

# HOW TO IDENTIFY AND AVOID COUNTERFEIT COMPONENTS

*John Jones*

*Alter Technology Group*

*1000 Lakeside, North Harbour, Portsmouth Hampshire, UK, PO6 3EZ*

*Tel: +44 (0)2392 704246, Fax: +44 (0)2392 704001, [john.jones@altetechnology.com](mailto:john.jones@altetechnology.com)*

## **Abstract**

There is nothing new about the counterfeiting of EEE Components. However, with the increase in component obsolescence, the problem of counterfeiting is reaching epidemic proportions. This is having a serious impact on the manufacture and maintenance of Military and Avionics equipment.

This white paper will consider what are counterfeit components, why are components counterfeited and how to identify and avoid counterfeit components.

## **Introduction**

From the Oxford English Dictionary (OED) counterfeit is defined as: -

- Made in imitation.
- Not genuine.
- Pretended.

In electronics counterfeiting is used as: -

- “Catch all” phrase for any problem with electrical functionality.

It is estimated that 9% of all electronic components are counterfeit.

In practice three classes of counterfeit component are recognised: -

- parts which are non-functional .
- parts which have some functionality but fail to meet the users expectations.
- Components which appear in all aspects to be genuine.

Considering these classes of components in turn: -

a) The non-functional component: -

- The user requires a part in a 16 pin dual in-line package.
- Parts are supplied which are in the expected package and with the expected branding.
- But only the package and branding are what the user expects. The contents can be anything.

This is the most blatant form of counterfeiting. It seems that the counterfeiters are able to intercept requests for quotations (RFQ) and obsolescence searches find a suitable package/pin combination and re-brand these parts so that they appear to be the sought after part. The nations of Northern Europe and North America are inadvertently assisting the counterfeiters by shipping scrapped electronic equipment to the Far East for disposal thus providing a ready source of material for re-branding.

b) The semi or partially functional components: -

- The user requires a specific version of a part. Often the latest die revision or highest performance.

- The parts supplied appear to be the specific version required but in practice performance is well below what might be expected.
- An earlier version of the part has been supplied but re-branded to appear to be the required version.
- Counterfeit MIL Qualified and screened parts are achieved by re-branding commercial product and falsifying screening data.

This is more dangerous than the blatant counterfeiting described in a) above, where failure at board switch-on is the commonest indication of a problem.

If an earlier version of a die is sold as the latest it may be slower or have inferior supply or output currents. In extreme cases if the circuit was operating towards the extremes of the new die characteristics it simply may not function in all applications.

More dangerous still are components re-branded as a higher temperature range than the standard product. The good component is manufactured from die selected at silicon wafer level. The original component manufacturer knows that not all die will meet the extended temperature requirement, hence the selection and of course the higher unit price. The counterfeiter has no interest in this but by re-branding the value of standard product has been increased and the counterfeiter will pocket the difference for very little effort. The user will only find such counterfeits when the board or system is operated at temperature.

Counterfeit MIL-Qualified parts may have neither the ability to operate over the MIL temperature range, nor for the expected lifetime with the failure rate expected.

- c) Most dangerous are the components assembled in the same facility as the genuine product. This seems to happen because the die manufacturers expect to see a certain yield from subcontracted assembly houses and if this yield is met the die manufacturer (or “fabless” manufacturer) is happy. Unscrupulous staff in assembly houses may process die stock left when the expected yield has been met. Parts finished in this way appear identical to the “good” product. The dangers are: -
- short cuts in the assembly process may reduce reliability.
  - parts may not be tested and border line parametric failures may enter the market place.

### **Why are Components Counterfeited?**

\$\$\$\$

The warning to all EEE component users is that counterfeiters follow the market.

If it becomes known that a user is searching for a particular rare product that product will suddenly become available.

If a new product is announced by a component manufacturer, particularly if PC, Games Consoles or mobile communications applications are involved the counterfeit will appear within days.

It is not just the high value components which are counterfeited. ATG have also identified counterfeit COTS diodes. Where is the profit margin in faking such a low value item?

### **Anti-Counterfeiting Tools**

A suite of tools are available for identifying counterfeit components: -

- External Optical Inspection.
- Resistance to Solvents.
- Radiographic (X-ray) Inspection (Fine Focus).
- Scanning Acoustic Microscopy (CSAM).
- Sample De-Encapsulation and Internal Optical Inspection.
- Sample Parametric Testing across the specified temperature range.

