COUNTERFEIT ELECTRONICS: A THREAT FOR NEW SPACE ECONOMY

Giovanna Mura

University of Cagliari, Department of Electrical and Electronic Engineering, Piazza D'Armi, Cagliari, 09123, Italy, 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. In the new space application sector, counterfeit electronics can quickly spread as the utilization of commercial-off-the-shelf components is a must as they limit the cost and the procurement time. The present work raises the awareness that using commercial-off-the-shelf components acquired from unauthorised suppliers exposes to the risk of procuring counterfeit devices. Moreover, it provides an overview on the methodologies to mitigate the risks of using suspect fake parts that could be implemented when procuring parts from non-certified suppliers.

1 INTRODUCTION

Counterfeit electronic components are fraudulent copies, imitations, or substitutes that have been represented, marked as genuine, or altered without the legal right to mislead or defraud.
The presence of counterfeit electronics in critical systems can cause reliability risks, human safety, and security problems. Counterfeit devices were detected in defence systems, radiation detectors, secure communications devices, space applications, medical devices, high-speed train brakes, and airport landing light systems where failures were or could have been catastrophic [1-3].
Given their long service life, defence and traditional aerospace systems are susceptible to subsystem, material, part, and technological obsolescence. Replacing components produced several years ago could be very difficult. The problem of avoiding counterfeit parts and materials emerges when obsolescence forces to obtain parts from other than the original manufacturer, which may no longer manufacture them, or their authorized wholesalers.
In the new space application sector, counterfeit electronics can quickly spread as the utilization of commercial-off-the-shelf components (COTS) is a must as they limit the cost and the procurement time. COTS shortage has represented a fertile field for counterfeiting businesses.
The infiltration of counterfeits into the supply chain has been dramatically boosted, initially by the electronic component shortage during the COVID-19 pandemic and further exacerbated by the Russia-Ukraine conflict. This has led to a saturation of the electronic parts market, as the high demand far outstrips the limited availability and extended lead times. The current geopolitical tensions in Taiwan, coupled with the threat of extreme weather events, have only served to heighten concerns about the future stability of the supply chain.
In the unofficial (grey) market, low prices and immediate availability become very attractive even without absolute assurances about quality and reliability.
On the other hand, quality and reliability are vital characteristics of critical and non-reparable systems and must be adequately evaluated to meet the mission objectives. Counterfeit devices must be detected before reaching the field application to achieve mission accomplishment and ensure space sustainability.
Due to the variability in the counterfeiting activity, the detection is quite often very tricky.

Small Satellites Systems and Services Symposium (4S 2024), edited by Max Petrozzi-Ilstad,
Proc. of SPIE Vol. 13546, 1354646 · © 2025 The Authors. Published under a Creative Commons Attribution CC-BY 3.0 License · 0277-786X · doi: 10.1117/12.3062781

The present work raises the awareness that using COTS acquired from unauthorised suppliers exposes to the risk of procuring counterfeit devices. Moreover, it provides an overview on the methodologies to mitigate the risks of using suspect fake parts that could be implemented when procuring parts from non-certified suppliers.
The author is of the opinion that is worth sharing knowledge on this critical aspect and reducing the blind confidence in unauthorised sellers of consolidated technologies.

2 THE COUNTERFEIT PROBLEM

Counterfeit electronics is defined as [4]:

- 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, quality, handling, and storage of counterfeit devices are 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. As they can be produced with sub-standard materials, the risk of overheating, electric shocks, fire, and explosions is not negligible. As they can be improperly stored and dismounted from PCBs, the risk for delamination, corrosion, electrostatic discharge, and thermal fatigue is high.
The origin of the counterfeit electronics problem has been explained in [5-7].
Systems that fail to contain counterfeit EEE can cause reliability risks, problems with human safety and security, and harm to the economy.
Several incidents, failures and preventive detections testify to the deep penetration of counterfeit electronics, even in critical sectors such as the military and space. It can carry national security implications.

