Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P9109-cd

Counterfeit Electronics in Industry 4.0: Risks and Detection

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

Alessandro Urru, Michela Musa, Pietro Andronico
Nurjana Technologies srl, Via Mario Betti 27/29, Elmas, Cagliari, Italy

Counterfeiting in electronics is a growing fraudulent business and a challenging detecting activity. Industry 4.0 can be easily affected by counterfeit electronics, considering the massive use of physical devices and the large amounts of data generated that could be disclosed, causing safety risks and know-how loss. If not detected, counterfeit electronics can lead to software, hardware, network and information security problems and disastrous system breakdowns during field operations. The range of counterfeit electronics, from recycled to tampered parts, adds to this complexity, highlighting the need for advanced detection methods.
This work aims to raise awareness about the risks of using electronics purchased from unauthorized distributors, which could lead to the procurement of counterfeit devices. It will also provide an overview of methodologies to mitigate these risks when forced to procure components from unauthorized suppliers. Finally, it will propose a non-destructive detection approach that relies on electrical measurements and machine-learning algorithms, which could be trained during in-line operation. It could offer a low-cost solution to this pervasive problem, at least for simple electronic devices.

Keywords: Counterfeit electronics risks, Fake electronics, Non-destructive detection, Machine learning, IoT, Industry 4.0.

1. Introduction

The transformation of the industrial structure facilitated by the extraordinary technological advancement through the utilization of Artificial Intelligence (AI), the Internet of Things (IoT), and big data is called the Fourth Industrial Revolution. IoT and digitalization have become usual for Industry 4.0, and many data characterizing processes are generated. They could be disclosed, causing security problems and know-how loss. In addition, as the IoT already involves heterogeneous field applications (Borgia 2014, Kelly et al. 2013, Mohammadrezaei et al. 2020, Pettorru et al. 2023, Dhingra et al 2019, Singh et al. 2020) and brings numerous new possibilities, it is expected to be widely applied even more and more to industry and home solutions. As IoT integrates various internet technologies - powerful devices capable of sensing, processing, and exchanging data, new low-energy communication protocols, big data, and cloud systems - it is obviously very strategic to use security technologies to deal with security issues. Up to now, several research groups have considered cyberattack security aspects and significant risks and vulnerability to privacy and security (Radovan 2017, Mishra 2021, Farkas 2024, Hasan 2019), neglecting the critical issues of hardware reliability caused by electronic devices acquired from unauthorized distributors. In the IoT ecosystem, hardware plays a crucial role and hardware trust across the IoT supply chain is an urgent issue (Yang et al. 2017). More cost-effectiveness is generally obtained by using commercial off-the-shelf (COTS) electronic components in the IoT perception layer (Sauter 2023). In the unofficial (grey) market (Bopp et al. 1995, Mura 2018), low prices and immediate availability become very attractive even without absolute assurances about quality and reliability. Simply over-relying on unofficial distributors is no longer safe considering the risk of acquiring counterfeit electronics. Moreover, it's crucial to recognize that even minor components within an

IoT system can significantly influence the overall application. If these components do not function correctly, are low-performing, or catastrophically fail, they can seriously impact the system. Therefore, attention to every aspect and hardware involved in the IoT application is essential for ensuring robust performance and high availability.

Counterfeit electronic components are fraudulent copies, imitations, or substitutes marked as genuine or altered without the legal right to mislead or defraud. They can be recycled, re-marked, scrapped and tampered parts. The buyer is unaware they can have reduced lifespan, show design weaknesses or internal defects, or give access to sensitive functionalities/information of the system. In conclusion, they will probably not work as expected in terms of performance, quality, reliability and security. The presence of counterfeit electronics in critical systems (military, biomedical, automotive, and space) can cause substantial reliability risks and safety and security problems. Reliability risks from counterfeit electronics are clearly explained in (Brett 2025, SASC 2012, Stradley 2006, DiMase 2016, Mura 2022, Mura 2024). Avoiding counterfeit parts becomes particularly acute when obsolescence necessitates using parts from sources other than the original manufacturer or when procurement from an authorized distributor requests a long lead time. One could be forced to procure the part from unauthorized distributors, and the possibility of acquiring fake devices is not negligible. Consequently, there is an increasing need for non-destructive detection methods to spot counterfeit devices and mitigate counterfeit issues in the IoT perception layer without incurring high costs.

