ON SAFETY AND DEPENDABILITY OF AUTOMOTIVE ENGINEERING REGARDING APPLICABLE TOOLS AND LEGISLATION

Tímea Fülep

Department of Automobile Engineering
Budapest University of Technology and Economics, Hungary
Stoczek St. 6, Budapest, Hungary, H-1111
tel.: +36-1-463-1982
e-mail: fulep.timea@auto.bme.hu

András Voith

Knorr-Bremse Fékrendszerek Kft.
Kecskemét, Hungary
e-mail: andras.voith@knorr-bremse.com

Abstract

In today's automotive industry, companies are organized into simultaneous engineering teams to develop their new products. The new way of doing business enables some companies to develop their new products quicker and cheaper with higher quality and reliability. In the past few years there has been the tendency to increase the safety of vehicles by introducing intelligent assistance systems that help the driver to cope with critical driving situations. These functions are characterized by the active control of the driving dynamics by distributed assistance systems, which therefore need a reliable communication network.

The faults in the electronic components, which control these functions, are safety-critical. However, the assistance functions deliver only an add-on service in accordance with a fail-safe strategy for the electronic components. If there is any doubt about the correct behaviour of the assistance system, it will be switched off. For by-wire systems, without a mechanical back-up, a new dimension of safety requirements for automotive electronics is reached. After a fault the system has to be fail-tolerant until a safe state is reached. Realizing that road vehicles, mostly commercial vehicles taking part over proportionally in accidents, become more and more complex indicates that suitable and adaptable analysis methods are crucial to be applied with appropriate certification body.

Keywords*: transport, safety, dependability, safety-related*

1. Introduction

The importance of the road traffic has been grown during the last decades, and stills growth. Although this development is demanded and promoted by the society needs, slowly it becomes unsustainable. As the traffic density increases, the traffic situations become more complex, difficult to handle by the human driver, which leads to accidents. All the communities around the world are looking for solutions, which would increase the road safety, but not really willing to pay for that. The term 'accident free' vehicle appears more and more in research projects and some of these technologies slowly go into serial production as well.

The traffic accident analyses show that in over 90% of the cases the driver is the primary cause of the accident. Taking a deeper insight into the analyses a result, most of the failure what the driver makes is in the sensing part of the control loop (71%), followed by the decision (20%) and the action (9%). This suggests the application of intelligent vehicle systems, which compensates for the driver's deficiency in these phases.

2. Reliability (r)evolution

If the required power of most electronic devices invented in the 1920s and 1930s failed, the device failed to operate and thus the system reliability depended on the electric power. Some reliability-aware USA cities put the electric power distribution lines underground in order to improve reliability. Electric power line unreliability is most often caused by something on those lines that cause them to break. Triode was invented in the 1920s and radios came into use. They were popular, but the major reliability difficulties with them were the electron tubes [18].

In the 1950s the great majority of designers used point characteristics of piece parts as stated by parts vendors. A few designers recognized that most piece part characteristics were distributed rather than point [20], developed error analysis and calculated performance in terms of an expected value and its variation. In organizations with strong manufacturing management, pressure was exerted on the designers to develop alternate methodologies. One result was worst case design, in which worst case characteristics were assumed for all parts. These years were also marked the beginning of efforts to approach the area of reliability from a quantitative standpoint [19] and early efforts at measurement were aimed primarily at electronic parts.

The importance of quantitative measurement to scientific progress was perhaps best stated by Lord Kelvin: 'I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be.'

During World War II, electronic tubes were by far the most unreliable component used in electronic systems. This observation led to various studies and ad hoc groups whose purpose was to identify ways that their reliability and the reliability of the systems in which they operated, could be improved [22]. One group in the early 1950s concluded that:

There needs to be better reliability data collected from the field.

- Better components need to be developed.
- Quantitative reliability requirements need to be established.
- Reliability needs to be verified by test before full scale production.
- A permanent committee needs to be established to guide the reliability discipline.

Item 5 was implemented in the form of the Advisory Group of Reliability of Electronic Equipment (AGREE), whose charter was to identify actions that could be taken to provide more reliable electronic equipment.