Considering each test in turn: -

a) External Optical Inspection

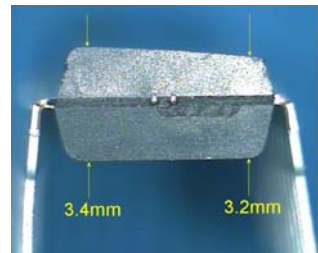
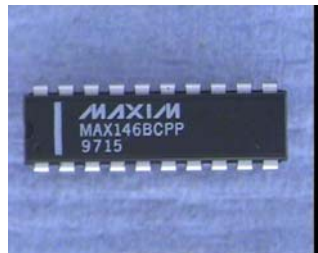
Sometimes the counterfeiter makes life easy: -



ATG have never encountered an assembly house that could not spell the name of the country of it's location. PHILIPPIHES (sic) above is a giveaway.

The previous image is a good example of re-branding, but we cannot rely on the counterfeiter's poor spelling, there are other optical clues: -

- The marking, if ink, may be removed by grinding and this is the only way to remove laser etched markings.
- Again sometimes the counterfeiter can be helpful: -



The example shown above has had the marking removed by hand grinding (probably with a sheet of sandpaper) hence the very obvious taper. These are the types of anomaly any good inspector will identify.

b) Considering part marking, there are two methods: -

- Printing using water and solvent proof inks.
- Laser etching.

Again the counterfeiters can be helpful: -

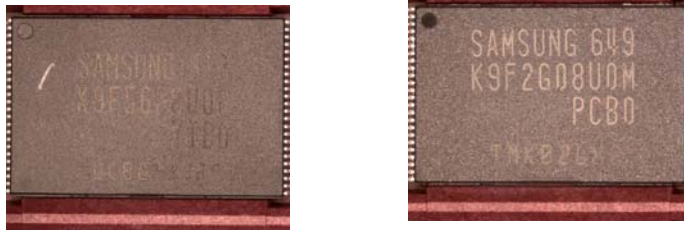
- Genuine marking inks are expensive and have a short shelf life.
- If the ink is water soluble and effected by common solvents such as Propanol or Ethanol, the component is probably counterfeit.

The resistance to solvents tests referred to at the start of this section is a good starting point in counterfeit detection. Detailed test methods are described in: -

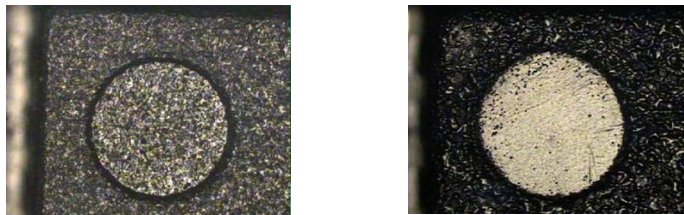
- MIL-STD-883 Method 2015
- MIL-STD-750 Method 1022
- ESCC No. 24800.

Counterfeiters are becoming more sophisticated: -

- Ground back or “sanded” surface – optically detectable.
- Surface painted or “black topped” – optically detectable at edges or by resistance to solvents.
- Surface refinished or re-polished – detectable by reduction in mould mark depth.



The marking may look genuine but



The moulded mark is only 20µm deep – 40 to 60µm would be expected.

The methods so far described to identify counterfeit components may be labour intensive but do not involve the use of major capital equipment. To move to the next level of detection if is necessary to introduce more sophisticated tools.

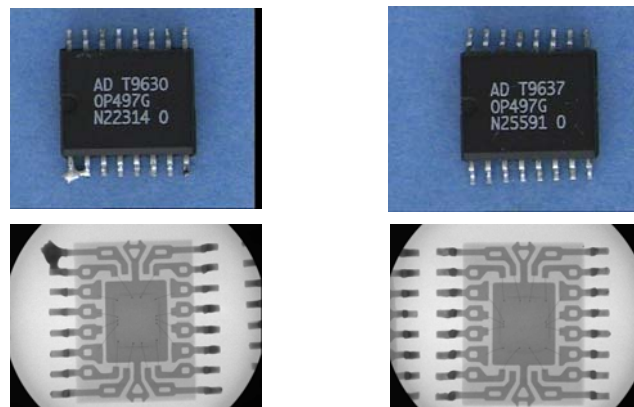
#### c) Radiographic Inspection

Component ‘X-ray’ inspection has improved dramatically in recent years with the move away from fixed focus systems and wet plates to high resolution, fine focus or dynamic radiographic imaging: -



Not a counterfeit but a example of the usefulness of fine focus x-ray. The sample on the left was an intermittent open circuit due to inadequate soldering of the anode termination to the die.

