3.1.12]

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

[SOURCE: IEC TS 62668-1:2016, 3.1.13]

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

[SOURCE: IEC TS 62668-1:2016, 3.1.14]

3.1.15
piracy
willful copyright infringement

[SOURCE: IEC TS 62668-1:2016, 3.1.15]

3.1.16
purchasing agency
organization which groups the quantities of electronic components required by a series of companies in order to constitute significant buying power and thereby obtain the best possible supplier conditions for purchasing (especially as regards pricing and purchasing conditions) as well as for assistance with management, documentation, financing, etc.

3.1.17
reseller
general supplier which offers a selection of electronic components to order from a catalogue

[SOURCE: IEC TS 62668-1:2016, 3.1.16]

3.1.18
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.

[SOURCE: IEC TS 62668-1:2016, 3.1.17]

3.1.19
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.

[SOURCE: IEC TS 62668-1:2016, 3.1.18]

3.1.20
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 may 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).

[SOURCE: IEC TS 62668-1:2016, 3.1.19]

3.1.21
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.

[SOURCE: IEC TS 62668-1:2016, 3.1.20]

3.1.22
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.

[SOURCE: IEC TS 62668-1:2016, 3.1.21]

3.1.23
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 handling precautions including ESD and MSL. This authenticates the electronic components being supplied are unused, brand new components with no ESD, MSL or other damage. This ensures that the electronic components are protected by any manufacturer's warranties, have all of their useful life remaining and function according to the manufacturer's published data sheet, exhibiting the expected component life in the application for the OEM's reliability predictions and product warranty.

[SOURCE: IEC TS 62668-1:2016, 3.1.22]

3.1.24
untraceable
property of electronic components which have lost their traceability (see 3.1.23)

[SOURCE: IEC TS 62668-1:2016, 3.1.23]

3.2 Abbreviated terms

ACTF	Semiconductor Industries Association Anti Counterfeit Task Force
ADHP	aerospace, defence and high performance
COTS	commercial off-the-shelf
CEM	contract electronic manufacturer
CSAM	C-mode scanning acoustic microscopy
DSCC	Defence Supply Centre Columbus (see http://www.dscc.dla.mil/), now known as DLA
DLA	Defense Logistics Agency
EMS	electronics manufacturing services
ERAI	Electronic Reseller Association International (see http://www.erai.com)
ESCO	Electronic Systems Challenges and Opportunities (see http://www.esco.org.uk/about-v2/)
ESD	electrostatic discharges
G-19	SAE Counterfeit Electronic Parts Committee
GIDEP	Government-Industry Data Exchange Program
GIFAS	Groupement des Industries Françaises Aéronautiques et Spatiales (French Aerospace Association)
HTRB	high temperature reverse bias
IDEA	Independent Distributors of Electronics Association
LTB	last time buy
LDC	lot date code
MSL	moisture sensitivity level
MTBF	mean time between failure
MTTF	mean time to failure
OCM	original component manufacturer
OEM	original equipment manufacturer
SEM	scanning electron microscopy

4 Technical requirements

4.1 General

IEC TS 62668-1 minimises counterfeiting, recycling and fraudulent activities by providing guidelines and requirements for maintaining intellectual property and recommends purchasing traceable components from the OCMs or their franchised distributors (see Annex A). IEC TS 62668-1 references this part of the IEC 62668 series when purchasing components outside of the franchised distributor network in order to avoid and manage suspect components (see 3.1.22 for the definition of “suspect component” and Figure 1).

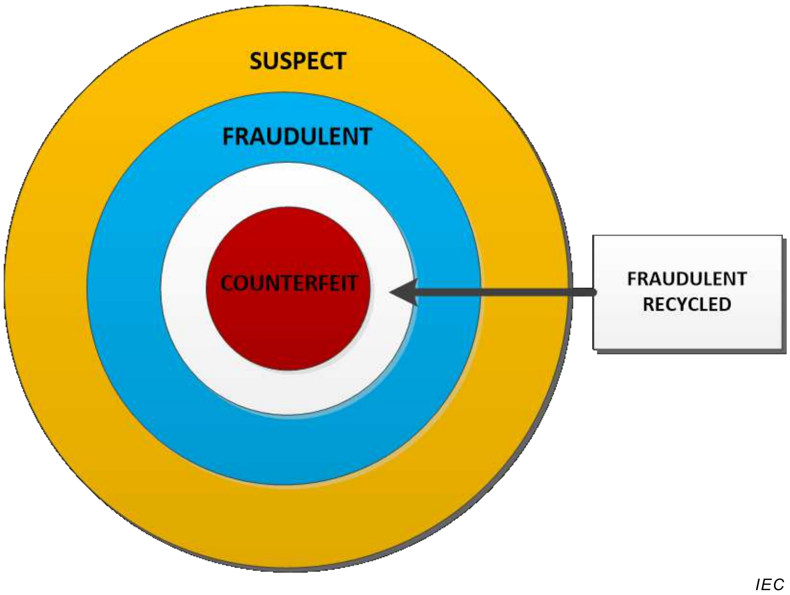

Figure 1 – Suspect components perimeter

4.2 Overview

OEM companies have numerous sourcing channels available to procure components for their equipment. It is the original equipment manufacturer's (OEM) responsibility to ensure that its electronic component procurement process is robust.

As a rule, the original equipment manufacturer, or subcontractor (which includes purchasing agents acting on its behalf), which places orders for these components, orders directly from a component manufacturer, the manufacturer representative or its franchised distributor. This is the only supply system that can guarantee component compliance with specifications and component origin (see IEC TS 62668-1).

Under exceptional circumstances, and after having exhausted all options within the franchised system and after having reviewed other possible alternatives, the OEM may decide to purchase components through a non-franchised distribution network. Purchasing through non-franchised channels is considered a derogation process for which the OEM is fully responsible.

The OEM is responsible for ensuring that its products do not include counterfeit components. Moreover, it guarantees that the reliability of its equipment is not affected when this equipment includes components purchased from non-franchised sources.

The OEM shall have anti-counterfeit management plans in place, to comply with IEC TS 62668-1.

Subclauses 4.3 to 4.5.10 apply to OEMs and their subcontractors when purchasing components from sources of supply other than from the OCM or from franchised distributors.

However, there are the following exclusions to this specification:

1) In situations where purchasing agents are under contract to the OEMs to order components on their behalf, the purchasing agent is considered to be 'the OEM' and is not considered to be a non-franchised distributor.
2) In situations where an approved logistics supply agency, for example the DLA in the USA, supplies components for logistics purposes to a national defence customer and associated OEMs, the approved logistics supply agency is not considered to be a non-franchised distributor.

4.3 Risks associated with purchasing from non-franchised distributors

4.3.1 General

There are the following risks to consider (see 4.3.2 to 4.3.7).

Various risk assessment tools exist which the OEM may consider when assessing risks. For example:

1) ISO 31000 describes risk management and ISO/IEC 31010 describes risk management techniques together with ISO Guide 73 on risk management vocabulary.
2) The iNEMI project on counterfeit components, i.e. its assessment methodology and metric development provides three free internet based anti-counterfeit calculator tools using spreadsheets (see Annex C).
3) SAE AS6171 includes a thorough risk assessment of the supplier, the product, and the application with various adjustment factors (see Annex D); it then defines the type of component anti-counterfeit mitigation testing needed using the SAE AS6171 series of anti-counterfeit component test methods.

This technical specification advises the OEM on the relevant risk assessment test methods that are available for use. It allows the OEM to determine whether all or only part of the SAE AS6171 series is invoked when selecting test methods.

4.3.2 Risk origins

Counterfeit and fraudulent products have been repeatedly identified by electronic equipment manufacturers. The purchase, use and reselling of fraudulent components is illegal. A major difficulty lies in recognizing these fraudulent components, as electronic components may be counterfeited in many ways. Increased market demand encourages this illicit activity and counterfeiters continue to improve their manufacturing processes, the disguises they use and their falsification methods. OEMs shall consequently take increasingly strict measures to mitigate risk. The equipment manufacturer shall take all necessary measures, both internally and with regard to its chosen supplier, to ensure that components acquired are OCM (original component manufacturer) produced, that they have not been modified, remarked, or previously installed in applications, nor undergone testing, that might impact their performance or reliability.

Fraud and specifically counterfeiting of electronic components has most often been detected with components supplied by brokers or non-franchised distributors. Therefore, the information that follows in this document will refer essentially to this type of supplier which cannot generally supply traceability back to the OCM. The electronic equipment manufacturer should remember, however, to use caution when purchasing from any source outside of a franchised network.

4.3.3 Quality risks

4.3.3.1 General

Quality risks include the following.

4.3.3.2 Lots

There is a high risk of receiving non-homogeneous lots of components, having different manufacturing date/codes and produced at various manufacturing sites. A large lot of obsolete components with a single lot date code (LDC) should be considered suspect by the purchaser (risks of refurbished/relabeled components for example).

