SOME METHODS FOR ELECTRONIC COMPONENT AUTHENTICITY ASSESSMENT

Petr Neumann[a], , Josef Houser[b], Martin Pospíšilík[a], Petr Skočík[a], Milan Adámek[a]

[a]Faculty of applied informatics, Tomas Bata Univerzity in Zlin, Nad Stráněmi 4511, Zlin 76005, Czech Republic,
[b]Faculty of Technology, Tomas Bata University in Zlin, Vavrečkova 275, Zlin 76272, Czech Republic

Abstract

The spurious aka counterfeit components represent still a serious danger for functionality, reliability and lifetime of any electronic device these components are part of its manufactured assembly. There exist a lot of methods aimed at revealing counterfeit components before they are used in electronic module production. Those methods differ in complexity and also in counterfeit component filtering yield. In short, any efficient method based on specification parameters manifestation, functionality and appearance comparison is applicable. This presentation illustrates the diagnostic abilities of some representative methods for counterfeit components preventive filtering from a production process. As a result of our research activities, the capability of popularly known Analogue Signature Analysis method is mentioned and illustrated as well as laser decapsulation method and a comparison of visual features accentuated with light exposure.

Keywords: Analogue Signature Analysis; I-V characteristics; Pin Print; laser decapsulation; coaxial light; dark field light; SoC System on Chip

This Publication has to be referred as: Neumann, P[etr]; Houser, J[osef]; Pospisilik, M[artin]; Skocik, P[etr] & Adamek, M[ilan] (2016). Some Methods for Electronic Component Authenticity Assessment, Proceedings of the 26th DAAAM International Symposium, pp.0018-0026, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-07-5, ISSN 1726-9679, Vienna, Austria
DOI:10.2507/26th.daaam.proceedings.003

1. Introduction

The electronic component authenticity verification represents a very important act especially for any company producing application specific assemblies nowadays. The problem of disingenuous electronic components represents an increasing worldwide problem in course of about last twelve years. These components are presented as original products by OCMs (Original Component Manufacturers) according to their labeling, logos, delivery accompanying documentation etc. [1] There are some very frequent notions distinguishing such kind of electronic components from genuine ones, as for instance counterfeit components, fake components, bogus. The sources for component counterfeiting are quite varied ones. It could be a discarded batch originating from the component original manufacturer, or it could be a refurbished component from a trash of electronic modules which were not recycled properly that means according to the Basel Convention [7] and following national legal acts. The reason which attracts those who are counterfeiting electronic component is a same one as at other illegal or criminal activities, gain interesting amount of money and invest less than in legal activities. The components counterfeited types are also varied ones and demand dependent. The surveys and reports [1] are showing that we can encounter counterfeited discrete components, integrated circuits up to very sophisticated ones, passive components, relays etc. Briefly stating, the range of electronic components counterfeited types is very wide, and only its proportion in supply varies according to the market demand and in particular cases. The counterfeited component level of technology can also differ from obsolete components up to modern advanced types which are of latest design, but there is a shortage of them because of limited production capacity in relation to the interest on the market at that very moment. The occurrence of components having been remarked from a lower cheaper class to a higher one being fraudulently misrepresented as military grade components for sensitive applications is also very frequent [1].

The obsolete components business represents a chapter for itself in activities related to counterfeited electronic components. The long life time systems with the time period of operation up to twenty or thirty years are supposed to be repaired and maintained with original spare parts which are at the time of repair obsolete and no more in production. The fighter F-15 can serve as an example because it was put into service in 1975 and was scheduled to be in service well beyond 2010 eventually. That means that it had been used far after its original end-of-life projections. Moreover, the electronic component life cycle gets shorter because of new designs and new production technologies, and it could be well as short as two years only [3] [1]. It is possible to procure obsolete components from an original manufacturer in some cases, nevertheless, it always depends on ordered quantity, and it is fully understandable that the price will be much higher than at the time of active production and delivery time will be much longer. Such situation motivates and encourages the obsolete components counterfeited alternatives offer because that is an ideal opportunity to utilize that refurbished electronic trash supply. The general effort for cost reduction acts as a joint influence promoting the counterfeit components penetration the electronic systems production [1].

