What is wrong with Reliability Engineering?

R.W.A. Barnard
Lambda Consulting
PO Box 11826, Hatfield 0028, South Africa
Mobile : +27 82 344 0345
ab@lambdaconsulting.co.za

Abstract. Notwithstanding the implementation of reliability engineering programs by companies, it is not uncommon to observe many instances of low field reliability. This paper briefly describes the essence of reliability engineering, which has prevention of failure as primary objective. Possible reasons for the apparent failure of reliability engineering, especially as practised by the defence industry, are given. It argues that incorrect practices are often applied, frequently performed by incorrect people in the organisation, and at the incorrect time during the product or system life cycle. The value of reliability engineering as specialty area of systems engineering can be improved by learning from best practices used by industry leaders.

The essence of reliability engineering

"I believe that the concept of failure is central to understanding engineering,
for engineering design has as its first and foremost objective the obviation of failure."

Henry Petroski

High field reliability is a highly desirable attribute of any product, system or plant. For defence products and systems, reliability may be the differentiating factor determining mission success or loss of life. For industrial systems and plants, reliability directly influences inherent availability and therefore return on investment. For commercial products, high reliability may provide a supplier with a competitive advantage, resulting in increased market share and therefore higher profits.

In all cases, reliability of a product or system is strongly influenced by decisions made during the design and development process. Deficiencies in design affect all items produced and are progressively more expensive to correct as development proceeds. It is often not practical and becomes increasingly uneconomical to change a design once production has started. Reliability is a design parameter, and as such requires specific design and development effort to achieve the required level of reliability.

Any proposed design solution (whether conceptual or detail design) should be verified against stated requirements before production can commence. Verification primarily involves analysis and testing to confirm compliance with requirements, although inspection and demonstration may be applicable.

A simple illustration of this development process where design (synthesis) is followed by verification (analysis and/or test) is shown in Figure 1. The iterative nature of this process is evident from the illustration. If verification identifies any design weaknesses, the design has to be improved, and verified again before production starts. Iteration of the process is applicable to all performance requirements, including reliability. Reliability engineering activities are "integrated" during design (eg by part selection), as well as during subsequent verification (eg by tolerance analysis based on parts selected). Figure 1 highlights two fundamental aspects of reliability engineering:

- Reliability engineering is iterative in nature
- Reliability engineering is an integral part of systems engineering processes