4.3.3.3 Packaging

The origin and storage conditions of the components proposed by non-franchised distributors are generally unknown. This presents a risk that the components proposed by a non-franchised distributor were not stored under manufacturer-recommended conditions. This is important for components that are sensitive to electrostatic discharges (ESDs) or moisture.

These components may also have been removed from their original packaging and handled without the proper protective measures.

4.3.3.4 Disassembled or recycled components

There is a great risk that these components were recovered from board or equipment at the end of their life cycles or no longer in use. As component removal conditions are strictly unknown, the integrity, performance and reliability of the components cannot be guaranteed.

4.3.3.5 Failed or scrap components

There is also the risk that the proposed components come from OCM lots rejected by a manufacturer or customer after discovery of a manufacturing or specification non-compliance issue.

NOTE Often EMSs dispose of surplus stock onto the open market without identifying if these were scrap parts or good parts. Damaged components from fires, floods, earthquakes, etc., also can be sold onto the open market. These can also be products rejected by the customer due to specific requirements not being met, such as an unsatisfactory parameter sort.

4.3.3.6 Traceability

Purchasing through non-franchised distributors cannot often provide traceability back to the OCM.

NOTE Moreover lack of traceability can lead to supply stolen components or components issued from uncontrolled midnight production. Certificates of conformance can themselves be counterfeited.

4.3.4 Industrial risks

Use of components whose origin is uncertain can result in industrial risks during equipment manufacturing and utilization:

- during production of boards, potential poor storage and handling of components supplied by non-franchised distributors may impact these components. Oxidation, pollution, moisture, warping or imperfect flatness of connections may cause visible or hidden faults during board wiring;
- late detection of defective or counterfeit components during board and/or equipment functional testing may seriously impact management of production and costs, due to potential part scrapping or repair;

- detection of defective or counterfeit components during equipment utilization may require retrofitting the equipment concerned, with probable serious consequences for the OCM.

4.3.5 Reliability risks

Use of components whose origin is uncertain can directly and gravely impact the operational reliability of the equipment concerned.

4.3.6 Financial risks

4.3.6.1 Part costs

Purchasing components from a non-franchised supplier can have impacts on the purchasing costs. The unit price of the component may be extremely high, because of market demand, the degree of obsolescence, and the technical specification and quality levels required for certain applications (defence applications, for example). Requests sent out to numerous brokers can create an inflated, artificial demand for a given inventory, whose price will subsequently rise.

4.3.6.2 Reimbursement

Many brokers, and more generally non-franchised distributors, work exclusively with sales agreements that contain non-cancellation clauses. In some countries once components have been identified as counterfeit they have to be stored for the regional law enforcement bodies and cannot be returned back into the supply chain as in those countries it is illegal to sell counterfeit or fraudulent components.

4.3.7 Legal risk

An electronic equipment manufacturer may be held legally liable for equipment failure having serious consequences. Sourcing components from outside the franchised network makes it nearly impossible to hold the OCM liable for product failure during utilization. Because this type of purchasing does not provide OCM warrantees, only the OEM is held responsible.

The OEM is considered contractually liable for the sale of equipment containing counterfeit or suspect parts. The vendor’s extra-contractual liability (or tort liability) may also be invoked if the sale is considered an act of negligence or carelessness.

Damage caused by failure of components integrated into equipment is covered by the electronic equipment manufacturer’s liability insurance. If the damage results from failure of a counterfeit or suspect component, the electronic equipment manufacturer may be held criminally responsible. These aspects should be considered in the context of the applicable legislation in the countries in which the various supply chain vendors operate.

4.4 Reasons to initialize the derogation process

4.4.1 General

If there are no other reasonable or practical alternatives, then the OEM or the subcontractor shall use the following derogation process when they are considering procuring untraceable components from a non-franchised distributor. This process shall be used in exceptional circumstances and shall not be normal practice.

4.4.2 Obsolescence notice failure

The last time buy (LTB) has expired. No LTB date was published by the manufacturer or the obsolescence process failed to detect the LTB.

4.4.3 Allocation

A shortage caused by high market demand. The supplier cannot provide a firm delivery date.

This situation was not detected or foreseen during the production planning.

4.4.4 Insufficient end-of-life inventory

The end-of-life inventory accumulated at the last time buy (LTB) order is not sufficient for the current program or to fill new orders.

4.4.5 Late orders

Late-stage modifications (quantities, lead time, etc.) were made to production planning. The standard supply period for a needed component is not compatible with the modifications made.

4.4.6 Minimum order quantity

The minimum order quantity greatly exceeds required quantities.

4.4.7 Technical requirements

Upon request of the OEM design authority when the design or manufacturing data pack requires use of a specific version of a component (date/code, mask, production site, lead finish, etc.) that is no longer available through franchised distributors.

4.5 Derogation process

4.5.1 Notification to the OEM

Under the circumstances described in 4.4, the subcontractor shall notify the OEM defined authority of the unavailability of a given component with traceability through the franchised distributor network; AS/EN/JISQ 9120 certified non-franchised distributors which can provide traceability back to the OCM are exempt from these requirements.

Figure 2 describes the derogation process when supplying without traceability from non-franchised distribution.

Figure 3 describes potential avionics supply chain scenarios which may exist.

