Analysis of fake amplifiers

G. Mura, R. Murru, and G.Martines

Abstract - Counterfeiting electronics is a cause of labour exploitation, environmental harms and potentially dangerous products. It is a form of fraud and represents a critical reliability concern. In manufacturing, the use of undetected counterfeits can lead to increased scrap rates, early field failures, and increased rework rates causing a dramatic reduction of the reliability of systems.

I. Introduction

Counterfeit electronic components are fraudulent parts that have been confirmed to be a copy, imitation, or substitute that have been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud [1].

The most significant risks of using fakes parts are personal injury, mission failure and dramatic reduction of the reliability of a system and apparatus. Counterfeiting is of concern to consumers because of the significant health and safety risks that substandard electronics pose to those who use the items.

An exemplary analysis of the counterfeit problem, the screening/detection methods and the gray market's reliability concerns are proposed in [2]-[9]. Lack of caution on buyers, obsolescence, lower prices, costly inspection procedures, and absence of origin verification tools contribute to the widespread of fake electronics [10]- [12]. With the global emergency of COVID-19 last year, the global production of electronics suffered from slowing downs and stops. A year after, the consequences of this troublesome situation are causing a vital shortage of semiconductor devices. The shortage is due to substantial fluctuation in demand because of the pandemic and the increased use of semiconductors in advanced vehicles. COVID-19 has resulted in some impact on the sales of some consumer electronic products as well as the supply chain that supports consumer electronics manufacturing [14]-[17]. Foundries are currently unable to produce electronics fast enough to cope with the surge in demand. Counterfeiters have been encouraged from the lack of availability of the original product. The market of electronic parts will be overrun by counterfeit components, as a high demand corresponds to a small availability and increased lead time. Nowadays, some official distributors are informing their customers the lead time of some of their devices will be extended up to 54 weeks. The global semiconductor shortage may likely extend through 2022.

The global chip shortage is creating the perfect environment for fake electronics to enter the market. This is likely to become a big risk even for critical sectors such as defence, aerospace, medical and automotive. The present work aims at adding a piece of information in this context supporting evidence regarding the capillary penetration of counterfeit devices. Two case studies are proposed to contribute, highlighting the problems associated with the growing global traffic in counterfeit electronics parts. Finally, the aim is to show to the reader that, in case an analysis from a certified laboratory is not affordable, a reduced set of procedures can be used to reduce the incremented risk for counterfeiting. It could give more confidence regarding the quality of the devices.

II. Identifying fake devices

Identifying counterfeit devices can be a difficult task because not everything that seems suspect is necessarily a fake. The most common practices that have been used to identify fakes are proposed in [3], [4], [8]-[13]:
marking and packaging inspection,
- x-rays analysis,
- electrical measurements,
- material characterization,
- decapsulation physical analysis.

Moreover, Standards such as AS5553, AS6171 provide specific workflow of procedures that can have potentially higher costs but the highest chance of minimizing the risk.

III. Case I

A set of commercial low voltage audio power amplifiers bought from a third-party seller on a popular electronics consumer website (A) failed in a consumer application. One of them was replaced by another device purchased from a local retailer (B1). The former showed the same kind of problem. Another set of devices was bought from a second local retailer (B2), showing low gain performances than expected. It worked but indeed, not as it should have done. Finally, the same amplifier was bought from an online authorized retail sales company (C) that gained the AS6496 accreditation for anti-counterfeit measures. The device was replaced, and the problem was fixed. The analysis was carried out to understand if # A, B1, B2 are counterfeit devices. The investigation concluded that A and B1 are the same fake amplifier, and even B2 should be considered fake [10].

Some further evaluations are proposed to enlarge the knowledge of approaches that could help minimise the risk, mainly if an in-house test facility is not available.

The devices passed the permanency marking test. The complete procedure is defined in Mil-STD-883G

G. Mura, R. Murru, and G.Martines are with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D’Armi, 09123 Cagliari, Italy, E-mail: gmura@diee.unica.it

Method 2015.13. Using a Leica CLS 150x, a low magnification optical comparison is proposed in fig. 1.

