RELIABILITY OF WSN HARDWARE

Johanna Virkki[1], Yao Zhu[2], Yuewei Meng[2], and Liquan Chen[2]

[1]Tampere University of Technology, Department of Electronics, Tampere, Finland
`johanna.virkki@tut.fi`
[2]Southeast University, School of Information Science and Technology, Nanjing, China

ABSTRACT

Wireless sensor network (WSN) is an important wireless technology that has wide variety of applications and provides unlimited future potentials. WSN hardware presents some unique reliability challenges, which arise from the nature of WSNs themselves. In this paper, two possible methods, standards based reliability prediction and accelerated testing of WSN hardware are introduced and discussed. In addition, two examples of lessons learned during WSN hardware reliability research are introduced.

KEYWORDS

Wireless sensor network, reliability standards, hardware, accelerated testing.

1. INTRODUCTION

Internet of Things (IOT) is a conceptual vision to connect things in order to create a ubiquitous computing world. In order to create such an ever-present network, a trouble-free, reliable, and cost-effective technology is needed [1]. Wireless sensor network (WSN) is an important wireless technology that already has wide variety of applications and also provides unlimited future potentials for IOT. A WSN consists of sensor devices with computing, data processing, and communicating components. Ideally, researchers would like to deeply embed WSN devices into the physical world and power the devices solely from energy scavenged from the ambient environment. WSN already has many applications in different environments, typical ones being monitoring, tracking, and controlling. Thus, WSN-based applications will be used in varying and challenging environments. Since WSNs are relatively youthful topics with few long-term field deployments, the effects of a lack of hardware reliability may not have yet caused a worry-inducing impact. Thus, it may seem that hardware reliability is not among the most important things when designing a WSN. However, in many WSN applications, reliability of hardware is essential and field failures may have catastrophic results. In addition, reliability prediction of hardware is important, since sensor devices are planned to be unattended for long periods without maintenance [2, 3].

This paper is a combination of a literature review and results from reliability research of WSN applications: We examine the standards based reliability prediction and accelerated testing of WSN hardware, their advantages and disadvantages. In addition, we will introduce two important lessons learned during this research: First example introduces how simple accelerated tests without expensive equipment can give the desired information. The second example introduces what was learned about the use of reliability software packages.These commonly used

commercial software tools include, e.g. Isograph [4], Reliasoft [5], and Windchill (formerly Relex) [6]. One application in this reliability research was a WSN system for an automatic meter reading of electricity (Figure 1).
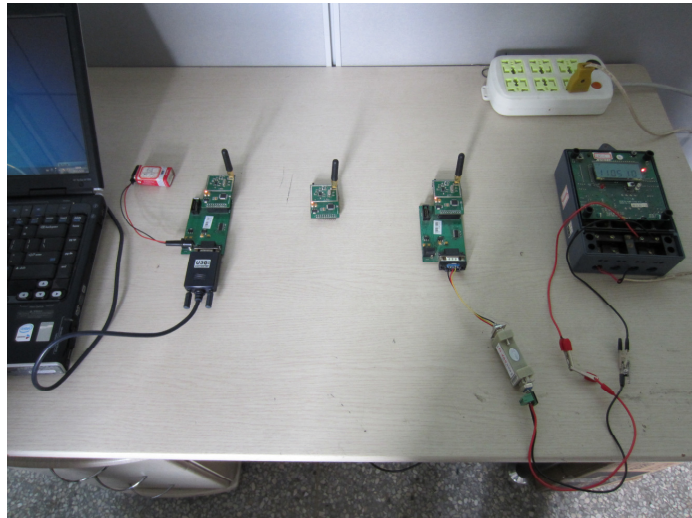

Figure 1. A simplified scene of a laboratory test of automatic meter reading of electricity.

