Detection of counterfeit microchips and electronic components

COULD YOU TELL THE DIFFERENCE?

SGS

Contents

Summary

When the supply of chips is short, people do not look too closely. Delivery dates have to be met and the product description must be correct. The temptation is to secure the last batches with less attention to detail.

But how can one ensure that the promised quality is delivered?

CHIP CRISIS AND ITS CONSEQUENCES

Often, players in the supply chain have no choice but to buy on the open market. The risks are obvious, because it is easy to make money with counterfeit chips.

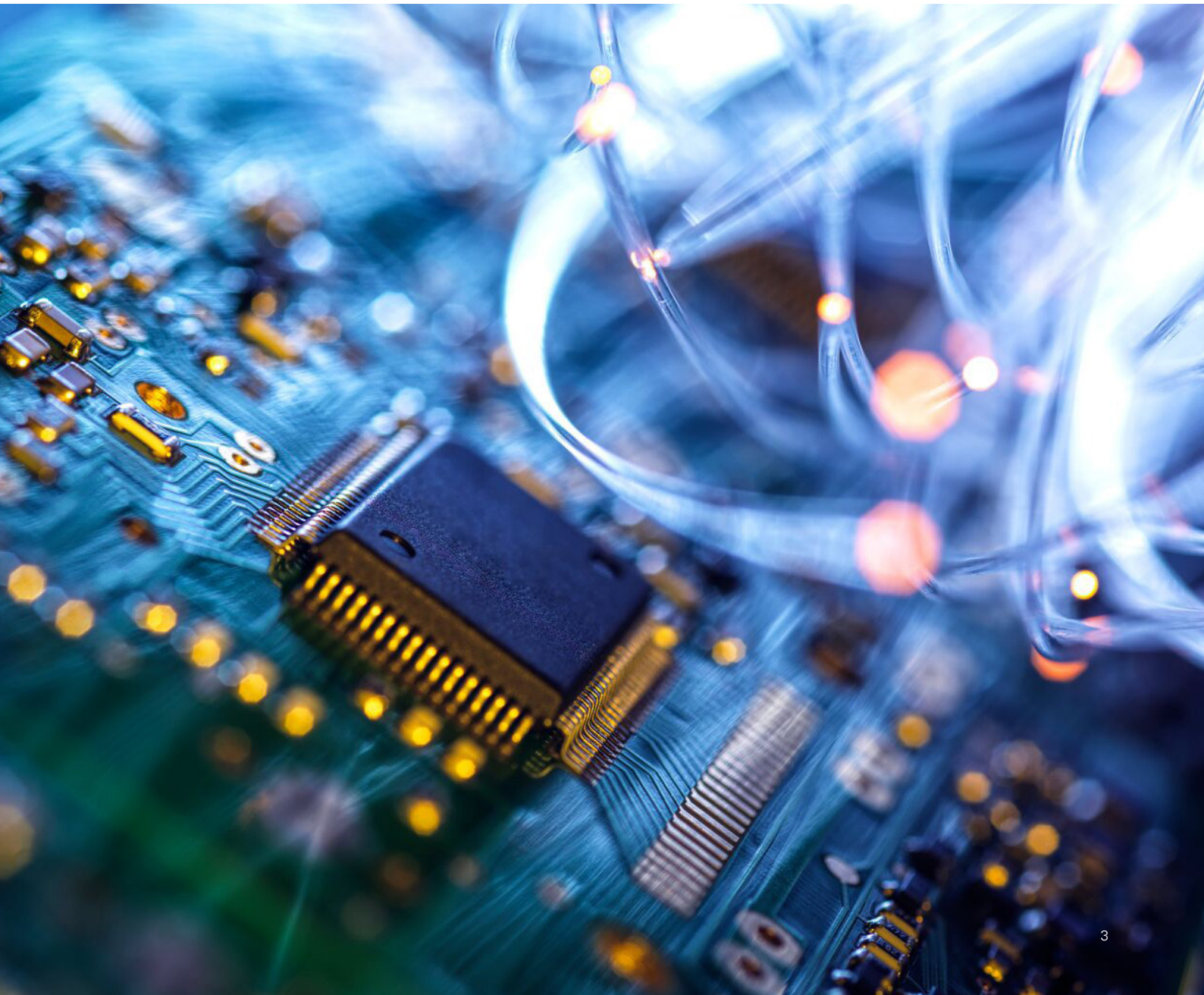
Internet forums are full of instructions on how to fake chips: by manipulating serial numbers or reusing chips that have already been installed. In the Far East, this kind of chip counterfeiting is already being done highly professionally and on a large scale.
Source: nepp.nasa.gov