Counterfeits found at board level: -

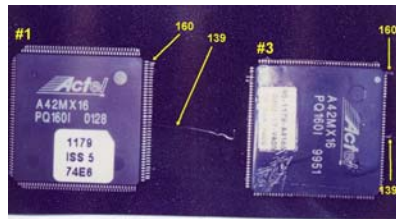


Incorrect Wire Bonding

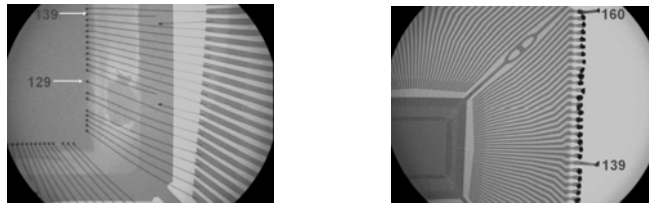
Correct Wire Bonding

A good example of product from an “over-run”. Everything is correct except the way the part is orientated.

Orientation problems found at board level: -



Two FPGA's #3 failed when the board was first tested

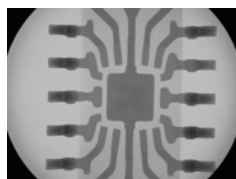


X-Ray Images showing how the parts are wire bonded

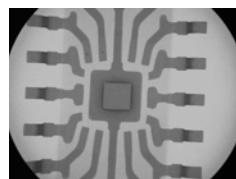
These parts are not deliberately counterfeited but show the dangers where subcontractors are used by 'fabless' manufacturers.

Components like the example shown above tend to get included with counterfeits although the problem is more simple in that two subcontractors have different encapsulation (moulding) equipment and orientation of the part marking. Failures occurred because the user had always placed the part on the circuit board using the part marking to give the orientation not the Pin 1 ident.

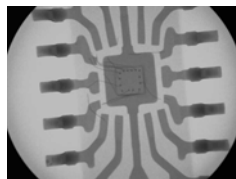
However, the next examples are undoubtedly counterfeit: -



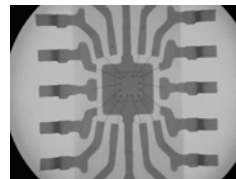
No Die



No Bond Wires



Broken Bond Wires



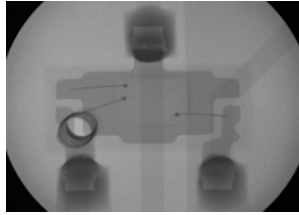
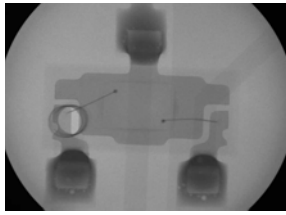
Missing Bond Wire

These examples came from 36,000 parts delivered as tape & reel. Other defects were identified with this delivery including at least 3 different die options and an anomalous plastic encapsulation, which will be discussed later.

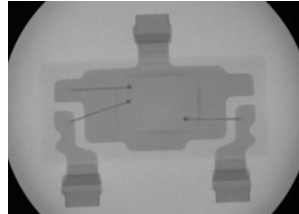
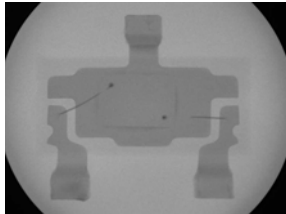
Similarly the information on two tape & reels looks good



but failures occurred when mounted and tested



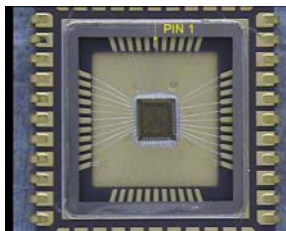
Radiographic inspection found differences in the wire bonding layout of the mounted parts which was confirmed by inspection of samples from each reel.



### Internal Optical Inspection

As indicated above counterfeit components have been found using radiographic inspection to have different die. X-Ray will provide information about die size but to make a detailed assessment it is necessary to de-encapsulate the component and make an internal optical inspection.