2. WIRELESS SENSOR NETWORK

A WSN can have from a few to several thousand collaborating nodes with computing, data processing, and communicating components. Each node is connected to one or more sensors. The sensors are used to collect and transmit information about their surrounding environment. The node collects the information from a group of sensors and facilitates communication with a control center. In a WSN, these sensor nodes can be deployed in controlled environments, such as factories, homes, or hospitals. They also can be deployed in uncontrolled environments, such as disaster areas, forests, or battlefields. Some common reasons for failures of WSN hardware are environmental contaminants and conditions such as temperature, temperature changes, and humidity, with other failures deriving, e.g., from vibration, ripple voltage, and overvoltage. Each environment and application has different demands for hardware reliability, which makes it crucial for manufacturers to know the reliability of their products. WSN hardware does not have to function beyond its intended life, for this would only impose unnecessary costs. Yet it is not desirable either that its mission duration falls short of the intended. Quality and reliability are not free, but poor quality and reliability usually cost more than good quality and reliability.

There are several different hardware systems designed for WSNs. These systems differ in circuit techniques, architecture approaches, and support for applications. Unfortunately, standard benchmark suites do not exist for the WSN space. Devices in a WSN collaborate to monitor the physics or environment conditions, e.g. temperature, humidity, motion, gases, sound, vibration, or pollutants. The use environment of WSNs can significantly vary and the environment will also vary between the life-phases of the node from manufacturing to disposal; the node may spend considerable time in a storage environment before being actually used or it may be redeployed during its service life. All of these stresses combine and interact to produce a complex environment for the node. This is difficult enough to analyse for reliability, but is further complicated by unpredictable stresses such as a node being accidentally dropped. These may not

be enough to cause instant failure but will weaken the node sufficiently to make it more vulnerable to an earlier failure. In addition, WSN electronics generate own internal stresses purely by functioning, like electronic products in general do. Components heat up and cool down during their use cycles and, by doing so, generate thermo-mechanical stresses. Power saving strategies in nodes may accelerate this problem because there may be more frequent wake-sleep cycles. Also, node is often woken up for data transmission, which generates the greatest amount of heat of which the node is capable of enduring. In addition to thermally induced stresses, there will also be the voltage and current stresses that are inherent to any electronic device [3, 7-11].

Hardware reliability is only one of the demands for a working WSN. A large WSN, with sufficient node capacity, can afford to lose nodes to hardware failure without the entire system failing through the use of redundancy, re-routing and preventative maintenance, managed at higher levels of the stack. This is a major benefit over conventional electronic systems where sub-system failure may impose major overheads. However, the design of a WSN with sufficient node capacity for redundancy, re-routing and preventative maintenance requires information on the probable node failure rates at field conditions. This, in turn, requires a detailed hardware reliability analysis [3].

3. STANDARS BASED RELIABILITY PREDICTION

3.1 Standards

A design of WSN hardware should meet a certain reliability goal before the project is allowed to move on to the following phases (building prototypes and manufacturing) thus avoiding committing money and time to a product that has not shown acceptable reliability in the design stage. The design can involve components that have not been tested before, have no history of being used in the field, and are not redesigned components with prior histories. In addition, often there are no capabilities, resources or time to test components of a product and there is need for estimates of the failure rate of these components to complete the product reliability analysis.

Standards based reliability prediction relies on defining failure rates for the components of a product based on predefined standards. These failure rate estimates depend on the types of components and connections, the use environment, and the used reliability prediction standard. These component failure rates are then used to obtain an overall product failure rate. Over the past few decades, several standards [5, 12-14] have been introduced by various governments and industry organizations to assist in conducting this type of analysis.

3.2 Standards based reliability prediction of WSN hardware

Standard prediction methods are based on models developed from data, which may have been collected from field, in-house, or from manufacturers. Standards provide an approximation of field failure rates and advantages of standard based methods include:

- Easy to use, and a lot of component models exist.
- Relatively good performance as indicators of inherent reliability.
- Provide a rough estimate of field failure rates.

Although empirical prediction standards have been used for many years, it is always wise to use them with caution. Disadvantages of standard based method include:

- A large part of the data used by the traditional models is out-of-date and standards have not followed latest advances in various technologies used in WSN applications.