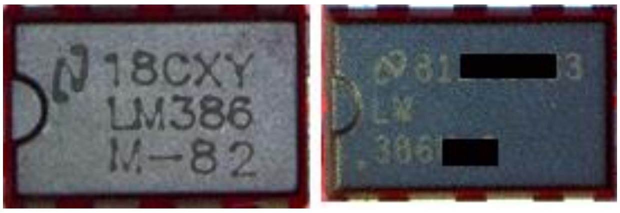

Fig.1. Optical comparison between #B1 and C. The marking of the original has been intentionally covered.

Differences in the marking and the manufacturer logo are observed. In addition, the pin 1 indentation is missing in A and B1 and not aligned in B2. (fig.2).

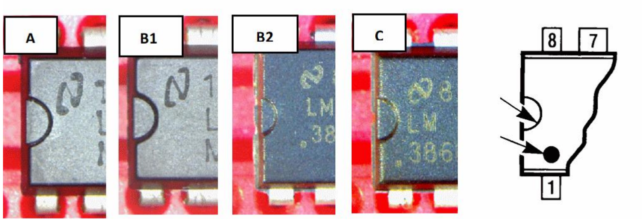

Fig. 2. The pin 1 indentation indicated in the datasheet is missing in #A and B1, not aligned in #B2

Consequently, the quiescent current versus voltage measurements was acquired through an Agilent B1500A. It was done in comparison with the original device C, showing that #A, B1 and B2 are, at different levels, out of electrical specification parameters (fig 3).

A further non-destructive test was conducted using a Nordson DAGE Quadra7 for the x-rays analysis performed at 120KV and 12W. The investigation revealed differences in the die paddles and die orientations (fig.4).

A manual wet chemical decapping was performed using hot nitric acid. It enabled the inspection of the layout using an Olympus BX43. #A and B1 showed the same layout. It differs from both #B2 and #C (fig.5). Moreover, a marking consistency inspection revealed the final part of the marking code of A and B1 is unknown to the original manufacturer. Compared with C, they showed differences in shipping packages, price, package marking, information encoded in the mark, weight, die paddle and die orientation, electrical characteristics, plastic package, and layout. The previous conclusion is confirmed. A and B1 appear as fraudulent copycats of the original. Otherwise, the product marking code of B2 is compatible with the original C. B2 appears much more similar to C. Differences were detected in price, package marking, die paddle, electrical characteristics, plastic package, and layout. As revised designs are not available, B2 could be a more accurate copy- cat or a scrapped/ harmful storage part.

