Analysis of counterfeit electronics

G. Mura, R. Murru and G. Martines

Abstract – Counterfeit electronics pose reliability risks and severe harms. The failures of systems that use counterfeits can cause safety and security problems. Lack of caution on the part of buyers, obsolescence, lower prices, costly inspection procedures, absence of origin verification tools is contributing to the widespread of counterfeit electronics. Two case studies are proposed to add a piece of information in this context supporting evidence regarding the capillary penetration of the counterfeit devices. It should contribute to arise some concerns.

1. Introduction

The counterfeiting is an illegal procedure which involves the fraudulent imitation of the original copy for lucrative business or criminal activity. Counterfeit electronic components are defined as [1]:

- Substitutes or unauthorized copies of a product,
- A product in which the materials that are used or the performance of the product has changed without notice,
- A substandard component misrepresented by the supplier.

The origin of the counterfeit electronics problem has been exemplarily explained in [2, 3], and how it is threatening health, safety, security and why it is causing significant harm to the economy has been reported in [1, 4, 5]. Its risk priority aroused when some counterfeit devices were identified in military systems, aerospace applications, medical devices, radiation detectors, high-speed trains brakes and airport landing light system with a high risk to the safety of the people involved [6, 7, 8, 9].

Counterfeit electronics are unauthorized copy that could be remarked/repackaged/recycled/refurbished or even cloned. Counterfeiting also includes providing out-of-spec/ defective parts. The availability of over-production or rejected devices not destroyed but re-introduced and sold "as is" in the market through the broker chains has presented in [10]. The counterfeit electronics show material and characteristics that may lead to severe risks due to potentially degraded quality, unknown reliability, and reduced performances.

A detailed taxonomy of counterfeit types and an analysis of the vulnerabilities in the electronic component supply chain has provided [2, 11]. A comprehensive review of recent counterfeit detection and avoidance techniques is proposed in [12].

In the following, two case studies have proposed to add a piece of information in this context. They add evidence regarding the capillary penetration of the counterfeit devices. It furthermore emphasizes the widespread lack of knowledge regarding the problem that is spreading among the final customers without any control. It should contribute to arise some concerns.

The first case is a wide input voltage low power audio amplifier, and the second is a general-purpose gallium arsenide FET.

2. Case studies

2.1. First case: A commercial power amplifier.

The IC under analysis is a low voltage audio power amplifier that can be used in a variety of applications. It is suitable for battery-powered devices such as radios, guitar amplifiers, and hobby electronics projects and consists of an 8 pins plastic dual in-line package.

A set of commercial power amplifiers designed for use in low voltage and bought from a third-party seller on a popular electronics consumer website failed in a consumer application.

One of them was replaced by another device bought from a local retailer. The former showed the same kind of problem. Another set of devices was bought from a second local retailer showing low gain performances than expected. It worked but surely not as it should have done. Finally, the same type of amplifier was bought from an online authorized retail sales company and replaced, it fixed the problem.

Even if this type of device is cheap and not crucial, it is quite popular among many users. In the following, it will be shown the differences among the four devices, here recalled A (bought from a popular online broker), B1 (from a local retailer), B2 (from a second local retailer), and C (from an authorized retailer). Assuming that C is the original device, an analysis has conducted to detect possible discrepancies among them.

The incoming inspection started verifying the conditions of the materials used for the shipping. The authorized seller only provided a regular shipping package through an ESD bag and properly trays.

The evaluation of the packages was not able to identify any possible defect caused to create a counterfeit. The external visual inspection included the observation of the leads, and no signs of refurbishing or damage have detected.

Marking permanency tests for external compliance were performed and did not erase the marking in the suspected counterfeits. No traces of relabelling were observed.

In Fig.1 is proposed an optical microscope comparison that clearly shows differences in the plastic packages and the entire marking.

Fig. 2 is an enlarged view of the manufacturer's logos, the N symbol is intended to mislead in A, B1, B2.