The big customers with substantial needs for electronic components can mitigate the counterfeit components problem easier than smaller ones because they can arrange the component supply directly from the original manufacturers. Nevertheless, there is also possible that the original component manufacturer can detect counterfeit components warehouses because of global logistics [1]. Smaller customers may quite frequently experience situation when they need to look for required components supply from alternative sources. Especially the odd and unproven supplier represents an extremely high risk in spite of its attractive prices and very short delivery times. It is just for that attractiveness recommended to be very careful and distrustful.

2. How to prevent counterfeit components invasion

There have elapsed about twelve years since the counterfeit components were detected in sensitive military, space research and life influencing medical systems. These detections were an alarming reality calling for immediate countermeasures development and acceptance [4]. The counterfeit components prevention encompasses quite a wide range of activities nowadays. These activities can be categorized according to their content and way of contribution to the common effort to stop the counterfeited electronic components penetration in crucial assemblies and systems. Sharing experience is a very important activity because it can help the others to be oriented, warned and inspired how to notice or reveal suspicious features at the particular consignment. There is a lot of websites operated by qualified and experienced professionals and expert organizations [5]. Presenting pictures illustrating a particular experience with stressed signs of counterfeiting is a sensitive concern not to influence negatively the reputation of component manufactures being blameless and not involved, only their names and logos were misused for labeling a fake component, or their SoC were misused for the integrated circuit assembly. Also subjects reporting their own experience with disingenuous components should be kept in anonymity when they do not wish to go public. There are also websites related to the government or to other authorities involved in the counterfeit components problem solution. These websites are offering comprehensive information and instructions for preventive measures [6].

The instructions what to do and the company counterfeit component prevention policy is one important aspect of reasonable preventive behavior. The other aspect covers methods for revealing definite attributes or proves of counterfeiting. Those detection methods range from very simple and relatively cheap ones, like a visual inspection of component and its accompanying documentation and packaging appearance, up to very sophisticated and expensive methods, like X-ray inspection, scanning acoustic microscopy, scanning electron microscopy, parametric testing etc.

[2]. In fact, all methods comprising equipment and procedures being able to detect any difference between an original genuine component and its alternative to be verified are theoretically applicable. Their implementation depends on particular subject situation and on expected components quantity to be tested. Simple and cheaper methods are affordable even for small companies. However, the reliable verdict in many tricky cases calls for in-depth tests with corresponding equipment and trained experienced personnel. Such analytical laboratories are frequently independent subjects and certified as experts for counterfeit component assessment as those randomly selected references are illustrating [8] [9] [10] [11]. Some advanced testing laboratories are offering also inventory for electronic components, incoming tests for counterfeit components, repackaging and delivery to customers. We can mention Equality Process, Inc. and North Shore Components, Inc. as illustrative example among many others [12] [13].

The independent laboratories and laboratories controlled by the government are offering paid services in relation to production technology problems as well as to component counterfeiting attributes tracing for companies interested in an external assessment. However, the big suppliers of electronic components including obsolete components have introduced gradually their own test procedures and they have qualified reliable electronic component sources to guarantee customers a counterfeit-free delivery by themselves. We can mention again only two examples on behalf the others [14] [15].

There are not only technical means engaged in defense against counterfeit components invading electronic assemblies and systems. Organizational means are also playing an important role, especially in relation to portfolio of suppliers and their credibility. Even standardization process in the field of counterfeit components penetration preventive measures has been developing since early after the first counterfeit components incidence, and there exist a lot of standards, regulations and written rules guiding and helping subjects to behave according to the risk and threat involved [22] [23].