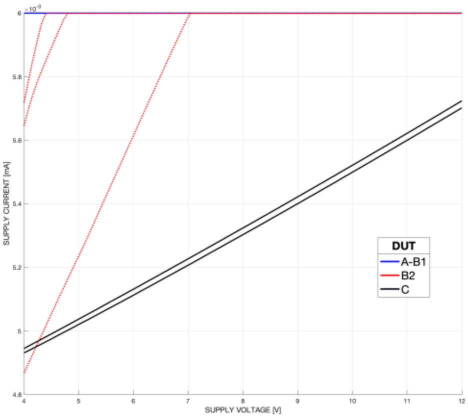

Fig. 3. Electrical comparison between #A, B1, B2, C

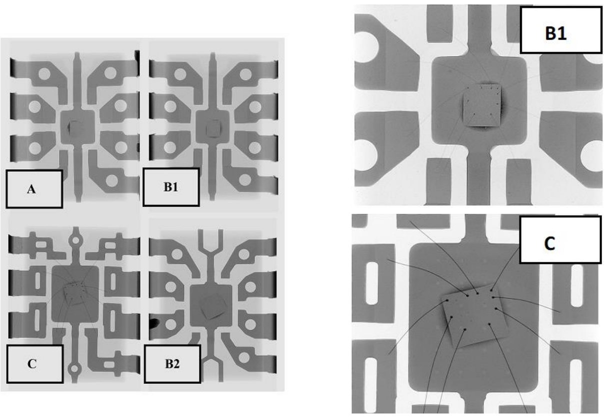

Fig. 4. X-rays comparison between #A, B1, B2, C

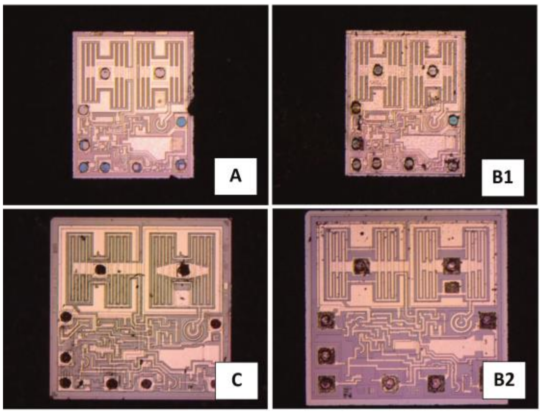

Fig. 5. Optical comparison between #A, B1, B2, C after the chemical removal of the plastic packages

IV. Case II

After a decade of intense operation, a high-speed JFET input dual operational amplifier failed in an old electronic system. From the original manufacturer, the DIP8 package resulted obsolete. A set of amplifiers was purchased from a broker to replace it. Before mounting it, permanency marking test was carried on to examine the resistance of part markings to solvents. A laser-marked package was expected, but in some devices (#D), the solvent was able to remove the marking (fig.6). No ghost marking was detected. At the same time, to conduct an analysis, a set of SO-8 packaged of the same device (#E) was purchased from an authorized seller.

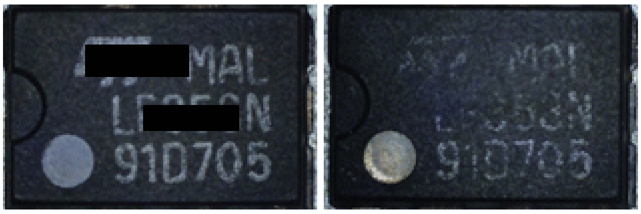

Fig.6. #D after permanency marking test (intermediate step)

Genuines (#E) and suspected fakes (#D) were electrically characterised using an Agilent 22330 and a Digilent Analog Discovery 2.

In particular, the first test measured the current drawn from the power supply by the devices, with no load and no sources connected. All the devices draw current from 2.7mA to 3.2mA, which is in the range indicated by the manufacturer. The second test was oriented to check the slew rate (SR) of the devices. Firstly, by setting the input to Vi=10V, the SR was measured. The SR of all the devices stayed within the range stated in the datasheet, from 12V/µs to about 16V/µs.

Moreover, abnormal behaviour was observed in the suspected ones (#D). As reported in fig.7 in the negative half-waves, the dampening appeared to be absent, leading to an oscillation of the output until it reached the positive half-wave again.

In addition, by setting the input to Vi=20mV, the rise time and the overshoot were measured. The rise time stated in the datasheet is typically 100ns. The devices went from 30ns to 70ns, so all were within the range. As reported in fig. 8, the suspected devices showed a higher peak overshoot and undershoot (almost absent in the original ones) and subsequent oscillations, leading to a higher settling time after the overshoot.

This result suggests that device #D may be prone to oscillation when inserted into a complete circuit.

The chemical removal of the plastic packages of #D and E enabled the analysis of the dies. #D resulted correctly marked (even if the logo in #D is in a different position in the die) and without macroscopic differences in the layouts (fig. 9). The devices #D are not copy-cat/ reproduction of the original. #D appears out of specification/defective represented as conforming, probably scraped and remarked or overproduced devices. They can be reasonably suspected of being fakes, as even the easy removal of the marking point to this interpretation.