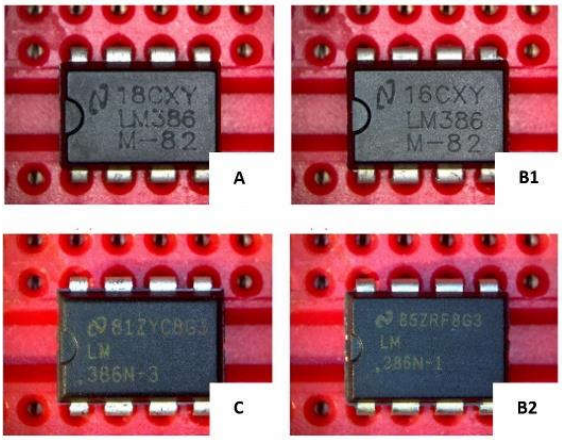

Fig.1 Light optical microscope comparison among the DUTs. Authentic device (C) is compared to three suspictious ones (A, B1, B2).

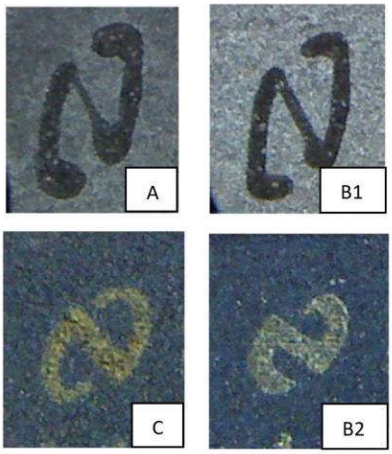

Fig.2 Enlarged optical comparison among the manufacturer's logos.

A further check of the date codes and lot numbers reveals the final part of the marking code of A and B1 is unknown at the original manufacturer.

Otherwise, the product marking code of B2 is compatible with the original. N-1 and N-3 are in theory indicating the same device with the same package, and their performance should not change from one to another.

The quiescent supply current versus the supply voltage has proposed in Fig. 4. The electrical comparison (limited to the range recommended in the datasheet) shows that devices A, B1 and B2 are out of spec.

Fig. 5 shows the corresponding layouts after the wet chemical etching of the plastic packages performed by using hot HNO_3. The etch rate was higher for A and B1 devices, lower (but not the same) for B2 and C.

Optical pictures have taken in the same conditions, and the comparison clearly shows differences in the layouts and the dimensions of the dies.