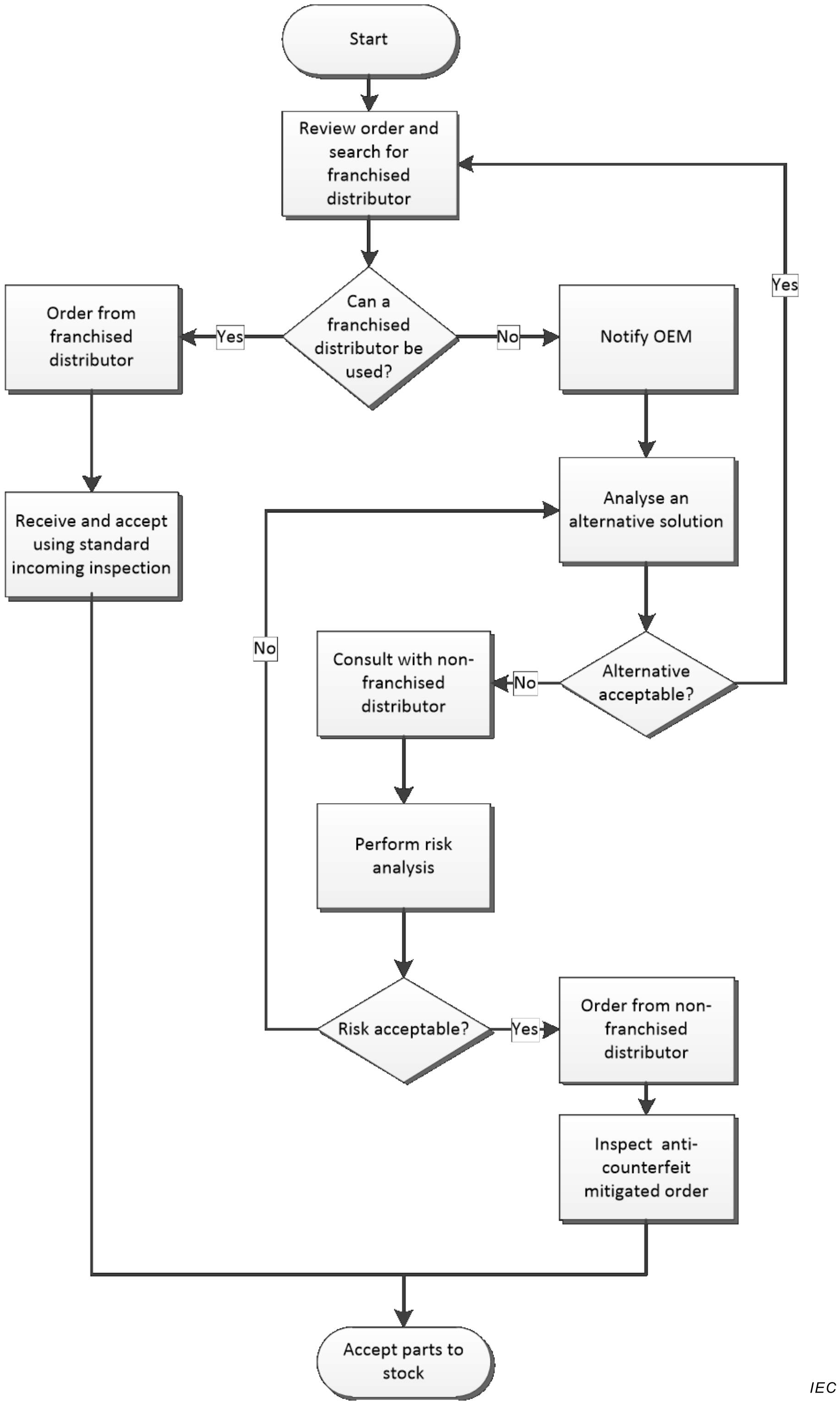

Figure 2 – Derogation process when supplying from non-franchised distribution

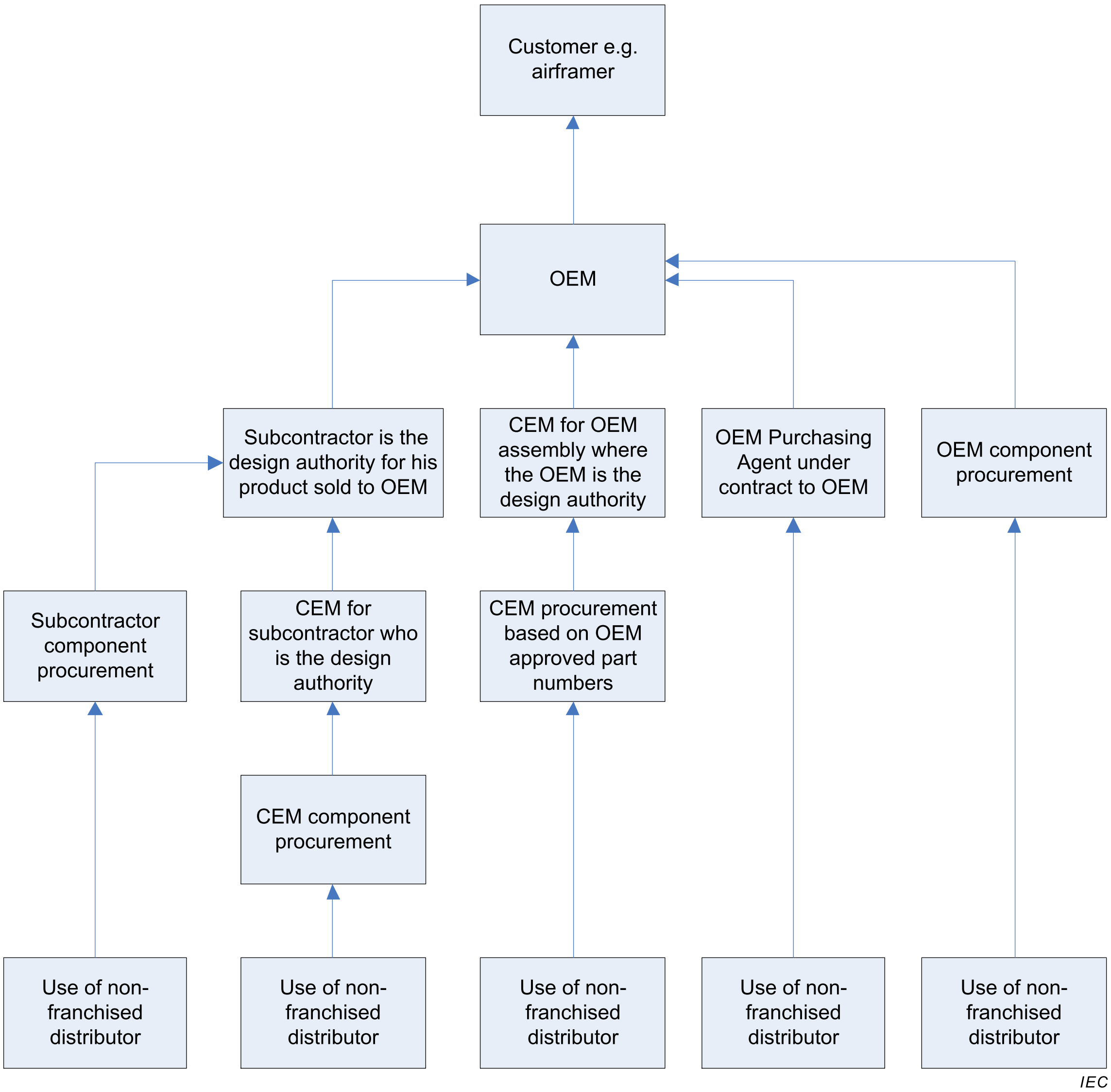

Figure 3 – Potential avionics supply chain scenarios

4.5.2 Analysis of alternative solutions

Alternative solutions shall be examined by the OEM with the subcontractor to take into account the technical and financial impacts for each program concerned, as well as the reasons behind the sourcing difficulty.

The following alternative solutions should take precedence, as they provide the best guarantees with regard to component origin:

a) Definition maintained (no change in the bill of material):
   - Production cycle rescheduled to coincide with the component supply lead time using a franchised network.
   - The individual who defined the need authorizes use of an equivalent component as an alternate solution by waiver.

b) Definition modified (change in the bill of material):
   - Search for components that comply with the original specification through a manufacturer approved by the OCM or by a third-party certifying body (DSCC, etc.).
   - The design authority which defined the need replaces the component or introduces an equivalent component for the application into the nomenclature.

4.5.3 List of approved non-franchised distributors

The OEM or its subcontractor shall maintain a restricted list of approved non-franchised distributors, managed directly through on-site audits.

As minimum, the approved non-franchised distributor shall:

– be a member of a trade organization involved in the detection/fight against fraudulent/counterfeited components, such as ERAI, IDEA, Brokerlinx, etc., or be identified as Trusted Supplier (in compliance with NDAA: H.R.1540 – National Defense Authorization Act for Fiscal Year 2012 / Sec**.** 818. Detection and Avoidance of Counterfeit Electronic Parts – became Public Law No: 112-081 i.e. DFARS 252.246.7007 and DFARS case 2014-D005);

– be in line with international data-sharing organizations related to anti-counterfeiting activities, such as IDEA, ESCO anti-counterfeiting forum, ACTF, GIDEP, etc.;

– have implemented internal rules and means to deal with suspect fraudulent/counterfeited components, i.e. have its own anti-counterfeit management plan (including technical and document management capabilities for reseller business);

– maintain a mini-laboratory at its own disposal, for realizing directly the first steps of inspections (visual inspections at low magnification, photos, acetone tests, etc.);

– have IDEA-ICE-3000 (or equivalent) certified operators for incoming inspection activities;

– own directly in its place an important proprietary components inventory;

– be able to give a pertinent risk analysis for the proposed components, associated with the destructive/non-destructive inspection/test procedure to be processed by the non-franchised distributor for mitigating the risk, before component delivery to the OEM.

It is essential that the non-franchised distributor be able to provide not only its own certificates of conformance for the components it manages, but also whenever possible the certificate of conformance of the entire supply chain back to the component manufacturer and to know the supply chain details of how the components were handled and stored.

Non-franchised distributor approval maintenance criteria include periodic audits, number of counterfeited lots identified by the non-franchised distributor (supply chain efficiency), etc. Whenever possible, non-franchised distributors should also be AS/EN/JISQ 9120 Third Party Certified.

4.5.4 Non-franchised distributor consultation

Information regarding the existence and price of inventories of the component equivalent to the part defined may be obtained through approved non-franchised distributor consultation.

This consultation shall also allow the OEM to collect data for risk analysis of this solution versus other alternate solutions. This data includes:

– origin (original delivery slip, photos of packaging and labeling, etc.);

– part traceability documents;

– component package (type, condition, leads, etc.);

– date codes, parts quantity per date/code and component marking (with photographic evidence);

– copy of component test certificates;

– possibility of performing a pre-delivery conformance test;

– copy of original certificate of conformance;

– payment conditions.

Moreover, the approved non-franchised distributor shall provide its own risk analysis related to the proposed component, together with the mutually agreed detailed inspection/test procedure dedicated to the risk mitigation. The documented inspection/test procedure shall be performed by the approved non-franchised distributor before delivery to the OEM (or its subcontractor), unless the OEM claims to do it by itself.

4.5.5 Risk analysis

The electronic equipment manufacturer shall use the data relative to potential alternate solutions and the data obtained from the various non-franchised distributor consultations (including the risk analysis proposed by the approved non-franchised distributor) and from the OCM to perform risk analysis, as described in 4.3. The OCM may cooperate and confirm if the component lot date codes and part markings are genuine or not.

Table 1 provides some typical procurement scenarios and suggests guidance for procurement risk assessment.

Table 1 – Typical procurement risk scenarios and guidance for procurement risk assessment

1 – Supply from non-franchised distributors (see risks listed in 4.3.3.2 to 4.3.3.6)		
1	Comments	AS/EN/JISQ 9120 certification requires distributors to state clearly on all bids, invoices and orders if components are being supplied without traceability.
1	Low risk	Traceable components purchased from OEM approved and audited non-franchised distributors which are AS/EN/JISQ 9120 certified.
1	Medium risk	--
1	High risk	--
1	Very high risk	Untraceable components purchased from non-franchised distributors which are AS/EN/JISQ 9120 certified.

2 – Traceability paperwork was lost (see risk listed in 4.3.3.6)		
2	Comments	Components where the OEM has lost internal traceability paperwork are genuine and not counterfeit, recycled or fraudulent. In some situations the franchised distributor may have evidence that the components were originally traceable. In these situations the OEM may wish to review how these components have been stored and test them accordingly. Components where the supplier claims they have lost the traceability but have no evidence are considered high risk.
2	Low risk	--
2	Medium risk	Components received with full traceability into an OEM which has subsequently lost this paperwork internal to its organization and wishes to assemble them into its products.
2	High risk	Components whose paperwork has been lost externally between the franchised distributor and the OEM, where the supplier has some evidence to prove that the components originally had traceability.
2	Very high risk	Components whose paperwork has been lost by the distributor or broker which cannot prove that it ever existed.

