INTEGRATION OF RELIABILITY ENGINEERING INTO PRODUCT DEVELOPMENT

RWA Barnard

Lambda Consulting
Pretoria, South Africa
ab@lambdaconsulting.co.za
www.lambdaconsulting.co.za

ABSTRACT

Reliability can be defined as the absence of failures in products. This common sense viewpoint implies that reliability engineering should focus on the prevention of failure during development and production, and not on the correction of failure during operations. Understanding and anticipating the possible causes of failure are fundamental to preventing them. How can this be achieved during product development?

Failure prevention can be pursued by using *Analysis* and *Test* activities, which should be used to identify and to eliminate both design and production deficiencies. *Analysis* includes engineering analyses (eg component derating analysis) and failure analyses (eg Design Failure Mode and Effects Analysis). *Test* includes HALT (Highly Accelerated Life Testing) used during design, and HASS (Highly Accelerated Stress Screening) used during production.

This paper uses a common sense viewpoint to define reliability and reliability engineering, provides some detail on the integration of reliability engineering into product development, and concludes with examples of good practices used by successful industrial and aerospace companies.

1 INTRODUCTION TO RELIABILITY ENGINEERING

> "Unfortunately, the development of quality and reliability engineering has been afflicted with more nonsense than any other branch of engineering."
>
> (O'Connor 2001)

Many people believe that reliability (and reliability engineering) is a specialised discipline of engineering (or a specialty area of systems engineering), that it is based on mathematics and statistics (such as probability theory), and that it should be relegated to the logistics or maintenance departments in the organisation. However, many of these believes are questionable when we apply common sense to this issue.

Reliability can simply be defined as the absence of failures in products and systems. When a product does not fail, it is reliable, and when it fails, it is not reliable! When a failure occurs, and the failure mode is analysed to determine its root cause, it is nearly always the result of human error. This implies that failures are primarily caused by errors made by people such as systems engineers, design engineers, production personnel, product users and maintenance personnel. Such mistakes are inevitable due to human nature and the complexity of engineering.

Further analysis will reveal that all failures, in theory and almost always in practice, can be prevented. Note that failure prevention does not imply that a product should be designed and produced to be infallible, but rather that the failure mode is prevented from occurring (eg a system failure can be prevented by replacement of a component subject to wear-out). It is the responsibility of management to prevent or at least reduce the probability of human error throughout the product or system life cycle. Therefore, using a common sense viewpoint, reliability and reliability engineering can be defined as follows:

Reliability is the absence of failures in products and systems

Reliability engineering is the management function that prevents the creation of failures

These definitions are in agreement with viewpoints of world leaders on quality, such as Philip Crosby, who wrote "All non-conformances are caused. Anything that is caused can be prevented" (Crosby 1995). This viewpoint implies that reliability engineering should focus on the prevention of failure during design and production, and not on the correction of failure during operations. We need to practise proactive approaches to reliability (ie failure prevention), rather than reactive approaches (ie failure correction or failure management).

2 VERIFICATION OF RELIABILITY DURING DESIGN AND PRODUCTION

Understanding and anticipating possible causes of failure are fundamental to preventing them. How can this be achieved during product development and production? Figure 1 shows that both design and production should be followed by verification (eg *Analysis* or *Test* to verify compliance with specifications). If a design or process deficiency is identified, it has to be corrected, and verified again. Iteration of this process is applicable to all performance requirements, including reliability.