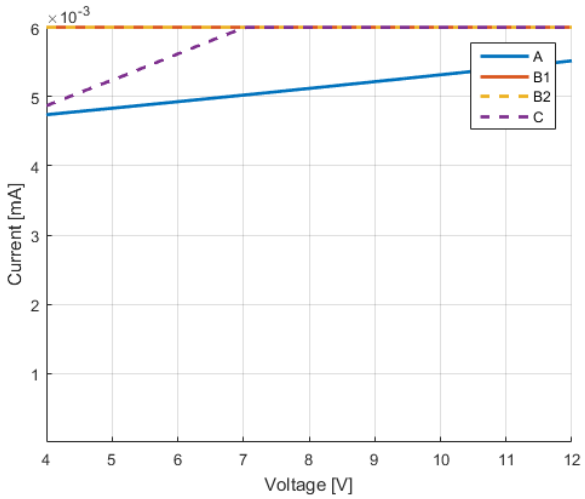

Fig.4 Devices A, B1, B2, and C: I-V measurements

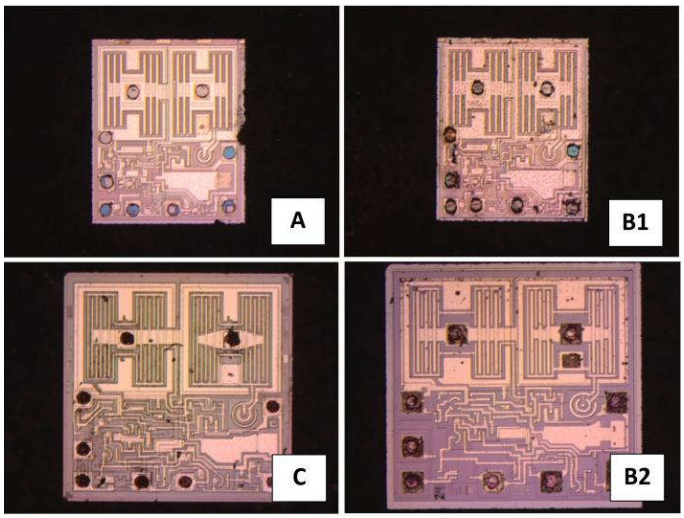

Fig.5 Optical microscope images of A, B1, B2, C layouts after the chemical de-capping.

By comparing C and A, B1 and B2 devices, discrepancies have observed in the following items:

the shipping package, the price, the marking, the electrical characteristics, the layout of the die and its dimensions. Moreover, A and B differ even for the information encoded in the mark and the surface package.

It seems evident that: device A is not original, B1 is not original as A and probably the local retailer acquired the devices from the same broker (A), B2 is not original.

Devices A, B1 and B2 appear as fraudulent copycats of the original device (C).

They must be considered counterfeits because of substitutes or unauthorized copies of an original product.

2.2. Second case: general-purpose GaAs FET.

The device under analysis is a high-performance gallium arsenide Schottky barrier-gate field-effect transistor housed in a cost-effective microstrip package. This device has designed for use in oscillator applications and general-purpose amplifier applications in the 2-16 GHz frequency range.

The production of these devices was discontinued. Consequently, three entire reels (3000 pcs) were purchased in the gray market and mounted on an amplifier application. Several boards did not pass the final electrical tests. The problem had attributed to the devices. As the lots had mounted indistinctly on the boards, the customer was not able to recognize the failed lots neither to perform any analysis. All of them were just dismounted.

The incoming inspection of the reels showed differences. Lot #A date code indicated as date of manufacturing August 2000 while lot #B and #C date codes indicated May 2001.

The external inspection of the plastic packages showed identical geometry. As #B and #C showed the same features, the former has not reported in this analysis.

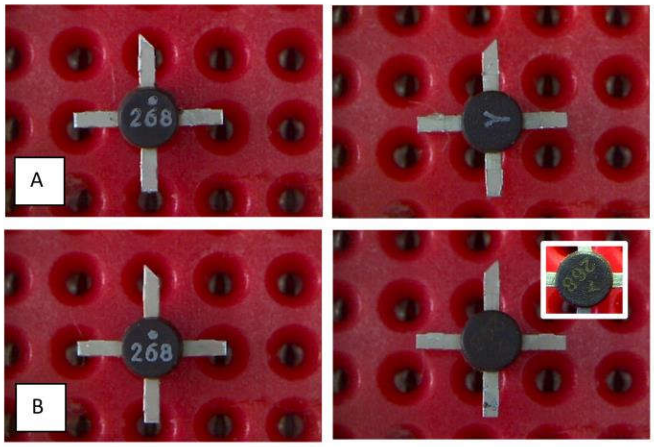

Fig. 6 (first row) upper marking and bottom of the package #A.
(second row) upper marking and bottom of the package #B. In the onset the bottom of device B acquired with different illuminating conditions.

At low magnification, the marking on the upper side of the devices appeared similar. Different marks are on the bottom surface: a Y appeared on all the devices that belong to reel #A, a three number- code and the sign "<" is printed on the devices of the other reels (#B, C) (see fig.6).