3 – Apparent reworked component (see risks listed in 4.3.3.2 and 4.3.3.4)		
3	Comments	Traceable reworked (i.e. altered items) components which are re-identified but which are controlled by the OEM through specifications and part numbers cross referenced to the base part, are not counterfeit, recycled or fraudulent components.
3	Low risk	Traceable components which have been reworked by either OEM controlled external suppliers or internally at the OEM and re-identified because they are ‘altered items’, for example re-balled microcircuits, components where the terminations have been tin/lead solder dipped.
3	Medium risk	--
3	High risk	--

3 – Apparent reworked component (see risks listed in 4.3.3.2 and 4.3.3.4)		
3	Very high risk	Externally reworked components which have lost traceability back to the original manufacturer of the part selected for rework, where the supplier has some evidence to prove that the components had traceability (this is mandatory when the supplier doesn't have that evidence. The use of that component is strictly forbidden and is incompatible with avionics applications).

4 – Use of surplus components (see risk listed in 4.3.3.5)		
4	Comments	An OEM often provides traceable components to a CEM and then requests the surplus stock back. Occasionally this stock is shipped back without any traceability paperwork or information and requires assessment to determine if it is useable or not.
4	Low risk	Traceable surplus components returned with their paperwork from an OEM audited and approved CEM for use at the OEM.
4	Medium risk	Surplus components returned from an OEM audited and approved CEM for use at the OEM, where the CEM can prove that the parts were originally ordered and received with traceability for example from the OEM.
4	High risk	--
4	Very high risk	Untraceable surplus components returned from a CEM for use at the OEM.

5 – Order by an independent purchasing agency (see risks listed in 4.3.3.2 to 4.3.3.6)		
5	Comments	Components purchased without traceability are always high risk components. All independent purchasing agencies or distributors need to be assessed and audited to mitigate against their supplying untraceable stock.
5	Low risk	Traceable components ordered by an OEM approved purchasing agency which is under contract and acting on behalf of the OEM.
5	Medium risk	Traceable components ordered by an independent purchasing agency or distributor not under contract to the OEM.
5	High risk	--
5	Very high risk	Untraceable components ordered by an independent purchasing agency or distributor.

6 – Supply from non-franchised distributors (see risks listed in 4.3.3.2 to 4.3.3.6)		
6	Comments	The OEM shall approve all sources of supply before they are added to the OEM approved supplier list. On-line brokers need to be assessed using procurement tolls.
6	Low risk	Traceable components purchased from the OEM approved OCM or their OEM approved franchised distributors.
6	Medium risk	
6	High risk	Traceable components purchased from non-franchised distributors or brokers which are not AS/EN/JISQ 9120 certified.
6	Very high risk	Untraceable components purchased from independent distributors or on-line brokers.

7 – When the OCM has just gone bankrupt (see risk listed in 4.3.3.6)		
7	Comments	Traceability documentation can be counterfeited. Franchised distributors should be able to assist with defining the last lot date codes the OCM manufactured. Independent distributors need to be assessed particularly against the ERAI database, etc. There is a risk here that needs to be investigated further, particularly if the OCM's quality data is lost completely.
7	Low risk	Traceable components purchased from an OEM approved franchised or an AS/EN/JISQ 9120 certified non-franchised distributor when the OCM has just gone bankrupt.
7	Medium risk	--
7	High risk	--
7	Very high risk	Components which are being offered with traceability from an independent distributor where the OCM has just gone bankrupt and did not issue any information defining its final deliverable lot date codes.

8 – When the OCM has been purchased by another manufacturer (see risk listed in 4.3.3.6)		
8	Comments	--
8	Low risk	Traceable components purchased from an OCM or an OEM approved franchised distributor when the OCM has just been purchased by another manufacturer and the OCM has issued information regarding the lot dates codes when the components are marked with the new logo.
8	Medium risk	Traceable components purchased from an OEM non-approved non-franchised distributor when the OCM has just been purchased by another manufacturer with no further information.
8	High risk	--
8	Very high risk	Components offered from independent distributors and brokers when the OCM has been purchased by another manufacturer with no further information.

9 – Obsolete components (see risks listed in 4.3.3.2 to 4.3.3.6)		
9	Comments	--
9	Low risk	Obsolete components purchased with traceability from the franchised aftermarket distributor.
9	Medium risk	Obsolete components purchased with traceability from the non-franchised distributor.
9	High risk	--
9	Very high risk	Obsolete components purchased from a broker on the internet with no traceability back to the OCM.

The conclusions of this risk analysis may lead the OEM to agree to purchase components from a non-franchised distributor.

Certain risk indicators shall be considered:

- A lot size too large for a same date/code may indicate that the components are counterfeit.
- Vast differences in date/codes may indicate that the components are recovered scrap, which represents a significant quality risk.
- Bulk packaging may hide counterfeit components (hidden in the middle of a strip, for example).
- Incoherence between the printed date/code and the official last production date is a blatant example of counterfeit marking.
- Inaccuracy or uncertainty with regard to component origin or history can be a sign of fraudulent business activity.

Mitigation techniques, based on greater supplier auditing and component inspections, are described in 4.5.8.2, Table 2, and Annex B.

4.5.6 Non-franchised distributor order authorization

The individual who defined the need shall draft a written authorization for supply through the selected non-franchised distributor. According to the conclusions of risk analysis conducted by the OEM (with the selected approved non-franchised distributor), this authorization shall include specific requirements and/or detail the non-franchised distributor supply inspection and testing procedure to be performed by the non-franchised distributor (unless the OEM claims to do it by itself) before delivery, to guarantee the compliance of the components delivered (reinforced incoming inspection, qualification tests, reliability tests, destructive physical analysis, counterfeit detection, etc.).

4.5.7 Order processing

In addition to general requirements for all orders, the information collected during the non-franchised distributor consultation (see 4.5.4) shall be included in order to secure supplier terms and conditions and manage potential discrepancies at delivery. The following requirements shall be mentioned:

– date codes,
– lots sizing,
– conformance certificate delivered,
– risk analysis related to the proposed components,
– detailed non-franchised distributor supply inspection and testing procedure and results before delivery (if the tests flow was performed directly by the non-franchised distributor).

Consequently, the control of the order receipt is particularly important to check the supplier commitment against the order requirements.

4.5.8 Incoming processing

4.5.8.1 General

For deliveries of orders made through non-franchised distributors, the incoming department which may be at the OEM facilities or at their approved subcontractor ones (e.g. test laboratory) shall be informed of the type of supplier and the associated inspection/tests requirements for this type of order. These operations shall be performed by trained operators aware of the risks associated with counterfeit components and fraudulent products. Specific requirements or the non-franchised distributor supply inspection and testing procedure mentioned in the order authorization shall be followed (detailed documentary evidence/photographs and tested components shall always be provided by the non-franchised distributor with the supplied components, if the tests flow was performed directly by the non-franchised distributor).

Where specialist external test laboratories are used to inspect suspect stock, they shall be AS/EN/JISQ 9100 certified.

4.5.8.2 Administrative compliance

All documents relating to the order shall be included at delivery and be authentic (manufacturer and/or reseller conformance certificates and packing slips (based on NIGP 111.00), inspection and/or test reports, measurements, analysis reports, etc.).

The date codes of the delivered components shall comply with those provided in the shipping documents and in the order. These date codes shall be verified for all delivered parts by checking the component marking (when marked by the manufacturer). For components delivered in strips and/or dry packs, this operation may require specific unpacking and repacking means.

Component packaging shall be checked to ensure that it meets the specific requirements set out in the order.

4.5.8.3 Technical compliance

In the absence of the OCM’s original warrantee certificate, and depending on the reliability of the information available by the reseller, specific inspection and testing protocols shall be implemented to ensure that supplied components are not counterfeit or of poor quality.

In addition to specific requirements set forth upon ordering, packaging shall be inspected and components shall be properly fitted in their packaging, in the correct orientation, if applicable. Components with different production date codes shall be packaged separately. All other types of anomaly shall be conveyed to the inspector as a potential risk with regard to component origin.

SAE AS6171/1 contains information about how to create a component anti-counterfeit mitigation test plan depending on the risk and test coverage desired.

Alternatively the following inspections, wherever possible compared to known good authentic samples (see Table 2 and Annex B), should be carried out in order of priority, according to the risks identified:

a) Constitution of inspection lots

   The verification of date codes allows inspection lots to be created. One inspection lot per date code should be created as testing is on a manufacturer's lot date code basis. Be wary of components packaged onto a reel as they may not be of one lot date code.

b) Visual inspection to IDEA-STD-1010 or SAE AS6171/2, the data sheet and any relevant test methods for the following:

   1) Physical dimension verification: check compliance with the manufacturer specifications as well as the consistency of the dimensions of all components in a same lot, in order to detect rework (package sanding, etc.).

