Model for selecting test methods of detecting fraudulent electronic components

Ya A Shchenikov, S V Michurin and V O Sidorov
Saint-Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya str. 67A, Saint-Petersburg, 190000, Russian Federation

E-mail: yar2409@mail.ru

Abstract. The article deals with the issues of electronic components incoming inspection processes risk management. A comparative analysis of the cost of using instruments used to identify fraudulent electronic components is carried out. A model developed using principles similar to FMEA-analysis is presented to select plans for detecting counterfeit and fraudulent electronic components based on the influence of factors such as the size of the batch, the criticality of application, and the source of supply.

The use of inauthentic, i.e. fraudulent, counterfeit electronic components in the repair of aircraft leads to losses for manufacturers and endangers flight safety. At present, there is a sufficient amount of data in the world that confirms the wide prevalence of fraudulent products [1-3]. The turnover of all inauthentic products in the Russian Federation is estimated by Rospatent at 80-100 billion rubles a year.

According to research, the share of fraudulent and counterfeit components in the world reaches 10 percent. Therefore, the problem of detecting fraudulent electronic components is relevant all over the world. Over the past decade, several important standards have been adopted in the world and the Russian Federation to prevent the supply of fraudulent electronic components [4, 5].

In accordance with the requirements [4], the company must develop and apply a control plan to detect fraudulent electronic components, and the electronic components verification process rigidity must be commensurate with the risk that may occur when using fraudulent components in product.

The factors that can affect the choice of methods for detecting fraudulent components are shown in figure.

The factors determine the set of methods for detecting fraudulent components (table 1), arranged in order of increasing complexity, and, as a result, the cost of testing.

Figure 1. Factors affecting the selection of a set of methods for detecting fraudulent electronic components.
### Table 1. Methods for detecting fraudulent components, instruments used and the cost of their use.

| Method number in table 3 | Method | Instruments used and their cost |
|--------------------------|--------|--------------------------------|
| 1                        | Checking documentation and packaging | No instruments are required |
| 2                        | Visual inspection to detect re-marking or replacement of the coating | Inexpensive optical microscope or camera |
| 3                        | Solvent-based testing to detect re-marking and surface coating changes | Inexpensive set of chemical reagents |
| 4                        | Scanning with an electron microscope (SEM) | Expensive electronic microscope |
| 5                        | Scanning with an acoustic microscope (SAM) | Expensive scanning acoustic microscope |
| 6                        | Radiological examination (in x-rays) | Expensive x-ray machine |
| 7                        | Assessment of lead content in the coating using x-ray spectroscopy (XRF) or energy-dispersive x-ray spectroscopy (ESD/EDX) | Expensive x-ray machine |
| 8                        | Electrical tests: analog and digital signature analysis | Relatively inexpensive equipment for electrical testing |
| 9                        | Burn-in testing | Expensive climate chamber |
| 10                       | Temperature cycling tests (TCT) | Expensive climate chamber |
| 11                       | Hermeticity testing of the component: weak and strong leakage | Expensive helium leak detector |
| 12                       | Physical destructive analysis with opening of the package and subsequent visual inspection | Inexpensive set of chemical reagents, inexpensive optical equipment, such as an optical microscope or camera |
| 13                       | Destructive physical analysis (DPA): internal connections and external leads test, die shear testing | A relatively inexpensive connection tester, bond strength and die shear tester |

### Table 2. Required test sample sizes accepted in table 3.

| Designation in table 3 | Required test sample size |
|------------------------|---------------------------|
| A                      | Test a small percentage of the total number of components |
| B                      | Test some percentage of batches with each date/batch code |
| C                      | Test 100 percent of all products |

If you know the sources of supply and the criticality of the use of electronic equipment produced, then the table 3 can help to choose the best plan in terms of economic costs for testing. The table 3 helps to select the most cost-effective control plan for the electronic component if tester knows the source of its supply and the criticality of its use. For example, the designation "10A" means that a temperature cycling test (TCT) is used and a small percentage of the components in the test batch are tested.

### Table 3. Model for selecting methods for detecting fraudulent electronic components for drawing up a control plan.

| Products and applications | Non-critical use | Critical use |
|---------------------------|-----------------|--------------|