If a manufacturer has only produced 200 pieces of a series, but 40,000 pieces of just this series are offered by a broker, the miraculous multiplication is certainly due to criminal chip counterfeiting.
Source: nepp.nasa.gov

WHAT ARE COUNTERFEIT CHIPS?

Counterfeit chips pretend to be OEM parts and look deceptively similar to them at first glance. In fact, they come from other sources:

- Relabeled chips: chips from other manufacturers or designs
- Extracted chips: chips that were already built into an electronic
- Rejects: chips that have been discarded due to insufficient electrical properties. Obsolete chip series



Methodology for fake chip analysis

Various methods exist to detect component counterfeits. Depending on the risk assessment, these can be combined in a meaningful way to detect fake chips with a high probability.

In the aerospace sector, the test strategy is already defined by the SAE AS 6081 standard. For other industries, it is also useful to follow this standard.

OPTICAL INSPECTION

To detect counterfeit chips, sometimes a good optical microscope is enough to find the first signs of tampering.

Most counterfeit chips have altered labeling to hide the real manufacturer. The original lettering on the casing is ground off or lasered away. These processes leave a rough surface that can be made visible under microscopic magnification.

The mechanical processing also releases silicon dioxide particles, which are used as fillers in the molding compounds. These are clearly visible on the manipulated surfaces.

Further indications of counterfeiting are slight deviations in the dimensions of the chips and their connecting wires. Using an original part as a reference for dimensions and material - the so-called golden sample - provides useful clues.

WIPE TEST (SOLVENT TEST FOR REMARKING)

The "new," incorrect markings are often only stamped on and can be easily detected by the wipe test. An organic solvent is used which can dissolve ink and other printing inks.

INSPECTION WITH X-RAY / ULTRASOUND

These analyses are nearly non-destructive and give an overview of the construction and dimensions of the chip and its connecting wires. In some cases, relabeling can be detected.

However, detailed information on design and construction cannot be obtained. As a sole test strategy, inspection with x-ray or ultrasound is not suitable.

CHIP EXTRACTION

The next step is to examine what the chip looks like underneath the encapsulation. Wet chemical processes remove the epoxy moulding compounds and expose the chip.

The top metallisation layer is now visible. In this way, design deviations or different serial numbers can be found: clear indications of fake chips.

WETTING TEST / SOLDERABILITY TEST

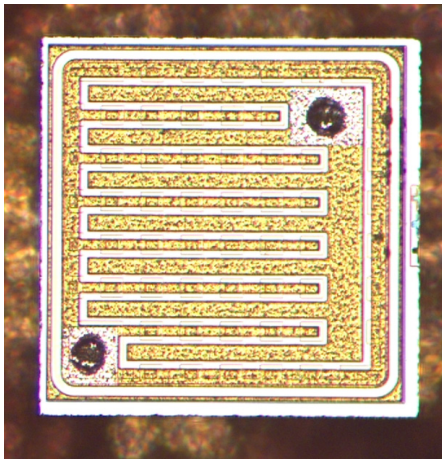
The contact legs on the package of OEM components show perfect solderability: the solder forms an even layer. This is not the case with tampered parts. If a chip has already been soldered onto a PCB, the surface properties of the contact legs have changed: dewetting and voids in the solder layer are visible.

The same effect is present if inferior material with poor soldering properties was used. There is already a standard for the solderability test: EN 60068-2-58.