Hermetic encapsulated components are de-capped mechanically and plastic encapsulated components chemically: -

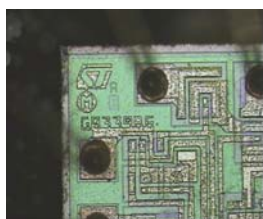


Mechanical and Chemical de-encapsulation are standard processes in DPA (Destructive Physical Analysis) and FA (Failure Analysis)

A suspect Phillips PEM was de-capped: -



Phillips PEM



Containing an STM Die

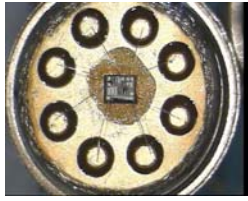
Die swapping between component manufacturers is accepted practice but the findings above were only part of the identification of a suspect lot.

The problem is not confined to PEMs, the following sequence of images of 8 MIL Qualified components relate to the most blatant piece of counterfeiting identified by ATG: -

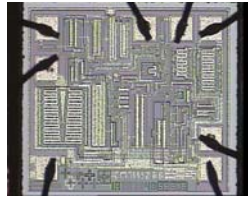
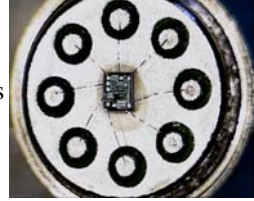


Same Date Code

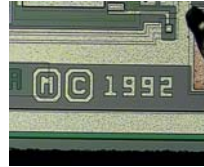
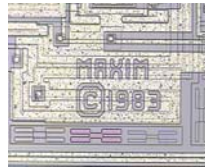
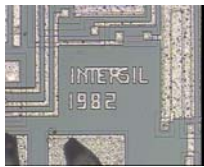
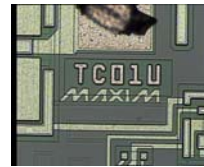
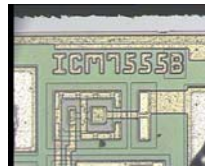
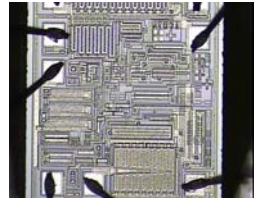




Different Headers



Different Die

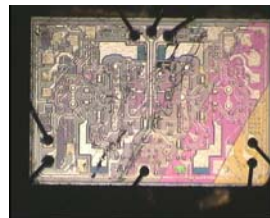


In eight samples the user had two die manufacturers and six different die revisions.

Finally, in de-encapsulation another board level failure of a seemingly genuine part: -

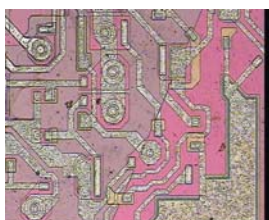


Looks Good

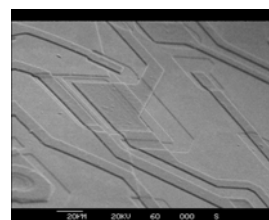


Not So Good

De-cap



Highly Suspect



Manufactured From \*\*\*\*

Optical inspection supported by scanning electron microscopy (SEM) found that the die was incompletely processed having come from the edge of the wafer. Another example of a part manufactured on a genuine production line but never tested.

**ROHS – Restriction on Hazardous Substances**

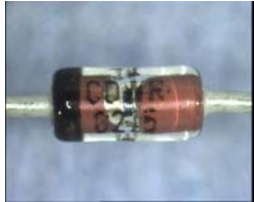
ROHS may help in the battle against counterfeiters.

All current commercial components (COTS) may be reasonably expected to be ROHS compliant.

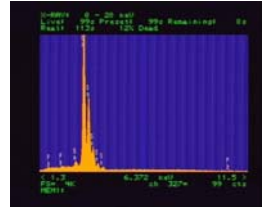
Most significantly this means a lead (Pb) free solder finish on the leadouts.

Older components would be expected to have a tin (Sn) lead (Pb) solder finish on the leadouts.

The lead out finish may be monitored optically, pure tin (ie lead (pb) free) having a dull or matt appearance, or by X-Ray Fluorescence: -



JTXVIN5711  
Date Code 0215



EDS\* Spectrum of the  
lead finish

\*X-Ray Dispersive Spectroscopy = X-Ray Fluorescence in the SEM

Finding a pure tin finish on a JTXV qualified diode manufactured in 2002 week 15 was somewhat surprising and justified further investigation.

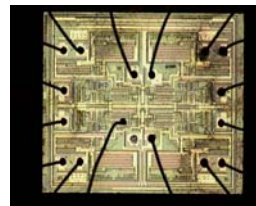
Microsemi Corporation are one of the companies that have opted to use the accepted (by ROHS) option of having a low lead (Pb) content in the lead out finish rather than going to the lead (Pb) free pure tin (Sn) option. Caution must be exercised when analysing the lead out finish.