Counterfeit devices in critical sectors, such as the military, are reported in [8-12].
On several occasions, remarked commercial-grade components were deceptively sold as military-grade. Counterfeit electronic parts misrepresented as military-grade have been found in U.S. Department of Defense supply chain, including counterfeit memory devices in the mission computers of missile systems [13-14].
An inquiry of the Committee on Armed Services of the United States Senate released in 2012 reported the detection of counterfeits in vehicles conducting anti-submarine and anti-surface warfare activities. Implications of counterfeits in military supply chains include degraded functionality of weapon systems and infrastructure, physical harm to troops, and the interception of sensitive data via Trojans and malware [15]. In 2002, an Air Force pilot died because the parachute did not deploy from his malfunctioning ejection seat due to ten counterfeit and faulty transistors and chips. Quality and safety concerns from counterfeited batteries that are widely used in various fields including military and space applications [16] are reported in [17,18]. During the Kepler space telescope development, NASA discovered that a component was not exactly what ordered. It contributed to the expensive, nine-month delay of the Kepler spacecraft launch. The parts were also used on U.S. Air Force F-15s, F-22s, and C-17s [19].

The problem of counterfeiting in electronics is not recent but still critical today. Its widespread is significantly facilitated by component users' lack of knowledge and attention. Counterfeiting represents a threat to the new space economy that is opening space to all kinds of activities, industries, and even end-users.

The new space economy, specifically CubeSats, relies on low costs and quick development, representing a fertile field for counterfeiting businesses.
The advent of CubeSats has revolutionized the traditional approach, favouring cutting-edge COTS components for enhanced low-cost performance. However, the 'buy-and-fly' strategy exposes the mission to the risk of using unsuitable COTS in space and the massive counterfeiting problem, posing a significant threat to the space environment. In this context, concerns should arise about the entry of several private actors, as the number of tests performed can be reduced to zero due to budgetary and time constraints. To ensure reliable results, it is imperative to make an appropriate selection of COTS electronics. It is recommended to avoid purchasing from unlicensed distributors, unofficial resellers, or "brokers." However, in certain circumstances such as design, obsolescence, or market conditions, it may be necessary to acquire components from unofficial (grey) market sources. When buying from unofficial sellers, it is essential to request that reputable sources supply the parts. It is advisable to be cautious when purchasing products that are much cheaper than market prices. Extreme caution and mitigation strategies must be used if forced to deal with unauthorized sellers, and their credibility and the quality of their products must be verified before purchasing.

3 COUNTERFEITS TAXONOMY

Counterfeit electronics include recycled, remarked, scrapped and tampered parts. The entire taxonomy is provided in [20].
Even if they operate at first, recycled devices are not brand-new, and the aging brought on by previous use may shorten their lifespan. Furthermore, electronics that have been recycled might have been handled, disassembled, or stored in an uncontrolled environment incorrectly. Failure mechanisms, such as electrostatic discharge, delamination, popcorning, thermo-mechanical stress, and corrosion, might result in latent damage or disastrous breakdowns during field operations.
Remarked electronics may be sanded, microblasted, acid etched, blacktopped, or subjected to other marking processes. The part's functionality may be impacted by these actions. Scrapped devices are parts that have 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 [21]. Tampered devices are generally intended for sabotage, so they can cause dangerous consequences because, for example, can give access to critical functionality of the system that incorporates them.
A variety of anti-counterfeiting techniques are in use, being developed, and still need to be discovered. All will be required to ensure that only authentic components make their way into finished products. On the other hand, 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 [6, 20-29] and summarised in the following:

- Product documentation or shipping documentation analysis.

During the incoming inspection, the conditions of the materials being shipped must be verified. It is important to carefully read the product and shipping documentation as any typos or errors could indicate potential issues. Additionally, the label on the reels can provide helpful indications. Only authorized sellers provide regular shipping packages through ESD bags and properly trays.

- External visual inspection: marking and packaging inspection.