This work proposes a case study where a viable non-destructive detection method based on pure electrical measurements and simple machine learning algorithms is developed and tested. It represents a potentially trained in-line low-cost solution, at least for simple electronic devices.

2. Industry 4.0 and the counterfeit problem

The Industrial IoT (IIoT) refers explicitly to the use of IoT in the fourth-generation industry. The aim is to optimize production, quality control, and predictive maintenance to reduce system downtime. Data can contain information about monitoring and controlling the production process or related to the place, time, design documents, materials and parts. By unauthorized propagation of this information, the production process and the product can be disclosed. Moreover, devices that cannot accomplish the intended function can cause system unavailability or production unconformities. The prevalent focus regarding IoT problems concerns securing critical IoT networks, e.g., by emulating cyberattacks to protect the connected devices and the networks they use for communication. Safety, security, and continuity are the principal challenges in this context. Considering electronic devices in the perception layer, the IoT anti-counterfeiting approaches proposed in the literature rely, in most cases, on traceability using identifiers/enablers such as EPC, IMEI, even by employing NFC and RFID technologies, and DOA-based systems (Yang 2017, Gayialis et al. 2022, Al-Bahri et al 2018) The physical analysis of the hardware, such as sensors and their conditioning signals, used for the realization of IoT systems is not considered at the state-of-the-art. The present work would raise awareness that using COTS acquired from unauthorized distributors exposes one to a high risk of procuring counterfeit devices and emphasizes that detection procedures can help minimize the potential introduction of counterfeit devices in the supply chain.

3. Counterfeit electronics detection techniques

When dealing with suspect devices, 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. The SAE Aerospace Standard AS6171A (SAE International 2018) and its slash sheets provide guidance and plenty of helpful examples for suspect counterfeit part detection. It includes non-destructive and destructive approaches. 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).

4. The proposed case study

The devices under analysis are low-power audio amplifiers designed for low-voltage consumer applications and provided in a plastic dual-in-line package. This kind of device is widely used in IoT applications, especially for signal conditioning in sound sensors-based systems or COTS speakers and can be integrated into external audio modules as reported in (Rivadeneira et al. 2024, Jafarzadeh et al. 2021, Babu et al. 2022, Maity 2020, Zhang 2022). Standard-based destructive approaches are proposed to authenticate these devices in (Mura 2020, Mura 2021). The physical destruction of a suspected device to prove its authenticity can be necessary when performing failure analysis, but it is not an affordable approach in a systems production line where authentic devices must be mounted. This work compares the electrical characteristics of counterfeit amplifiers acquired from unauthorized distributors with a vast set of original amplifiers acquired from an official distributor to train algorithms to detect counterfeit devices. Electrical characterization plays a fundamental role (Deen 2017, Mura et al. 2013, Vanzi et al. 2017) in detecting parametric and manufacturing defects, anomalies, and failures and, most importantly, in this context, can ascribe differences in layouts (SAE International 2016).

4.1. *Machine learning based approach*

For the study, 233 original and 318 counterfeit devices were measured. Original devices are representative of different production lots, while counterfeit devices belong to three different kinds of copycat of the original ones. Counterfeit devices are parts of some sets already analyzed destructively. According to the manufacturer's datasheet information, three electrical characteristics were acquired for each device. The study was structured into two phases. The first phase involved the study of the features. In addition to the three features corresponding to the three measurements, a further feature, the slope, was included in the set. The analysis of the features' distribution and correlation enabled the second phase, which focused on the selection of the algorithms. The pairplot of the dataset is reported in figure 1. KNN (k-nearest neighbours) and linear SVM (support-vector machines) were selected. The KNN and SVM test performance comparison is outlined in Table 1 and Table 2.