In the 1960s the drive for higher reliability forced most design organizations to initiate reliability analysis and prediction as a part of the design process. Organizations using distributed-part characteristics in performance design adapted easily to reliability prediction based on failure rate distributions. Analysis of field failure data, environmental tests and material behaviour suggested the great influence of the operational environment on field failures. In the 1960s and 1970s many design organizations and project managements prepared design guidelines and mandated their use to improve reliability which was also dominated by electronic device improvements and their application. The emphasis placed on reliability demonstration in the AGREE [21] report led by the early 1960s to numerous military specifications and standards requiring factory 'reliability acceptance tests' for both equipment and parts. This was an era of intense missile and spacecraft development activity with many new problems and urgencies. It began with failures, in many cases more numerous than successes and ended with the triumphs of the Apollo program [19]. The judicious application of Fault Tree and Failure Modes, Effects and Criticality Analysis (FMECA) helped to pinpoint the source of failure when detailed data was missing.

Starting early and continuing through the 1980s computer programs have played an increasing role in reliability. Widespread availability of personal computers has resulted in ever increasing use of reliability programs in design. The most evident factor was the increasing importance of quality in the commercial marketplace. One negative note in the picture of reliability progress in the 1980s was in the space program where an epidemic of launch failures, in the last half of the decade, included the tragic loss of the space shuttle Challenger. One might ask whether the early vigilance of the space effort was gradually eroded by overconfidence endangered by past success.

Attempts to delineate an independent set of tasks for mission assurance engineering resulted in the development of applied statistics for mission assurance [22]. Mission failures in a well-developed system come from necessary risks that remain in the system for the mission. Risk management is the key to mission assurance. The traditional tasks of applied statistics, reliability, maintainability, system safety, quality assurance, logistics support, human factors, software assurance and system effectiveness for a project are still important and should still be performed. The trends of the 1980s with regard to electronic equipment are continuing. The reliability is increasing; the maintainability decreasing and field data are still usually useless [18].

The vast majority of available safety tools and methods support severity analysis also combining other system features from different aspects. The overall goal in designing a safety-critical system is eliminate hazards from the design or to minimize risk by modifying the design so there is a very low probability of the hazard occurring. Safety in design means that the examined specification is correctly implemented, no failure occurs, the system operation will not result in a catastrophic event. Safety of a system can be expressed by the strategy of design, which means that the risk of faults or failure leading to an undesired event must be eliminated or minimized by using fail-safe or fault-tolerant procedures. The length of time of hazard occurrence must be maximally reduced if the hazard can not be completely eliminated.

3. Overview of design techniques concerning legislative requirements

The used techniques to enhance reliability can also call tools to their aid, e.g. fuzzy logic, neural networks and Pascal programs or combination of methods, e.g. functional block diagrams, BDD (Binary Decision Diagram), RBD (reliability block diagram) with a simplified Markov model and conditional probabilities that reflect the dependence among system elements, Markov chains or confidence level (PVCL – Probabilistic Varied Confidence Level) [1]. Reliability prediction can be conducted by pattern recognition (statistic classification), which is called a certain mathematical-statistical method of concluding from a number *n* of known variables on another – unknown – variable [2]. Classification of analysis techniques (Fig. 1.) according to [3]:

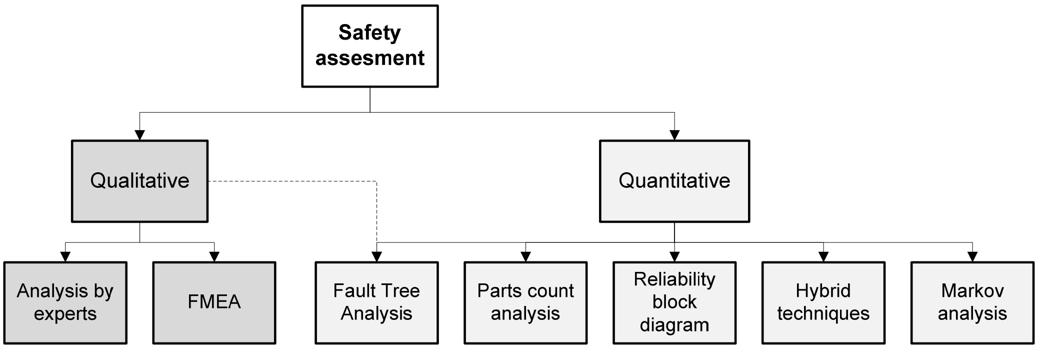

Fig. 1. Classification of qualitative-quantitative techniques

The most wide-spread and legally prescribed (UN-ECE Reg. 13, Annex 18) two techniques are the Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), which are usually combined before their use with systematic, functional techniques, e.g. RBD. It can be ambivalent how to classify these techniques, because on the one hand it is stated and visible that FTA has proper quantitative nature, but on the other hand it has also qualitative nature, because of e.g. sensitivity analysis. For FMEA there are solutions about integrating failure costs [4] into these forms and to order according their highness. According to this aspect we can call FMEA a quantitative technique as well, however not from the reliability point of view, but the possible integrated expenditure for it. Combination of different techniques with FMEA is often used, e.g. combining with sneak circuit analysis (SCA), fault tree analysis, event sequence analysis. SCA and FMEA focus on a different, but vital, aspect of the system functioning. Both analyses should be performed to validate and produce a robust design. Solutions for FMEA automation are presented in several articles. Flame is a knowledge based system which is able to automate the failure mode and effects analysis for electrical systems, spans the entire design cycle for electrical/electronic circuits.

The literary work of FMEA is quite extensive and in terms of interpretation and explanation the understood is extremely flexible. It can be stated facetiously that ‘So many houses, so many customs’. It refers also to the used terminology of types, the forms, the ranking. There are FMEAs mentioned at a specified functional level (Functional FMEA) and at the component level (Detailed FMEA). These kinds of differences can give rise to misunderstanding, because it can be comprehended like similarities and compared to the fundamentally accepted types: system, design, process. In these cases negotiations should be accepted; obviously it makes the comprehension impede.

FMEA is a Six Sigma tool (Juran, Deming and others developed statistical tools and methods after World War II. These ideas became part of today’s body of knowledge for manufacturing quality. One of the offshoots of their effort is a business quality doctrine called Six Sigma.) for identifying, analyzing and prioritizing failures and recommended actions. FMEA provides a detailed framework for a cause and effect analysis. FMEA requires the analysis and quantification of the relationships among failure modes, causes, effects and controls. It is especially prevalent in the automotive and aerospace industries. FMEA is neither easy to learn nor easy to use. A tool is difficult to learn when its conceptual model is inadequate, wrong or non-existent. The meanings and relationships for the FMEA concepts of cause, failure mode and effect are ambiguous and weakly defined [5]. Entries in a FMEA worksheet are voluminous and consequently very brief [6]. These copious brief entries make the FMEA hard to produce, hard to understand and hard to maintain. FMEA does not group items with like effects together [7]. FMEA, as implemented in Excel, is unwieldy, with much scrolling required. Scrolling detracts from a user’s mental representation of a document as a whole [8]. The use of expected costs was suggested in prioritizing failures. An expected cost is the cost of an event multiplied by its probability. Expected costs can be summed to show the impact of all failure modes for a root cause. For hundreds of years, it has been generally agreed that the way to express severity has been in financial terms [9].

There are many benefits of performing FMEA, including a systematic approach to classify hardware failures, reduces development time and cost, reduces engineering changes, easy to understand, serves as a tool for more efficient test planning, highlights safety concerns to be focused on, improves customer satisfaction. It is an effective tool to analyze small, large, and complex systems, useful in the development of cost-effective preventive maintenance systems, provides safeguard against repeating the same mistakes in the future, useful to compare designs, a visibility tool for manager, a useful approach that starts from the detailed level and works upward improving communication among design interface personnel [10].

FMEA is an analytical method of the preventive quality assurance. It serves to find the potential failure of a product/process, to recognize and evaluate its importance and to identify appropriate actions to prevent the potential failure or to discover it in time. The systematic analysis and removal of weak points leads to the minimization of risks, to the reduction of failure costs and to an improved reliability. In the mid 1960s, this method was developed within the Apollo project in the USA. It has first been used by the aerospace industry and the nuclear technology and later by the automobile industry and also in other sections.