Visual inspection is a crucial step in detecting counterfeit products. It involves checking the attributes of the markings, pins, and packaging (physical molding compound features, part surface and

markings, indents) for any inconsistencies (Fig.1). It is important to look for misplaced or incorrectly aligned marks, incorrect formats, poor contrast, and discrepancies in the marking data codes and lot numbers. Differences in marking styles should also be considered but cannot be used alone to determine whether a product is fake. Simply looking at the package markings may not be sufficient to verify the authenticity of a product. During external visual inspection, the leads should also be observed for any signs of refurbishing or damage. This phase can also verify the dimensions and weight of the product as reported in the official datasheet. External inspection of a package and its pins can reveal if recycled parts have been reintroduced into the market. If grooves are present on the package, it is likely that the device has been sanded for remarking. To check the mark permanency of a device and detect remarked devices that have undergone sandblasting and blacktopping, marking permanency tests described in Mil-Std-883 Method 2015 can be conducted. However, if a device has a removable marking, it increases the chance of counterfeiting. To detect delamination, Scanning Acoustic Microscopy (SAM) is a useful technique for surface evaluation. Fourier-transform infrared spectroscopy (FTIR) is another technique that can be employed, especially to determine the presence of blacktopping. However, visual inspection methods or marking permanency tests are not very helpful when it comes to excess inventories or salvaged scrap devices. They can only provide clues for detecting remarked, refurbished, and recycled devices.

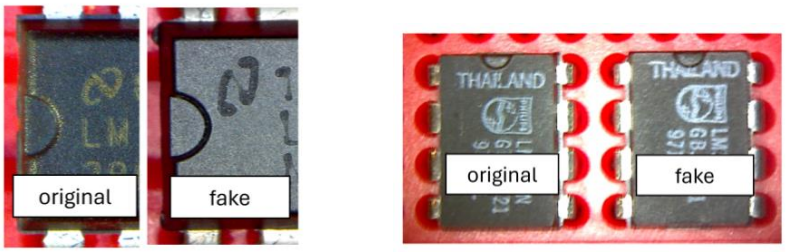

Figure 1. Optical external comparison shows differences in the marking attributes and the manufacturing logos.

- X-ray analysis.

This analysis can effectively distinguish externally similar components with different lead frames, geometry, or dies inside the package. X- ray 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. Differences in the lead frames can add suspects for counterfeiting (Fig.2). This technique is not helpful in detecting excess inventories or salvaged scrap devices.

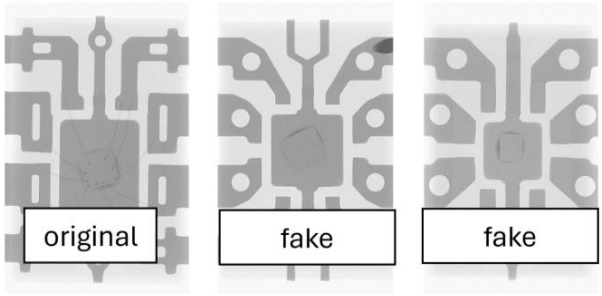

Figure 2. X-ray comparison between externally similar components. Differences in lead frames, dice shapes and bonding are detected [26].

- Electrical measurements.

The process of electrical characterization allows genuine and fake devices to be compared from a functionality perspective. The electrical tests include curve tracing, full DC testing, key electrical parameters for AC, switching, functional tests, and tests for ambient or over temperature conditions (including environmental, burn-in, and seal). Most of these tests provide non-destructive information that can reveal possible degradation, aging, or non-conformities. This phase can detect substandard parts such as electronics that have been scrapped, mishandled, or stored improperly. The electrical measurements are performed by comparing them with the original devices, as indicated in the datasheets.

- Destructive physical analysis for microscopic inspection.