- Failure of the components is not always due to component itself but can be caused by the product design.
- The reliability prediction models are usually based on industry-average values of failure rate, which are neither vendor-specific nor component-specific.
- The end result from standard based predictions is a constant failure rate estimation that can only be used within the context of an exponential reliability model (i.e. no wearouts, no infant failures). This is not usually true.

However, standards based reliability predictions can be used as s starting point. For WSN hardware, there are several possible standards. The MIL-HDBK-217 (originally written for the military and military grade components) and the Telcordia SR-332 (originally written for telecommunication industry) are both designed for electronics products and are commonly used. Many engineers are still using MIL-217 predictions even though it is out-of-date. However, more companies are moving more toward Telcordia predictions recently and Telcordia components are also more updated. Much of the choosing decision should depend on the type of components used and whether the components fit into the specific categories of the standards. Also, depending on the project, the customer may request a specific standard, which they would expect to be used. During our research, the achieved results between different standards were very different. There are reasons for this variation. First, MIL-217 is used in the military so it is more conservative than the commercial standards. Second, the underlying methods seem to be significantly different.

In a WSN, even a single node is a system-in-package, a highly heterogeneous collection of electronic and mechanical components, typically encapsulated into a small volume. Therefore, for the individual nodes, we have a multi-component and multi-material hardware assembly subject to a varying, difficult-to-predict environment and a varying, difficult-to-predict operating cycle. One important thing that was learned during this research was that although standards address predictions under different usage levels and environmental stresses (Telcordia has 5 environment classifications: 3 ground, 1 air, 1 space, and MIL-217 has 14 environments: 3 ground, 8 air, 1 space, 2 sea), standards cannot take into account the effects of actual field stresses of WSN devices. Thus, predicting reliability of WSN hardware only with the help of reliability standards does not give accurate enough results and making decisions based only on standard based reliability predictions can be seriously misleading.

4. ACCELERATED TESTING

Reliability testing usually means simulation of actual use conditions. This kind of testing is very time-consuming and thus accelerated testing is needed. In accelerated testing, test stresses are increased to cut down the time required to obtain a weakening effect similar to one resulting from normal service conditions. There are many ways to define the stress limits. In our research, we divided them into three: specification limits, design limits, and destruct limits. The specification limits are set by the manufacturer to limit the stresses during field use. The design limits are the limits that the product will survive without failure. The destruct limit is the fundamental limit of technology, where the product falls apart [14]. Normally, stress levels in accelerated tests will fall outside the product specification limits but within the design limits.

4.1 Qualitative and quantitative accelerated tests

Usually, accelerated testing can be divided into two areas: qualitative and quantitative. The former focuses on identifying failures without attempting any predictions as to the product's operation under normal use conditions. It is used primarily to reveal probable failures for the product so that product engineers can improve the product design. Qualitative accelerated tests should first be used to reveal probable failure modes and mechanisms that WSN devices may

experience in field use. All stresses that a particular device is subjected to in the field should be considered when testing the reliability. After qualitative testing, quantitative accelerated tests can be designed to produce the data required for estimating lifetime of the product under normal use conditions: quantitative testing predicts how adding stress accelerates a particular failure mechanism and decreases lifetime [14, 15]. Thus, accelerated tests deal with the two major areas of reliability engineering – physics and statistics of failure. Failure analysis and data-analysis are done in order to understand the results of accelerated testing.

4.2 Failure analysis and data-analysis

Failure analysis of failed components/products is necessary to clarify the cause of failure and to provide rapid feedback to the process stages of design and manufacture. Failure analysis investigates the mode and mechanism of failure using optical, electrical, physical, and chemical techniques.