Table 1. KNN and SVM test performance comparison. The lines refer to the training with three features.

ML model	Accuracy	Precision	Recall	F-Score
KNN n=11	99.4%	98.8%	99.7%	99.3%
SVM C=10	94.3%	92.5%	93.9%	93.2%

Table 2. KNN and SVM test performance comparison. The lines refer to the training with four features.

ML model	Accuracy	Precision	Recall	F-Score
KNN n=11	100%	100%	100%	100%
SVM 1≤C≤10	100%	100%	100%	100%

The test results revealed that both algorithms perform excellently on devices of the same type of those used in the training phase when four features are considered. Performances of 100% reported in Table 2 derive from the data distribution obtained from the introduction of the fourth feature (the slope of the quiescent current vs supply voltage). In Figure 1, in the pair plots containing the slope current, the two classes of devices are perfectly separated, leading to an effective classification of the devices in the test phase.

This enables the model to recognize original devices and counterfeits of the same kind as those used in the training phase. On the contrary, when the current slope is not considered, a partial superposition of the data distributions can be observed, as in the top-left 3x3 matrix in Figure 1, leading to less accurate test results for the three-features model, reported in Table 1.

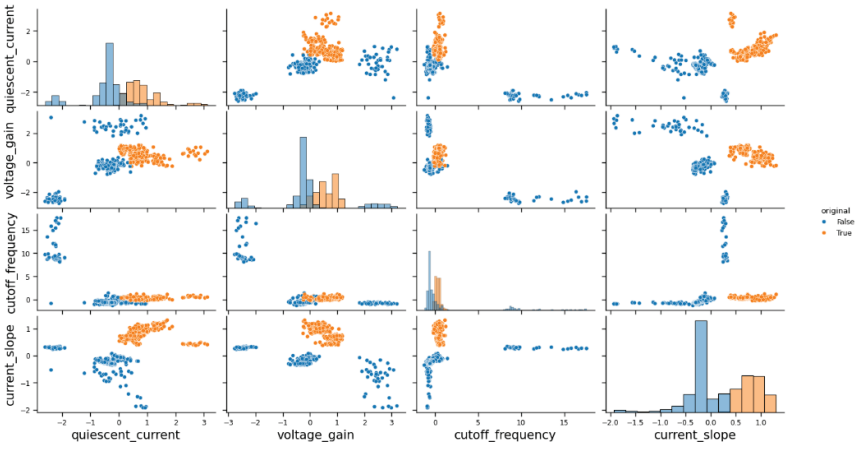

Figure 1. Pairplot of the dataset under analysis.

Further sets of devices acquired from unauthorized distributors (A, B, C and D) were verified with best-performing algorithms to test the algorithm's capability of recognizing even other counterfeit types. Results from the classification are reported in Table 3.

Table 3. Original and counterfeit authentication by using the algorithms.

ML model	A	B	C	D
KNN	Original	Original	Counterfeit	Counterfeit
SVM	Counterfeit	Original	Counterfeit	Original

KNN and SVM coherently classify device B as original and C as counterfeit (C is from the same kind of those used in the training phase but different lot), while devices A and D are classified differently. In these cases, a prudent strategy should prioritize the "*counterfeit*" given by at least one of the algorithms.

The chemical removal of the plastic packages enabled the analysis of the layout, confirming that B is original, and A, C, and D are counterfeits.