3. Our laboratory for electronic component analysis

As also our experience from meetings, seminars and from cooperation with local companies in the field of counterfeits components testing has revealed, that local companies have limited budgets and product profit reserves to cover costs for establishing an incoming electronic component inspection at a necessary level. They are willing to detect some discrepancies in accompanying documentation, during visual inspection in rare cases, but they care mostly for a specialized external laboratory to perform qualified tests for them. We have decided to react proactively on that motivating impulse, and we started to build up a diagnostic laboratory for that purpose in frames of our educational themes focused on security technologies about three years ago. We had already a helpful initiation into counterfeited electronic components worldwide problem thanks to a very useful device based on analogue signature analysis principles [18] [21]. That device was designed directly for counterfeit integrated detection, and our experiments with it has aroused our curiosity and need to learn more about that problem. The counterfeit IC detector is a very useful part of our laboratory equipment now. It has 256 channels to be assigned arbitrarily to the tested component pins. If the component has more than 256 pins, the test can be accomplished in more than one step until all pins are tested. Of course, the crucial part of the whole test arrangement is the test contact adapter corresponding with the component package. Fig. 1, Fig. 2 and Fig. 3 illustrate the workplace with counterfeit IC detector, its contact interface and some SMD contact adaptors.

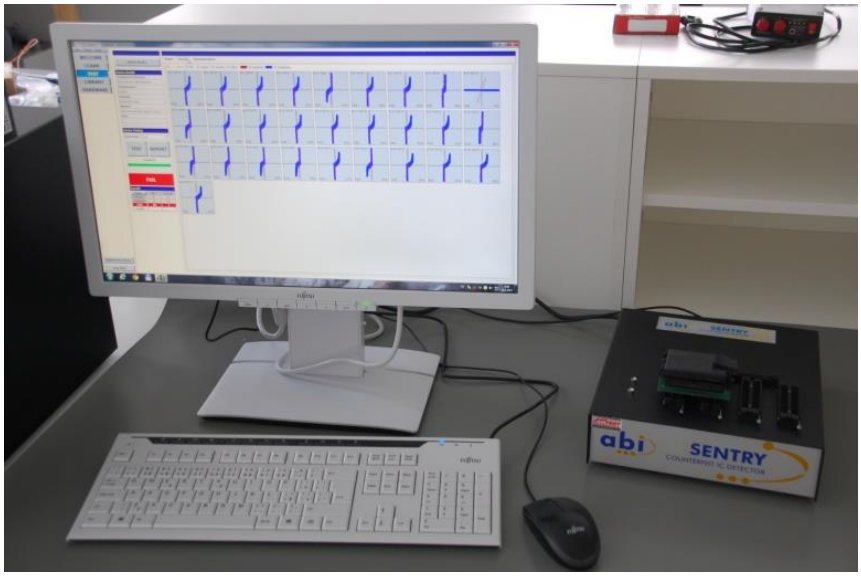

Fig. 1. Component I-V characteristics evaluation arrangement

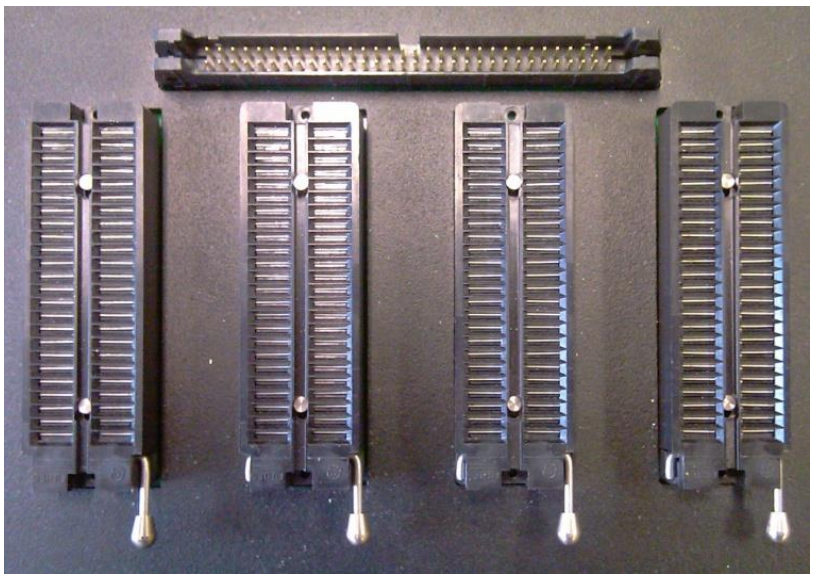

Fig. 2. The counterfeit IC detector contact interface

Fig. 3. The counterfeit IC detector contact interface

The counterfeit IC detector has a wider application possibility than its original orientation. We are also using it for the evaluation of the laser beam influence on the SoC (System on Chip) functionality in course of laser decapsulation procedure development. The initial component I-V characteristics set serves as a reference model for comparison how deep we can perform the package material ablation until the I-V characteristic deformation starts. The fiber