   2) Marking verification: verify that the component was not remarked; verify marking coherence with the original components or documents (manufacturer logo, component reference, production date code, production line or site code, release code, "direction mark", etc.) using resistance to solvents techniques, micro blasting, quantitative surface analysis (QSA), etc., where considered appropriate.

   3) Encapsulant verification: verify the consistency of encapsulants for each production date code. For plastic-encapsulated integrated circuits, verify the consistency of resin color and appearance, as well as the consistency and legibility of the molding stamp. This stamp is generally located on the underside of the component. Verify package geometry and look for evidence of sanding or reworking on plastic package.

   4) Pin or ball verification: check specifically for component integrity, the absence of oxidation, warping, cracks, evidence of repair or prior use (traces of tinning, broken or bent pins, damaged balls, bridged pins or balls, missing solder balls, etc.).

   5) Inspection of ESD and moisture barrier bags, humidity indicator cards, per IPC JEDEC J-STD-033 or equivalent if required for sensitive electronic components.

c) Non-destructive physical analysis

   1) X-ray imaging:

      i) Inspection of the component's internal assembly and its consistency in the lot inspected.

      ii) Checking for presence of chips with identical dimensions, presence of bonding leads, and lead frame structure.

      iii) Verification of absence of die cracks, voids in the die attach.

   2) CSAM acoustic microscopy. Verification of the absence of delamination, whose presence would indicate that the component has been subjected to mechanical stress for example caused by desoldering during recycling operations.

d) Destructive physical analysis

   1) Different methods can be performed at component level for internal inspection according to the risk cause:

      i) Mechanical or chemical removal of lid, or top layers of the component body to expose the die and internal structures.

      ii) Chemical dissolution of the plastic after jetting various acids onto the surface of the component.

      iii) Laser decapsulation as alternative to chemicals which are not always appropriate.

   2) Tests to perform:

i) Solderability or wettability tests.

ii) Visual inspection of the component's internal assembly comparing it against a 'good 'component.

iii) Verification of chip geometry and marking, and its coherence with manufacturer data (manufacturer logo, mask reference, etc.).

iv) Bonding tensile strength.

v) SEM analysis.

e) Electrical tests

These are tests conducted at room temperature on a per unit or sampling basis, depending on the inspection lot and/or package size, in order to verify the electrical characteristics specified by the manufacturer. These tests may be accompanied by tests at operating temperature and life testing, depending on the level of quality required and the criticality of the application.

f) Material characterization:

If relevant, for advanced analysis of termination plating materials, moulding compound, attached materials, laminate or substrate materials for component with interposer, etc., different techniques could be considered, particularly by comparison with authentic samples.

All electrical and physical tests and analyses shall be performed by a specialist and recognized laboratory.

The typical tests identified in Table 2 should be performed. If performed, these tests should be conducted in the order stated.

Where yields are less than 90 % (tests 8 and 9) a review shall be carried out of all data to determine if it is acceptable to use the components.

A detailed test list is given for example in Annex B, linked with procurement risks levels.

Table 2 – Typical testing

Test	Method	Sample size	Destructive test	Comments
1. Visual inspection	Use IDEA-STD-1010 as a minimum requirement and the manufacturer's data sheet, up to ×30 or higher magnification and MIL-STD-883 method 2010, IPC JEDEC J-STD-033 for correct MSL packaging, and/or SAE AS6171/2 or equivalent. Also inspect all lot dates codes, certificates of conformance and packing slips using NIGP 111.00 to ensure part number, lot date code and signatories are accurate against the purchase order requirements.	100 % of the lot	No	Look for evidence of prior use, check for 'black-topping', etc., including checking part marking and dimensions. Check against authentic baseline parts and/or archived information on authentic baseline parts.
2. Package testing	Lead material analysis, marking permanency and solderability testing. Or use SAE AS6171/3, SAE AS6171/2, SAE AS6171/8, and SAE AS6171/9 or equivalent documents.	Three components per OCM lot	Yes	Confirm package material, lead-free termination material, marking permanency, solderability, etc.

Test	Method	Sample size	Destructive test	Comments
3. Destructive physical analysis (DPA)	Use MIL-STD-1580 where applicable, or SAE AS6171/4 or equivalent.	Three components per OCM lot	Yes	Check for good workmanship standards, internal materials consistency, contamination, die orientation, check die metallisation marking with manufacturer, wire bonding arrangement, etc.
4. X-ray	Use SAE AS6171/5 or equivalent.	100 % of the lot	No	Show consistency of manufacturing of each lot and correlate to original die. Check against authentic baseline parts and/or archived information on authentic baseline parts.
5. Acoustic microscopy	Use SAE AS6171/6 or equivalent.	Three components per OCM lot		For plastic encapsulated components, look for internal voids and poor workmanship.
6. Functional DC electrical test at room temperature	Verify to data sheet. Percent defective no greater than 10 %. Yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance. This is an optional test but recommended so that the burn-in yield can be established.
7. Burn-in screening	Microcircuits: use MIL-STD-883 method 1015, 168 hours at +125 ºC with voltage bias applied. Diodes and transistors: use high temperature reverse bias (HTRB) per MIL-PRF-19500:2012, screening requirements, Table E-IV. Ceramic chip resistors: conduct thermal shock to MIL-STD-202 method 107 un-mounted test condition F (5 cycles) except that temperatures shall be +150 °C to –65 °C. Ceramic chip capacitors: conduct voltage conditioning per MIL-PRF-55681 group A subgroup 1 inspection. Leaded ceramic capacitors: conduct thermal shock and voltage conditioning per MIL-PRF-39014 group A subgroup 1. Tantalum capacitors: conduct thermal shock, surge current when specified in part number, voltage aging (CSR91 style only) per MIL-PRF-39003 group A subgroup 1. Or SAE AS6171/7 or equivalent.	100 % of the lot or sample test	No	Confirm there are no infant mortality failures.
8. Functional DC electrical test at room temperature	Yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance.
9. Functional DC electrical test at $T_{min.}$ and $T_{max.}$ °C	Yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance.

4.5.9 Records

The results of all inspections and tests shall be recorded and archived to provide traceability and contribute to an ongoing lessons-learned process.

4.5.10 Processing during storage and manufacturing

For components that must be packaged in a dry atmosphere, and when compliance with dry chain conditions cannot be guaranteed, applicable internal procedures for repackaging shall be applied. According to inspection and test results, storage and assembly recommendations may be provided to relevant manufacturing departments (baking, terminal re-tinning, etc.).

During the storage and manufacturing phases, the traceability of component batches shall be guaranteed. Traceability per date code shall be guaranteed in the production from receipt up to customer level. When necessary, parts may be identified by a specific internal reference or some other identification system (colored dot, label, etc.).

4.5.11 Failed electronic components

Electronic components that fail testing shall be immediately marked as failed suspect counterfeit components and stored in special anti-counterfeit quarantine storage for a review by quality and legal teams. The failed suspect counterfeit components shall not be returned to the supplier or to the OCM, or retransferred to the OEM if testing is performed outside the OEM facility. Reporting to the end customer is typically required together with any special reporting requirements as defined in the customer contract (for example USA DFARS 252.247.7007 reporting requirements). Reporting to local law enforcement may also be required. The legal team will advise when and how to dispose of these failed components depending on local law.

Annex A
(informative)

Flowchart of IEC TS 62668-1 requirements

Annex A introduces the flowchart of the IEC TS 62668-1 requirements (see Figure A.1).

