Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Counterfeit Electronics Detection Via Physical Analysis

Simone Carta, Giovanna Mura

DIEE University of Cagliari, Cagliari, Italy

Keywords: counterfeit electronics, fake electronics, physical detection, visual inspection, electrical characterization, decapsulation

Counterfeiting is an illegal procedure that involves the fraudulent imitation of the original copy for lucrative or criminal activity. This work will discuss the issue of counterfeits in electronics in terms of quality, reliability, and safety of use. The problem of counterfeit electronic products is not new, but it remains critical; it can cause personal injuries, mission failures and a dramatic reduction in the reliability of systems (DiMase, 2016; Mura, 2018, 2022; Sood, 2011). Detecting counterfeit electronics throughout the supply chain by analyzing their physical properties can help identify suspicious components. The best practice is not sourcing from unlicensed distributors. Still, design, obsolescence, or shortage may force one to purchase in the unofficial market, where acquiring counterfeits is highly probable. Counterfeit components can be produced and distributed in several ways in the unofficial market. Recycled devices may have a lifetime reduced than expected due to the prior usage, and, in addition, they could have been subjected to improper dismantling, handling or storing in an uncontrolled environment. These conditions may favour failure mechanisms such as delamination, pop-corning, thermo-mechanical stress, corrosion, electrostatic discharge, etc., due to unchecked exposure to temperature, humidity, and static electricity, which can cause latent damage or catastrophic failures in field operation. Remarked devices are subjected to sanding, microblasting, acid etching, blacktopping, or other remarking activities that could impact the parts' functionalities and even hide the devices' performances, indicating higher performances than the real ones. Remarked commercial-grade components are deceptively sold as military-grade. Scrapped devices are parts that have failed screening production tests due to design weaknesses or internal defects. Instead of being destroyed, they have been re-introduced in the market. They can fail early due to their increased failure rate and unconformities. Tampered devices are generally intended for sabotage, and they can cause dangerous consequences, giving access to critical functionalities of the systems that incorporate them. Different techniques are required to deal with many distinct counterfeiting possibilities. Moreover, the detection and avoidance methods are evolving because counterfeiting techniques may adapt (Aramoon, 2020; Dogan, 2014; Guin, 2014; Hoveida, 2023; Stern, 2018). The most common fake detection practices are product or shipping documentation analysis, external visual inspection (EVI), x-ray analysis, electrical measurements, destructive physical analysis (DPA), and material/layers characterization (AS6171A, 2018). Above all, the EVI intends to detect gross visual anomalies on the marking, the packaging, and the leads. Electrical measurements represent an important non-destructive step in the verification process because, through them, it is possible to determine if the device is functionally conformed with the datasheet and are conclusive in identifying the failure modes in defective units. Generally, more is needed to determine if a device is counterfeited (Mura, 2020). The DPA for microscopic inspection is a destructive removal of the package used when examining the internal structure, which is fundamental to determine if the part is suspected to be counterfeit. The previous techniques are applied in the subsequent case to show some limits and how discrepancies in the analysis can or cannot be "red flags" in the identification process of counterfeit devices.

The devices under test are some LMxxx power amplifiers designed for low-voltage consumer applications purchased from an official distributor (O) and different unofficial sellers (A, B, C). Optical and electrical comparison is proposed in Figure 1 and Table 1. The markings on devices A and C are different but can be easily read under the same conditions of light and magnification, and B cannot. Markings on devices A and B follow the manufacturer's guidelines; the C ones do not. In addition, the logo on device C appears irregular, probably due to a low-quality laser-marking process. Table 1 reports the electrical parameters, referring to the typical values declared in the manufacturer's datasheet and the measurements done on devices O, A, B, and C. Electrical

characterization can help identify suspicious components, but the analyst should keep in mind that differences with typical values do not necessarily indicate a counterfeit part but, e.g., the variability of the process.

