Electronic components authentication via physical analysis

G. Mura, S. Carta, P. C. Ricci and G. Martines

Abstract - Counterfeit electronics is a reliability problem. Undetected counterfeits can lead to increased scrap rates, early field failures, and rework rates, causing a dramatic reduction in the reliability of systems. Identifying counterfeit devices can be challenging because not everything that seems suspect is necessarily fake. On the other hand, counterfeiters keep growing and adapting.

I. INTRODUCTION

In today's interconnected and technology-driven world, the reliability problem affecting the global electronics supply chain is a matter of primary importance. Starting from the simplest components (resistor, capacitor, etc.), passing by complex integrated circuits, arriving at entire PCBs, there is not a single device that can be considered immune from the plague of counterfeiting.

However, several case studies in the literature [3]-[8] demonstrate that even inexpensive devices have a high chance of counterfeiting and that the associated threat is not insignificant.

Counterfeit electronics includes recycled, remarked, refurbished, overproduced, defective, cloned, and tampered devices. They may be reclaimed from e-waste, product overruns, modified authentic parts, or copies. [1], [2]

The Covid pandemic is the cause of the electronics shortage that, in turn, is a golden opportunity for counterfeiters. The electronic parts market is overrun by counterfeit electronics. Low prices and immediate availability become very attractive even without real assurances about quality and reliability. Even sensitive sectors such as the medical, military and aerospace industries are probably forced to evaluate purchases in the grey market.

Counterfeit parts pose a severe threat to national security and human lives. Counterfeit defence needs constant awareness and effort. In addition, counterfeiters keep growing and adapting, so it is necessary to address evolving threats.

External inspection cannot provide complete information to determine if the device is from the original equipment manufacturer (OEM) or a counterfeit, even when the device under analysis physically looks identical and has identical labelling. In the identification process, many techniques can be used, both simple and sophisticated. On the other side, not everything that seems suspect is necessarily fake.

In the following, a case study of an IC amplifier is presented, with some techniques and approaches, from most superficial optical inspection to complex Raman analysis, that combined can lead to the quest for counterfeit identification.

Moreover, starting from the case presented in [9], further investigations are proposed on new sets of devices to confirm that detecting a counterfeit is a challenging task, and more than a simple analysis of the external details is needed to state if it is fake. A customized sample test sequence for very low-risk applications is performed.

The conclusion is that devices with several different external characteristics are, in the end, proved to be authentic.

In general, excluding gross visual anomalies, e.g. due to re-use, re-furbishing or re-marking, which are sure indicators of counterfeiting, some differences between devices can be inconsistent with counterfeiting because they are only related to product change processes.

During this electronic shortage phase, more accurate analysis must be performed before rejecting parts after a simple external inspection/ x-rays analysis. It is a mandatory constraint when dealing with the authentication of electronics.

II. DETECTION PROCEDURES

The methods that have been most frequently used to spot fakes are suggested in [1], [2]: analysis of shipment/ product documents, external visual inspection, x-ray analysis, and electrical tests. These procedures are quick, non-destructive processes that anybody may easily carry out to offer the bare minimum of protection, and they are simple to include in the printed circuit board fabrication process. They should be applied to the entire lot. In addition, deeper verifications could necessitate analytical methods, specialized labs, and knowledge. It increases the cost of the analysis, especially in case of a destructive procedure.

The material characterization and delid/decapsulation physical analysis (DDPA) are needed for the microscopic examination. Many of these techniques are generally used during the diagnostics and failure analysis of electronic devices, they can contribute to understanding

G. Mura, S. Carta, and G. Martines are with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D'Armi, 09123 Cagliari, Italy, E-mail: giovanna.mura@unica.it

P.C. Ricci is with the Department of Physics, University of Cagliari, 09042 Monserrato, Italy.

counterfeiting techniques and the effectiveness of monitoring and reporting [10]-[13].

III. THE CASE STUDY

The devices under analysis are some LMxxx low-voltage power amplifiers, designed for use in consumer applications and acquired from different sources. The device is provided in a plastic dual-in-line package.