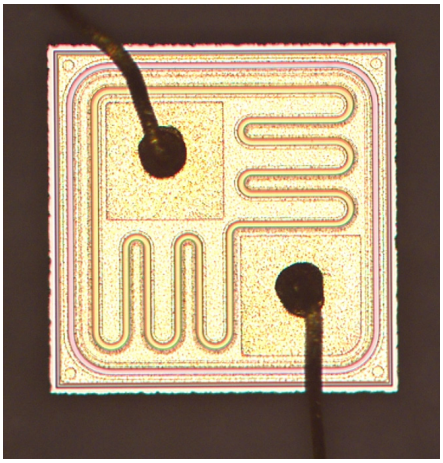
Case studies

CASE STUDY 1: CHIPS WITH DIFFERENT ELECTRICAL PROPERTIES

Chip opening: obviously different designs.

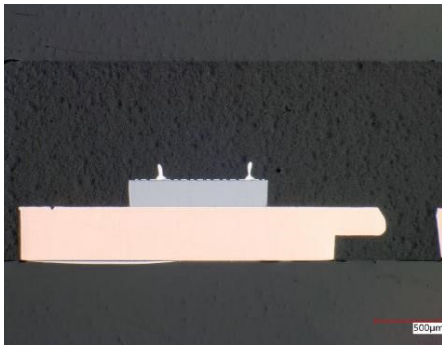


Test chip

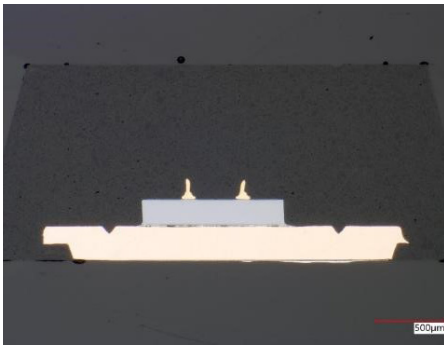


Reference chip

Generating cross-sections: different design.

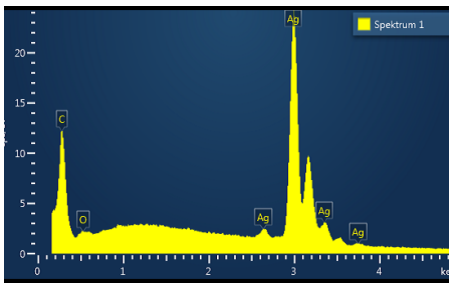


Test chip

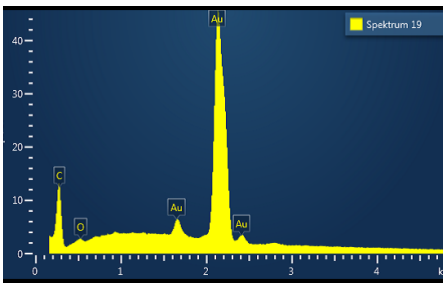


Reference chip

Analysis of wire material with EDX: silver instead of gold.