laser decapsulation equipment is the other tool component in our laboratory [19]. We have preferred laser decapsulation equipment to a wet etch automated equipment because of laser higher flexibility and wider range of application. Unlike laser, etch equipment is able to provide a very clean SoC revelation and preserve the component full functionality what is important for subsequent functional and failure analysis. Nevertheless, the laser equipment ablation recipe flexibility was decisive for us so that we have decided to combine the functionality safe partial laser ablation with a final wet etch process. The goals for the final etch process were simplicity, material consumption, temperature and waste reduction. Fig. 4, Fig. 5 and Fig. 6 are illustrating the workplace with fiber laser and ablation process results. Fig. 5 illustrates the partially ablated package material before the final etching. Fig. 6 illustrates the possibility to perform ablation exclusively by laser when the functionality is not important, and only the SoC label is to be identified. It is quite apparent that the laser beam energy has destroyed the protection layer of nitride oxide and also partially the SoC upper layers. Nevertheless, it was well possible to conclude that the package label differed from the SoC one. That pure laser ablation result can be still improved by using a better tuned recipe.

Fig. 4. Fiber laser suite for component package selective ablation

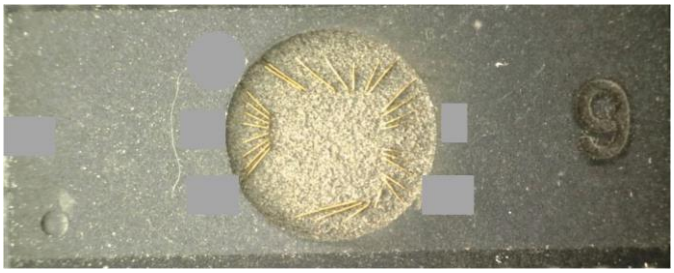

Fig. 5. The partially laser ablated component package material before final etch

The sort of materials standardly used for chip protection, chip bonding interconnection with outer contact system is a varied one [16]. That is why every component type group has to be approached carefully and experimentally because especially suspicious components do not have any trustful reference to be queried. The failure analysis experience reports can also help during a component behavior manifestation [17] and its analysis.

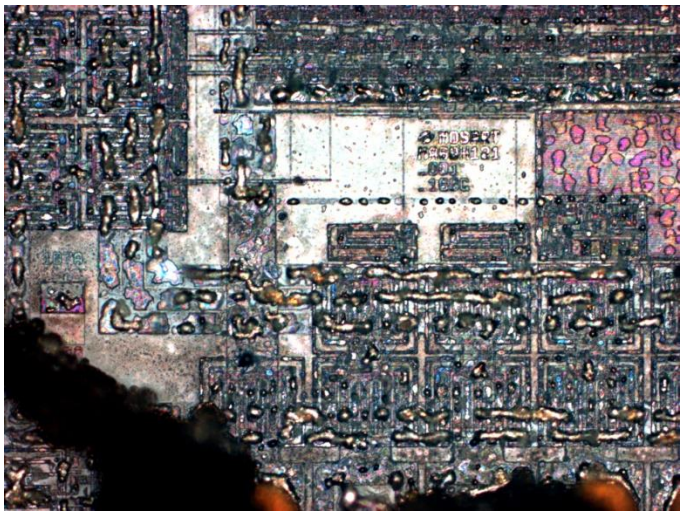

Fig. 6. System on chip ablated only by a laser beam

.

A combined process of preparatory laser ablation in the first stage and wet etching in second stage seems for us to be a solution corresponding with our particular situation. The result of after final standard etch ablation process with nitric and sulfuric acid mixture is documented with Fig. 7.