A "Customer Change Notice" provided by the manufacturer reported that "to improve product lot traceability, … a data code mark will be added to the bottom of the package". The data code character mark "Y" corresponds to August 2000. The character "<" corresponds to May 2001. But the document reported that the new character would not be concatenated to the already existing product marking code. The marking of #B and C are, therefore, inconsistent due to the coexistence of two marking code.

Besides, a further document should be considered.

On December 2000 a "Product Obsolescence Notice" informed this specific device was being obsoleted due to low sales and the last time buys would be offered through January 2001. Consequently, the possibility that devices #B and #C could not have produced in May 2001 is not negligible. The analysis started considering type A as the original device due to the consistency between marking and data code.

The external visual inspection of the packages was not able to detect any evidence for repackaging or refurbishing.

A closer examination of the marking is proposed in the following figures. There are visible differences in the type and the registration of the marking that is not centred in A type.

In fig. 7 the grooves on the package #A are evident. They indicate the device had probably sanded for remarking.

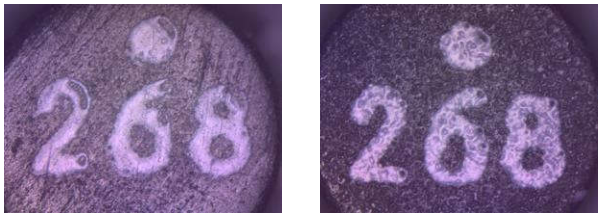

Fig. 7 (left) upper marking of #A, (right) upper marking of #B.

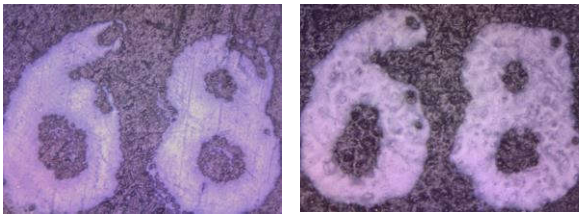

Fig. 8 Enlarged views of Fig. 7

By using solvents, marking permanency tests for external compliance were performed and did not erase the marking in both devices. Even if the marking appears very poor in both cases, using a tweezer, it was easier to remove it from type A.
Slightly differences in the resin moulding have been observed at higher magnification.
These details have forced revising the initial interpretation.
The electrical measurement of the saturated drain current I_{DSS} resulted significantly higher than that declared by the manufacturer (in A more than 30%, in B more than 50%) even if none of the measured values exceeds the one reported as maximum.
The plastic packages have selectively removed to analyze the bare-dies. The conventional top side approach has proven poor results. By following the procedure proposed in [13], the plastic encapsulated devices have been mounted to a polishing stud, grounded from the backside up to the exposure of the GaAs substrates and then chemically back- etched to detect any possible discrepancy.
By using the solution: 1part H_3PO_4: 9 parts H_2O_2: 1part H_2O the removal of the GaAs substrate has completed from the backside, allowing a unique view of the process metals.
Optical microscope comparison is proposed in the following picture (Fig. 9).

At a macroscopic level, the layouts, including the die marking, seem without any difference.

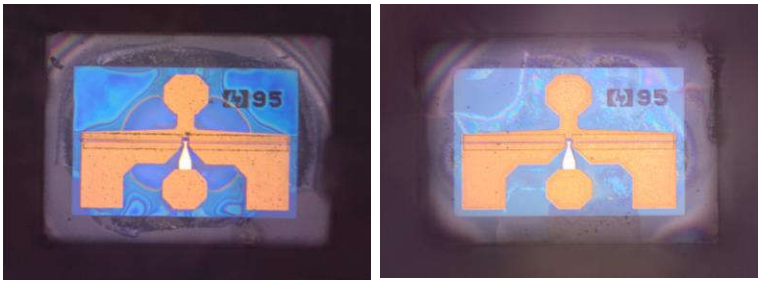

Fig. 9 Optical micrographs showing the comparison between the chip layouts after back- etched. #A on the left, and #B on the right.

As can be noticed, the dies show the same marking, an enlarged view of the logo is proposed in Fig. 10.