The pin layout is illustrated in Fig. 1

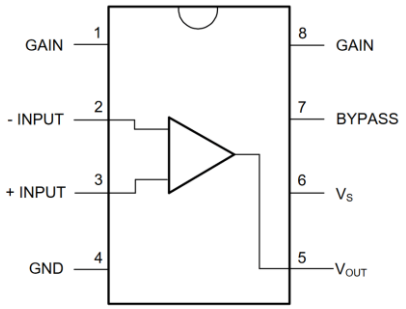

Fig.1. Pin layout.

Three set of devices (namely #1, 2, 3) acquired from official and unofficial distributors are here compared to show that a simple external inspection cannot demonstrate whether the devices are original. A systematic counterfeit detection approach is proposed, including optical inspection, size measurements, electrical parameter measurement and package plastic decapping.

The devices' external visual inspection (EVI) is shown in Fig. 2. At the same lighting condition, only the marking of device #1 is visible. The pin 1 identification is the same in devices #1 and 2 but differs in device #3, and, in addition, in the latest even the notch is missing.

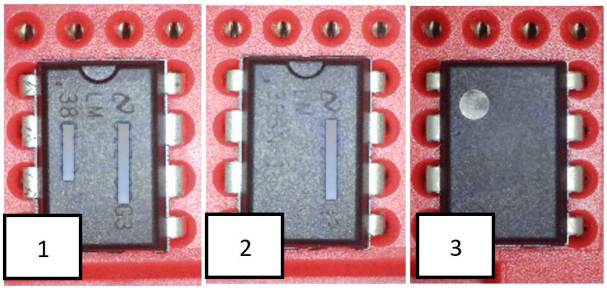

Fig. 2. External inspection and comparison (same lighting condition). The marking is intentionally partially covered.

The analysis of devices' dimensions (package length, width and thickness, lead width) is consistent with the dimensional range reported in the datasheet.

By means of an Agilent B1500A semiconductor parameter analyzer, the electrical measurements in terms of the quiescent supply current vs the supply voltage were acquired, resulting in agreement regarding trends and values with the datasheet for all the devices (#1, 2, 3). Specifically, the quiescent current at 6 V resulted in the acceptable range (4-8 mA). The measurement setup is proposed in Fig. 3.

In addition, gain voltage measurements (supply voltage = 6 V) were acquired, they resulted once again for all the devices in agreement with the data sheet. In fig. 4 the measurement setup is proposed.

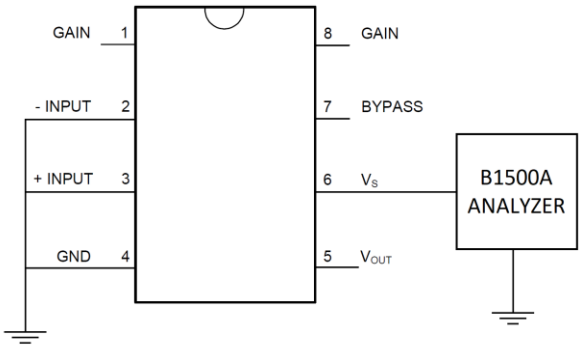

Fig. 3. Set up for the quiescent current measurement.

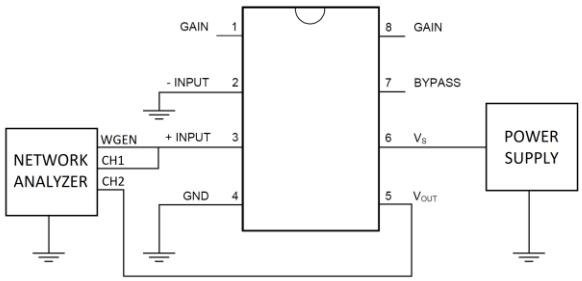

Fig. 4. Set up for the gain voltage measurement.

To avoid the luminescence from the samples, the Raman chemical analysis of the plastic packages was performed by a Fiber coupled Raman system BW-tek i-Raman Plus, at 1064 nm. This technique is an analytical method that can contribute to the authenticity assessment of electronic components [14].

The devices do not show significant differences and have very similar Raman spectra with slight variations in signal strengths as shown in Fig. 5.