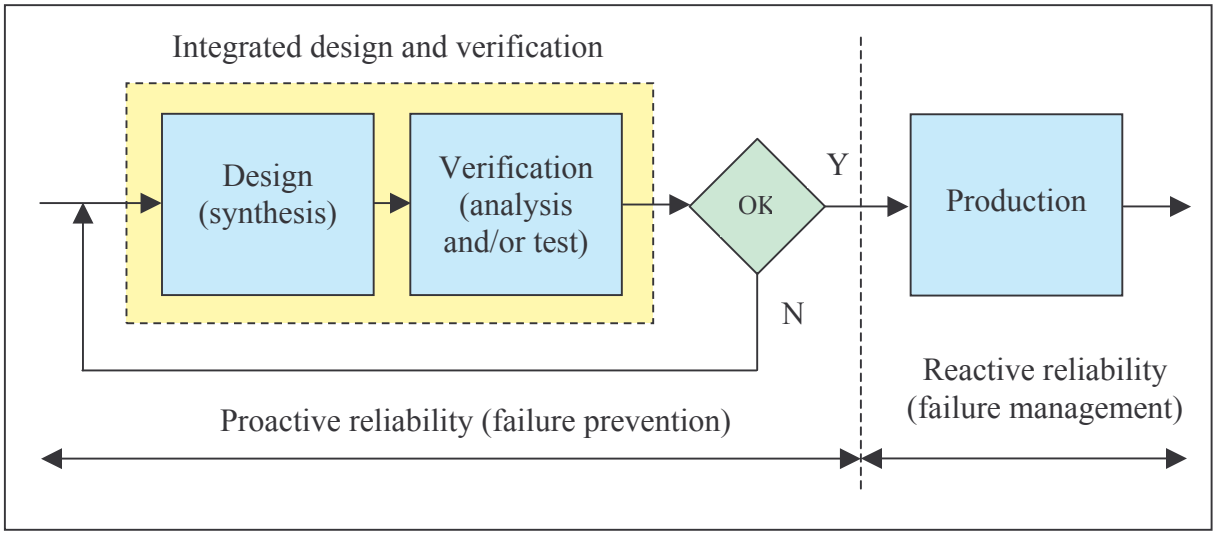

Figure 1. Verification of design prior to production

Once produced, reliability cannot be improved to levels higher than the inherent reliability. Reliability can only deteriorate to lower levels due to various other factors. Figure 1 clearly shows that reliability activities change from proactive to reactive once production has started. For low risk products, the activities of design and verification are totally integrated and performed intuitively by the designer. However, when the risk or cost of failure is high, a formal reliability engineering program is required.

Many companies, and particularly the defence industry, are placing too much emphasis on the quantification of reliability as performance requirement (Barnard 2004). This focus necessitates the continued use of incorrect and misleading "industry standards", since it is not possible to predict (or measure reliability) accurately. An exception to this is the prediction of wear-out failures, where the physics of the failure mechanism is applicable to the given situation.

Using a fundamental point of view, reliability and reliability engineering can be defined as:

- Reliability is the absence of failures in products and systems
- Reliability engineering is the management function of preventing the creation of failures in products and systems

Whenever a failure is observed, engineers should ask whether the specific failure could have been prevented. All failures have root causes, and all failures in theory, and almost always in practice, can be prevented. There is no fundamental limit to the extent to which failure can be prevented. Notwithstanding the implementation of reliability engineering programs by companies, it is not uncommon to observe many instances of low field reliability.

For example, from 1985 to 1995, according to the US Army Armament Research, only 41% of army systems were meeting their reliability goals. From 1996 to 2000, the situation became worse, with only 20% of army systems meeting their reliability goals (Kuper 2004). In the keynote address presented at the 2006 Annual Reliability and Maintainability Symposium, the US Army stated that only 34% of current US army systems comply with reliability requirements (Sorenson 2006).

This paper discusses possible reasons for the apparent failure of reliability engineering, especially as practised by the defence industry. The arguments are based on observations made by the author over many years of consultation to numerous companies. The paper argues that incorrect practices are often applied, frequently performed by incorrect people in the organisation, and at the incorrect time during the product or system life cycle.

Incorrect practices

"There is nothing so useless as doing efficiently that which should not be done at all."

Peter F Drucker

Reliability engineering activities should be performed based on the objectives of the reliability program, which should be tailored according to the requirements of the product or system under consideration. For example, a reliability program for a defence product or system should be different to a program used for a nuclear system or for an automotive product. Literature on reliability engineering suggests that reliability tasks and activities can be either of a management, engineering or accounting nature. Examples of these types are the development and implementation of a preferred parts list, performing a thermal analysis, and performing a reliability prediction, respectively.

The continued emphasis on reliability "accounting" is seen as a primary reason for not achieving high reliability in many products and systems. As long as companies continue to focus on "counting" failures, or "managing" failures instead of "preventing" failures, they are not making much progress. How can any non-engineering activity help in solving complex engineering problems?

A leading author on reliability stated that "the development of quality and reliability engineering in the West has been afflicted with more nonsense than any other branch of engineering." (O'Connor 2002). The "numbers game" approach of these accounting activities is evident from the following three examples:

Example 1: Internet reliability prediction reports

Some companies today offer reliability predictions on the Internet. The customer simply enter quantities of each part type in given data input sheets, pay by credit card, and receive an "Instant MTBF Report" delivered within minutes to an e-mail address!

Since reliability is a design parameter, what contribution to reliability can be made by a reliability prediction report derived merely from re-typing a parts list? Note that zero engineering input is required to perform this activity.