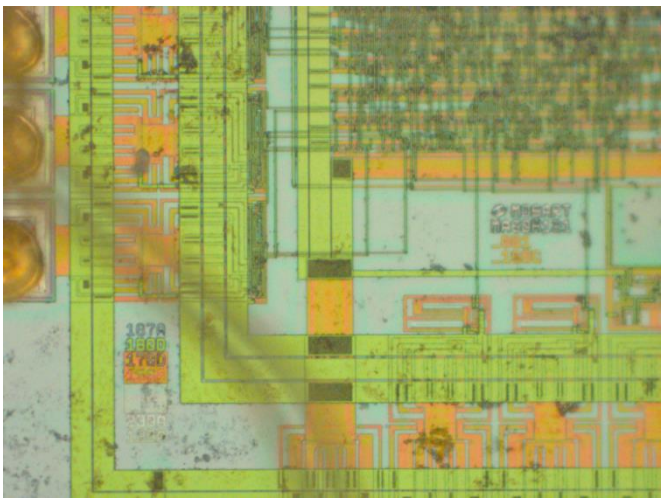

Fig. 7. The SoC after final etch process

4. The analytical methods application results

Our research and feedback experiment effort aims at laser ablation process refinement to make better use of all adjustable process parameters. The simple ablation process modification at fiber laser equipment leads to a quick verification possibility of any idea how the particular component should be ablated. The following Fig. 8, Fig. 9 and Fig. 10 illustrate some variants of experimental ablation process. The circular shape first stage ablation opening is very apt for the successive chemical etch treatment because it holds the etch mixture on required area without any supporting gasket, and there is only a little tendency to damage area outside the circular barrier providing the etch agent is dosed accurately and carefully. The etch process is done manually to keep simplicity in our case. That was also a reason for process temperature decrease effort to have that process more under control.