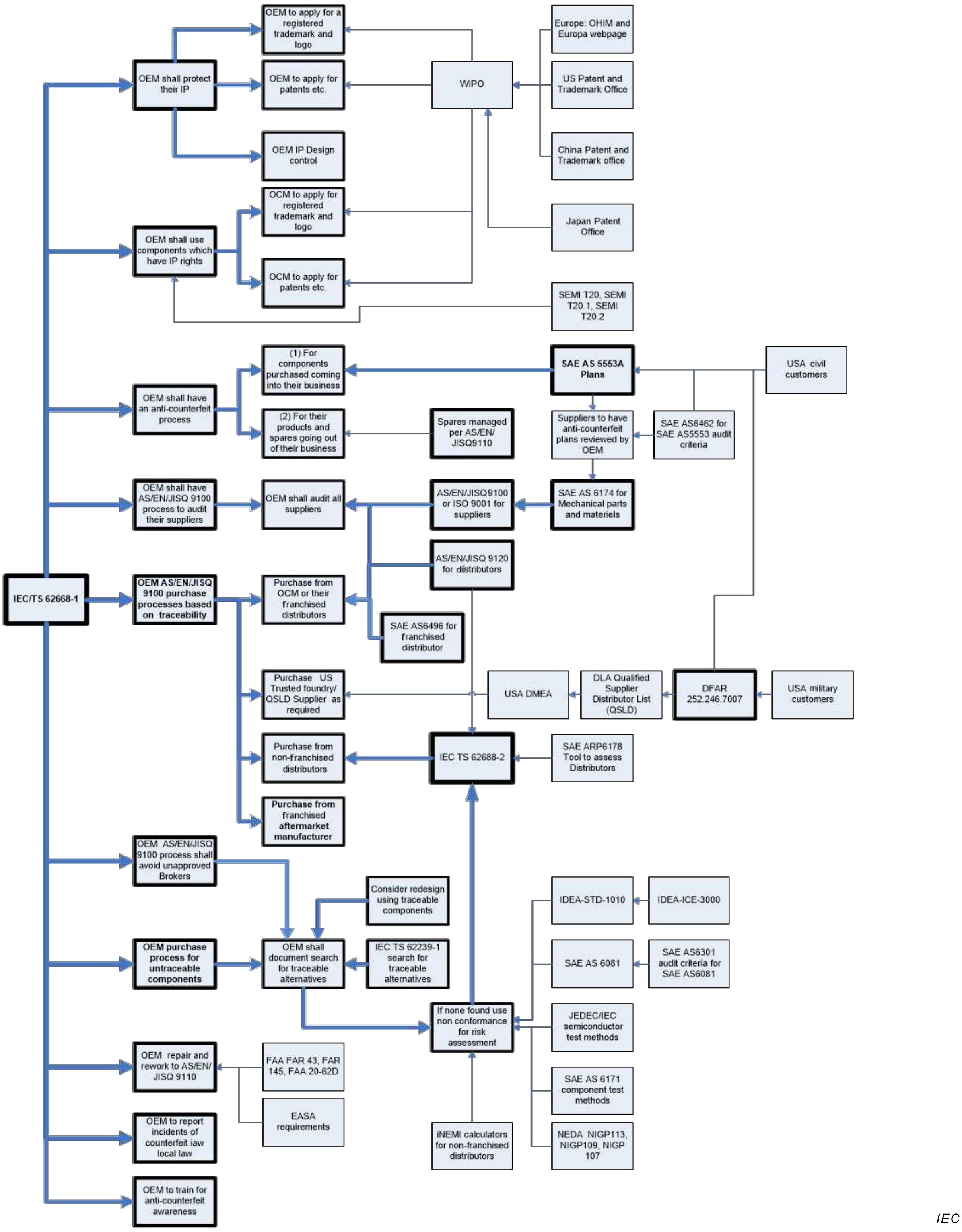

Figure A.1 – Flowchart of IEC TS 62668-1 requirements

Annex B
(informative)

Example of detailed tests list, linked with procurement risks levels

Table B.1 gives an example of detailed revalidation testing of suspect stock, depending on procurement risk assessment (see Table 1).

For low risk, the focus is on additional supplier auditing and improved relationship.

Table B.1 – Example of detailed revalidation testing of suspect stock

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Visual inspection	Use IDEA-STD-1010 and/or and MIL-STD-883 method 2010 and the manufacturer's data sheet, up to x30 magnification to look for evidence of (a) prior soldering or de-soldering (b) to record part marking/exterior packaging marking (including ESD and MSL marking per IPC JEDEC J-STD-033) for comparison to a genuine part and/or review by manufacturer. All deliverable paperwork shall also be inspected and cross checked using for example NIGP 111.00 to ensure part number, lot date code and signatories are accurate. Or use SAE AS6171/2 or equivalent.	100 % of the lot	No	Look for evidence of prior use, check for 'black-topping', etc., including checking part marking and dimensions. Check against authentic baseline parts and/or archived information on authentic baseline parts.	Yes	Yes	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Package testing	Lead material analysis using XRF testing where results are compared against that specified by the OCM. Test methods include ASTM B487, ASTM B568 or MIL-STD-1580 or equivalent, or SAE AS6171/3 or equivalent. Marking permanency shall as a minimum be tested in accordance with JESD22-B107D or equivalent test methods, or SAE AS6171/2 or equivalent. Use the new surface analysis test methods and new solvents as required to detect counterfeit marking per SAE AS6171/8 or equivalent. Analyse the package material per SAE AS6171/9 or equivalent. Conduct solderability testing per IPC JEDEC J-STD-002.	Three parts per OCM lot	Yes	Confirm package material, lead-free termination material, marking permanency, solderability, etc.	Yes	Yes	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Destructive physical analysis (DPA) which includes SEM analysis	Use MIL-STD-1580 where applicable. Three components shall be de-encapsulated or de-lidded and the semiconductor die or passive design element photographed, with particular attention being made to photographing any die metallization markings or OCM original markings on the exterior and interior of the component. Where possible the OCM shall be contacted to establish whether the die or passive design element is authentic and/or results should be compared to a 'good authentic sample'. Or use SAE AS6171/4 or equivalent. And/or use SAE AS6171/11 or equivalent.	Three parts per OCM lot	Yes	Check for good workmanship standards, internal materials consistency during assembly of a given lot number, contamination, die orientation; check die metallisation marking with manufacturer, wire bonding arrangement, etc.	Optional	Yes	Yes
X-ray	Use MIL-STD-883 method 2012 at the lowest possible voltage to confirm OCM package dimensions, internal wire bonding, internal termination arrangement, semiconductor die sizes and internal passive component features which can then be compared to a genuine component. The OCM may need to be contacted for information on a genuine part or SAE AS6171/5 or equivalent.	100 % of the lot	No	Show consistency of manufacturing of each lot and correlate to original die. Check against authentic baseline parts and/or archived information on authentic baseline parts.	Yes	Yes	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
CSAM	Scan from above, bottom and sideways. Share results with the OCM. There will always be some evidence of minor voiding in genuine parts. However, large areas of delaminations should not be observed. Or use SAE AS6171/6 or equivalent.	Sample	Yes	Scanning electron microscopy can be used to look for delaminations within encapsulated components indicating poor workmanship quality.	Optional	Optional	Yes
Functional DC electrical test at room tempera-ture	Conduct electrical test to published data sheet parameters or to select key data sheet parameters on a read and record basis, where the percent defective allowed is no greater than 10 %, i.e. yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance and yield. Typical electrical test production yields should be > 99 % so any failures are suspicious.	Yes	Yes	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Burn-in screening	Microcircuits: use MIL-STD-883 method 1015, 168 h at +125 ºC with voltage bias applied on a read and record basis. Diodes and transistors: conduct high temperature reverse bias (HTRB) per MIL-PRF-19500:2012 screening requirements Table E-IV. Ceramic chip resistors: conduct thermal shock to MIL-STD-202 method 107 un-mounted test condition F (5 cycles) except that temperatures shall be 150 °C to –65 °C. Ceramic chip capacitors: conduct voltage conditioning per MIL-PRF-55681 group A subgroup 1 inspection. Leaded ceramic capacitors: conduct thermal shock and voltage conditioning per MIL-PRF-39014 group A subgroup 1. Tantalum capacitors: conduct thermal shock, surge current when specified in part number, voltage aging (CSR91 style only) per MIL-PRF-39003 group A subgroup 1. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm there are no infant mortality failures.	Optional	Optional	Yes
Functional DC electrical test at room temperature	Conduct electrical test to published data sheet parameters or to select key data sheet parameters on a read and record basis, where the percent defective allowed is no greater than 10 %, i.e. yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance. Yields should be very high and are suspicious if not.	Optional	Optional	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Functional DC electrical test at $T_{min.}$ and $T_{max.}$ °C	Conduct electrical test to published data sheet parameters or to select key data sheet parameters on a read and record basis, where the percent defective allowed is no greater than 10 %, i.e. yield no less than 90 %. Or use SAE AS6171/7 or equivalent.	100 % of the lot	No	Confirm data sheet performance. Yields should be high.	Optional	Yes	Yes

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Qualification testing	Either qualify samples within the final assembly qualification process or qualify at the component level. Suggested component qualification testing at the component level can be based on AEC Q100, AEC Q101 or AEC Q200 or JESD47 or IEC TS 62686-1 or as follows: Life testing: – Microcircuits: use JESD22-A108 or MIL-STD-883, 1 000 h at T_a=125 °C. – Memories: conduct write/erase endurance per MIL-STD-883 method 1033 or JESD47 NVCE or JESD94 for the application. – Transistors and diodes: use MIL-STD-750, 1 000 h at 150 °C or 175 °C or intermittent operating life testing. – Resistors and capacitors: conduct load life per MIL-STD-202 method 108, or IEC 60115-8 for 1 000 h. – Other components: use MIL-STD-202 method 108, 1 000 h at max temp or equivalent. Humidity testing: – Microcircuits, diodes and transistors: use JESD22-A101 THB, testing at 85 °C/85 % RH for 1 000 h biased. – Passives: use MIL-STD-202 method 106 or IEC 60068-2-78. – Other components: use MIL-STD-202 method 106 or equivalent.	77 45	Yes		Optional	Optional	Yes. For flight critical applications where there is no circuit redundancy and the possibility of a single point failure. The lot size available has to be large (>170 parts + number of parts needed) if qualifying at the component level

Test	Method	Sample size	Destructive test	Comments	Medium risk assessment 1 testing	High risk assessment 2 testing	Very high risk assessment 3 testing
Qualification testing continued	Temperature cycling – Microcircuits: use JESD22-A104 or MIL-STD-883 method 1010 temperature cycling 1 000 h at –55 °C to +125 °C. – Diodes and transistors: use MIL-STD-750 method 1051 temperature cycling 1 000 h at –55 °C to +125 °C. – Passives: use MIL-STD-202 method 107 or IEC 60068-2. – Other components: use MIL-STD-202 method 107 or equivalent.	45	Yes		Optional	Optional	Yes. For flight critical applications where there is no circuit redundancy and the possibility of a single point failure. The lot size available has to be large (>170 parts + number of parts needed) if qualifying at the component level
If performed, these tests should be conducted in the order stated.							