Example 2: Mil-Hdbk-217 derivatives

A number of databases were developed to replace the cancelled Mil-Hdbk-217 (Reliability Prediction of Electronic Equipment). It is disappointing to observe that some companies continue to promote Mil-Hdbk-217 (or derivatives thereof) as useful reliability engineering tool. Dr Gregg Hobbs suggested "Mil-Hdbk-217 should be immediately placed in the shredder and all concepts there from simultaneously placed in one's mental trash can." (Hobbs 2000).

Example 3: Failure rate for a mirror assembly

NPRD-95 (Non-electronic Parts Reliability Data) is a database with failure rates for almost any part (including electronics). The failure rates provided are typically grouped per environment (eg Ground Mobile), and a reference to the source of the data is given. The author sees no value whatsoever in the failure rates given by this type of database, since it is impossible to relate given failure rates to reality faced by a design engineer.

For example, from an engineering viewpoint, it does not make sense to use the failure rate of a bearing or valve, without considering numerous other engineering parameters. In this database, one can even find the failure rate for a mirror assembly! Everybody knows that mirrors do fail, but does it mean that a mirror has a failure rate, and that this failure rate serves any useful purpose for a design engineer?

It may be argued that many companies think they are performing reliability engineering, while they are actually performing reliability accounting. They are not even close to complying with one of the fundamental aspects of reliability engineering, which is "*paying attention to detail*" (Mil-Hdbk-338B, 1998). These companies are "unconsciously incompetent" as far as reliability engineering is concerned. Engineering management should carefully examine reliability programs to determine whether they are "playing the numbers game". If this is the case, these activities are most probably wasting resources, add no value to the development effort, and should be terminated. The product should "know" that reliability activity has been performed, and not the project manager showing that a specific task has been performed!

Incorrect people

"Furious activity is no substitute for understanding."

HH Williams

If reliability is primarily a design characteristic (as indicated in Figure 1), it then follows that the design engineer is ultimately responsible for reliability. However, in practice the designer cannot perform formal reliability activities together with other design activities. Furthermore, a designer cannot effectively review his or her own work, resulting in these activities frequently being delegated to another person. This person is called the reliability engineer, or in smaller companies, a person responsible for reliability. However, this reliability engineer will frequently be found in either logistics engineering, quality engineering or in maintenance. The author is of the opinion that the reliability engineer, in general, cannot adequately perform the fundamental task of preventing failures, when allocated to these departments:

Maintenance engineering. It is almost impossible for a reliability engineer to add value in this situation, since the focus is on maintaining a given product or system. The maintenance department may perform several activities related to reliability, such as collection of failure data, statistical data analysis, etc. The vast majority of attempts to prevent failure will prove to be almost impossible due to the reactive nature of these attempts. Applicable reliability activities may, of course, contribute significantly in restoring products or systems to their inherent reliability levels.

Quality engineering. A reliability engineer located in quality engineering may be slightly more effective in preventing failures. Quality personnel typically have a good understanding of what should be done in terms of reliability, especially if they practise quality engineering, and not only quality control. However, they are usually not skilled or trained to debate merits of detail design with designers, and therefore may lack credibility in the view of a design engineer.

Logistics engineering. The majority of reliability engineers (at least in the South African context) appears to be located in the logistics engineering department. Logistics engineering usually consists of "designing" the logistic support (also called front-end analysis or LSA) and "producing" maintenance items (eg support documents). However, similar to personnel from the quality department, they are not skilled or trained to debate merits of detail design with designers, and therefore may lack credibility in the view of a design engineer.

The systems engineering specialties of Reliability (and Availability, Maintainability, Testability, Manufacturability, etc) should be implemented during design and development phases (as shown in Figure 1). If these are not performed, or are inadequately performed, or are not timeously performed, one can expect failures during operations. Consider the following erroneous reasoning:

- Reliability is a discipline "about failures", and since
- Operations are responsible for handling failures, therefore
- Reliability is delegated to the maintenance or logistics departments!

The following important questions show how technical detail (which can definitely lead to failure), is far outside the scope of the average maintenance, quality or logistics engineer:

- Which part will have the highest thermal or electrical stress in the intended environment?
- What will the natural frequency of this printed circuit board be in its intended environment?