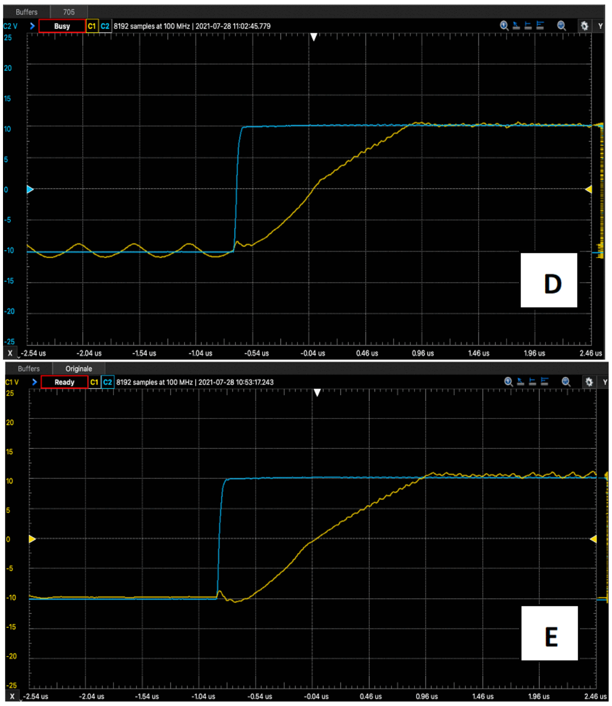

Fig. 7. Original on the bottom, suspected on the top. Slew rate measurements. An oscillation of the output appears only in D.

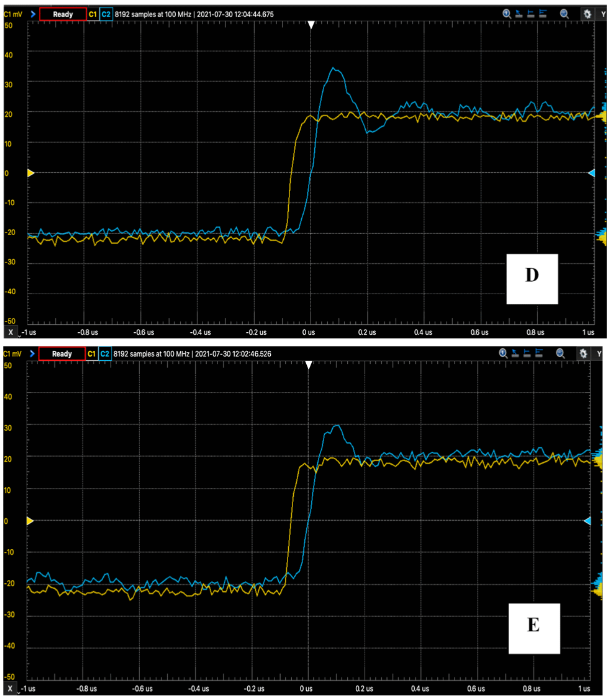

Fig. 8. The rise time and the overshoot measurement. Higher over peak and settling time appear only in D.

Further studies in terms of HAST/ MIL-STD 883 Burn-in could help to support this hypothesis.

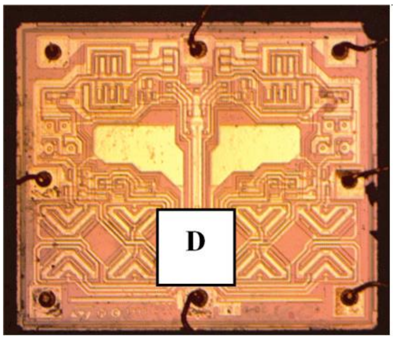

Fig. 9. Suspected fake #D after decapping. The genuine is intentionally not reported.

V. CONCLUSION

Counterfeit electronics is a reliability problem. Uncontrolled storing, counterfeiting manipulation, and inaccurate handling can frequently create the potential for product malfunction and significantly increase the risks of introducing reliability criticalities in terms of sudden or latent failures in electronics systems.

The COVID-19 pandemic has impacted the technology with a huge request and a consequent critical shortage of microelectronics. This fact is going to increase the proliferation of counterfeit electronic parts. While it may be impossible to completely prevent the distribution of counterfeit parts into the supply chain, more than ever, it is mandatory to have extreme vigilance when purchasing semiconductors. The best practice is not sourcing from unlicensed distributors or “brokers”. However, design, obsolescence, or the actual market conditions may force to pursue gray market sourcing.