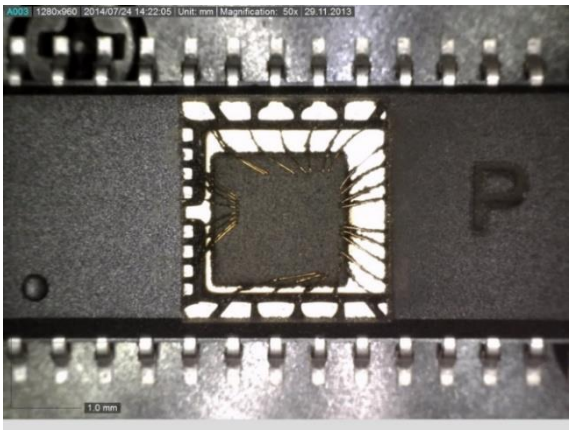

Fig. 8. Package material laser ablated only in micro-bonding area

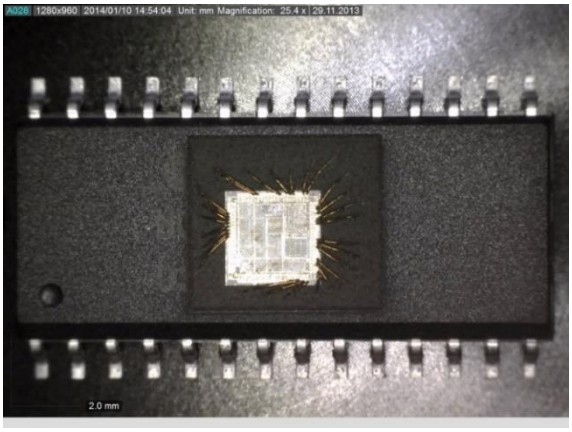

Fig. 9. Package material laser ablated in chip and vicinity area

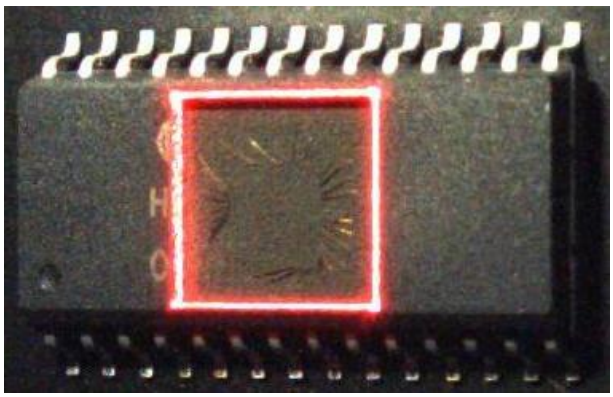

Fig. 10. Camera view of a laser beam activity area

We have succeeded to decrease the etch process temperature down to 50°C and less preserving a reasonable process speed with very good results. We have reached that positive achievement with some additives to standard mixtures of nitric and sulfuric acids. Fig. 11 shows the SoC after our modified etch treatment. The SoC label readability is perfect and the functionality is predominantly influenced by the laser ablation process.
As was reported in reference [20], the component package filling material can influence not only the laser ablation process but even the laser marking process, especially when the filling material are glass globules. They can act not only as lenses but also as an optical channel for the laser beam allowing it to penetrate deeper than expected during estimating the layer to be ablated with laser. We have concluded that some partial damages of nitride oxide protection layer were caused by that effect. Fig. 12 and Fig. 13 illustrate our own experience with filling material having been spread in decapsulated opening. That means that a residual layer for final etch treatment shall be thicker than was assumed before.

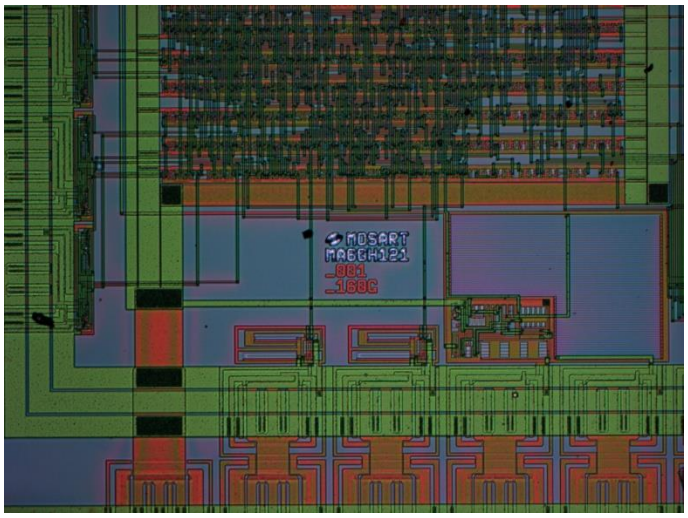

Fig. 11. SoC after modified etch process treatment

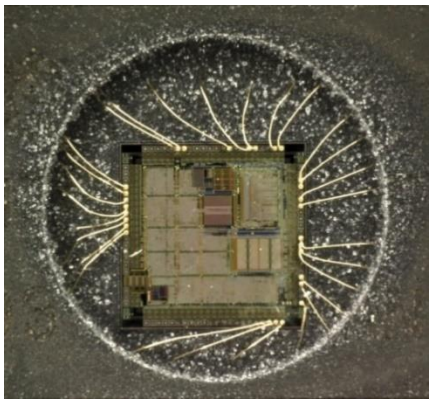

Fig. 12. Globules of glass in formed socket

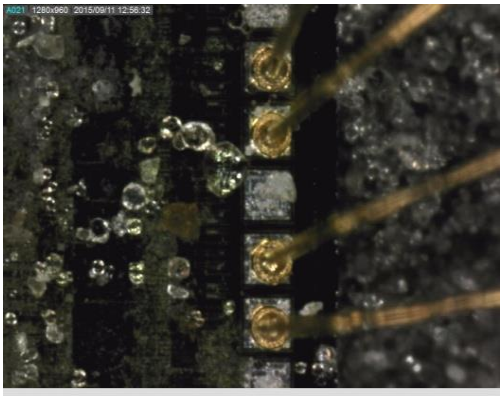

Fig. 13. More detailed picture of glass globules

The important part of preventive testing procedures is to procure and keep verified original components with relevant documentation to all sensitive electronic parts to be assembled in a particular production process because of comparison possibility during the alternative components delivery testing. That should be a rule not only for a test laboratory but for any company which is assembling systems from electronic components to prevent tricky situations in the future. Those model components should be archived immediately during the product development and always when the alternative components are tested for the circuitry.