Fig. 10 Enlarged view of die marking. It is the same in both devices.

The "95" could be related to the real date of manufacturing. That would be in contrast with the data code and the marking of both A and B type.

In this case, the devices would have remarked possibly by different counterfeiters and then collected from the broker upon the customer enquire. The impossibility to obtain confirmation from the original manufacturer lets it just as a possibility.

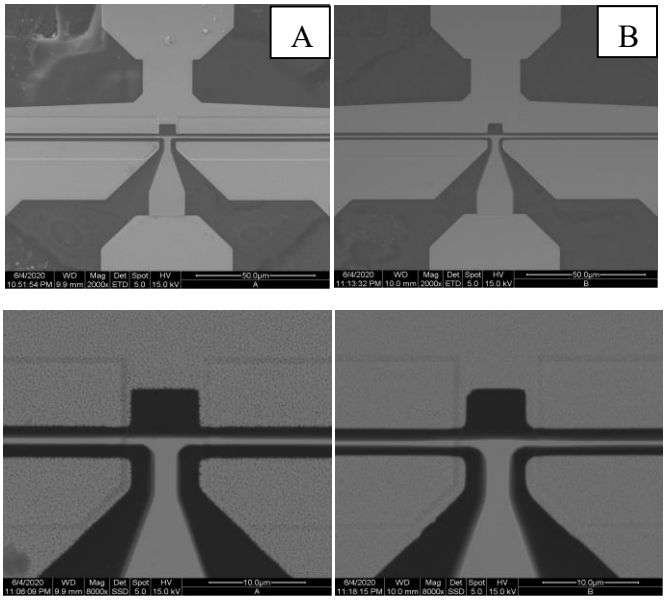

Fig. 11 SEM images showing further differences in the shape of the upper metal layer. #A on the left, and #B on the right

The back-exposed dies have inspected by using a scanning electron microscope (SEM) to add further information regarding the quality of the devices under analysis.

The most evident differences are visible in fig. 11. The shape and the dimensions of the metal layer appear different. The devices were fabricated by using different masks.

The set of information acquired induces to the conclusion that all the devices (Lot #A, B, C) for different reasons should be considered counterfeits. The discrepancies detected are sufficient to suspect for their originality. They are counterfeits because they have modified to allow the counterfeiters to have profit. A more accurate inspection of the labels on the reels adds the conclusive element that all of them have in common: the manufacturer's logo is presumably not original. It should confirm our hypothesis.

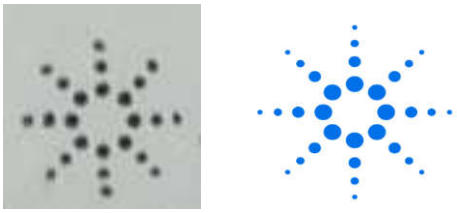

Fig. 12 Manufacturer's logo: presumably fake (on the left) and original (on the right).

The reported analysis has performed on a "cold" case study. But the impossibility to obtain confirmation from the original manufacturer and the unavailability of a genuine device enables only to a hypothesis.

It is worth proposing it, in any case, for two reasons. First of all, the customer was not able to obtain a refund. Moreover, this type of devices is still available in the gray market with evidence for discrepancies as the ones highlighted in this analysis.

Conclusion

Counterfeiting electronics is a cause of labour exploitation, environmental harm and potentially dangerous products. Nevertheless, it is a form of fraud and represents a critical reliability concern. It could cause personal injury, mission failure and dramatic reduction of the reliability of systems.

The lack of attention on the part of the component users meaningfully contribute to the widespread use of counterfeit electronics.

The most efficient method to assure product authenticity is the incoming product inspection. Enabling end-customers to recognize if a component is false before paying for it or at least before mounting it, substantially can reduce counterfeiting side effects.

It could not be necessary to do all tests proposed in the protocols to assure product authenticity. The inspection of exterior labelling and the marking font could help to detect counterfeits.