If the devices are no longer available from the official market, unauthorized distributors in the gray market will fill the gap, and an increase in purchases is expected.

Customers are quite often unaware of the risks associated with using unreliable electronics.

In case of purchase from unofficial sellers, it must be requested that reputable sources have supplied parts.

Furthermore, the examples show that even in cheap devices, the risk of counterfeiting is high, and the potential danger is not negligible. On the other hand, the identification of a counterfeit is not easy and straightforward. It requests several steps of investigation.

Mitigation methods should be in the knowledge of final customers to reduce the potential for acquiring fake parts.

The complete sequence proposed by the international standards and performed by accredited labs will provide the highest chance of minimizing the risk of fakes entering the production line. If not affordable, a risk reduction strategy using a flexible set of tests could be applied for detecting clues for possible counterfeiting.

ACKNOWLEDGEMENT

This work has been founded by “Fondazione di Sardegna” under project “ARGOSAT – Microsatellite cluster for the observation of optical transients in Astronomy”, CUP: F74I19001070007.

The authors are in debt with A. Furlani and S. Frantellizzi from Cabiotec Srl for x-rays analysis.

REFERENCES

[1] SAE Aerospace Standard AS6081

[2] M. Pecht, S. Tiku,” Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics” *IEEE Spectrum*. 2006, 43(5), pp. 37-46.

[3] B. Sood, D. Das, M. Pecht,” Screening for counterfeit electronic parts” *J. of Material Science: Materials in Electronics*, 2011, Vol 22, I. 10, pp. 1511-1522.

[4] U. Guin, M. Tehranipoor and D. Dimase, “Counterfeit IC detection and challenges ahead”, *Journal of Electronic Testing*, 2014, 30, 1, pp. 9-23.

[5] J. Stradley; D. Karraker, “The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications”, *IEEE Trans. on Comp. and Pack. Tech*. 2006, vol. 29, 3. pp. 703-705

[6] K. Huang, J. M. Carulli, Y. Makris, “Counterfeit electronics: A rising threat in the semiconductor manufacturing industry” 2013, *Proc. Of IEEE International Test Conference (ITC).*

[7] G. Mura, “Reliability concerns from the gray market”, *Microelectron. Reliab*., 2018, 88-90, pp.26-30.

[8] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proc. of the IEEE*, 2014,102, pp. 1207-1228.

[9] U. Guin D. DiMase and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead,” *J. of Electr. Testing: Theory and Applications*, 2014, 30, 1, pp. 9-23.

[10] G. Mura, R. Murru, G. Martines, “Analysis of counterfeit electronics” *Microelectron. Reliab*., 2020, 114, pp.1-4.

[11] Y.L Wang, XJ Kuang, CM Huang, S.P Li, “Case studied of failure threat caused by counterfeit plastic encapsulated microcircuits”, *Proc. Of IEEE IPFA*, 2013, pp 574-577

[12] A.H Olney, “Eliminating the Top Causes of Customer-Attributable Integrated Circuit Failures”, *Proc. Of IEEE IPFA*, 2013, pp.8-14.

[13] G. Mura, M. Vanzi, “The interpretation of the DC characteristics of LED and laser diodes to address their failure analysis”, *Microelectron. Reliab*, 2010, 50(4), pp. 471–478.

[14] Z. Xu; A. Elomri; L. Kerbache; A. El Omri “Impacts of COVID-19 on Global Supply Chains: Facts and Perspectives”, *IEEE Engineering Management Review,2020,* pp. 153-166.

[15] J. Nayak, et al. “An impact study of COVID-19 on six different industries: Automobile, energy and power, agriculture, education, travel and tourism and consumer electronics”, *Expert Systems*, 2021, pp. 1-32.

[16] T. Coughlin “Impact of COVID-19 on the Consumer Electronics Market”, *IEEE Consumer Electronics Magazine*, 2021, 10, 1, pp.58-59.

[17] https://www.semiconductors.org