Conclusion

The outlined results proposed in this work demonstrate that machine learning-assisted electrical measurements can be a highly effective way to authenticate electronic products when non-destructive verification is required. This approach represents a quick and cheap way to introduce mitigation against the penetration of counterfeit devices in IoT systems. In non-critical applications, where the electrical measurements are a daily part of a non-destructive screening approach before mounting the devices, the availability of a vast set of features from original devices can be quickly obtained. The additional little effort is related to the population of a dataset with features belonging to counterfeits. The huge advantage is that an improved daily in-line approach for detecting counterfeits is quickly available, minimizing the risk of counterfeits entering the production line. It provides a good balance between risks, testing costs, and benefits for non-critical applications. Moreover, it can support a properly planned standard-based detection strategy in critical applications. The proposed approach could be adapted for more complex devices if a reasonable number of custom features highlighting the analyzed device's specific characteristics can be identified. As it can detect different LM copycats, remarked, and out-of-spec/defective devices, currently, activities on the LMxxx aim to enlarge the dataset, train the algorithms for new kinds of counterfeits and inspect whether even aged devices are easily detectable with this approach. Additionally, this work paves the way towards the authentication of the LM when already integrated into commercial modules, assuming that if the key

device is authentic, the module is highly likely to be authentic.

Acknowledgement

This work has been partially founded by "Fondazione di Sardegna" under project "DACE – Detection and Avoidance of counterfeit electronics", CUP: F73C22001310007 and partially founded by "Regione Sardegna" under the project "NoDeCI- Non-Destructive Counterfeit Identification".

References

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1-31, doi: 10.1016/j.comcom.2014.09.008

Kelly, S. et al. (2013). Towards the Implementation of IoT for Environmental Condition Monitoring in Homes. *IEEE Sensors* J., 13, 10, 3846-53, doi: 10.1109/JSEN.2013.2263379

Mohammadrezaei, M. et al. (2020) Internet of Things (IoT) and the Energy Sector. *Energies*, 13(2), 494, doi: 10.3390/en13020494

Pettorru, G. et al. (2023). An IoT-based electronic sniffing for forest fire detection. *IEEE Int. Conference on Consumer Electronics (ICCE)*, 1-5, doi: 10.1109/ICCE56470.2023.10043411

Dhingra, S. et al. (2019). Internet of Things Mobile–Air Pollution Monitoring System (IoT-Mobair). *IEEE Internet of Things Journal*, 6, 3, 5577-84, doi: 10.1109/JIOT.2019.2903821

Singh, R. et al. (2020) Internet of things (IoT) applications to fight against COVID-19 pandemic, *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 14, 4, 521-24, doi: 10.1016/j.dsx.2020.04.041.

Radovan, M. and B. Golub, (2017). Trends in IoT security. *Int. Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* 1302-08. doi: 10.23919/MIPRO.2017.7973624

Mishra, N. and S. Pandya, (2021). Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. *IEEE Access*, 9, 59353-77. doi: 10.1109/ACCESS.2021.3073408

Farkas, T. and E. Hronyecz, (2024). The Risks and Danger of Smart Devices Exposing Personal Information: Dark Side of Convenience. *IEEE Int. Symposium on Intelligent Systems and Informatics (SISY)*, 39-44. 10.1109/SISY62279.2024.10737613

Hasan, A. et al. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*. 100,144-164. doi: 10.1016/j.future.2019.04.038.

Yang, K. et al. (2017). CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability, and Authentication in the IoT Supply Chain. *ACM Transactions on Design Automation of Electronic System*, 22, 3, 1 – 31 doi: 10.1145/3005346

Sauter, T. and A. Treytl, (2023). IoT-Enabled Sensors in Automation Systems and Their Security Challenges. *IEEE Sensors Letters*, 7, 12, 1-4, 7500904 doi:10.1109/LSENS.2023.3332404

Bopp, R. L. et al. (1995). The gray market trojan horse [used electrical equipment]. *IEEE Transactions on Industry Applications*, 31, 3, 535-41, doi: 10.1109/28.382114.