Even only a data sheet and shipping documentation verification, an extensive external visual inspection of product

using an optical microscope, and a marking permanency test could reduce the chance of mounting counterfeit parts.

In the proposed case studies, a sequence of detection steps and techniques has applied for detecting clues for possible counterfeiting.

Furthermore, the first example shows that even in cheap devices, the risk of counterfeiting is high, and the potential danger is not negligible. By comparison with a reference component, the analysis has detected many discrepancies among 3 suspected devices and the original one.

The labelling scheme and the code were not replicated accurately in A and B1 devices.

Even only this check would have suggested the hypothesis of counterfeiting. Moreover, the electrical characterization reinforced the suspicion confirmed after the de-capping.

The second example highlights the near impossibility of the final users to perform a thorough analysis, able to reject a part that has a risk of being counterfeit. A few details have detected able to arise the alert for counterfeiting. This insidious case should require a more in-depth analysis, even if reasonably, the devices could be:

1) Produced by lesser-trained personnel in midnight fabs and sold discounted and prone to quality issues. It may operate, but they will not work correctly in a more demanding environment, and they could even fail after months of operation.
2) Scrapped parts remarked able to fail immediately when electrically tested or first used.

The cases proposed in the paper should contribute warning for the many risks for small users of electronics devices showing blind confidence in the unreliable gray market.

There is no safer alternative than the official supply chain (manufacturers or authorized distributors) as a defence against counterfeit electronics parts.

If the devices are no longer available from the manufacturer due to obsolescence, unauthorized distributors will probably fill the gap. Mitigation method and simple strategic approaches should be in the knowledge of final customers to reduce the potential for acquiring fake parts, being conscious that the solution is far from over.

Acknowledgments

The research activities described in this paper have been conducted within the R&D project “Cagliari2020” partially funded by the Italian University and Research Ministry (grant# MIUR_PON04a2_00381). Roberto Murru is in debt with Georg Kell (www.ecworld.ru) for fruitful discussion.

References

[1] SIA Anti-Counterfeiting Task Force (2013)
[2] B. Sood et al., ”Screening for counterfeit electronic parts” J. of Mat. Science: Materials in Electronics Vol 22, I. 10, (2011)
[3] K. Chatterjee, D. Das, and M. Pecht “Solving the counterfeit electronics problem”, in Proc. Pan Pacific Microelectron. Symp. (SMTA), pp. 294–300 (2007)
[4] H. Livingston Avoiding Counterfeit Electronic Components IEEE Transactions on Components and Packaging Technologies 30(1):187 – 189 (2007)
[5] M. Pecht, The Counterfeit Electronics Problem Open J. of Social Sciences Vol.1, No.7, 12-16 (2013)
[6] https://www.erai.com/
[7] A.H Olney, “Eliminating the Top Causes of Customer-Attributable Integrated Circuit Failures” Proc. Of IPFA (2013)
[8] D.P. Hartgerink, “Case studies of counterfeit part detection in assembled products” Proc. Of ISTFA (2010)
[9] R. K. Lowry, “Counterfeit electronic components-an overview” Military, Aerospace, Spaceborne and Homeland Security Workshop (2007)
[10] G. Mura, “Reliability concerns from the gray market”, Microel. Reliab., 88-90 (2018)
[11] U. Guin D. DiMase and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead,” J. of Electr. Testing: Theory and Applications, vol. 30, 1, pp. 9-23, (2014)
[12] E. Oriero, S. R. Hasan, “Survey on recent counterfeit IC detection techniques and future research directions” Integration, the VLSI J. 66, 135–152 (2019)
[13] G. Meneghesso, A. Cocco, G. Mura, S. Podda, M. Vanzi, Backside failure analysis of GaAs ICs after ESD tests, Microel. Reliab., 42, 9-11, pp. 1293-1298 (2002)