Test chip: silver

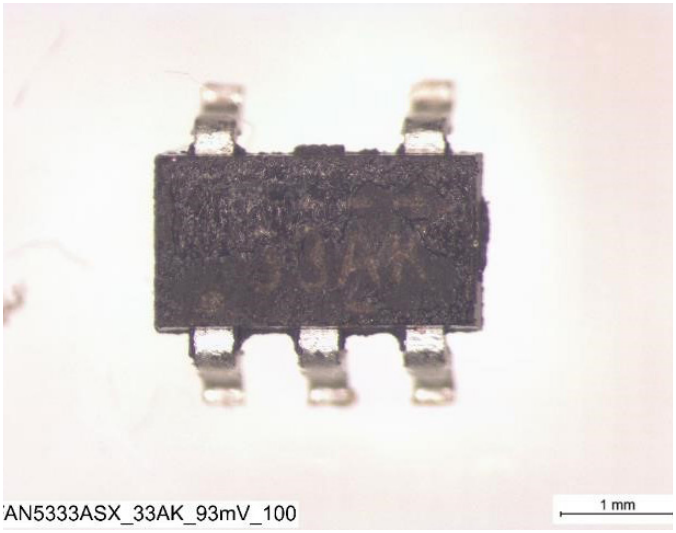


Reference chip: gold

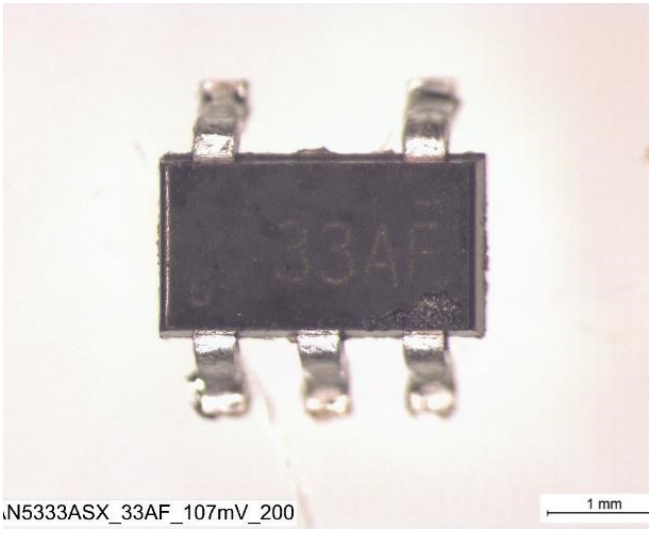
Test result:
Different chip to the one declared.

CASE STUDY 2: FAILURES AT THE CUSTOMER / IN THE FIELD

Light microscopic examination: rough surface, traces of silicon dioxide visible, edge chipping from sandblasting.

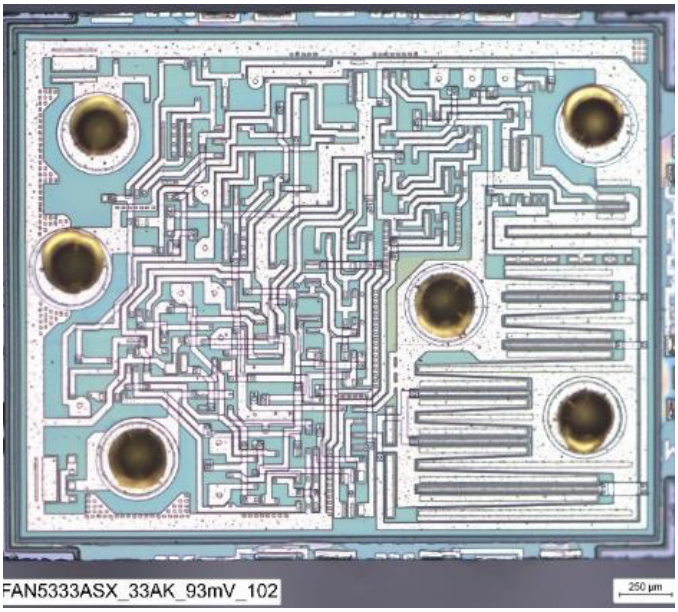


Test chip

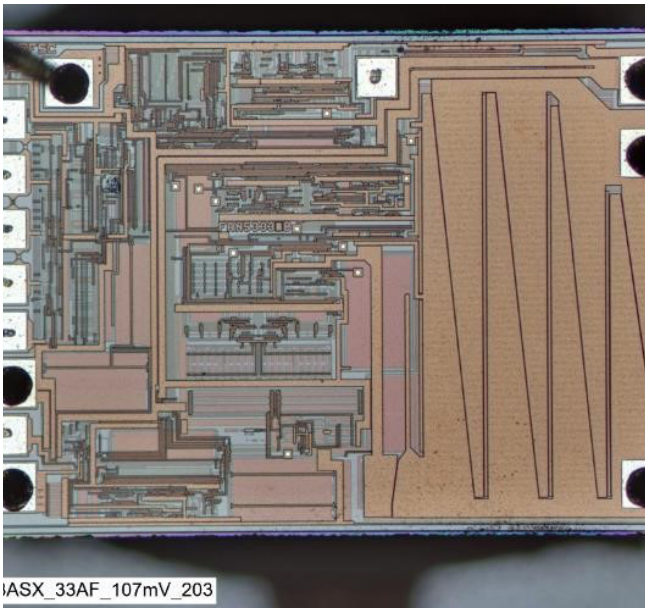


Reference chip

Opening: Completely different chip design.