A FMEA is a good means to analyze risks caused by individual failures. The individual risks are weight against each other to recognize priorities. FMEA does not provide a statement on the total failure risk. For the analysis of failure combinations, the fault-tree analysis is more appropriate.

The advantages of a FMEA prove that the efforts to prevent failures from the beginning of the development process of a product are justified because the very much higher resulting costs are eliminated later. Advantages are, e.g.:

- prevention of failures in design and development,
- prevention of repeated failures through systematic consideration of expert/failure knowledge on the product or process,
- less subsequent product changes and thus reduction of costs.

An argument which is often used against FMEA is its high expenditure. The following topics play an important role (especially the two last topics offer big saving potentials):

- complexity of the product,
- level of analysis/type of FMEA,
- methodological experience of moderator/team,
- quality of preparations,
- terms of reference/scope of analysis.

The scope of analyses can be reduced in co-ordination with the client and the team. Approaches for savings are:

- priority system and selection of analyses,
- decision analysis that shows the critical component groups,
- use of existing products/processes with similar FMEA,
- use of a ‘Basis-FMEA‘ [11] with parts/products processes which are repeatedly analysed.

The implementation of a FMEA is necessary when products are newly developed, when there are changes on the product or procedures, products with safety regulations or customer requirements. Besides all that, the FMEA implementation shows the following positive aspects, for example:

- all project participants are ready for team work at an early stage,
- better understanding of the system for all participants,
- early detection of problem areas,
- consequent taking of actions up to implementation.

The biggest benefit is gained when the FMEA is made at an early stage simultaneous to the development and planning of the production. It is important that the results can be used in the product development process and so unnecessary recurrences are avoided.

The main objective of FMEA is to assist and support the design process (it does not only refers to the Design FMEA) by identifying the effects of component or module failures on system operation [12], moreover eliminating causes of the potential failures, thus serving a positive influence on the failure chain. It can be stated that the focus is on preventing the occurrence of failure causes and the intervention must happen as early as possible.

Fig. 2. shows a typical product development cycle beginning with conceptual design and progressing to deployment in the field. During the conceptual design and preliminary design phases the FMECA serves primarily to verify the adequacy of the system requirements; during the detailed design phase it is used to verify design compliance with the requirements [13].

The IEC 61508 is provided as a generic approach for all safety lifecycle activities. However, only the careful selection of certain methods and procedures of the IEC 61508 can ensure the achievement of the proposed goal for the respective area of application.

The risk is reduced to a tolerable level (Fig. 3.) by applying safety functions which may consist of E/E/PES and/or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of

IEC 61508. IEC 61508 has the following views on risks:

- zero risk can never be reached,
- safety must be considered from the beginning,
- non-tolerable risks must be reduced.

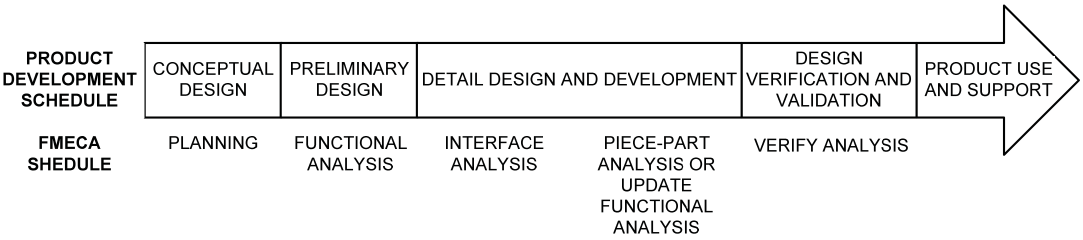
PRODUCT DEVELOPMENT SCHEDULE
CONCEPTUAL DESIGN
PRELIMINARY DESIGN
DETAIL DESIGN AND DEVELOPMENT
DESIGN VERIFICATION AND VALIDATION
PRODUCT USE AND SUPPORT
FMECA SHEDULE
PLANNING
FUNCTIONAL ANALYSIS
INTERFACE ANALYSIS
PIECE-PART ANALYSIS OR UPDATE FUNCTIONAL ANALYSIS
VERIFY ANALYSIS

Fig. 2. Typical product development cycle and FMECA schedule

One should avoid a black and white decision of categorizing systems as ‘safety-critical’ or ‘non-safety-critical’, instead it is better to use levels of safety integrity. These SILs are based on Tolerable Hazard Rate (THR) determinations. The standard also provides different methods to derive tolerable hazard rates using different principles:

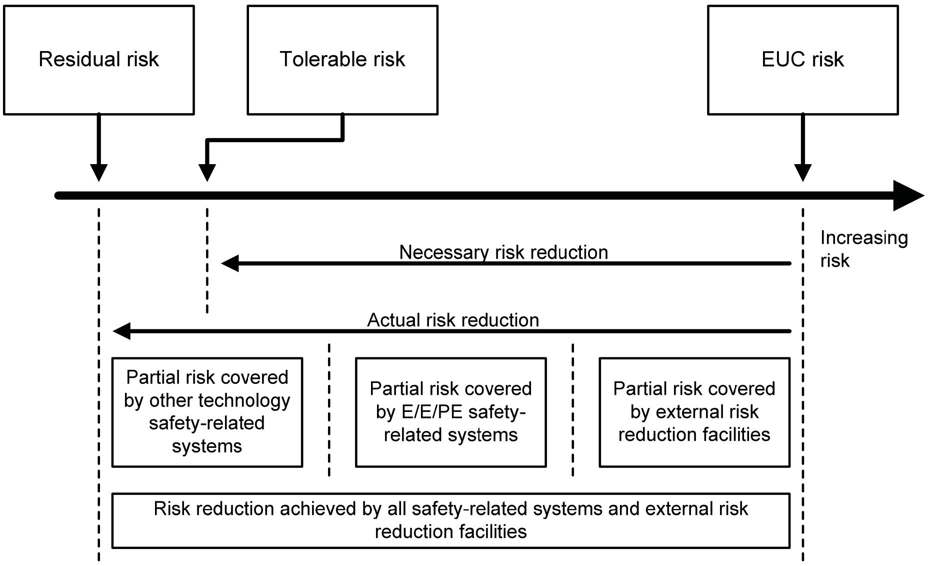
Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other technology safety-related systems
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by external risk reduction facilities
Risk reduction achieved by all safety-related systems and external risk reduction facilities

Fig. 3. General concepts of risk reduction, IEC 1 661/98

- Globalement Au Moins Aussi Bon (GAMAB): ‘All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system.’
- As low as reasonably practicable (ALARP): ‘Societal risk has to be examined when there is a possibility of a catastrophe involving a large number of casualties.’
- Minimum endogenous mortality (MEM): ‘Hazard due to a new system of transport would not significantly augment the figure of the minimum endogenous mortality for an individual.’

The quantitative safety objective of an application is derived from the risk accepted by society. Operators of safety-critical applications impose this safety objective on manufacturers in the form of a THR. The THR results in an appropriate safety integrity level as indicated in Tab. 1. [14].

A SIL is usually associated with a system function or a subsystem and it is used for two purposes [15]: First, a certain SIL is used to give an interval for a rate of safety-critical failures. This characteristic applies to so called ‘random faults’, i.e. failures that occur in an unpredictable manner. Mostly, these faults are caused and accompanied by intrinsic physical processes such as ageing. Second, a SIL defines measures to be applied in the design and during the manufacturing process to keep the frequency of occurrence of so called ‘systematic faults’ small in comparison with random faults.

Tab. 1. Classification of SILs concerning THRs

SIL	Low demand mode of operation (Average probability of failure to perform its designed function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

The reason for systematic faults is mainly a design error or a manufacturing process error that causes failures of identical replications of the same type of component or equipment under similar circumstances. These faults might reveal themselves also in the form of common cause failures. Usually, the higher the SIL, the harder the requirements for the system function. In many cases, SIL4 is the highest SIL, whereas SIL1 is the SIL with the lowest requirements. In addition, there can be system functions that do not even fall into the lowest SIL (SIL1). Sometimes, this is denoted as ‘SIL0’. Design of SIL 3 or 4 systems (that one finds in many fields related for example to transport, energy production, as in many sectors of industrial production) is subjected to the respect of technical reference frames [16]. In determining a SIL, parts 1 and 5 of IEC 61508 take a hazard and risk based approach with progressive refinement [17].

