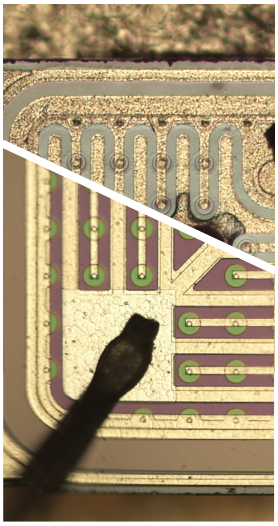
Are there still risks in out-sourcing electronic component buying?

The number of identified electronic component counterfeits is dropping. The systematic implementation of counterfeit detection tests from brokers to components users has contributed to this. It has made it possible to clean up the sector, with the percentage of rejects by the end user passing from 25% to 15% in just a few years. Supplier selection and scoring, certification, integrated test laboratories... the changes to the brokering trade have moved it on from being a pure trader to being a partner supplier. What are the remaining pitfalls?

PART ORIGIN

Counterfeiting as such is not the only fraud on batches supplied from the grey market. There are few parts on which the chip is not the one that was expected, and even less chips that have purely and simply been copied. In the rejected batches, you will find:

- re-used components;
- components that were scrapped in production;
- genuine counterfeits.

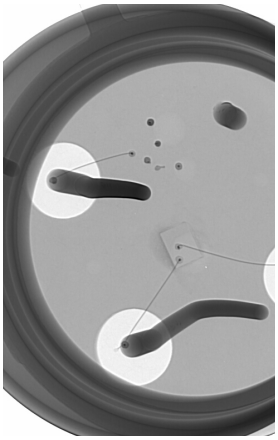


Every origin can be detected, but not using the same types of test. This is why a single analysis is not enough to guarantee that the batch is fraudulent or not. Several standards have been drawn up to determine the test flows, but all the major customers have also specified their own procedures. For the others, we have chosen 3 procedures (of which two under ISO-17025 accreditation), each having a different level of residual risk, but also a different cost, to adapt to all possible component applications.

cofrac
ESSAIS
ACCREDITATION N°1-2378 PORTÉE DISPONIBLE SUR WWW.COFRAC.FR

RISKS

The worst that can happen with a fraudulent component is that it is in working order! Otherwise a defect is detected and the product is blocked. What remains is to analyse the board or the system to discover the failing part of the component. A test on it will highlight an anomaly that will indicate the fraudulent origin of the parts. There is no point in asking the part manufacturer, as few of them take charge of analysing components from unauthorised sources. All that remains is to find replacement parts for the entire incriminated batch.



Even if the board or system functional tests don't reveal any defects, who knows when the failure will occur: when using an untested configuration? After the thermal-mechanical stresses? Never? It's impossible to say. The same analysis as before will be able to detect the same fraud, only the costs for the analysis and the replacement will be multiplied, not to mention the loss of brand image.

TESTS

The tests carried out are not fully complete. Whatever procedure is used, they are based on the absence of proof of fraud, or rather, the failure to detect proof of fraud. The farther we look without finding proof, the lower the risk of being confronted with fraudulent parts. Until we consider that, in the end, either the component is good, or sufficiently good to operate in the application. Some tests, however, are common to all the procedures:

- External visual check (no oxidation, sanding, re-marking, camouflage, etc.)
- X-rays (assembly consistency, chip presence, bonding, etc.)
- Electric tests (parametric, functional tests, etc.)
- Destructive tests (opening, chip marking, solderability, etc.)

From one procedure to the next the depth of testing may vary, as may the number of samples. Other analyses can also be added, such as determining the terminals finish alloy, the integrity of the packing...most often depending on previously encountered cases of fraud. Even though the visual inspection and X-rays can detect over 70% of cases of counterfeiting, the destructive and electric tests remain necessary for the remaining 30%. But we should never lose sight of the fact that, even if the components are new, they weren't manufactured yesterday.

STANDARDS

AS5553 : Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

AS6081 : Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - DistributorsCounterfeit Electronic Parts; Avoidance Protocol, Distributors

IDEA-STD-1010 : Acceptability of Electronic Components Distributed in the Open Market

CONTACT

Jean BASTID
Tame-Component Manager
Tel. +33 (0)2 51 41 89 35
jbastid@tame-component.com