5. Methods extension and development plans

Our current test laboratory activities feel the lack of X-ray equipment designed especially for counterfeit components detection. Such device is very useful not only for a non-destructive inspection of components and the comparison of internal chip, lead-frame and bonding wires structural appearance inspection. X-ray device can help laser device to aim more accurately at the chip position inside the package before ablation starts. There is even possible for laser to orient the location of ablation process according to the X-ray imported picture of the particular component. The project for X-ray equipment procurement is running currently and we expect it to be installed by the end of this year.

We also plan to extend the range of component package adapters for counterfeit IC detector to be able to react more flexibly to particular component types test requirements. Last but not least task is the contact resistance treatment before I-V characteristic recording and analysing because the storing and handling history of suspicious component is unknown. The leads appearance, oxides and damages presence optical inspection is always necessary before any electrical measurement and the relevant preparatory treatment for decreasing the contact resistance is required.

The laser ablation process and final etch process development and refinement belongs logically to our close future plans. The supporting fixtures design and realization as well as light sources range extension for optical inspection are also indispensable for our further research activities.

6. Conclusion

Our research project was aimed at establishing a laboratory equipped with affordable equipment for electronic component authenticity analysis at the very beginning. We have started that equipping process in a modest way because the university budget is limited and it has to cover many other projects. The government and European Community funding support allowed us to obtain also more expensive equipment like a fiber laser and special X-ray equipment which should be only shipped. Nevertheless, the comprehensive electronic component authenticity analysis represents the application of a wide range of special equipment like for instance acoustic microscopy, IR spectroscopy and X-ray spectroscopy. That poses a certain analytical limit for our laboratory currently. We take our project task as a continuous development of methods, learning by experiment and trying to involve more methods and equipment which are at disposal for other projects or which will be possible to procure in the future. Among the others, we can mention Raman spectroscopy [25] and atomic force microscopy (AFM) [24]. Our faculty possesses that equipment in other projects laboratories. Those laboratories are engaged in the field of security technologies what is tightly interlinked also with electronic component authenticity assessment. Raman spectroscopy is a very promising method for electronic component assembly materials composition analysis and also for component production quality grade assessment [26].

Our project is not a one-time task to be fulfilled and terminated. It represents a dynamic set of activities being adapted according to experience, research results and conditions for further development and extension. In spite of that, we are already cooperating with local companies in the field of electronic component authenticity assessment with very good and applicable results. We are still not in position of a certified expert laboratory that is why we are doing all analysis on a voluntary basis so far. The experience gained during all voluntary analyses means a precious knowledge and feedback for our further development. It also gives us an important inspiration for our analytical methods modification and completion.

We are working on a promising assumption that the role of suspicious components inspection methods is still of extreme high topicality and it always has sense to look for new principles and methods highlighting the component queer appearance and behavior to be evaluated and implemented.

7. Acknowledgements

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Program project No. LO1303 (MSMT-7778/2014).

8. References

[1] M. Crawford et al., Defense Industrial Base Assessment: Counterfeit Electronics, Report of U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, Available at: https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010, Accessed: 2015-09-24.

[2] M. Tehranipoor, U. Guin, D. Fort, Counterfeit Integrated Circuits: Detection and Avoidance, first ed., Springer, 2015.

[3] R. Solomon, P. Sandborn, M. Pecht, Electronic Part Life Cycle Concepts and Obsolescence Forecasting, IEEE Trans. on Components and Packaging Technologies, Dec. 2000, pp. 707-717.

[4] R.Hammond, Counterfeit Electronic Components are Putting Millions of Lives at Risk, Available at: http://www.aeri.com/counterfeit-chinese-electronic-parts-can-lead-to-disaster/, Accessed: 2015 -09-28.

[5] R. Hammond, Counterfeit Electronic Component Detection, Available at: http://www.aeri.com/counterfeit-electronic-component-detection/, Accessed: 2015 -09-28.