Annex C
(informative)

iNEMI assessment methodology and metric development

The iNEMI webpage http://www.inemi.org/content.asp?contentid=97 describes the assessment methodology and metric development.

The iNEMI counterfeit risk assessment calculator tools are available at http://inemi.membershipsoftware.org/content.asp?contentid=456

These anti-counterfeit calculator tools are designed to analyse:

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

These tools are free to download and use. For further information, contact Mark Schaffer (marks@inemi.org) or email infohelp@inemi.org for instructions.

The webpage http://www.inemi.org/content.asp?contentid=262 provides the access to iNEMI's white paper on this subject, see http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf which explains the background to these calculator tools.

Annex D
(informative)

Summary of SAE AS6171 proposed test methods under consideration by SAE International

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

The SAE G-19 Counterfeit Electronic Parts committee (see webpage http://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG19) is currently working to publish the documents mentioned in Table D.1. These documents are currently in draft form.

Table D.1 – Summary of SAE AS6171 test methods (under considerations)

SAE document	Title	Scope
AS6171[1]	Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts	This document standardizes practices to detect suspect counterfeit electronic parts, to maximize the use of authentic parts, and to ensure consistency across the supply-chain for test techniques and requirements.
AS6171/1[2]	Suspect/Counterfeit Test Evaluation Method	This document describes an evaluation method which measures the effectiveness of a specified test plan used to screen for counterfeit parts. The method includes the determination of the types of defects detected using a specified test plan along with the related counterfeit type coverage. The output of this evaluation will produce the counterfeit defect coverage (CDC), the not-covered defects (NCD), the under-covered defects (UCD), and the counterfeit type coverage (CTC). This information will be supplied to the test laboratory's customer in both the test report and the Certificate of Quality Conformance. This evaluation method does not address the effectiveness of detecting tampered type devices.
AS6171/2[3]	Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Test Methods	This document describes the requirements of the following test methods for counterfeit detection of electronic components: General External Visual Inspection (EVI), Detailed External Visual Inspection, Remarking and Resurfacing, Lead Finish Analysis, SEM Surface Analysis.
AS6171/3[4]	Techniques for Suspect/Counterfeit EEE Parts by X-Ray Fluorescence Test Methods	XRF technique for counterfeit detection is applicable to electronic and other parts as listed in the AS6171 General Requirements. In general, the detection technique is meant for use on piece parts prior to assembly on a circuit board or on the parts that are removed from a circuit board. The applicability spans a large swath of active, passive and electromechanical parts.

[1] Reprinted with permission from the draft version of SAE document AS6171 (c) 2016 SAE International.

[2] Reprinted with permission from the draft version of SAE document AS6171/1 (c) 2016 SAE International.

[3] Reprinted with permission from the draft version of SAE document AS6171/2 (c) 2016 SAE International

[4] Reprinted with permission from the draft version of SAE document AS6171/3 (c) 2016 SAE International

SAE document	Title	Scope
AS6171/4[5]	Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Methods	This method standardizes inspection and test procedures and minimum training and certification requirements to detect Suspect, Fraudulent, & Counterfeit (SFC) Electrical, Electronic, and Electromechanical (EEE) components or parts utilizing Delid/Decapsulation Physical Analysis. The requirements of this document are employed to either delid or remove the cover from a hermetically sealed package or to remove the outer protective coating or encapsulation of an EEE Part, in order to examine the internal structure to determine if the part appears authentic. Information derived may be used to: a. preclude installation of inauthentic parts or parts having obvious or latent defects b. aid in disposition of parts that exhibit anomalies c. aid in defining improvements or changes in design, materials, or processes d. evaluate Supplier production trends. This test method should not be confused with Destructive Physical Analysis as defined in MIL-STD-1580.
AS6171/5[6]	Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods	The intent of this document is to define the methodology for suspect parts inspection using radiological inspection. The purpose of radiology for suspect counterfeit part inspection is to detect deliberate misrepresentation of a part, either at the part distributor or OEM level. Radiological inspection can also potentially detect unintentional damage to the part resulting from improper removal of part from assemblies, which may include, but is not limited to, prolonged elevated temperature exposure during desoldering operations or mechanical stresses during removal. Radiological inspection of electronics includes film radiography and filmless radiography such as digital radiography (DR), real time radiography (RTR), and computed tomography (CT). Radiology is an important tool used in part authentication of microelectronic devices. Radiographic analysis is performed on parts to verify that the internal package or die construction is consistent with an exemplar item.
AS6171/6[7]	Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods	Through the use of ultra-high frequency ultrasound, typically above 10 MHz, Acoustic Microscopy (AM) non-destructively finds and characterizes physical features and latent defects (visualization of interior features in a layer by layer process) — such as material continuity, sub-surface flaws, cracks, voids, delaminations and porosity. AM observed features and defects can be indicators that the components were improperly handled, stored, altered or previously used.
AS6171/7[8]	Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods	The scope of this document is to: 1. Specify techniques to detect suspect SFC parts using electrical testing. 2. Provide various levels of electrical testing that can be used by end user to define test plans for detecting SFC parts. 3. Provide guidelines to end users for determining which test houses have the necessary capabilities. (i.e., equipment, procedures and protocols) for performing electrical testing for authenticity analysis.
AS6171/8[9]	Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods	To define capabilities and limitations of Raman spectroscopy as it pertains to counterfeit detection of EEE parts and suggest possible applications to these ends. Additionally, this document outlines requirements associated with the application of Raman spectroscopy including: Operator training; Sample preparation; Data interpretation; Computerized spectral matching including pass/fail criteria; Equipment maintenance; and Reporting of data.

5 Reprinted with permission from the draft version of SAE document AS6171/4 (c) 2016 SAE International.

6 Reprinted with permission from the draft version of SAE document AS6171/5 (c) 2016 SAE International.

7 Reprinted with permission from the draft version of SAE document AS6171/6 (c) 2016 SAE International.

8 Reprinted with permission from the draft version of SAE document AS6171/7 (c) 2016 SAE International.

9 Reprinted with permission from the draft version of SAE document AS6171/8 (c) 2016 SAE International.

SAE document	Title	Scope
AS6171/9[10]	Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods	This document defines capabilities and limitations of FTIR as it pertains to counterfeit electronic component detection and suggests possible applications to these ends. Additionally, this document outlines requirements associated with the application of FTIR including: operator training, sample preparation, various sampling techniques, data interpretation, computerized spectral matching including pass/fail criteria, equipment maintenance, and reporting of data. The discussion is primarily aimed at analyses performed in the mid-infrared (IR) from 400 to 4 000 wavenumbers; however, many of the concepts are applicable to the near and far IR.
AS6171/10[11]	Technique for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Method	This test method provides the capabilities, limitations, and suggested possible applications of TGA as it pertains to the detection of counterfeit electronic components. Additionally, this document outlines requirements associated with the application of TGA including: equipment requirements, test sample requirements, methodology, control and calibration, data analysis, reporting, and qualification and certification.
AS6171/11[12]	Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods	This method outlines the requirements, capabilities, and limitations associated with the application of Design Recovery for the detection of counterfeit electronic parts including: Operator training; Sample preparation; Imaging techniques; Data interpretation; Design/functional matching; Equipment maintenance and; Reporting of data. The method is primarily aimed at analyses performed by circuit delayering and imaging with a scanning electron microscope or optical microscope; however, many of the concepts are applicable to other microscope and probing techniques to recover design data. The method is not intended for the purpose of manufacturing copies of a device, but rather to compare images or recover the design for determination of authenticity.
AS6171/12[13]	Techniques for Suspect/Counterfeit EEE Parts Detection of Capacitors By Acoustic Microscopy (AM) Test Methods	Acoustic Microscopy Test Methods for Counterfeit Capacitors
AS6171/13[14]	Technique for Suspect/Counterfeit EEE Parts Detection by Secondary Ion Mass Spectrometry (SIMS) Test Method	To define capabilities and limitations of SIMS as it pertains to counterfeit detection of EEE parts and suggest possible applications to these ends. Additionally, this document outlines requirements associated with the application of SIMS including: Operator training; Sample preparation; Data interpretation; Equipment maintenance; and Reporting of data.
AS6171/17[15]	Technique for Suspect/Counterfeit EEE Parts Detection by Laser Scanning Microscopy (LSM) Test Methods	This document defines capabilities and limitations of LSM and CLSM as they pertain to counterfeit electronic component detection and suggests possible applications to these ends. Additionally, this document outlines requirements associated with the application of LSM and CLSM including: operator training, sample preparation, various sampling techniques, data interpretation, equipment maintenance, and reporting of data. This test method is primarily directed to analyses performed in the visible to near infrared (400 nm to 1 100 nm approximately). If SAE AS6171/17 is invoked in the contract, the base document, AS6171 General Requirements shall also apply.