Data-analysis of results from accelerated tests at higher stress levels makes it possible to estimate the reliability and product lifetime at high stress level and at use stress level. Product lifetimes at higher stress levels are recorded and then analyzed. Product lifetime can be measured in cycles, hours, or any other common measure of life. Since time is a common measure, product life is often called lifetime or time-to-failure. A lifetime distribution is a theoretical population model, which is used to describe measurements of product lifetime. Each distribution has its own parameters on which it depends and that are estimated from the data [14, 15]. Lifetime distributions should not be chosen blindly, but they should be chosen for one or more of the following three reasons: There is a physical argument that theoretically matches the observed failure mechanism to a particular distribution, a particular distribution has previously been used successfully for the same or a very similar failure mechanism, or a convenient distribution provides a good empirical fit to all the failure data. The most commonly used distributions include Exponential, Weibull, and Lognormal [16-19]. Even when a model is assumed, the mapping possibilities are still infinite since they depend on the parameters of the chosen model. The task of parameter estimation can vary from trivial to impossible. Available basic methods for estimating the parameters of a model include, e.g. graphical methods, Least squares method, and Maximum likelihood estimation method [14, 18].

Usually we are not interested analyzing accelerated test data at these test levels. Instead, we want to calculate reliability results at actual field use stress levels. Thus, in accelerated test analysis we need to determine a way to project from the high stress to the use stress level. Obviously, there are infinite ways to do that and thus we will assume some model: the life-stress relationship describes how a specific life characteristic changes with the application of stress. Even when this relationship is assumed, we need a minimum of two higher stress levels to calculate reliability results at use stress level. Commonly used life-stress relationships [14, 19, 20] include, e.g.: Arrhenius, Eyring, Inverse power law, and combination models. Each life-stress relationship also has its own parameters on which it depends and that are again estimated from the data. Great care is essential in choosing the most appropriate model, and in selecting the appropriate range of validity for the chosen model in a specific application.

4.3 Accelerated testing of WSN hardware

The main challenge in WSN hardware is to produce low cost and small size electronics. Still, WSNs can be deployed in controlled, uncontrolled, and even harsh environment. In addition, WSNs can be deployed in the field for many years without maintenance, because of the difficulty and cost of sensor replacement. Accelerated tests can be used for quickly finding possible failure modes and estimating lifetime at field conditions.

However, a major worry is that an accelerated reliability test will somehow miss a failure mode that will cause disaster in normal operation. On the other hand, an accelerated test may condemn a well-working product by identifying an artificial failure mode as real [21-23]. Occasionally, in accelerated testing, increasing what is thought to be an accelerating variable might, in fact, cause deceleration. For example, an increased temperature may result as lower humidity in the "accelerated" test and the primary failure mode in the field can be caused by corrosion that would not occur at high temperature and low humidity. Sometimes the accelerated test conditions can lead to a situation where a dual mechanism of failure takes place. It is important to make sure that these failures are well separated: if more than one failure mechanism are present but not recognized in data analysis, seriously incorrect conclusions on lifetime of a product are possible. It is also important to recognize that the statistical estimates used in reliability testing always contain uncertainty, which should be taken into account in predicting the lifetime of a product [21-23].

All stresses that a particular WSN hardware is subjected to in the field should be considered when testing the reliability. As presented earlier, these devices are used in very varying environments, with multiple different internal and external stresses. Thus, WSN hardware to all applications cannot be tested with same accelerated tests and design of accelerated tests for WSN hardware is demanding. For all devices, the main concerns in design of accelerated tests are the temporal variations in externally induced stresses. However, for WSN electronics, we must add the complication of spatial variations in these stresses depending on the physical location of the node. The stresses of a single node can also vary between the life-phases from manufacturing to disposal. As it is unlikely, except in cases where the spatial variation in stresses is extreme, that a custom node will be designed for each environment, there is the challenge of having to design and test a generic node that will have to endure temporally and spatially varying stresses.

5. LESSONS LEARNED

This chapter introduces two examples of lessons learned during this WSN hardware reliability research: First example introduces how simple accelerated tests without expensive equipment can give the desired information. The second example introduces what was learned about the problems in use of reliability software packages.