The analysis directly proceeded with the DDPA for internal inspection. The manual chemical decapping of the devices is shown in Fig. 6. The sample preparation aimed to preserve the copper frame to save the cost of an x-ray analysis. Devices #1 and 2 were easily de-processed by using hot nitric acid. The frame structure of device #3 was not preserved using the same chemical wet etch. Consequently, device #3 was deprocessed using a nitric-sulfuric mixture solution at room temperature. Low-magnification optical pictures enable the comparison of the copper frames and the position of the dies. Devices #1 and 2 have the same lead frame structure but opposite

orientations of the dies. Devices #3 show a different lead frame.

Altogether, the devices show differences in term of marking, pin 1 identification (printed or indented), notch, lead frames, and slightly even in plastic packages.

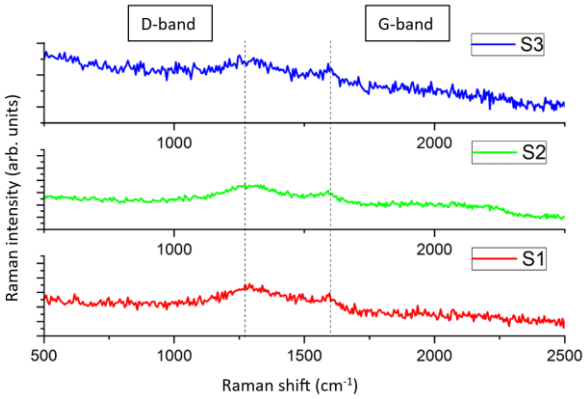

Fig. 5. The chemical analysis of the plastic packages by using Raman spectroscopy. The comparison does not show significant differences among the plastic packages but only the spectra of a graphitic layer.

On the other side, the optical inspection of the dies reveals the same layouts and internal marking for all the sets (#1, 2, 3), confirming that the three devices are authentic.

Moreover, devices #1 and 3 are purchased from official distributors, and #2 is from the grey market.

Devices #1 and 3 are authentic, and device #2 can be assumed original with a very high confidence. In this case study neither differences in the marking and package appearance nor in the frame structure or orientation could be able to identify a counterfeit, since these variations are physiological in the life cycle of a device or in its production process.

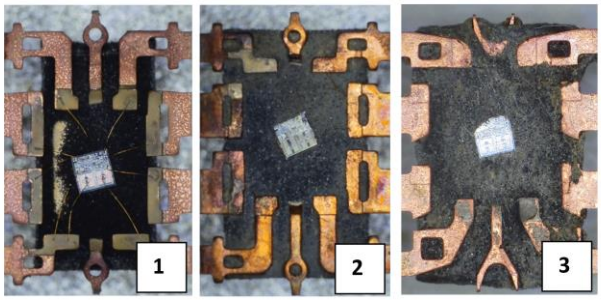

Fig. 6. Removal of the plastic packages. The optical comparison of the deprocessed devices maintaining the same chip orientation shows three different lead frames.

In addition, two sets of devices were subjected to a thermal screening to precipitate, in devices #2, potential latent defects related to storage in a hostile environment or mishandling. Set #3 was tested in parallel just for electrical comparison.

A MIL-STD-883 - method 1015 burn-in test was performed on devices #2 and 3. The manufacturer indicates in the datasheet that the maximum storage temperature is 150°C. Consequently, the selected conditions were 150°C for 80 hours. At the end of the burn-in test, non-relevant electrical degradation was observed in the sets #2 and 3.

III. Conclusion

Customers frequently need to be aware of the dangers of utilising counterfeit devices.

The wisest practice is to not purchase from unlicensed distributors or “brokers”. However, design, obsolescence, or market conditions may force an OEM or electronic contract provider to pursue grey market sourcing. If the devices are obsolete and may only be available from unauthorised distributors in the grey market, an increase in the risk for counterfeiting must be expected. Likely, critical sectors must also evaluate purchases made on the grey market. For example, the automotive industry continues to be plagued by a chip shortage, and, at the same time, automotive EEE components are increasingly more eligible for New Space Economy applications [15]-[17].

