

UNICA UNIVERSITÀ DEGLI STUDI DI CAGLIARI



UNICA IRIS Institutional Research Information System

This is the Author's *accepted* manuscript version of the following contribution:

Giovanna Mura, Giovanni Martines "Reliability risks from counterfeit electronics" in 4th International Conference on System Reliability and Safety Engineering (SRSE), Guangzhou, China, 2022, pp. 297-301.

©2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

The publisher's version is available at:

http://dx.doi.org/10.1109/SRSE56746.2022.10067413

When citing, please refer to the published version.

This full text was downloaded from UNICA IRIS https://iris.unica.it/

Reliability risks from counterfeit electronics

Giovanna Mura and Giovanni Martines
Dept. electrical and electronic engineering
University of Cagliari
Cagliari, Italy
e-mail: giovanna.mura@unica.it

***Abstract*— Counterfeit electronics is a critical reliability concern. It is a form of fraud that could cause personal injury, mission failure and a dramatic reduction of the reliability of systems. Physical detection is a helpful approach against supply chain counterfeits penetration. The present work addresses the fundamental steps for verifying electronic components to mitigate the risks of receiving or using suspect fake parts.**

Keywords: counterfeit electronics; electronics supply chain; grey market; reliability; physical detection.

I. INTRODUCTION: THE COUNTERFEIT PROBLEM

A counterfeit electrical, electronic, and electromechanical (EEE) part is defined as [1]:

- an unauthorized copy, imitation, substitute or modified EEE part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine item from an original component manufacturer or authorized aftermarket manufacturer; or
- previously used EEE part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used.

The origin of the counterfeit electronics problem has been explained in [2-4].

The failures of systems that contain counterfeit EEE can cause reliability risks, human safety and security problems and, in addition, harm the economy. It has been reported that counterfeit devices were detected in situations where failures could have been catastrophic such: as defence systems, radiation detectors, secure communications devices, space applications, medical devices, high-speed trains brakes and airport landing light systems with high-risks to the people involved [5-10].

A counterfeit electronic component significantly threatens product quality and reliability, even in non-critical systems. In these cases, detecting a counterfeit before or during the assembly phase is preferable because the highest costs are associated with failures or anomalies in field applications. The failure after the customer receives the product or service is usually more expensive than the component.

In the case of critical systems, detection as soon as possible becomes a mandatory constraint.

It must be remembered that sometimes counterfeit devices fail immediately when electrically tested or first used, but others could even fail after months or years of operation. Latent defects could suddenly fail in field operation or, more insidiously, cause erratic performance. In the following, several examples are proposed to provide helpful support during screening suspected devices.

II. UNRELIABILITY OF COUNTERFEIT ELECTRONICS

The reliability of an electron device is defined as the probability that when operating under specified conditions, it shall perform satisfactorily for a given period. Two approaches generally available for assessing the reliability of electronics during design are device failure rate prediction and physics-of-failure [11, 12].

The reliability of electronics depends on their capability to withstand stresses. The most prominent stress affecting electronics are temperature, humidity, bias, vibrations, and electrostatic discharges.

Counterfeit electronics include recycled, scrapped and tampered parts.

Recycled devices, as they are not new even if they initially work, may have a lifetime reduced than expected due to the ageing introduced by prior usage. In addition, recycled devices may be subjected to improper dismantling, handling or storing in an uncontrolled environment. It may favour failure mechanisms such as electrostatic discharge, delamination, pop-corning, thermos-mechanical stress, corrosion, etc., 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. These actions could impact the part's functionality. Moreover, the fake marking can hide the performance of the real device and even indicate higher performances than those rated by the original component manufacturer. On several occasions, remarked commercial-grade components were deceptively sold as military-grade.

Scrapped devices are parts that had failed screening production tests due to design weaknesses or internal defects. Instead of being destroyed, they are re-introduced in the market. They can fail early due to their increased failure rate and unconformities.

Tampered devices are generally intended for sabotage, so they can cause dangerous consequences because, for example, they can contain backdoors that give access to critical functionality of the system that incorporates them.