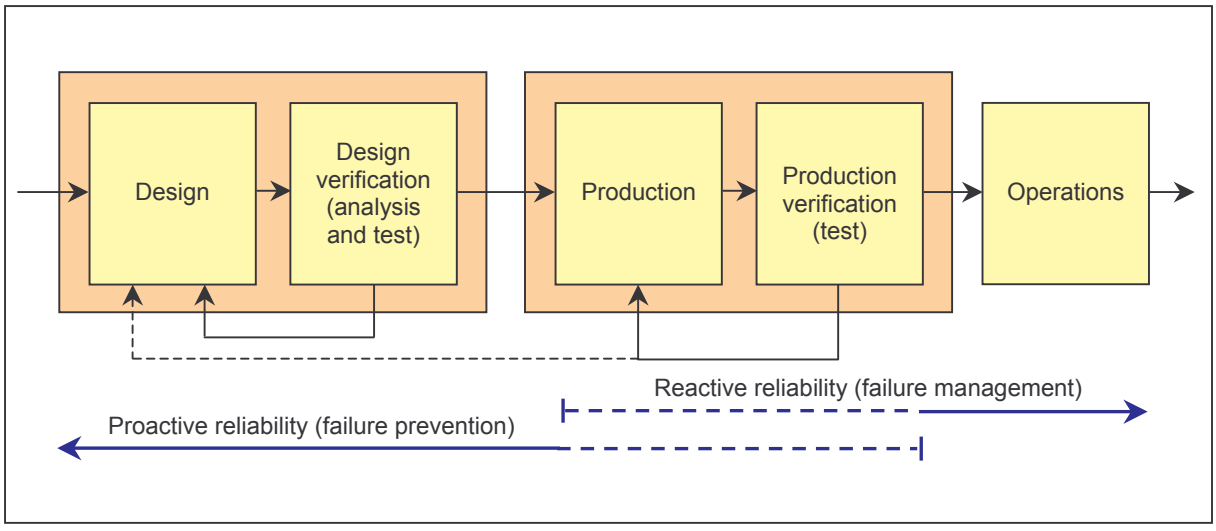

Figure 1: Verification of design and production

Once in operation, reliability cannot be improved to levels higher than the inherent reliability. Reliability can only deteriorate to lower levels due to various other factors. It is evident that reliability activities change from proactive to reactive once production has started, although some reliability engineering activities are applicable to the production phase. What is meant by *Analysis* and *Test* in this context?

2.1 Analysis

Any **engineering analysis** that provides knowledge on potential product failure modes, and the prevention thereof, can be used as valuable reliability engineering tool. Examples include electronic component derating analysis, tolerance analysis, thermal analysis, finite element analysis, vibration analysis, etc. Activities generally considered as reliability accounting (such as reliability prediction) are based on fundamentally flawed assumptions, and should not be used during development (Barnard 2008).

Failure analyses, performed with the objective of understanding how the product or system will react to potential failure modes, are extremely useful to influence design during development. Typical analyses include reliability block diagram analysis, design (and process) FMEA (Failure Mode and Effects Analysis) and FTA (Fault Tree Analysis).

2.2 Test

HALT (Highly Accelerated Life Testing) and HASS (Highly Accelerated Stress Screening) are overstress test methods that provide early knowledge on design and production weaknesses, providing opportunities for improvements that will lead to higher field reliability. The application of these methods requires the use of special test equipment to subject development models or production units to environmental stresses far beyond specification levels. HALT is used during design, and HASS during production. It should be noted that reliability demonstration testing based on PRST (Probability Ratio Sequential Testing) is fundamentally inadequate and should not be used, especially not for development testing (O'Connor 2001).

3 GOOD PRACTICES

3.1 Commercial company A

This company followed a design-for-reliability process that focussed on reliability engineering activities (and not on reliability accounting activities such as prediction and demonstration). In fact, this company did not specify MTBF (Mean Time Between Failure) as design goal or metric, but mandated a specific design process, which includes the following (Dzekevich 2006):

- reliability is a concurrent engineering process
- reliability is part of Integrated Project Teams
- reliability is part of design reviews
- mechanical and electrical stress predictions
- component derating analysis
- thermal analysis
- electrolytic capacitor expected life calculations
- FMEA and FTA
- system modelling during concept stages
- HALT performed during development
- HASS 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

3.2 National Instruments

National Instruments is 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 and 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 MTBF is not used in this technical publication. It seems that market share, HALT and HASS and warrantee are sufficient to address reliability!