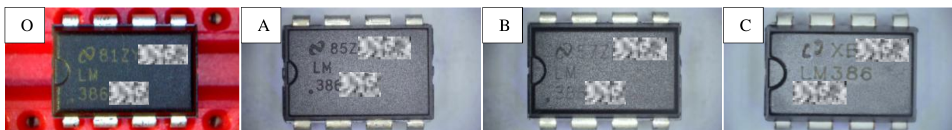

Figure 1. Top side of four LMxxx amplifiers under the same conditions. The marking is intentionally partially covered.

Table 1. Typical and measured values for three different parameters.

Electrical characteristics	Datasheet	Originals	Device A	Device B	Device C
Quiescent current [mA] (at V_S=6V, V_I=0V)	4	4.67 (0.08)	3.70	4.60	3.72
Voltage gain [dB] (at V_S=6V, f=1 kHz)	26	27.11 (0.04)	27.6	27.1	26.2
Bandwidth at 3 dB [kHz] (at V_S=6V)	300	605 (12)	901	583	1479

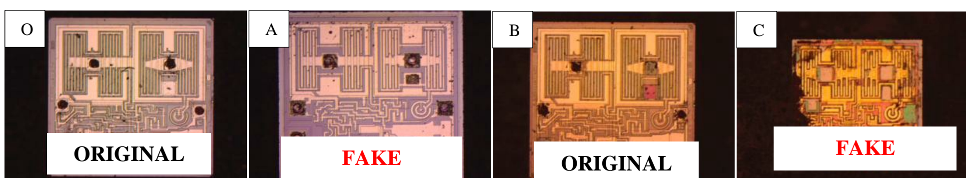

Figure 2. LMxxx amplifiers layouts optical comparison.

This kind of difference should be considered a red flag. In this case, the DPA proposed in Fig. 2 is conclusive for the authentication. Only type B is original. A and C are counterfeit devices.

In conclusion, while it is almost impossible to prevent the penetration of counterfeit parts into the supply chain, more than ever, it is mandatory to have extreme vigilance when purchasing semiconductors. If an analysis from a certified laboratory is not affordable, a reduced set of procedures can be used to decrease the increased risk of counterfeiting. It could give more confidence regarding the quality of the devices. Even critical sectors are probably forced to buy in the unofficial market. It should raise concerns if one considers that EEE components are eligible even for new space economy applications. (Enrici Vaion, 2017).

The authors believe it is worth sharing knowledge on this critical aspect and reducing the blind confidence in unauthorized sellers of consolidated technologies.

Acknowledgements

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

References

Aramoon, O. et al. 2020. Impacts of Machine Learning on Counterfeit IC Detection and Avoidance Techniques, Int. Symp. on Quality Electronic Design, Santa Clara, CA, 352-357.

AS6171A, 2018 SAE International, Aerospace Standard.

DiMase, D. et al. 2016. Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems. Risk Analysis 36(10), 1834-1843.

Dogan, H. et al. 2014. Aging analysis for recycled FPGA detection. IEEE Int. Symp. on Defect and Fault Tolerance in VLSI, 171-176.

Enrici Vaion, R. et al. 2017. Qualification extension of automotive smart power and digital ICs to harsh Aerospace mission profiles: Gaps and opportunities. Microelectronics Reliability 76–77, 438-443.

Guin, U. et al. 2014. Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead, J. of Electr. Testing: Theory and Applications 30, (1), 9-23.

Hoveida, P. et al., 2023. Terahertz-readable laser engraved marks as a novel solution for product traceability. Scientific Reports 13, 12474.

Mura, G. 2018. Reliability concerns from the gray market. Microelectronics Reliability 88-90, 1-4.

Mura, G. et al. 2020. Analysis of counterfeit electronics. Microelectronics Reliability 114, 1-4.

Mura, G. et al. 2022. Reliability Risks from Counterfeit Electronics. Int. Conf. on System Reliability and Safety Engineering, 297–301.

Sood, B. et al. 2011. Screening for counterfeit electronic parts. J. of Material Science: Materials in Electronics 22(10), 1511-1522.

Stern, A. et al. 2018. EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection with Demonstration on Remarked and Cloned ICs. IEEE Int. Test Conf, Phoenix, AZ, 1-9.