Finally, counterfeit components can cause severe risks to a system's performance, security, and reliability. Inserting these components can pose severe threats to the entire hardware infrastructure.

III. THE SUPPLY CHAIN VUNERABILITIES

An interesting analysis of the vulnerabilities in the electronic component supply chain has been provided in [2, 13- 16].

The situation worsened due to the COVID-19 emergency. The production of electronic components has suffered a dramatic slowdown and diversification, which are still observed effects. This situation is still causing great difficulty in procuring many semiconductor devices. The conflict between Russia and Ukraine, moreover, has caused problems in finding some raw materials needed for electronics and increases in energy costs that result in increases in production costs which, together with the rise in inflation and speculations, are leading to a significant increase in the price of electronics. With the tension that continues to soar across Taiwan, the apprehension in the global microelectronic market is not decreasing.

Nowadays, semiconductor manufacturing is still dealing with a worldwide electronics shortage. Counterfeiters have been encouraged by the lack of availability of the original product. The electronic parts market is overrun by counterfeit electronics, as a high demand corresponds to a small availability and increased lead time. Low prices and immediate availability become very attractive even without real assurances about quality and reliability.

The wisest practice is not purchasing from unlicensed distributors or "brokers". However, design, obsolescence, or the actual 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 unauthorized distributors in the grey market, an increase in the risk for counterfeiting must be expected.

In case of purchasing from unofficial sellers, it must be requested that reputable sources supply parts. End-users are quite often unaware of the risks associated with using unreliable electronics.

Generally, it is necessary to:

- buy from authorized sellers or suppliers who provide EEE parts obtained exclusively from authorized sources.
- use caution in dealing with non-authorized sellers and verifying their credibility.
- avoid buying products that are much cheaper than market prices. They are not a good deal, but they could indicate a fake product.

IV. COUNTERFEIT TAXONOMY

A detailed taxonomy of counterfeit types has been provided in [5,13]. Counterfeit components can be produced and distributed in several different ways in the grey market. Apart from re-labelled, re-furbished and re-packaged devices, a rich source of material for counterfeiters is excess inventories and scrapped parts [15]. The history of counterfeit devices (origin, quality, handling and storing) is generally unknown. There is no way to predict how long they will last. Their intrinsically weak presence could have an extremely negative effect on the system's reliability.

V. DETECTION TECHNIQUES

A comprehensive review of recent counterfeit detection techniques is proposed in [14, 16].

There is a variety of anti-counterfeiting techniques that are in use, being developed and still need to be discovered. All will be needed to ensure that only authentic components make their way into finished products.

Identifying counterfeit devices can be difficult because not everything that seems suspect is necessarily fake.

The most common practices that have been used to identify fakes are proposed in [5, 8, 14-17]:

- product documentation or shipping documentation analysis,
- marking and packaging inspection,
- x-rays analysis,
- electrical measurements.

The previous steps are rapid non-destructive procedures that anyone can execute to provide the minimum level of protection, and that can be easily integrated into the production line of a printed circuit board. The following ones require analytical techniques and need for dedicated labs and expertise. Reverse engineering irreversible steps are included.

- destructive physical analysis (DPA) for microscopic inspection,
- material/layers characterization.

Generally, non- destructive and destructive practices should be conducted by comparison with genuine/authentic devices. One discrepancy in the comparison does not constitute a "*smoking gun*". Although revealing, it does not immediately suggest counterfeiting. The analyst has to collect several "*clues*" before the "*final verdict*". When the authentic device is unavailable, much more effort must be put into reaching the correct interpretation.

The previous steps can detect possible parts modification (re-marked, re-packaged and re-furnished) and no conformities to minimize the risk of introducing counterfeits. Some can be efficiently executed, assuring at least a minimum level of protection.

Moreover, standards such as AS5553, AS6171 and IDEA STD 1010 provide specific procedures and checklists that can have potentially higher costs but even the highest chance of minimizing the risk.

Providing an in-depth inspection of every component within a supply chain is a difficult task, but current best practice does not require checking every part's risk. Therefore, the availability of procedures and approaches to mitigate the likelihood of including counterfeits in the electronic systems production chain is particularly interesting.