5.1 Use of simple accelerated tests

Accelerated tests should be carefully planned and tailored for each device, based on its structure and conditions of use [24-27]. This is particularly important with WSN hardware, since field conditions can vary radically. Often the problem is that accelerated testing requires preliminary knowledge, a lot of complaint, and suitable equipment, which can be very expensive. Also buying of such tests can cost loads. However, this is not a reason to forget reliability. There are many ways to do basic qualitative accelerated tests without expensive equipment. All in all, in accelerated testing, we want to simulate and accelerate the actual use environment. Some accelerated tests can be done without a testing laboratory. For example, high temperature tests can be done in a normal oven that has a stable temperature, low temperature tests can be done in a normal freezer with a stable temperature. The effects of vibration can be tested during normal transport where vibration occurs. The effects of high humidity can be tested in a place where humidity is stable and high and temperature is controlled. These tests may not be as accurate as those in a testing laboratory, but they can be used to precipitate failures in order to identify failure modes and thus can give important information about the reliability of a product.

Tantalum capacitors of a maximum voltage of 50V, a capacitance of 10μF, and an operating temperature of -55°C to +125°C (Figure 2) are used in a WSN application. We wanted to examine

the possible effects of temperature changes on these tantalum capacitors. This was done in order to simulate normal WSN environment, where devices heat up and cool down during their use cycles and, by doing so, generate thermo-mechanical stresses.
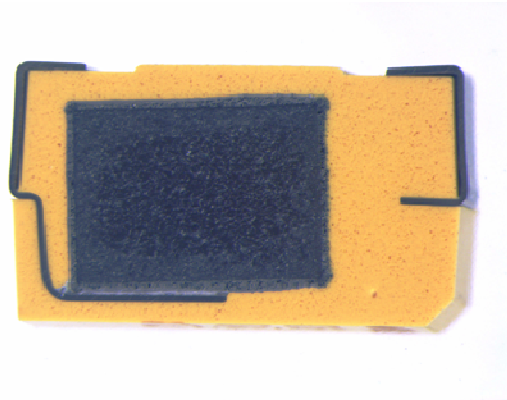

Figure 2. An example of a tested tantalum capacitor.

The effects of temperature changes were tested with the help of normal oven and freezer. In test A, capacitors were first held for 30 minutes at 85°C and after that for 30 minutes at -40°C. The test was repeated 5 times over five hours. Tests B, C, and D were similar to test A, but the upper temperature was 100°C, 125°C, and 150°C, respectively. In all tests, 18 capacitors were tested. Because the capacitors were rated for an operating and non-operating temperature of -55°C to +125°C, they were tested here within their specification limits, except for the upper temperature in test D. After reliability testing, capacitors were tested for their failure voltage, which was slowly increased from 0V to 90V, provided no failure occurred. Tests, test conditions, and number of failures can be seen in Table 1.

Table 1. Tests, test conditions, and number of failures in Tests 2A-2D.

Test	Test 2A	Test 2B	Test 2C	Test 2D
Conditions	85°C, -40°C	100°C, -40°C	125°C, -40°C	150°C, -40°C
Cycle time	1h	1h	1h	1h
N cycles	5	5	5	5
N capacitors	18	18	18	18
N failures	0	3	5	7

Capacitors not submitted to temperature cycling did not fail at voltages below 90V. This means that the capacitors can be expected to withstand voltages of over 90V. The results of test A showed that those 5 cycles at -40°C and 85°C were not enough to lower the failure voltages of these capacitors. In test B, in which temperatures changed between -40°C and 100°C, 3 failures occurred at under 90V. In test C with an upper temperature of 125°C, 5 failures occurred at voltages below 90V, and in test D with an upper temperature of 150°C, 7 failures. This means that even such simple and short temperature cycling inside their specification limits affected these tantalum capacitors, weakened their characteristics, and lowered their failure voltage. This needs be taken into account in field use, since it may have a significant effect on reliability of a WSN application.

5.4 Use of reliability software

Reliability software can be a great help in defining the reliability of WSN hardware. It can be used as an assistant and time saver: It moves the complexity of the statistical methodology into a behind-the-scenes engine. These commonly used commercial software tools include, e.g. Isograph, Reliasoft, and Windchill (formerly Relex).