| Sources of supply | Short expected life / non-critical application | Products can be repaired | Refurbished or faulty product | Repairs in the field conditions are not possible | Critical for purpose | Critical for safety | Critical for human life |
|-------------------|---------------------------------------------|--------------------------|-------------------------------|-----------------------------------------------|----------------------|---------------------|----------------------|
| Original component manufacturer (OCM) or certified component manufacturer | 1A,2A 8A | 1A,2A 8A | 1A,2A 8A,9A 10A | 1A,2A 8A,9A 8B,9B 8B,9B 8C,9C | 1B,2B 1B,2B 1B,2B 1B,2B | 1B,2B 1B,2B 1B,2B | 8C,9C |
| Authorized supplier | 1A,2A 3A | 1A,2A 3A,10A | 1A,2A 8A,9A 10A | 1A,2A 8A,9A 8B,9B 8B,9B 8B,9B 8C,9C | 1B,2B 1B,2B 1B,2B 1B,2B | 1B,2B 1B,2B 1B,2B | 8C,9C |
| Original Equipment Manufacturer (OEM) / contract manufacturer | 1A,2A 3A,8A | 1A,2A 3A,8A | 1A,2A 8A,9A 10A | 1A,2A 8A,9A 8B,9B 8B,9B 8B,9B 8B,9B 8C,9C | 1B,2B 1B,2B 1B,2B 1B,2B | 1B,2B 1B,2B 1B,2B | 8C,9C |
| Independent distributor with high quality, reputation and appropriate procedures | 1A,2A 3A,8A | 1A,2A 3A,8A | 1A,2A 8A,9A 10A | 1A,2A 8A,9A 8B,9B 8B,9B 8B,9B 8B,9B 8B,9B 8B,9B 8C,9C | 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B | 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B 1B,2B | 1B,2B |
| Independent distributor with unknown quality, reputation and procedures | 1C,2C 3B,4B 5B | 1C,2C 3B,4B 5B | 1C,2C 3C,8C | 1C,2C 3C,8C 8C,9C 8C,9C 8C,9C 10B,11B | 1C,2C 3C,8C 8C,9C 8C,9C 8C,9C 10B,11B | 1C,2C 3C,8C 8C,9C 8C,9C 8C,9C 10B,11B | 1C,2C 3C,8C 8C,9C 8C,9C 8C,9C 10B,11B |
| Unknown source of electronic components | 1C,2C 3A,4A 5A | 1C,2C 3A,4A 5A | 1C,2C 3C,8C | 1C,2C 3C,8C 8C,9C 10C,11C 10C,11C 10C,11C 10C,11C 12B,13B | 1C,2C 3C,8C 8C,9C 10C,11C 10C,11C 10C,11C 10C,11C 12B,13B | 1C,2C 3C,8C 8C,9C 10C,11C 10C,11C 10C,11C 10C,11C 12B,13B | 1C,2C 3C,8C 8C,9C 10C,11C 10C,11C 10C,11C 10C,11C 12B,13B |
| There is a report with a warning about the seller | 1C,2C 3A,4A 5A | 1C,2C 3A,4A 5A | 1C,2C 3C,8C | 1C,2C 3C,8C 8C,9C 6B,7B 6B,7B 6B,7B 6B,7B 6B,7B | 1C,2C 3C,8C 8C,9C 6B,7B 6B,7B 6B,7B 6B,7B 6B,7B | 1C,2C 3C,8C 8C,9C 6B,7B 6B,7B 6B,7B 6B,7B 6B,7B | 1C,2C 3C,8C 8C,9C 6B,7B 6B,7B 6B,7B 6B,7B 6B,7B |

The control plan selected from the table 3, for example, the control plan "1C, 2B, 6B, 7B, 10C, 11B, 12B, 13B" shown in the lower right corner of table 3, is implemented in order of increasing complexity and cost of tests. From simple documentation checking and visual inspection (1C, 2C), which does not require any means of measurement, to complex tests (10C, 11B, 12B, 13B), which may include, for example, electrical tests, destructive physical analysis, temperature cycling tests [6, 7].
To increase the probability of detection of fraudulent components, it is necessary to develop control plans, but how to develop them isn’t specified in the standards. The implementation proposed in the article model for selecting methods makes it possible to determine the cost-effective plan for identifying fraudulent electronic components.

To justify the control plans proposed above, a risk assessment methodology designed like the FMEA analysis can be used [8]. It should be noted that, thanks to the proposed model, the frequency of electronic equipment failure cases due to accidental using of fraudulent electronic components can significantly decrease.

The developed model, from the point of view of the international standard ISO 9000: 2015, can be considered as a model for implementing corrective actions. Of course, there shouldn’t be a situation when a company that produces electronic equipment periodically encounters falsified electronic components. Therefore, the developed model will be more effective if a preventive actions system is used together with it. It can be actions as: choosing a reliable supplier, choosing alternative suppliers, changing the design of equipment, improving the equipment reliability through redundancy.

References
[1] Chaudhry P E and Zimmerman A 2009 The Economics of Counterfeit Trade: Governments, Consumers, Pirates and Intellectual Property Rights (Heidelberg: Springer) p194
[2] The economic impact of counterfeiting and piracy: executive summary 2007 Retrieved from: https://www.oecd.org/sti/38707619.pdf
[3] Guin U, Huang K, DiMase D, Carulli J, Tehranipoor M and Makris Y 2014 Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain Proc. IEEE 102(8) 1207-28
[4] Aerospace standard SAE AS5553A:2013 «Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition» Retrieved from: https://saemobilus.sae.org/content/as5553
[5] Aerospace standard SAE AS6462A:2014 «AS5553A, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition Verification Criteria» Retrieved from: https://saemobilus.sae.org/content/as6462a/
[6] Tehranipoor M, Guin U and Forte D 2015 Counterfeit Integrated Circuits. Detection and Avoidance (Springer International Publishing Switzerland) p 269
[7] SAE, Test Methods Standard; Counterfeit Electronic Parts. Retrieved from: http://standards.sae.org/wip/as6171/
[8] Stamatis D H Failure Mode and Effect Analysis: FMEA from Theory to Execution 2003 (ASQ: Quality Press) p 488