Figure 1. Manufacturer's logo on the reel label, on the right the original one.

There are a variety of anti-counterfeiting techniques that are in use, being developed and yet to be discovered. Detecting and preventing the counterfeiting of electronic components must show the same creativity the counterfeiters show. In the following, several examples are proposed to provide helpful support during screening suspected devices.

A. Product documentation or shipping documentation analysis

The incoming inspection starts verifying the conditions of the materials used for the shipping. Reading the product or the shipping documentation could immediately raise a "*red flag"*. Typos represent a warning.

The label on the reels can provide helpful indications (Fig. 1).

Authorized sellers only provided regular shipping packages through ESD bags and properly trays.

B. Marking and packaging inspection.

Visual inspection plays an essential role in counterfeit mitigation. Crucial information can be obtained by checking the marking attributes, the pins, and the package.

Misplaced or out-of-alignment marks, wrong format and poor mark contrast, consistency and discrepancy in marking data codes and lot numbers must be considered.

Differences in the marking style must be considered, but generally, this only evidence is not definitive for establishing if the device under test is a fake. It is hard to establish if a device is fake by only looking at the package marking.

The external visual inspection included the observation of the leads to detect possible signs of refurbishing or damage. Dimensions and weight reported in the official datasheet can be verified in this phase. In Fig.2 proposes comparisons between original and fake devices [17].

External inspection of the surface of the package and the pins can put in evidence recycled parts brought back into the market. Fig.3 shows evident grooves on the package. They indicate the device had probably been sanded for remarking. Marking permanency tests, described by Mil-Std-883 Method 2015, are performed to test the mark permanency of a device. It can reveal remarked devices that have undergone sandblasting and blacktopped (Fig.4). A removable marking increases the probability of counterfeiting.

Scanning Acoustic Microscopy (SAM) can be useful for evaluating the surface and detecting possible delamination. Fourier-transform infrared spectroscopy (FTIR) can generally be in this phase to evaluate the presence of a blacktopping.

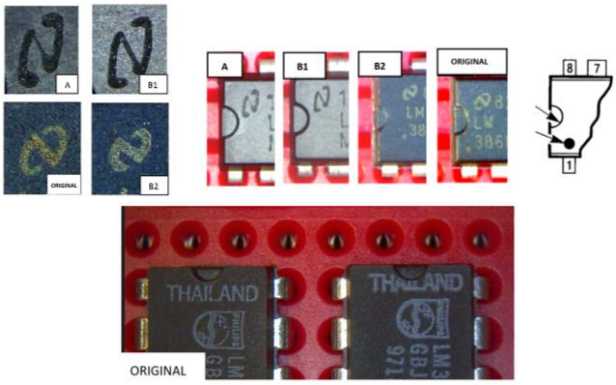

Figure 2. Checking the marking attributes and the manufacturing logo.



Figure 3. Sanded surface for remarking.

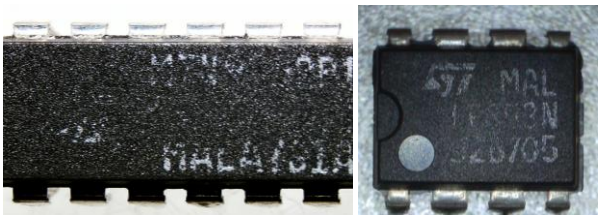

Figure 4. Residual marking after marking permanency tests.

Visual inspection methods or marking permanency tests are generally not helpful in the case of excess inventories or salvaged scrap devices. They can detect *clues* for remarked, refurbished, and recycled devices.

C. X-rays analysis.

This analysis can effectively distinguish externally similar components with different lead frames, geometry, or dies inside the package. An example is provided in Fig.5, where among four devices already reported in Fig.2, only one is the original. X- rays imaging is a non-destructive procedure able to detect defective parts where the die is missing or shows different dimensions, wires are broken and so on. This technique is not so helpful in detecting excess inventories or salvaged scrap devices.