DPA stands for Destructive physical analysis. This process involves opening up the package of an integrated circuit using chemical or mechanical means, so that the internal device can be inspected and verified. Optical microscopy and Scanning Electron Microscopy (SEM) are used to inspect the layout and internal logo (Fig. 3). In addition, bulk or Focused Ion Beam (FIB) cross-sectioning allows for the vertical inspection of the internal structure. This phase also allows for technological comparison and material characterization to be performed.

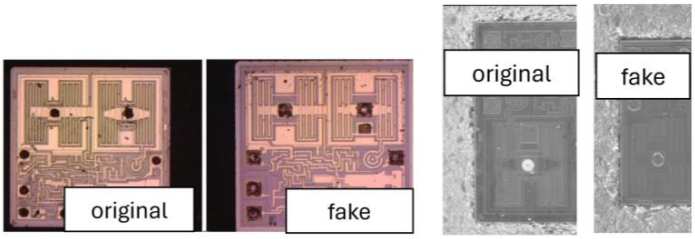

Figure 3. Optical and scanning electron microscopy comparison of externally similar devices after wet chemical exposure of the silicon die. Differences in the layout and in the dimensions of the dies are evident [25, 26].

- Materials/layers characterization.

Differences in the materials used in leads, packages, die attaches, and metal layers can add suspects for counterfeiting. Material characterization can be performed before and during the DPA through energy-dispersive spectroscopy (EDS), FTIR, and XRF analysis (EDXRF).

4 STANDARDS

It is important to use a standardized approach whenever it is possible or mandatory to do so. This will ensure consistency and clarity in the work being done.

SAE Aerospace Standards AS5553 and AS6081 were developed in response to a significant and increasing volume of fraudulent/counterfeit electronic parts entering the aerospace supply chain, posing significant performance, reliability, and safety risks.

More recently, SAE Aerospace Standards AS6171A [30] lists “the requirements that apply once a decision is made to use parts with unknown chain of custody that do not have pedigree back to the original component manufacturer or have been acquired from a broker or independent distributor, or when there are other known risk elements that result in the User/Requester to have concerns about potential suspected/counterfeit EEE parts”. The standard SAE AS6171A and its slash sheets provide guidance and plenty of examples helpful for suspect counterfeit part detection.

Fundamental documents are:

AS6171/1- Suspect/Counterfeit Test Evaluation Method.
AS6171/2A- Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods.
AS6171/3- Techniques for Suspect/Counterfeit EEE Parts Detection by X-Ray Fluorescence Test Methods.
AS6171/4- Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Test Methods.
AS6171/5- Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods.
AS6171/6- Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods.
AS6171/7- Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods.
AS6171/8- Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods.
AS6171/9- Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods.
AS6171/10- Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods.
AS6171/11- Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods.
Further Standards are published by Independent Distributors of Electronics Association (IDEA), JEDEC Solid State Technology Association, Institute of Printed Circuits (JEDEC), Institute for Interconnecting and Packaging Electronic Circuits (IPC), Electronic Industries Alliance (EIA).

5 CONCLUSION

Using commercially available off-the-shelf components from unauthorized suppliers can lead to the purchase of counterfeit devices. This paper provides an overview of methods that can mitigate the risks of using questionable fake parts when procuring electronics from non-certified suppliers.
The best way to reduce the risk of fakes entering the manufacturing line is to prevent sourcing from unlicensed distributors. International standards provide the best guidance and plenty of examples helpful for suspect counterfeit part detection. The author believes it is essential to share knowledge about this critical aspect and reduce blind trust in unapproved sellers of established technologies.

ACKNOWLEDGMENT

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

6 REFERENCES

[1] Semiconductor Industry Association, *Winning the battle against counterfeit semiconductor products*. A report of the SIA Anti-Counterfeiting Task Force, 2013.
[2] https://www.erai.com/
[3] Daniel, B., *10 shocking facts about counterfeit electronics [defense & aerospace]* [online] Available https://www.trentonsystems.com/blog/10-shocking-facts-counterfeitelectronics.
[4] SAE International, Aerospace Standard, AS5553 rev D, 2022.
[5] Pecht M., Tiku S., *Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics*, IEEE Spectrum, 43, 5, 37-46, 2006.