3.3 NASA Pilot Benchmarking Initiative

NASA recently engaged in a collaborative "Pilot Best Practices – Benchmarking" study with selected "best of the best" industry partners who are recognized leaders in complex systems developments (NASA 2007). This study identified seven Focus Topics, which are suggested as being essential elements for successful future space programs. One of these topics is titled "Achieving Robust Systems by rigorous analysis, robustness of design, HALT/HASS testing", and refers specifically to reliability and reliability engineering:

"Modern systems generally have a large number of functional requirements, and often exhibit an even larger set of potential failure modes. The characteristics of complex systems are such that simply designing to "meet the requirements" may not always be sufficient to fully assure safety to humans, or to achieve other critical performance aspects.

The use of enhanced methods to assure "robustness" of design provides additional layers of assurance that critical performance margins and safety characteristics are sufficiently verified, adding to system survivability and resilience to prevent inadvertent failure from unforeseen stresses and events.

The most stringent robustness disciplines are applied in general to new or "unprecedented" designs. A key emphasis in using HALT is to start "Early" with prototype hardware to allow for sufficient time and resources to correct the failure. "Layered" HALT/HASS testing is done in a sequentially increasing degree to find stress points and feed back into the system design to improve robustness where desired."

3.4 Airbus

Airbus requires "Product Maturity at Entry into Service" from its suppliers. To comply with this requirement, many suppliers, such as Thales Avionics, have embraced HALT and HASS (or derivatives thereof), as part of their design and production processes (Sound and Vibration 2006):

"In the case of mission critical applications, accelerated testing becomes essential because having extremely high product reliability represents the only way of doing business. In our industry, 'product maturity' means delivering products with a very high operational reliability, from the very first delivery. However, to get product maturity at entry into service was initially taking months, or sometimes years, due to the time required to discover any issues. But our customers do not want to wait and to have issues. So that is why we decided to introduce product maturity methodologies that included HALT to discover and fix weaknesses and HASS to catch infant failures."

4 CONCLUSIONS

Reliability engineering should focus on the prevention of failure in products and systems. Therefore, a proactive approach to understand and anticipate the cause of failure, and which is integrated into design and production phases, is essential to ensure high reliability. Good practices from successful companies are known, and can therefore be implemented by other companies. Some of the practices include well-known activities such as component derating analysis and design FMEA, but also new activities such as HALT and HASS.

5 RECOMMENDATIONS

Focus on failure prevention, not on failure correction or failure management. Integrate reliability engineering into design and production phases, since reliability cannot be added at a later stage. Learn from good practices as followed by successful companies. Implement activities such as component derating analysis and Design FMEA, and HALT and HASS.

6 REFERENCES

[1] Barnard, R.W.A., *What is wrong with Reliability Engineering?,* 18th Annual INCOSE International Symposium, Utrecht, The Netherlands, 2008
[2] Crosby, P.B., *Quality without tears*, McGraw-Hill, 1995
[3] Dzekevich, J.A., *We Need to Change the Way RMA Does Business*, 2006 Annual Reliability and Maintainability Symposium, 2006.
[4] *NASA Pilot Benchmarking Initiative, Exploring Design Excellence Leading to Improved Safety & Reliability*, Final Report, Abridged Edition, 2007
[5] National Instruments, *Measurement and Automation Catalog*, 2006
[6] O'Connor, P.D.T., *Test Engineering, A Concise Guide to Cost-effective Design, Development and Manufacture*, John Wiley, 2001
[7] Sound and Vibration, *HALT/HASS Testing*, June 2006

7 BIOGRAPHY

Albertyn Barnard received the degrees M Eng (Electronics) and M Eng (Engineering Management) from the University of Pretoria. He has provided consulting services in 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 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. He has presented numerous technical 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.