It can be argued that reliability engineers from these departments in the organisation have limited ability to enhance reliability. The behaviour of competent design engineers towards "incompetent" reliability engineers was aptly described with "Attempts to impose quality procedures without the requisite intellectual acceptance by the design team will fail. Academic blather and mumbo-jumbo will be defacto rejected, even if politely accepted at the superficial buzzword level". (Walker 1998).

If these arguments are valid, where should reliability engineering be located in the organisation? The more correct option is to make reliability the responsibility of the design engineer (and therefore the principal engineer or technical director), with support from a competent reliability engineer to form an effective design team. This reliability engineer needs a sufficiently high level of technical know-how to be respected by the designer on his own speciality field. He or she must in fact sometimes be more capable than the designer, to understand how the design works (in substantial detail) and to understand how the design does not work (ie how can it fail).

Incorrect timing

"All projects are iterative - it's just that some managers
choose to have the iterations after final delivery."

Urban Wisdom

The focus on reliability during design is not misplaced. Studies have estimated that the majority of all costs related to quality (and reliability) are created during product development. Typically 75% of failures originate during the design phase, but compounding the problem, around 80% of potential failures remain undetected until final test or when the product is in use.

Furthermore, consider a product whose product cost is *Pc*. The costs due to failure at the various stages of the product's life cycle have been investigated, and in terms of *Pc*, they have been found to be (Booker 2001):

- 0.1 *Pc* - internal failure cost due to rework at end of production line
- Pc - external failure cost for return from customer inspection
- 10 Pc - external failure cost for warranty return due to failure with customer in use

This relationship is commonly known as the '10x rule', and demonstrates how a design error, if not discovered, will give rise to ten times the original elimination costs in a later phase of the life cycle. Other surveys have found that these costs could be much higher!

It should be evident that timing of reliability engineering activities is critical for a successful reliability program. Due to tight project schedules, companies often proceed with production without allowing sufficient time for reliability engineering activities to be performed. Design and verification are, for obvious reasons, sequential activities that cannot be performed in parallel. The iterative nature of developing complex equipment, however, does allow for concurrent engineering to a certain extent.

"The single most important factor that differentiates between effective and ineffective implementation of a reliability program is timing of the reliability effort. The reliability activity must proceed as an integral part of the development project. If not, it becomes either a purely academic function or historical documentation process. Reliability engineering often becomes a numbers game after the real game is over. Reliability cannot be economically added after the system or product has been conceived, designed, manufactured and placed in operation." (Billinton 1996).

Not missing the window of opportunity is a major challenge for engineering managers faced with other technical and financial constraints. It is therefore not uncommon to encounter reliability engineering activities being performed far too late during the design and development phases. What value can be gained from performing a reliability analysis on a product that is already in production?

Guidance from industry leaders

"The amount of knowledge is not nearly as important as the productivity of knowledge."

Peter F Drucker

Much can be learned from reliability engineering practices used by industry leaders, especially those developing commercial and industrial products. After all, the defence industry has been urged to implement best commercial practices since the abolishment of many military standards and specifications more than a decade ago. A good example is to refer to a leading manufacturer of data acquisition products for industrial application. These products are as complex as typical avionics systems, albeit intended for use in less harsh environments, and produced in much larger quantities. The following paragraphs are the only reference made to reliability in a comprehensive technical catalogue:

"National Instruments has remained the market leader in data acquisition by providing quality products. All of our multifunction data acquisition devices feature a precision voltage reference for self-calibration, as well as temperature drift protection circuitry.

National Instruments screens data acquisition products for temperature, shock and vibration ruggedness. We may be able to custom screen products to meet your specific requirements using our HALT & HASS testing facilities. We include a standard 1-year warranty on all of our data acquisition products and a 3-year warranty on all our M Series products. Extended warranties are available." (National Instruments, 2006).

Note that reliability is not specified at all, and that the acronym MTBF, which the defence community so frequently uses, is nowhere to be found in this technical publication. It seems that market share, HALT & HASS and warrantee are sufficient to address reliability!