When buying from unauthorised merchants, it is necessary to demand proof that the components came from reliable sources.

The risk must be addressed. The detection of a fake, however, is a complex process. It necessitates a thorough inquiry, since determining if a device is fake or not requires more than a simple external analysis. Customers should be aware of mitigation strategies to lessen the chance that they may purchase counterfeit components. Moreover, more than a simple external inspection is required to discriminate, avoiding erroneous rejecting of original devices.

The best way to reduce the risk of fakes entering the manufacturing line is by following the procedures suggested by international standards and carried out by recognised labs. In particular, the standard and its slash sheets provide a complete guidance and plenty of examples helpful for suspect counterfeit part detection [18]. These provide detailed workflow of procedures that can have potentially higher costs but the highest chance of minimizing the risk.

If cost-effective, a risk-reduction method employing a flexible set of tests might be used to look for signs of potential forgery.

The Authors think the performed customized procedure is suitable in case the failure of the product is not severe enough to cause injury or system damage but only may result in unscheduled repair. Otherwise, only the entire standard SAE AS6171A is the appropriate guideline. On the other hand, in times of electronic shortage, an

evaluation must be performed before rejecting parts after a simple external inspection.

ACKNOWLEDGEMENT

This work has been founded by “Fondazione di Sardegna” under project “DACE – Detection and Avoidance of counterfeit electronics”, CUP: F73C22001310007.

REFERENCES

[[1] 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.

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

[3] Y. Hong, “Detection of a Counterfeit OTA Device and Certification of a Replacement Source” in *Proc. 37th International Symposium for Testing and Failure Analysis, ISTFA 2011.*

[4] A. Shrivastava, M. Pecht, “Counterfeit capacitors in the supply chain” J Mater Sci: Mater Electron, 2014, 25, pp. 645–652

[5] D.P. Hartgerink, “Case studies of counterfeit part detection in assembled products” in *Proc. 36th International Symposium for Testing and Failure Analysis, ISTFA 2010*

[6] Y.L Wang, XJ Kuang, CM Huang, S.P Li, “Case studied of failure threat caused by counterfeit plastic encapsulated microcircuits”, in Proc. *20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits, IPFA 2013*, Suzhou, pp 574-577.

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

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

[9] G. Mura, R. Murru, and G. Martines, “Analysis of Fake Amplifiers” in *Proc. 32nd IEEE International Conference on Microelectronics, MIEL 2021, Nis,* pp. 131 – 134.

[10] P. Martin, “Electronic failure analysis handbook” Soldering & Surface Mount Technology, 11 (3), 1999.

[11] L. C. Wagner, Failure Analysis of Integrated Circuits: Tools and Techniques L.C. Wagner, "Failure analysis of integrated circuits: tools and techniques”, Kluwer Academic Publishers, 1999.

[12] T. Gandhi, "Microelectronics Failure Analysis," Desk Reference-ASM International, 2019.

[13] G. Mura, M. Vanzi, “Failure Analysis of Failure Analyses: The Rules of the Rue Morgue, Ten Years Later” *IEEE Transactions on Device and Materials Reliability*, 2007, 7, 3.

[14] H. Vaskova, P. Neumann, M. Kozubik, K. Jelinek “Raman Spectroscopic Study of Counterfeit Electronic Components” *WSEAS Trans. on Systems and Control*, 2028, 13, 453-9.

[15] S. A. McDermott, A. Jacobovits and H. Yashiro, "Automotive electronics in space: combining the advantages of high reliability components with high production volume," Proceedings, IEEE Aerospace Conference, 2002.

[16] R. Ramesham "Environmental testing of COTS components for space applications", *Proc. SPIE 7206, Reliability, Packaging, Testing, and Characterization of MEMS/MOEMS and Nanodevices VIII, 72060H, 2009*.

[17] R. Enrici Vaion, M. Medda, A. Mancaleoni, G. Mura, A. Pintus, and M. De Tomasi, “Qualification extension of automotive smart power and digital ICs to harsh Aerospace mission profiles: Gaps and opportunities”, *Microelectron. Reliab*., 2017, 76–77, 438-443.

[18] SAE International, AS6171A: Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.