D. Electrical measurements.

The electrical characterization enables the comparison between genuine and fake from a functionality point of

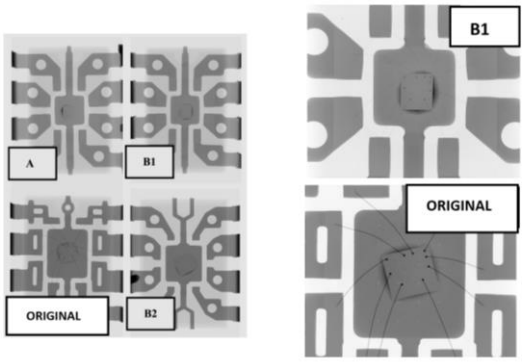

Figure 5. X-rays comparison between externally similar components.

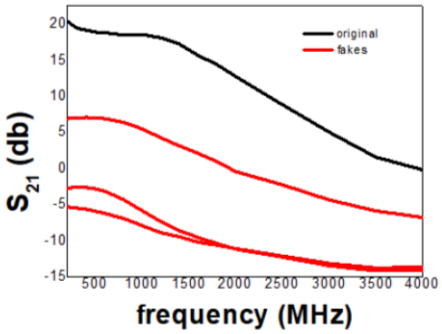

Figure 6. Scattering parameter S_{21}. Comparison between original and suspected fakes devices.

view. Regarding the electrical tests, the AS6171/7 includes curve trace, full DC, key electrical parameters for AC, switching, functional tests, and ambient or over temperature (incl. environmental, burn-in, seal). Most parts of the electrical testing can carry information to reveal possible degradation/ageing/no conformities in a non-destructive way [5, 14-17]. Specifically, substandard parts can be detected in this phase. These parts include electronics that are scrapped, mishandled, or stored improperly. Following the datasheets, the electrical measurements are performed by comparison with the original devices. As an example, in Fig.6, scattering parameter S_{21} was acquired from original and suspected fake RFIC amplifiers. S_{21} is the amplifier gain. Regular measurements were obtained on genuine devices. When suspected fake devices were tested, the measurements showed unstable S_{21}, sometimes even attaining negative gain values. The detected instability justifies the bad device performance, leading to the overall board failure. It caused dozens of field returns of the electronic systems in which the boards were installed.

E. Destructive physical analysis (DPA) for microscopic inspection.

DPA includes package decapsulation and sometimes selective delayering. The chemical or mechanical opening of the package enables the verification of the internal device. Optical (Fig.7) and Scanning Electron Microscopy (SEM)

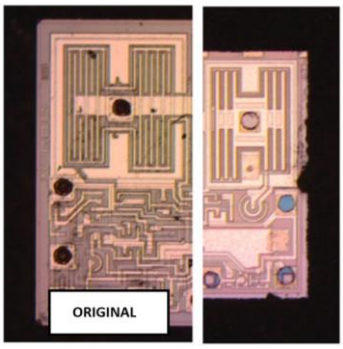

Figure 7. Optical microscopy comparison of externally similar devices after chemical de-capping. Differences in the layout and in the dimensions of the die are evident. On the left the original device.

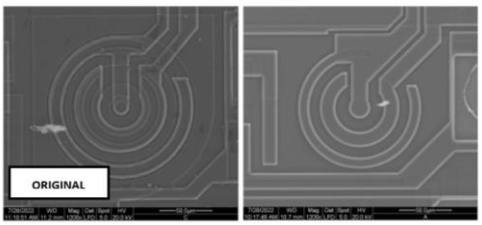

Figure 8. Scanning Electron Microscopy details comparison of the devices proposed in fig. 7. On the right the original device.

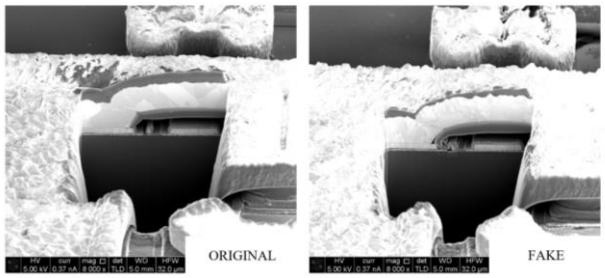

Figure 9. FIB cross-sectional views. The genuine device is on the left, the defective/scrapped part in on the right and its gate structure shows critical defects.