The commercial industry tends to follow an approach that rejects the accounting activities of reliability specification, prediction and demonstration, in favour of engineering activities. These are integrated into the development processes, and may include the following principles and activities (Dzekevich 2006):

- reliability is concurrent engineering process;
- reliability is part of Integrated Project Teams;
- reliability engineering is part of design reviews;
- mechanical and electrical stress predictions;
- component derating analysis;
- thermal analysis;
- electrolytic capacitor expected life calculations;
- FMEA (Failure Mode and Effects Analysis) and FTA (Fault Tree Analysis);
- system modelling during concept stages;
- HALT (Highly Accelerated Life Testing) performed during development;
- HASS (Highly Accelerated Stress Screening) performed during production;
- design verification testing beyond normal test scenarios;
- field return rates reviewed and managed on executive level;
- internal and external benchmarking and lessons-learned.

It is encouraging to observe that the defence industry appears to be moving from reliability accounting to reliability engineering. An example of this was evident from a panel discussion held at the 2006 Annual Reliability and Maintainability Symposium where reliability challenges for the Future Combat System (for US) were discussed by the DoD and main contractors. Reliability prediction as activity is being scaled down in favour for Reliability Enhancement Testing (being HALT and ALT (Accelerated Life Testing)) (RAMS 2006).

Conclusion

"A conclusion is the place where you got tired of thinking."

Unknown

Engineering management should review reliability activities throughout the life cycle of products and systems to determine whether these activities really add value. If not, they should be terminated, replaced by “real” engineering activities, performed timeously by competent engineers from the correct departments in the organisation, and with the sole objective of preventing failures. Reliability is the result of good engineering and good management, never the result of good accounting.

References

Barnard, R.W.A., "Reliability Engineering : Futility and Error", INCOSE SA Conference, South Africa, 2004

Billinton, R., Allan, R.N., *Reliability Evaluation of Power Systems*, 2nd edition, 1996

Booker, J.D., Raines, M., Swift, K.G., *Designing Capable and Reliable Products*, Butterworth-Heinemann, 2001

Dzekevich, J.A., "We Need to Change the Way RMA Does Business", 2006 Annual Reliability and Maintainability Symposium, January 2006.

Hobbs, G.K., *Accelerated Reliability Engineering: HALT & HASS*, John Wiley & Sons, 2000

Kuper, R.J., "Changing the reliability culture of the Army, DoD and our national industrial base", presentation at IEEE Boston Reliability Chapter, 8 December 2004

Mil-Hdbk-338B, *Electronic Design Reliability Handbook*, 1 October 1998

National Instruments, *Measurement and Automation Catalog*, 2006

O'Connor, P.D.T., *Practical Reliability Engineering*, 4th edition, John Wiley, 2002

Panel discussion, "R&M for Future Combat System", 2006 Annual Reliability and Maintainability Symposium, January 2006.

Reliability Analysis Center, *RAC Automated databook*, version 2.20

Sorenson, J.A., "Higher reliability and improvements in maintainability lead to lower life cycle costs : fact or fiction", keynote address at 2006 Annual Reliability and Maintainability Symposium, 23 January 2006

Walker, N.E., *The Design Analysis Handbook, A Practical Guide to Design Validation*, Newnes, 1998

Biography

Albertyn Barnard received the degrees M Eng (Electronics) and M Eng (Engineering Management) from the University of Pretoria. He has been providing consulting services in management, systems and reliability engineering to the defence, nuclear, aerospace and commercial industries since 1982. His company, Lambda Consulting, specialises in reliability engineering activities applicable to the design and development phase of products, with emphasis on reliability analysis of electronic design and HALT (Highly Accelerated Life Testing). He provides training in reliability engineering to local industry and at post-graduate level at the University of Pretoria. Albertyn has presented numerous papers at local and international symposia, and won the Ad Sparrius Best Paper Award at the INCOSE SA 2004 conference. He has been a member of the management committee of INCOSE SA for a number of years, and serves as President of INCOSE SA for 2008.