4. References

[1] Pickard, K., Leopold, T., Dieter, A., Bertsche, B., *Validation of similar based on FMEA assessment*, *Risk, Reliability and Societal Safety*, Aven & Vinnem (eds), Taylor & Francis Group, pp. 1859-1863, London, 2007.

[2] Michelberger, P., Barta, Gy., Farkas, T., *Reliability prediction of vehicles by pattern recognition*, Periodica Polytechnica (Transportation Engineering) 10, No. 1, pp. 41-52, 1982.

[3] Rouvroye, J. L., Brombacher, A. C., *New quantitative safety standards: Different techniques, different results?*, *Safety and Reliability*, Lydersen, Hansen & Sandtorv (eds), Balkema, pp. 305-309, Rotterdam 1998.

[4] Signor, M., *The failure-analysis matrix: A Kinder, gentler alternative to FMEA for information systems*, Proc. of Annual Reliability and Maintainability Symposium, Seattle, pp. 173-177, USA 2002.

[5] Lee, B. H., *Encoding design FMEA casual models as Bayesian network structures*, Int. Conf. on Engineering Design, pp. 165-170, 1999

[6] Montgomery, T. A., Pugh, D. R., Leedham, S. T., Twitchett, S. R., *FMEA automation for the complete design process*, Proc. of Annual Reliability and Maintainability Symposium, pp. 30-36, Las Vegas, USA 1996.

[7] Passey, R. D. C., *Foresight begins with FMEA*, Medical Device Technology, Vol. 10, pp. 88-92, 1999.

[8] Piolat, A., Roussey, J., Thunin, O., *Effects of screen presentation on text reading and revising*, Int. Journal of Human-Computer Studies, Vol. 47, pp. 565-589, 1997.

[9] Gilchrist, W., *Modelling failure modes and effects analysis*, Int. Journal of Quality and Reliability Management, Vol. 10, pp. 16-23, 1993.

[10] Dhillon, B. S., *Design reliability: Fundamentals and Applications*, CRC Press LLC, 1999.

[11] *Failure Mode and Effects Analysis*, FMEA, Robert Bosch GmbH, 1998.

[12] Kukkal, P., Bowles, J. B., Bonnell, R. D., *Database design for failure modes and effects analysis*, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, pp. 231-239, USA 1993.

[13] Bowles, J. B., *The new SAE FMECA standard*, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, pp. 48-53, USA 1998.

[14] Filippidis Dr., A. B. L., *Acceptable failure detection and negation times based on hazard rates and probabilities*, Forms/Format, Formal Methods for Automation and Safety in Railway and Automotive Systems, Schnieder, E. & Tarnai, G. (eds), Braunschweig, Germany pp. 44-51, 2004.

[15] Schäbe Dr., H., *Different approaches for determination of tolerable hazard rates*, Proc. of European Safety and Reliability Conference (ESREL), Vol. 1, pp. 435-442, Torino 2001.

[16] Boulanger, J. L., Schön, W., *Reference systems and standards for safety assessment of railway applications*, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), Taylor & Francis Group, pp. 2609-2613, London, 2007.

[17] Robinson, R. M., Anderson, K. J., *SIL Rating Fire Protection Equipment*, 8th Australian Workshop on Safety-critical Systems and Software (SCS'03), Canberra. Conferences in Research and Practice in Information Technology, P. Lindsay & T. Cant, Eds., Vol. 33.

[18] Evans, R. A., *Electronics reliability: a personal view*, IEEE Transactions on Reliability, Vol. 47, Iss. 3, Part 2, pp. 329-332, 1998.

[19] Knight, C. R., *Four decades of reliability progress annual reliability and maintainability symposium*, Proc. of Annual Reliability and Maintainability Symposium, Orlando, pp. 156-160, USA 1991.

[20] Kuehn, R. E., *Four decades of reliability experience*, Proc. of Annual Reliability and Maintainability Symposium, pp. 76-81, Orlando, USA 1991.

[21] Denson, W., *The history of reliability prediction*, IEEE Transactions on Reliability, Vol. 47, No. 3, pp. 321-328, 1998.

[22] Coppola, A., *Reliability engineering of electronic equipment: A historical perspective*, IEEE Transactions on Reliability, Vol. R-33, pp. 29-35, 1984.