[6] US Federal Register, Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), Available at: https://www.federalregister.gov/articles/2014/05/06/2014-10326/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic, Accessed: 2015 -09-29.

[7] Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, Available at: http://archive.basel.int/text/con-e-rev.pdf, Accessed: 2015-09-29.

[8] Oneida Research Services, Inc., Available at: https://www.ors-labs.com/pdf/MASH07CounterfeitDevice.pdf, Accessed: 2015-09-29.

[9] National Technical Systems – Trace Laboratories, Inc., Available at: http://www.tracelabs.com/our-services/testing-programs/counterfeit- component-testing, Accessed: 2015-09-29.

[10] ITRI Innovation, Available at: http://www.itrilabs.co.uk/services/counterfeit-components-detection/, Accessed: 2015-09-29.

[11] Process Sciences, Inc., Available at: http://www.process-sciences.com/Counterfeit_Parts_Detection, Accessed: 2015-09-29.

[12] Equality Process, Inc., Available at: http://www.equalityprocess.com/, Accessed: 2015-09-29.

[13] North Shore Components, Inc., Available at: http://www.nscomponents.com/, Accessed: 2015-09-29.

[14] AERI, Available at: http://www.aeri.com/, Accessed: 2015-09-29.

[15] Converge – Arrow Electronic Company, Available: http://www.converge.com/, Accessed: 2015-09-29.

[16] C.A. Harper, Electronic Materials And Processes Handbook, McGraw-Hill, 2004.

[17] P.L. Martin, Electronic Failure Analysis Handbook, McGraw-Hill, 1999.

[18] ABI Electronics, Sentry Counterfeit Detector, ABI Electronics Ltd., Barsley, United Kingdom,Available at: http://www.abielectronics.co.uk/Products/SENTRYCounterfeitICDetector.php, Accessed: 2015-09-26.

[19] V. Ter-Mikirtychev, Fundamentals of Fiber Lasers and Fiber Amplifiers, Springer Series in Optical Sciences, first ed., Springer International Publishing, Switzerland, 2014.

[20] J. Patterson, C. Schuring, An analytical technique to assess the risk of laser damage to encapsulated Integrated circuits during package laser marking, Abstract for ISTFA Conference, 2008.

[21] P. Neumann, M. Adamek, P. Skocik, How Can V-I Characteristics Help in Counterfeit Component Detection, In Annals of DAAAM for 2011 And Proceedings, 2011, s. 0057-0058,. ISSN 1726-9679.

[22] SAE AS 5553 Revision A, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, Available for fee at: http://standards.sae.org/as5553/ , Accessed: 2015 -09-28.

[23] SAE AS 6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - DistributorsCounterfeit Electronic Parts; Avoidance Protocol, Distributors, Available for fee at: http://standards.sae.org/as6081/, Accessed: 2015 -09-28.

[24] M. Navratil, V. Kresalek, F. Hruska, T. Martinek, J. Kudelka, J. Sobota, Diagnostics of ultra-thin tungsten films on silicon substrate using atomic force microscopy, International Journal of Materials, 2014, Vol. 1, pp. 142-148. ISSN 2313-0555.

[25] H. Vaskova, A powerful tool for material identification: Raman spectroscopy, International journal of mathematical models and methods in applied sciences, [online] 2011, vol. 5, iss. 7, pp. 1205-1212, ISSN: 1998-0140.

[26] H. Vaskova, Micro Raman analyses of epoxy cross-linking reaction, In: Proceedings of the 23rd International DAAAM Symposium, Zadar, Croatia, DAAAM International, Vienna, Austria, 2012, pp. 667- 670, ISBN 978-3-901509-91-9.

[27] K. P. Pfeuffer,et al, Detection of counterfeit electronic components through ambient mass spectrometry and chemometrics, Analyst 139.18 2014, pp. 4505-4511, ISSN 0003-2654.

[28] U. Guin, D. DiMase, M. Tehranipoor, Counterfeit integrated circuits: detection, avoidance, and the challenges ahead, Journal of Electronic Testing 30.1, 2014, pp. 9-23, ISSN: 0923-8174.