### Electrical Parametric Testing

Critical areas are: -

- Performance over the expected temperature range. One of the easiest counterfeits is to remark a 0-70°C rated part as one with a wider operating temperature range. The part will contain the “correct” die but not one which has been selected for temperature performance.
- Current/Voltage/Switching Time performance, again it is often possible to find a “lower grade” part that will perform many of the users requirements and mark the part as appropriate.

The example shown below was also identified when a board failed: -



This Analog Devices part appears to be rated at 85°C but stops working at 72°C.

The component level failure analysis undertaken revealed: -

- AD had not manufactured the high temperature version of the part during 2003 week 38.
- The part contains a MAXIM die with the correct functionality.

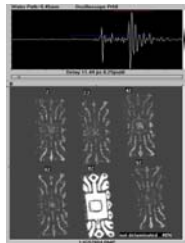
- One of the bond wires became detached during de-encapsulation. This was a result of poor wire bonding during component manufacture. This part would have been a potential reliability hazard even had it operated over the required temperature range.

### Acoustic Microscopy

Acoustic microscopy images the interfaces between different material layers in solid structures. In semiconductor manufacture and screening, acoustic microscopy is used to assess: -

- the bond between the plastic encapsulant and the die.
- the bond between the plastic encapsulant and the lead frame.
- the bond between the die and the lead frame.

The acoustic microscope signal is attenuated by the material through which the signal is passing. At the frequencies used for acoustic microscopy (1MHz to 100MHz) there is a recognisable difference in the attenuation of different encapsulants. The image below shows six samples taken from six tape & reels sold as a homogenous batch. One of the samples shows a completely different response.



This finding led to further investigation which identified differences in the composition of the plastic. This work and other developments are more fully described in “Counterfeit Components & Acoustic Microscopy” also available as a white paper from ATG.

### ATG Observations on Counterfeit Components

- Some manufacturers appear to be regular targets.
- Some product families appear to be regular targets.
- Counterfeit components are being seen every month.
- These are all products which the Avionics/Defence community use on a regular basis.
- How do we know this. ATG has a knowledge database where this information is stored and processed.

### Mitigation – Components to Avoid

Before considering mitigation measures the following list summarises those components which must be avoided: -

- Not authentic
- Misidentified
- Non-compliant
- Re-used
- Reworked
- Salvaged
- Mishandled
- Improperly stored
- Improperly tested
- Unknown pedigree
- Suspect for any reason

This list strays beyond the OED definition of counterfeit, but largely meets that accepted by the electronics industry.

## Counterfeit Mitigation – What to do?

- Procuring components not purchasing (Buying) – strong Supplier Chain Management is necessary. In a competitive world where purchasing must buy from the cheapest source with the shortest delivery, let the buyer beware.
- Approved supplier lists used rigorously.
- If you find a source of ‘hard to find’ / ‘obsolete parts’. Are you : -
  - Smarter than everyone else?
  - More naïve than everyone else?
- The main action to avoid counterfeit parts is to control the supply chain.
- Buy direct from manufacturers or authorised distributors.
- Avoid unauthorised distributors, brokers and the grey market.
- Demand a Manufacturer’s Certificate of Conformance and verify its authenticity.
- Be very careful if you enter the grey market or buy from brokers, what looks like a solution to a problem may be the start of a much bigger problem.

## Counterfeit Mitigation – Proactive & Reactive

### Proactive

- Good procurement practices
- Strong supply chain
- Rigorous use of approved supplier lists
- Where possible procure all parts needed
- Once parts are validated store them in a “safe” environment

### Reactive

- Increased receiving inspection
  - Visual, traceability and data checks
- Radiographic inspection
- Electrical measurement v temperature
- Scanning Acoustic Microscopy
- De-encapsulation & Internal Inspection

### Conclusions

- We will not stop people making counterfeit parts
- We can ensure that we do not purchase them
- AWARENESS IS THE KEY
- Publicity is required so procurers are aware of the risks

Is there light at the end of the tunnel

- UKEA Anticounterfeiting Forum “Counterfeit Data Base”.
- RECS - Reliable Electronics Component Source
- ORAFEC - Organisation Against Fraudulent Electronic Components

Can the Far Eastern component manufacturers police themselves?

Can the electronic component brokers clean up their act?