(Fig.8) enable the inspection of the layout and the internal logo. Bulk or Focused Ion Beam (FIB) cross-sectioning (Fig.9) enable the vertical inspection of the internal structure [15]. Technological comparison and material characterization can be performed in this phase.

F. Material characterization

Differences in the materials used in leads, packages, die attaches, and metal layers can add suspects for counterfeiting. The material characterization can be performed before and during the DPA by Energy-dispersive spectroscopy (EDS) and XRF Analysis (EDXRF).

CONCLUSION

Undetected counterfeits can lead to increased scrap rates, early field failures, and rework rates, causing a dramatic reduction in the reliability of systems. Manipulation, uncontrolled storage and handling can create the potential for electronic systems malfunction and significantly increase the risks of introducing reliability criticalities such as latent failures. 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.

The best practice is not sourcing from unlicensed distributors or "brokers". However, design, obsolescence, or the actual shortage in the electronics market may force one to purchase in the unofficial market. Even critical sectors are probably forced to evaluate purchases in the grey market. Moreover, the chip shortage still plagues the automotive sector in a phase where automotive EEE components are eligible even for New Space Economy applications. [19].

The complete sequence of detection steps proposed by 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 to detect *clues* for possible counterfeiting. The most efficient method to assure product authenticity is the incoming product inspection.

There are some procedures that anyone can execute to ensure the minimum level of protection without any laboratory facilities, even by simply reading the product documentation, shipping documentation, performing visual inspection methods, marking permanency tests and electrical measurements. In this way, poor imitations may be detectable. Depending on the device under test, additional analysis can be included in the strategy. It could give more confidence regarding authenticity. The lack of attention on the component users' part meaningfully contributes to the widespread use of counterfeit electronics. 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. The authors think it is worth sharing knowledge on this criticality and contrasting the widespread blind confidence in unauthorized sellers of consolidated technologies.

ACKNOWLEDGMENT

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

REFERENCES

[1] SAE International AS5553 rev C

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

[3] M. Pecht, "The Counterfeit Electronics Problem" Open J. of Social Sciences Vol.1, No.7, 12-16 (2013)

[4] K. Chatterjee, D. Das, and M. Pecht "Solving the counterfeit electronics problem", in Proc. Pan Pacific Microelectron. Symp. (SMTA), pp. 294–300 (2007)

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

[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] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," Technovation, 34 (7), pp. 342-353, (2014)

[11] M. J. Cushing, D. E. Mortin, T. J. Stadterman and A. Malhotra, "Comparison of electronics-reliability assessment approaches," IEEE Transactions on Reliability, vol. 42, no. 4, pp. 542-546, (1993)

[12] K. Ma, H. Wang and F. Blaabjerg, "New Approaches to Reliability Assessment: Using physics-of-failure for prediction and design in power electronics systems," in IEEE Power Electronics Magazine, vol. 3, no. 4, pp. 28-41, (2016)

[13] J. Stradley, D. Karraker, "The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications," IEEE Transactions on Components and Packaging Technologies 29, 3, (2006)

[14] 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)

[15] G. Mura, "Reliability concerns from the gray market", Microelectron. Reliab., 88-90 (2018)

[16] U. Guin, M. Tehranipoor and D. Dimase, "Counterfeit IC detection and challenges ahead", Journal of Electronic Testing, 30, 1, pp. 9-23, (2014)

[17] G. Mura, M. Vanzi, G. Marcello and R. Cao, "The role of the optical trans-characteristics in laser diode analysis" Microelectron. Reliab., 53, 9–11, (2013)

[18] G. Mura, R. Murru, G. Martines, "Analysis of counterfeit electronics," Microelectron. Reliab., 114, pp.1-4, (2020)

[19] 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., 76–77, 438-443, (2017)