Reliability software was used as an aid in analysis of product lifetime data from traditional (non-accelerated) and accelerated tests of WSN hardware. A software tool can help with parameter calculations to fit the lifetime distribution and life-stress relationship to your data set and calculate reliability results. Once data is entered to software, the software helps in choosing lifetime distribution and life-stress relationship, estimates parameters, and calculates variety of reliability results. Most software tools support both data types (complete data and censored data, where not all units failed) to be entered and all commonly used lifetime distributions and parameter estimation methods. Some of the many useful applications include: calculate the lifetimes of products at use stress level, compare designs based on reliability, and demonstrate if an item meets specified reliability. Software will also aid in graphical charts and reliability reports.

Reliability software is not worth the required investment if it is difficult to learn or to operate. Since they are rather expensive, users are likely to have only one package at their disposal. Vendors usually provide free demonstration versions of their software. When making the final selection among the software tools that seem to have the desired properties, demos should be carried out [12, 28] However, demo versions usually lack many important characteristics.

During this research, it was learned that the user can waste a lot of time clarifying what needs to be entered as input to software tool. In addition, outputs can be quite confusing. The calculation results achieved with different reliability software packages are found to be pretty much the same, small differences between the software packages are caused by differences in the underlying algorithms. Different results for software packages can also be caused by parameters that are defined differently. Packages can, e.g. give lognormal distribution in a different way. One determines parameters as μ and σ, which are the mean and standard deviation, respectively. The other determines these same parameters as μ, which is the mean of the natural logarithms of the times-to-failure and σ, which is the standard deviation of the natural logarithms of the times to failure. The literature provided with the packages is necessary to understand the used terms. However, it still is not easy to relate them to those used in books and publications. Some software packages have a theory help button that offers a brief overview of the principles and theory behind the user's selection, which is helpful. Other packages do not offer any information during analysis. Finally, some software vendors almost seem to tell that their products can replace expertise: it is to be remembered that suitable input information needs to be collected and expertise in use environment and characteristics of WSN devices is needed for understanding the results.

6. Conclusions

In a WSN, the devices can be deployed in varying controlled and uncontrolled environments. The environment can also vary between the life-phases of the hardware. In addition, devices are planned to be unattended for long periods without maintenance. Thus, reliability of WSN hardware is essential. In this paper, two possible methods, standards based reliability prediction and accelerated testing, for reliability analysis of WSN hardware were introduced and discussed. In addition, two examples of lessons learned during this research were introduced.

There is the challenge of having to analyze reliability of hardware that will have to endure temporally and spatially varying stresses. Thus, analyzing reliability of WSN hardware with the help of reliability standards does not give accurate estimations and making decisions based only on standard based reliability predictions can be seriously misleading. However, standard based reliability predictions can be used as s starting point.

Design of accelerated tests for WSN hardware is demanding. Often the problem is that accelerated testing requires preliminary knowledge, a lot of complaint, and suitable equipment, which can be very expensive. However, since in accelerated testing, we want to simulate and accelerate the actual use environment, basic accelerated tests can be done without a testing laboratory. Reliability software can be used as an assistant and time saver in reliability prediction of WSN hardware: it can aid in calculations and presenting the results. However, it is to be remembered that the most important factor in any reliability analysis is how well the analyst understands what he is doing.

ACKNOWLEDGEMENTS

REFERENCES

[1] Commission of the European Communities (2009) "Internet of Things — An Action Plan for Europe", http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf (accesed 13 October 2011)

[2] Qian, Y., Lu, K. and Tipper, D. (2007) "A Design for Secure and Survivable Wireless Sensor Networks", IEEE Wireless Communications, Vol. 14, No. 5, pp. 30-37.

[3] Barret, J. (2008) "Challenges for Hardware Reliability in Networked Embedded Systems", Delaney, K. (Ed.), Ambient Intelligence with Microsystems - Augmented Materials and Smart Objects, Springer, New York, 435p.

[4] Isograph Reliability Software Webpage, www.isograph-software.com (accessed 15 May 2011)

[5] ReliaSoft Reliabiility Software Webpage, www.reliasoft.com (accessed 15 May 2011)

[6] Windchill Quality Solutions Webpage, www.ptc.com/products/windchill/quality-solutions/ (accessed 20 May 2011)

[7] Dargie, W. and Poellabauer, C (2010) Fundamentals of Wireless Sensor Networks: Theory and Practice, John Wiley & Sons, New York, 336p.