Test chip



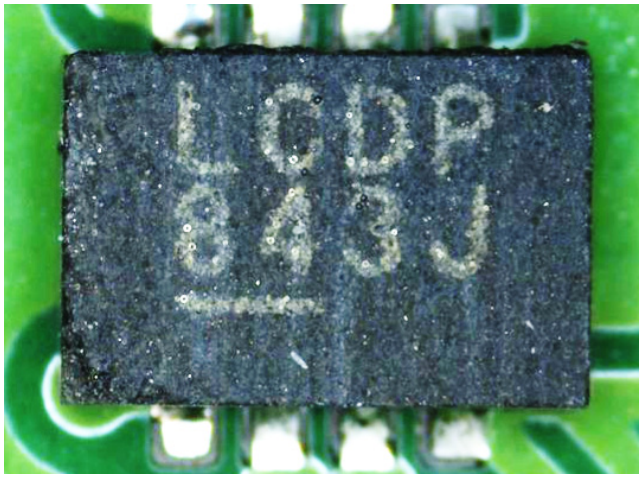
Reference chip

Test result:

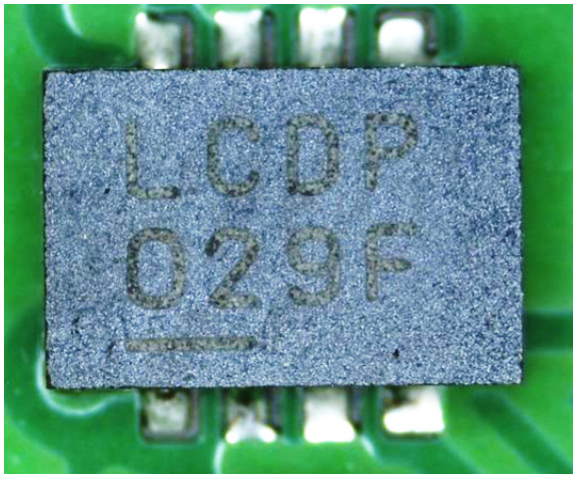
Markings on the housing have been removed by sanding, sandblasting, lasering, in fact it is a different chip than declared.

CASE STUDY 3: FAILURES IN THE FIELD

Light microscopic examination with contrast: silicon dioxide residues, edge chipping, different serial number.

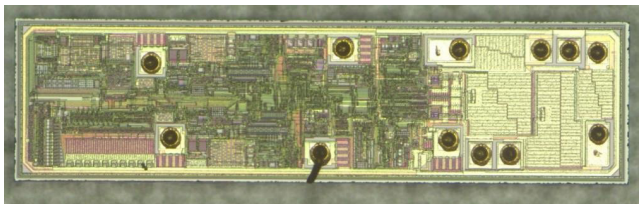


Test chip

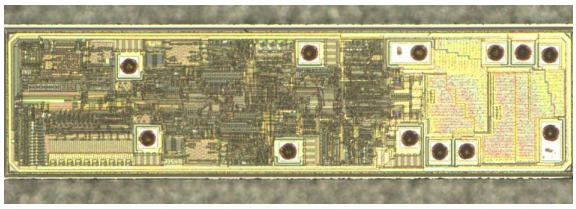


Reference chip

Chip opening: no design differences detectable, only minimal differences in topographical dimensions.



Test Chip



Reference chip

Test result:

Inscription on the housing was removed by grinding, sandblasting, lasering.

Manufacturer´s statement: the 843J series was never produced.

Fault hypothesis: Low yielding chips / B-merchandise was labeled and sold like full chips.

Conclusion

Physical analysis is able to detect counterfeit products with the help of authentic samples.

Initial indications are provided by light microscopic examination. However, certainty about the conformity of the design can only be obtained by opening the chip. For this, it is important to take meaningful samples.

By testing and identifying counterfeits, far-reaching damage can be avoided. These are transparent, objective testing procedures that should be firmly established in supplier relationships.

It makes sense to develop an inspection strategy adapted to the respective risk potential and to establish it as a fixed component of the incoming goods inspection.

Trusted means *Tested.*

WHEN YOU NEED TO BE SURE

SGS