[10] Reprinted with permission from the draft version of SAE document AS6171/9 (c) 2016 SAE International.

[11] Reprinted with permission from the draft version of SAE document AS6171/10 (c) 2016 SAE International.

[12] Reprinted with permission from the draft version of SAE document AS6171/11 (c) 2016 SAE International.

[13] Reprinted with permission from the draft version of SAE document AS6171/12 (c) 2016 SAE International.

[14] Reprinted with permission from the draft version of SAE document AS6171/13 (c) 2016 SAE International.

[15] Reprinted with permission from the draft version of SAE document AS6171/17 (c) 2016 SAE International.

Bibliography

IEC 60068-2-1, *Environmental testing – Part 2-1: Tests – Test A: cold*

IEC 60068-2-30, *Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)*

IEC 60068-2-78*, Environmental testing – Part 2-78:Tests – Test Cab: Damp head, steady state*

IEC 60115-8*, Fixed resistors for use in electronic equipment – Part 8: Sectional specification – Fixed surface mount resistors*

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

IEC TS 62686-1*, Process management for avionics – Electronic components for aerospace, defence and high performance (ADHP) applications – Part 1: General requirements for high reliability integrated circuits and discrete semiconductors*

ISO/IEC 31010, *Risk management – Risk assessment techniques*

ISO Guide 73, *Risk management –Vocabulary*

ISO 9001, *Quality management systems – Requirements*

ISO 14001:2004, *Environmental management systems – Requirements with guidance for use*

ISO 31000*, Risk Management – Principles and guidelines*

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

AEC Q100, *Failure Mechanism Based Stress Test Qualification For Integrated Circuits*

AEC Q101, *Failure Mechanism Based Stress Test Qualification For Discrete Semiconductors*

AEC Q200, *Stress Test Qualification For Passive Components*

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

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

ASTM B487, *Standard test method for Measurement of Metal and Oxide Coating Thickness by Microscopical Examination of Cross Section*

ASTM B568, *Standard test method for Measurement of Coating Thickness by X-Ray Spectrometry*

DFARS 252.246.7007, *Defense Federal Acquisition Regulation Supplement – Contractor Counterfeit Electronic Part Detection and Avoidance System* (http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007)

DFARS 252.247.7007, *Defense Federal Acquisition Regulation Supplement – Liability and Insurance* (*http://www.acq.osd.mil/dpap/dars/dfars/html/current/252247.htm#252.247-7007*)

DFARS case 2014-D005*, Defense Federal Acquisition Regulation Supplement – Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation, see http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf* or *https://www.federalregister.gov/articles/2015/09/21/2015-23516/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic*

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

GIFAS 5052/2008*, Guide for managing electronic component sourcing through non-franchised distributors, preventing fraud and counterfeiting*

IDEA-ICE-3000, *Professional Inspector Certification Exam (http://www.idofea.org/products/51--idea-ice-3000)*

IDEA-STD-1010 *Acceptability of Electronic Components distributed in the Open Market* (www.idofea.org)

IPC JEDEC J-STD-002, *Solderability Tests for Component leads, Terminations, Lugs, Terminals and Wires*

IPC JEDEC J-STD-033, *Handling, Packing,Shipping and Use of Moisture/Reflow Sensitive Surface Mount Devices*

JESD22-A101, *Steady state temperature humidity bias life test*

JESD22-A104, *Temperature cycling*

JESD22-A108, *Temperature bias and operating life*

JESD22-B107D, *Marking Permanency*

JESD47, *Stress-Test-Driven Qualification of Integrated Circuits*

JESD94, *Application Specific Qualification using Knowledge Based Test Methodology*

MIL-PRF-19500:2012, *Performance specification: semiconductor devices, general specification for*

MIL-PRF-39003, *Capacitors, Fixed, Electrolytic (Solid Electrolyte), Tantalum, Established Reliability, General Specification for*

MIL-PRF-39014, *Capacitor, Fixed, Ceramic Dielectric (General Purpose) Established Reliability and Non-Established Reliability, General Specification For*

MIL-PRF-55681, *Capacitor, Chip, Multiple layer, Fixed, Ceramic Dielectric, Established Reliability and Non-Established reliability, General Specification For*

MIL-STD-202 method 106, *Moisture resistance*

MIL-STD-202 method 107, *Thermal shock*

MIL-STD-202 method 108, *Life (at elevated ambient temperature)*

MIL-STD-750, *Test method standards for semiconductor devices*

MIL-STD-750 method 1051, *Thermal shock (temperature cycling)*

MIL-STD-883, *Test method standard microcircuits*

MIL-STD-883 method 2010, *Internal visual (monolithic)*

MIL-STD-883 method 1010, *Temperature cycling*

MIL-STD-883 method 1015, *Burn-in test*

MIL-STD-883 method 1033, *Endurance life test*

MIL-STD-1580, *Destructive physical analysis (DPA) for electronic, electromagnetic and electromechanical parts*

NDAA: H.R.1540, *National Defense Authorization Act for Fiscal Year 2012 / Sec. 818. Detection and Avoidance of Counterfeit Electronic Parts* (Became Public Law No: 112-081)

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

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

NIGP 111.00, *Guidelines for format of Packing Slips*

NIGP 113, *NEDA Guidelines for Product Returns*

OHSAS 18001:2007, *Occupational health and safety management systems*

SAE ARP6178[16], *Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors*

SAE AS5553A[17], *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition*

SAE AS6171[18], *Test Methods Standard: General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts*

SAE AS6171/1[19], *Suspect/Counterfeit Test Evaluation Method*

SAE AS6171/2[20], *Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Test Methods*

---

16 Reprinted with permission from the published version of SAE document SAE ARP 6178 (c) 2016 SAE International.

17 Reprinted with permission from the published version of SAE document SAE AS5553A (c) 2016 SAE International.

18 Reprinted with permission from the draft version of SAE document AS6171 (c) 2016 SAE International.

19 Reprinted with permission from the draft version of SAE document AS6171/1 (c) 2016 SAE International.

20 Reprinted with permission from the draft version of SAE document AS6171/2 (c) 2016 SAE International

SAE AS6171/3[21], *Techniques for Suspect/Counterfeit EEE Parts by X-Ray Fluorescence Test Methods*

SAE AS6171/4[22], *Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Methods*

SAE AS6171/5[23], *Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods*

SAE AS6171/6[24], *Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods*

SAE AS6171/7[25], *Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods*

SAE AS6171/8[26], *Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods*

SAE AS6171/9[27], *Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods*

SAE AS6171/10[28], *Technique for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Method*

SAEAS6171/11[29], *Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods*

SAE AS6171/12[30], *Techniques for Suspect/Counterfeit EEE Parts Detection Of Capacitors by Acoustic Microscopy (AM) Test Methods*

SAE AS6171/13[31], *Technique for Suspect/Counterfeit EEE Parts Detection by Secondary Ion Mass Spectrometry (SIMS) Test Method*

SAE AS6171/17[32], *Technique for Suspect/Counterfeit EEE Parts Detection by Laser Scanning Microscopy (LSM) Test Methods*

SAE AS6174[33], *Counterfeit Material: Detection, Mitigation and Disposition*

---

21 Reprinted with permission from the draft version of SAE document AS6171/3 (c) 2016 SAE International

22 Reprinted with permission from the draft version of SAE document AS6171/4 (c) 2016 SAE International.

23 Reprinted with permission from the draft version of SAE document AS6171/5 (c) 2016 SAE International.

24 Reprinted with permission from the draft version of SAE document AS6171/6 (c) 2016 SAE International.

25 Reprinted with permission from the draft version of SAE document AS6171/7 (c) 2016 SAE International.

26 Reprinted with permission from the draft version of SAE document AS6171/8 (c) 2016 SAE International.

27 Reprinted with permission from the draft version of SAE document AS6171/9 (c) 2016 SAE International.

28 Reprinted with permission from the draft version of SAE document AS6171/10 (c) 2016 SAE International.

29 Reprinted with permission from the draft version of SAE document AS6171/11 (c) 2016 SAE International.

30 Reprinted with permission from the draft version of SAE document AS6171/12 (c) 2016 SAE International.

31 Reprinted with permission from the draft version of SAE document AS6171/13 (c) 2016 SAE International.

32 Reprinted with permission from the draft version of SAE document AS6171/17 (c) 2016 SAE International.

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*

____

33 Reprinted with permission from the published version of SAE document SAE AS6174 (c) 2016 SAE International.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch