The Threat of Counterfeit Electronics to the Development of CubeSats

Giovanna Mura
Department of Electrical and Electronic Engineering, University of Cagliari,
Cagliari, Italy
giovanna.mura@unica.it

***Abstract*— Commercial-off-the-shelf components are essential in the new space application sector because they offer low costs and reduce procurement time. However, it also increases the risk of counterfeit electronics infiltrating the supply chain. The growing counterfeit electronics problem poses a serious threat to the development of CubeSats. It is crucial to be aware that obtaining commercial off-the-shelf components from unauthorized suppliers can lead to the procurement of counterfeit devices. Counterfeit electronics can trigger mission failure and a significant decrease in system reliability. The paper emphasizes these risks and underscores the critical importance of mitigation strategies when sourcing parts from non-certified suppliers. It also presents an overview of methods to minimize the risks of using suspicious counterfeit parts. Reducing failures in new space economy applications paves the way for a cleaner and safer space environment for future generations.**

***Keywords*— Counterfeit electronics; Fake electronics; Detection; New space economy; COTS; CubeSats; Reliability**

I. INTRODUCTION

Counterfeit electronic components are unauthorized copies or substitutes falsely represented as genuine or altered without the legal right to deceive or defraud. The infiltration of counterfeit electronics into critical systems is not just a potential threat but a clear reality. These counterfeit devices, often almost indistinguishable from genuine ones, have been discovered in defense systems, radiation detectors, secure communications devices, aerospace applications, medical devices, high-speed train brakes, and airport landing lighting systems. The consequences of their failure, which have been or could have been catastrophic, underscore the gravity of this issue. For instance, a counterfeit microchip in a defense system could lead to a breach in security, compromising sensitive information or even endangering lives [1-3].

Defense and traditional aerospace systems, with their long service life, are particularly vulnerable to the threat of counterfeit parts and materials due to subsystem, material, part, and technological obsolescence. The issue of avoiding counterfeit parts and materials becomes even more critical when obsolescence necessitates obtaining parts from sources other than the original manufacturer, which may no longer produce them. Furthermore, using commercial-off-the-shelf components (COTS) in the new space application sector can rapidly spread counterfeit electronics, posing a significant risk. The electronic component shortage has alarmingly amplified the infiltration of counterfeits into the supply chain during the COVID-19 pandemic. More recently, geopolitical crises and tensions have further destabilized the supply chain, raising further serious concerns. In the unofficial (grey) market, which refers to the trade of goods through channels that are unauthorized by the original manufacturer, 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.

The use of counterfeit devices in space applications can have severe consequences, potentially jeopardizing mission accomplishment and space sustainability. This alarming reality underscores the importance of preventing the use and detecting such devices before they reach the field application. In fact, debris issues can be addressed by reducing the probability of new debris, removing existing debris, and preventing future collisions. Mitigation strategies against counterfeits can consequently even limit the creation of new debris. Due to the variability in the counterfeiting activity, detection is often a complex and challenging task that requires utmost vigilance. The present work raises awareness that using COTS acquired from unauthorized suppliers exposes one to the risk of procuring counterfeit devices. Moreover, it provides an overview of the methodologies to mitigate the risks of using suspect fake parts that could be implemented when procuring them from non-certified suppliers.

II. THE COUNTERFEIT THREAT

The origin of the counterfeit electronics problem, as explained in [4-5 6], is a complex issue. It encompasses a variety of counterfeit electronics, including recycled, overproduced, remarked, scrapped, cloned, and tampered parts.

These devices can show a reduced lifetime due to prior usage and improper dismantling, handling, or storage in an uncontrolled environment, can be produced by less experienced personnel in unofficial manufacturing facilities, can be remarked with external specifications higher than their internal parts, can have weaknesses or internal defects, or can contain embedded malicious malware intended for sabotage. It is important to note that these devices are deceptively sold as new, original, and fully functional, despite their true nature adding elements of unpredictability. There is no way to foresee how long they will last. As they can be manufactured with substandard materials, the risk of over-heating, electrical shocks, fire, and explosions is not to be taken lightly. As they can be improperly stored and dismounted from electronic

This is the accepted version of G. Mura, "The Threat of Counterfeit Electronics to the Development of CubeSats," 2024 International Symposium ELMAR, Zadar, Croatia, 2024, pp. 223-226, doi: 10.1109/ELMAR62909.2024.10694162.

waste, the risk for popcorning, contamination, corrosion, ESD, and thermal fatigue is significantly elevated. Their inherently weak nature could have a profoundly negative impact on the system's reliability.

The failure effectively address the counterfeit issue can lead to significant reliability risks, jeopardize human safety and security, and inflict substantial economic damage.

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.

Several failures and preventive detections bear witness to the extensive infiltration of counterfeit electronics, even in critical sectors such as the military and aerospace. This infiltration can carry severe national security implications. Counterfeit devices in critical sectors, such as the military, are reported in [7-10]. 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 [11-12]. 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. The implications of these counterfeits in military supply chains are severe, including degraded functionality of weapon systems and infrastructure, physical harm to the troops, and the interception of sensitive data via Trojans and malwares. In 2002, an Air Force pilot tragically lost his life because the parachute did not deploy from his malfunctioning ejection seat due to ten counterfeit and faulty transistors and chips. These parts were falsely identified and discovered in the flight computer of U.S. Air Force F-15 fighter jets, and fakes were also used on F-22s, C-17s, and AV-8B Harrier [13]. Suspected unapproved parts have been notified by the European Union Aviation Safety Agency (EASA) on several occasions, recently regarding forged authorized release certificates covering dozens of parts for CFM56 engines used in Boeing 737 and Airbus 370 aircraft. Quality and safety concerns from counterfeited batteries that are widely used in various fields, including military and space applications, are reported in [14-17]. During the Kepler space telescope development, NASA discovered that a component was not exactly what was ordered. It contributed to the expensive, nine-month delay of the Kepler spacecraft launch [18]. This underscores the urgent need for increased vigilance and measures to prevent the use of counterfeit parts in military and aerospace equipment.

Counterfeiting represents a relevant threat to the new space economy that is opening space to all kinds of activities, industries, and even end-users.

In the new space economy segment, the advent of CubeSats has revolutionized the traditional approach, favoring cutting-edge COTS components for enhanced low-cost performance [19-21].

CubeSats are crucial for developing a new space economy, making space open and accessible for various activities and industries. However, their high failure rate significantly contributes to the congestion of low-Earth orbit. From a reliability perspective, CubeSats are complex systems with six significant subsystems: structure, communication, power, attitude determination and control, command and data handling, and the payload. An evaluation suggested that CubeSat reliability is strongly affected by high rates of dead-on-arrival (DOA) cases, where the satellite is deployed but never becomes functional [22]. After two years in orbit, the estimated reliability ranges from 65.49% to 48.49%. The authors proposed that more careful and adequate system-level functional testing on the ground could prevent a significant percentage of these failures. [23]

With their reliance on low costs and quick development, these small satellites can become a prime target for counterfeiting businesses. While expedient, the 'buy-and-fly' strategy exposes missions to the grave risk of using unsuitable COTS in space. This, coupled with the counterfeiting problem, poses a significant threat to the space environment. The potential consequences are dire: as infant mortality has been a persistent issue for CubeSats, there is evidence that CubeSats missions may increase the number of space debris [24]. In this context, it is crucial to emphasize the role of several private actors. If they ignore the problem and, due to budgetary and time constraints, acquire components from the grey market and reduce the number of tests performed to zero, they could potentially exacerbate the failures in space and the space debris problem. Moreover, counterfeiting makes satellite systems more accessible and vulnerable to cybersecurity threats [25].

It is imperative to make an appropriate selection of COTS electronics to ensure reliable missions. It is recommended to avoid purchasing from unlicensed distributors, unofficial resellers, or "brokers." However, in certain circumstances, such as design requirements, obsolescence, difficulty procuring, or shortage conditions, it may be necessary to acquire components from unofficial market sources. When buying from unofficial sellers, requesting that reputable sources supply the parts is essential. 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.

III. STANDARDS FOR COUNTERFEITS DETECTION

In critical sectors, when dealing with counterfeits detection, 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 Standard AS6171A [26] outlines the requirements that apply when necessary to acquire from the unofficial market. This standard and its slash sheets offer guidelines and numerous examples to help detect potential counterfeit components. The IDEA, IPC, EIA, and JEDEC Associations publish further Standards.

IV. COUNTERFEITS DETECTION

Identifying counterfeits can be challenging because not everything that seems suspect is necessarily fake, and several “clues” must be collected to establish if the device is original or not.

The most common practices that have been used to identify fakes are summarized in the following [5, 6, 14, 15, 26-31, 35, 36, 38]:

- Documentation analysis.

During the incoming inspection, the shipped materials' conditions must be verified. Any typos or grammatical errors in the product and shipping documentation or in the label on the reels could indicate potential issues.

- Marking and packaging visual 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. 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. Chemical analysis of the external pins plating can be performed through energy-dispersive spectroscopy (EDS). If grooves are present on the package, it is likely that the device has been sanded for remarking [29].

Scanning acoustic microscopy (SAM) is a useful technique for interface evaluation to detect evidence of delamination. Fourier-transform infrared spectroscopy (FTIR) is another technique that can be employed primarily to determine the presence of blacktopping.

- X-ray analysis.

By utilizing X-ray imaging, we can nondestructively differentiate between externally similar components with different lead frames or die geometries inside the package. Discrepancies in the lead frames can raise concerns about counterfeiting but cannot be conclusive [29, 31, 38]. Through this analysis, we can immediately identify defective parts in cases where the die is missing, has differing dimensions, or wires are broken. However, it is essential to note that this technique is unsuitable for detecting excess inventories or salvaged scrap devices.

- Electrical characterization.

Electrical characterization plays a key role in the detection of parametric and manufacturing defects and at the starting point of a failure analysis [29-34]. Electrical testing suitable for detecting a counterfeit device can include parametric, functional, burn-in, and structural tests. It allows genuine and fake devices to be compared from a functionality perspective. 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 the datasheets indicate.

- De-capping for microscopic inspection.

Reverse engineering procedures can be used for additional verification. This process is irreversible. Packages can be removed using chemical and mechanical methods, allowing for microscopic inspection of the top surface of the die [29, 31, 38]. Optical metallography and scanning electron microscopy can be used to inspect the internal structure and layout at high magnification. Materials/layers characterization to detect differences between original and suspected can be performed by using ESD, Raman, FTIR, and X-ray fluorescence analysis (XRF).

Several anti-counterfeiting techniques are under development, and new ones still need to be discovered. Due to the adaptability of counterfeiting techniques, detection and avoidance methods are evolving [35-37]. Many techniques, both simple and sophisticated, can be used in the identification process. The complete sequence of detection steps proposed by the Standards and performed by accredited commercial labs will provide the highest chance of minimizing the risk of fakes entering the production line. Finally, risk assessment methods proposed and discussed in [11, 26, 39- 41] provide a balance between risks, testing costs and benefits.

While detecting a counterfeit is a time-consuming and expensive process that demands expertise, developing a CubeSat stands in stark contrast, requiring significantly less time and costs. If not affordable, at least a risk-based strategy using a flexible set of tests should be applied to detect "*clues*" for possible counterfeiting. More than a simple analysis of the external details is needed for authentication because not everything that seems suspect is necessarily fake. Some differences can only be related to process changes introduced at the original producer or outsourced subcontractor plant, as reported in [38]. In addition to the visual inspection and shipping documentation verification, electrical measurements can provide a minimum screening for detecting less accurate fakes.

V. Conclusion

Counterfeit electronics components, a significant threat to the emerging new space economy, require immediate attention. The use of COTS from unauthorized suppliers could lead to the purchase of counterfeit devices. However, the new space economy community can significantly reduce the risk of fakes entering the manufacturing line by preventing sourcing from unlicensed distributors. Reassuringly, international standards provide the best guidance in mitigating the risks of using questionable fake parts when procuring electronics from non-certified suppliers. This paper provides an overview of methods crucial for suspect counterfeit part detection. Considering that Euroconsult's 2023 report forecasts an average of over 2,800 satellites launched annually in the next decade, reducing failures in new space economy applications can contribute to a cleaner and more sustainable space ecosystem for future generations.

Acknowledgment

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

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] B. Daniel, “10 shocking facts about counterfeit electronics [defense & aerospace]” [online] Available https://www.trentonsystems.com/en-us/resource-hub/blog/10-shocking-facts-counterfeit-electronics

[4] S. Bastia, “Next generation technologies to combat counterfeiting of electronic components”, IEEE Trans. on Comp. and Packaging Tech., vol. 25, 175-176, 2002.

[5] M. Pecht, S. Tiku, “Bogus”, IEEE Spectrum, 43, 5, pp. 37-46, 2006.

[6] B. Daniel, “Counterfeit Electronic Parts: A Multibillion-Dollar Black Market” [online] Available https://www.trentonsystems.com/en-us/resource-hub/blog/counterfeit-electronic-parts

[7] Committee on Armed Services United States Senate, Inquiry into counterfeit electronic parts in the departement of defense supply chain, 112–167, 2012.

[8] S. Mitra, H.-S. P Wong, S. Wong, “The Trojan-proof chip”, IEEE Spectrum, vol. 52, 2, pp. 46-51, 2015.

[9] Z. Abbany, “Has Germany’s Patriot missile system been hacked?” [online] Available: https://p.dw.com/p/1FvEy, 2015.

[10] J. Stradley, D. Karraker, “The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications”, IEEE Trans. on Comp. and Packaging Tech. 29, 3, 2006.

[11] M.S Ilinca, M. Rusu, V. Soare, S. Tonoiu “Considerations regarding the risk of using counterfeit products in the aerospace industry”, INCAS Bulletin, vol. 14,4, pp. 201-211, 2022.

[12] K.M. Koepsel, “Counterfeit Parts and Their Impact on the Supply Chain”, SAE International, 2018

[13] B. Grow, C.C Tschang, C. Edwards and B. Burnsed, “Dangerous Fakes” [online] Available http://www.businessweek.com/stories/2008-10-01/dangerous-fakes, 2008.

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

[15] F. C. Krause, J. A. Loveland, M. C. Smart, E. J. Brandon, R. V. Bugga, “Implementation of commercial li-ion cells on the MarCO deep spaceCubeSats”, J. Power Sources, vol. 449, 227544, 2020.

[16] J. Tapesh, “Safety and Quality Issues of Counterfeit Lithium-Ion Cells”, ACS Energy Lett., vol. 8, 6, pp. 2831–2839, 2023.

[17] L. Kong, D. Das, MG Pecht, “The distribution and detection issues of counterfeit lithium-ion batteries”, Energies, 2022.

[18] S. M Niebur, D.W Brown, NASA’s Discovery Program: the first twenty years of competitive planetary exploration by ch.7, [online] Available: https://www.nasa.gov/wp-content/uploads/2024/01/discovery-program-ebook.pdf.

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

[20] R. Ramesham, "Environmental testing of COTS components for space applications", Proc. of SPIE 7206, 72060H, 2009.

[21] R. Enrici Vaion, et al. “Qualification extension of automotive smart power and digital ICs to harsh Aerospace mission profiles: Gaps and opportunities”, Microelectron. Reliab., vol. 76–77, pp. 438-443, 2017.

[22] M. Langer. “Reliability of CubeSats – Statistical Data, Developers’ Beliefs and the Way Forward” Proc. of 30th Annual AIAA/USU Conference on Small Satellites, pp. 1-12, 2016.

[23] G. Fois, G. Mura. “Cubesats: Paving the way towards an effective reliability- oriented approach” Proc. of Trends in Earth Observation,vol. 2, pp.166-69, 2021.

[24] M. Langer, M. Weisgerber, J. Bouwmeester, A. Hoehn, "A reliability estimation tool for reducing infant mortality in Cubesat missions", Proc. of IEEE Aerospace Conference, Big Sky, MT, USA, pp. 1-9, 2017.

[25] N. Yadav, F. Vollmer, A-R. Sadeghi, G. Smaragdakis, A. Voulimeneas, “Orbital Shield: Rethinking Satellite Security in the Commercial Off-the-Shelf Era” Proc. of Security for Space Systems, 2024.

[26] SAE International, Aerospace Standard, AS6171A, Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts, 2018.

[27] G. Mura, “Reliability concerns from the gray market”, Microelectron. Reliab., vol. 88-90, 2018.

[28] R. K. Lowry, “Counterfeit electronic components- an overview”, Military, Aerospace, Spaceborne and Homeland Security Workshop, 2007.

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

[30] G. Mura, R. Murru, G. Martines, “Analysis of fake amplifiers”, Proc. of MIEL, 131-134, 173136, 2021.

[31] M. Goetz, R. Varma “Counterfeit Electronic Components Identification: A Case Study” Proc. of IPC APEX EXPO, 2017.

[32] S. Frank, W.Tan, J.F. West “Electrical Characterization” Wagner, L.C. (eds) Failure Analysis of Integrated Circuits. Springer, vol. 494, 1999.

[33] G. Mura, M. Vanzi, G. Marcello, R. Cao, “The role of the optical trans-characteristics in laser diode analysis” Microelectron. Reliab., 53, 9–11, 2013.

[34] M. Vanzi, et al. “Extended Modal Gain Measurement in DFB Laser Diodes” IEEE Photonics Tech. Lett., 29, 7762038, 2017.

[35] O. Aramoon, Q. Gang, “Impacts of Machine Learning on Counterfeit IC Detection and Avoidance Techniques”, Proc. of Int. Symp. on Quality Electronic Design, Santa Clara, CA, 352-357, 2020.

[36] B. Ahmadi, et al., “A novel crowdsourcing platform for microelectronics counterfeit defect detection”, Microelectron. Reliab, vol. 88-90, 2018.

[37] P. Hoveida, et al.“Terahertz-readable laser engraved marks as a novel solution for product traceability. Sci. Rep. 13, 12474, 2023.

[38] G. Mura, S. Carta, P. C. Ricci and G. Martines, “Electronic components authentication via physical analysis” Proc. of MIEL, 177483, 2023.

[39] Z. Collier, S. Walters, D. DiMase, J. Keisler et al., "A Semi-Quantitative Risk Assessment Standard for Counterfeit Electronics Detection," SAE Int. J. Aerosp. Vol. 7(1),pp. 171-181, 2014.

[40] M. Azarian, “An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171” Proc. Of ISTFA, 175925, 2028.

[41] Office of the Assistant Secretary of the Navy Acquisition and Business Management, “Counterfeit Materiel Process Guidebook Guidelines for Mitigating the Risk Of Counterfeit Materiel in the Supply Chain”, 2017. [online] Available: https://www.erai.com/