[6] Pecht M., *The Counterfeit Electronics Problem*, Open J. of Social Sciences Vol.1, 7, 12-16, 2013.
[7] Sood B., Das D., Pecht M., *Screening for counterfeit electronic parts*, J. of Material Science: Materials in Electronics, Vol 22, 10, 1511-1522, 2011.
[8] Committee on Armed Services United States Senate, *Inquiry into counterfeit electronic parts in the departement of defense supply chain*, 112–167, 2012.
[9] Mitra S., Wong H.-S. P., Wong S., *The Trojan-proof chip, IEEE Spectrum*, Vol. 52, 2, 46-51, 2015.
[10] Abbany Z., *Has Germany's Patriot missile system been hacked?* [online] Available: https://p.dw.com/p/1FvEy, 2015.
[11] Stradley J., Karraker D., *The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications*, IEEE Transactions on Comp. and Packaging Tech. 29, 3, 2006.
[12] Ilinca M.S., *Considerations regarding the risk of using counterfeit products in the aerospace industry*, INCAS Bulletin, Vol. 14,4, 201-211, 2022.
[13] Koepsel K.M., *Counterfeit Parts and Their Impact on the Supply Chain*, SAE International, 2018
[14] Shrivastava, A., Pecht, M., *Counterfeit capacitors in the supply chain*, J Mater Sci: Mater Electron Vol. 25, 645–652, 2014.
[15] Daniel DiMase D. et al., *Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems*, Risk Analysis, Vol. 36, 10, 2016.
[16] Krause F. C., Loveland J. A., Smart M. C., Brandon E. J., and Bugga R. V., *Implementation of commercial li-ion cells on the MarCO deep spaceCubeSats*, J. Power Sources, Vol. 449, 227544, 2020.
[17] Tapesh J., *Safety and Quality Issues of Counterfeit Lithium-Ion Cells*, ACS Energy Lett., Vol.8, 6, 2831–2839, 2023.
[18] Kong L., Das D., Pecht MG, *The distribution and detection issues of counterfeit lithium-ion batteries*, Energies, 2022.
[19] NASA's Discovery Program: the first twenty years of competitive planetary exploration / by Niebur S.M with Brown D.W., chapter7, [online] Available: https://www.nasa.gov/wp-content/uploads/2024/01/discovery-program-ebook.pdf.
[20] Guin U., DiMase D., and Tehranipoor M., *Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead*, J. of Electr. Testing: Theory and Applications, Vol. 30, 1, 9-23, 2014.
[21] Mura G., *Reliability concerns from the gray market*, Microelectron. Reliab., 88-90, 2018.
[22] Guin U. and Tehranipoor M., *Counterfeit detection technology assessment*, GOMACTech, 2013.
[23] Lowry R.K., *Counterfeit electronic components- an overview*, Military, Aerospace, Spaceborne and Homeland Security Workshop, 2007.
[24] Guin U., Tehranipoor M., and Dimase D., *Counterfeit IC detection and challenges ahead*, J. of Electronic Testing, 30, 1, 9-23, 2014.
[25] Mura G., Murru R., Martines G., *Analysis of counterfeit electronics*, Microelectron. Reliab., 114, 1-4, 2020.
[26] Mura G., Murru R., Martines G., *Analysis of fake amplifiers*, in Proc. of MIEL, 131-134, 2021.
[27] Mura G., Martines G., *Reliability risks from counterfeit electronics*, in Proc. of SRSE, 297-301, 2022.
[28] Ahmadi B. et al., *A novel crowdsourcing platform for microelectronics counterfeit defect detection*, Microelectron. Reliab, Vol. 88-90, 2018.
[29] Hartgerink D.P., *Case studies of counterfeit part detection in assembled products*. Proc. of ISTFA, 2010.
[30] SAE International, Aerospace Standard, *AS6171A, Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts*, 2018.