Mura, G. (2018) Reliability concerns from the gray market. *Microel. Reliab*. 88-90, 1-4, doi: 10.1016/j.microrel.2018.06.098

Brett, D. "10 shocking facts about counterfeit electronics [defense & aerospace]" February 18, 2021 accessed January, 27, 2025 https://www.trentonsystems.com/en-us/resource-hub/blog/10-shocking-facts-counterfeit-electronics

Committee on Armed Services United States Senate (2012). Inquiry into counterfeit electronic parts in the department of defense supply chain. 112–167

Stradley, J. et al. (2006). The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications. *IEEE Trans. Comp., Packaging Tech*. 29, 3. doi: 10.1109/TCAPT.2006.882451

DiMase, D. et al., (2016) Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems. *Risk Analysis*, 36, 10. doi: 10.1111/risa.12536

Mura, G., G. Martines, (2022). Reliability Risks from Counterfeit Electronics. *IEEE International Conference on System Reliability and Safety Engineering (SRSE)*, 297–301. doi: 10.1109/SRSE56746.2022.10067413

Mura, G. (2024). The Threat of Counterfeit Electronics to the Development of CubeSats. *IEEE International Symposium Electronics in Marine (ELMAR),* 203131, 223–226. doi: 10.1109/ELMAR62909.2024.10694162

Gayialis, S.P. et al. (2022). A Review and Classification Framework of Traceability Approaches for Identifying Product Supply Chain Counterfeiting. *Sustainability*, 14(11), 6666. doi: 10.3390/su14116666

Al-Bahri, M. et al. (2018) Combating Counterfeit for IoT System Based on DOA. *Int. Congress on UltraModern Telecommunications and Control Systems and Workshops (ICUMT)*, 1-5, doi: 10.1109/ICUMT.2018.8631257

Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts, AS6171A, SAE International, 2018

Rivadeneira, J.E. et al. (2024). CONFLUENCE: An Integration Model for Human-in-the-Loop IoT Privacy-Preserving Solutions Toward Sustainability in a Smart City. *IEEE Internet of Things Journal*, 11, 5, 8690-8714, doi: 10.1109/JIOT.2023.3321778

Jafarzadeh, P. et al. (2021). IoT-Based Household Energy Consumption Prediction Using Machine Learning. *EAI/Springer Innovations in Communication and Computing*. Springer, Cham. doi:10.1007/978-3-030-69705-1_8

Babu, E. et al. (2022). Predictive Analysis of Induction Motor using Current, Vibration and Acoustic Signals. *Int. Conference on Power Electronics & IoT Appl. in Renewable Energy and its Control (PARC)* doi: 10.1109/PARC52418.2022.9726688

Maity, A. and I. S. Misra, (2020). Prototype Design of An IoT Enabled Cost-Efficient Portable Heart-Health Data Acquisition System. *IEEE Calcutta Conference (CALCON)*, 137-141. doi: 10.1109/CALCON49167.2020.9106515

Zhang, Y. et al. (2022). Detection of Electromagnetic Signal Injection Attacks on Actuator Systems. *Int. Symposium on Research in Attacks, Intrusions and Defenses*, 10.1145/3545948.354594910.1145/3545948.3545949

Mura, G., Murru, R., and Martines, G. (2020). Analysis of counterfeit electronics. *Microel. Reliab*, 114, 11379 doi: 10.1016/j.microrel.2020.113793

Mura, G., Murru, R., Martines, G. (2021). Analysis of Fake Amplifiers. *Int. Conference on Microelectronics*, (*ICM*), 131–134 doi: 10.1109/MIEL52794.2021.9569080

Mura, G. et al. (2023). Electronic components authentication via physical analysis. *IEEE Int. Conference on Microelectronics (MIEL)*,10.1109/MIEL58498.2023.10315874

Deen, M. et al. (2017) Electrical Characterization of Semiconductor Materials and Devices. *Handbook of Electronic and Photonic Materials*. Springer, 10.1007/978-3-319-48933-9_20

Mura, G. et al. (2013). The role of the optical trans characteristics in laser diode analysis. *Microel. Reliab*, 53, 9–11 doi: 10.1016/j.microrel.2013.07.114

Vanzi, M. et al. (2017). Extended Modal Gain Measurement in DFB Laser Diodes. *IEEE Photonics Tech. Lett*., 29, 7762038, doi: 10.1109/LPT.2016.2633440

SAE International, Techniques for Suspect/ Counterfeit EEE Parts Detection by Electrical Test Methods, AS6171/7, (2016)