[8] Hempstead, M. Lyons, M.J. Brooks, D. and Wei, G.-Y. (2008) "Survey of Hardware Systems for Wireless Sensor Networks", Journal of Low Power Electronics, Vol. 4, No. 1, pp. 1-10.

[9] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) "Wireless Sensor Networks: a Survey" Computer Networks, Vol. 38, No. 4, pp. 393-422.

[10] Culler, D., Estrin, D. and Srivastava, M. (2004) "Overview of Sensor Networks", IEEE Computer, Vol. 37, No. 8, pp. 41-49.

[11] van Kranenburg, R. (2009) Internet of Things Europe, Conference Report http://ec.europa.eu/information_society/policy/rfid/documents/iotconferencereport2010.pdf (accessed 14 October 2011)

[12] Willis, R. (2006) "Survey of Support Software for Reliability Engineering" Washington Chapter, Society of Reliability Engineers, 20p.

[13] Reliability Hotwire (2005) The eMagazine for the Reliability Professional, Issues 50-52.

[14] Weibull Reliability Engineering Resource Website, www.weibull.com (accessed 15 February 2011)

[15] Meeker, W.Q. and Escobar, L.A. (1998) Statistical Methods for Reliability Data, John Wiley and Sons, New York, 712p.

[16] Ohring, M. (1998) Reliability and Failure of Electronic Materials and Devices, Academic Press, San Diego, 692p.

[17] Kapur, K.C. and Lamberson, L.R., (1977) Reliability in Engineering Design, John Wiley & Sons, Inc., New Jersey, 618p.

[18] Dodson, B. (2006) The Weibull Analysis Handbook, Quality Press, Milwaukee, 167p.

[19] Pascual, F., Meeker, W.Q. and Escobar, L.A. (2006) "Accelerated Life Test Models and Data Analysis", Pham, H. (Ed.) Springer Handbook of Engineering Statistics, Springer, Berlin, pp. 397-426.

[20] Escobar, L.A. and Meeker, W.Q. (2006) "A Review of Accelerated Test Models", Statistical Science, Vol. 21, No. 4, pp. 552–577.

[21] LuValle, M.J. (2007) "Identifying Mechanisms That Highly Accelerated Tests Miss", IEEE Transactions on Reliability, Vol. 56, No. 2, pp. 349-359.

[22] Meeker, W.Q. and Escobar, L.A. (1998) "Pitfalls of Accelerated Testing", IEEE Transactions on Reliability, Vol. 47, No. 2, pp. 114-118.

[23] Suhir, E. (2002) "Accelerated Life Testing (ALT) in Microelectronics and Photonics: Its Role, Attributes, Challenges, Pitfalls, and Interaction with Qualification Tests", Journal of Electronic Packaging, Vol. 124, No. 3, pp. 281-291.

[24] Virkki, J., Seppälä, T., Frisk, L. and Heino, P. (2010) "Accelerated Testing for Failures of Tantalum Capacitors", Microelectronics Reliability, Vol. 50, No. 2, pp. 217-219.

[25] Virkki J. and Raumonen, P. (2010) "Accelerated Tests for the Effects of Power Cycling on Tantalum Capacitors in a Humid Environment", Journal of Microelectronics and Electronic Packaging, Vol. 7, No. 2, pp. 111-116.

[26] Virkki, J., Seppälä, T. and. Raumonen, P. (2010) "Testing the Effects of Reflow on Tantalum Capacitors", Microelectronics Reliability, Vol. 50, No. 9-11, pp. 1650-1653.

[27] Virkki J. and Tuukkanen, S. (2010) "Testing the Effects of Temperature Cycling on Tantalum Capacitors", Microelectronics Reliability, Vol. 50, No. 8, pp. 1121-1124.

[28] Brall, A., Hagen, W. and Tran, H. (2007) "Reliability Block Diagram Modeling – Comparisons of Three Software Packages", International Symposium of Product Quality & Integrity, pp. 119-124.

.