Systems Reliability Demonstration

Zvi Benyamini and Dr. Avigdor Zonenshain
RAFAEL
P.O. Box 2250
Haifa, 31021
Israel
zvikab@rafael.co.il avigdorz@rafael.co.il

Abstract. This paper discusses the issue of system Reliability Demonstration. The classical reliability demonstration methods are discussed, as well as the difficulties associated with application of these methods in today's complex system and competitive project environment. Some insights are discussed, regarding the changes required in reliability demonstration methodologies, in order for them to be effective in today's environment - from both RAFAEL's experience and trends throughout the world. The methods presented are being successfully implemented in several projects.

INTRODUCTION

The demonstrated reliability of a system is defined an estimate of its reliability based on the analysis of testing results or direct field data. This, as opposed to the predicted reliability, which is based on theoretical models and generic data bases.

The process of reliability demonstration is the verification of the system's reliability vs. the requirements. From a customer's point of view, the results of this process are considered a credible and dependable reliability figure, as they are based on "real objective field data". From a program manager's perspective, focus is placed on the cost of this process (both time and money), and its effectiveness at discovering hidden flaws if such exist.

The world of reliability demonstration has gone through considerable changes over the past decade. In this paper we describe the classical reliability demonstration techniques, and discuss the difficulties associated with the application of these methods in today's systems. Next, we discuss some insights regarding the changes required in system reliability demonstration concepts. Some of these insights are the result of RAFAEL's experience in this field, while others reflect trends throughout the reliability engineering discipline.

CLASSICAL METHODS OF RELIABILITY DEMOSTRATION

The classical methods of reliability demonstration are based on direct statistical analysis of test results data or field data, using various models depending on the system's characteristics and type of available data. Examples of such statistical methods include binomial models, life testing, accelerated life testing, parametric models and more, see for example (MIL-HDBK-781D),(Modarres et al. 1998).

The demonstration is usually carried out using a dedicated series of tests, with test articles representing the final version of the product, in order to assure that test results are directly

applicable to the product involved. The reliability demonstration process is usually separated, as a matter of principle, from both the development and the reliability analysis processes, in order to assure an objective and independent verification process.

These characteristics of the reliability demonstration process pose certain difficulties:

- The mathematical-statistical framework causes the illusion of a well-defined and unambiguous measurement process, whose results and uncertainty can be accurately quantified. In reality, most models used rely heavily on statistical assumptions, which are not always justified or verifiable. Not all aspects of reliability, and especially of uncertainty, are covered by these models (for example – model uncertainty is rarely addressed). In fact, the entire process – from planning the test program to assessing the results - is subject to a great deal of interpretation, is far from unambiguous and in some cases can be simply misleading.
- The separation from the development process is not always practical. The independent and uncoordinated use of different methods (design considerations, reliability analysis techniques, and demonstration) results in high costs, and misses out on possible synergetic benefits.
- "Waiting for the final version" for testing causes harsh time constraints as the race for time-to-market grows, and greatly diminishes any chance for gaining any value for the development process.
- The sole focus of the entire process, which employs significant funds, is on measuring the reliability, rather than on improving it. Naturally, this lowers the motivation of project managers to place effort and resources into this process, at the expense of other, more "valuable" activities.

The nature of systems and projects has changed, since most reliability demonstration methodologies were developed. These changes require us to adapt and update demonstration methods:

- In the past, reliability problems were mainly component-oriented. Demonstration methods of systems were also focused on demonstrating parts separately. In today's complex systems and systems-of-systems, and thanks to component reliability improvements, the main causes of failure have to do with complexity, interfaces, system design issues. Demonstration methods must also change to be better able to address these issues.
- The reliability demonstration discipline originally stemmed from the 1950's and 60's military projects. Today's focus (even in the military market, let alone the consumer market) is more business oriented – with much greater emphasis to cost, cost-effectiveness and time-to-market issues. Application of classical methods in this new competitive environment is many times prohibitive.
- As technology improves, system reliability is constantly improving. Directly demonstrating ultra-high reliability, in a short time and with sufficient confidence is not practical.

RELIABILITY DEMONSTRATION CONCEPTS

Our goal is to develop reliability demonstration methods which are better suited to effectively handle the main relevant issues in today's projects –from both the technical perspective and the

project management and process integration perspective. In this section we will outline several concepts, which in our view are essential in order for any reliability demonstration method to be effective for today's systems:

- A combination of different reliability assessment methods, which give a joint and synergetic view of all reliability issues.
- Integration of the design and demonstration processes.
- Reasonable expectations from the quantitative aspects of the process.

A Combination of Methods. The Reliability Case Methodology (UK MOD, 1999) (and its Safety Case parallel) has been developing over the past few years, particularly in Europe. It is based on the idea of integrating all available evidence from different sources - testing, analysis and expert judgment, through an explicit logical series of arguments and assumptions - into an overall "case" (as in a courtroom). This "case" is used to justify claims as to the reliability or safety of the system (see figure 1).

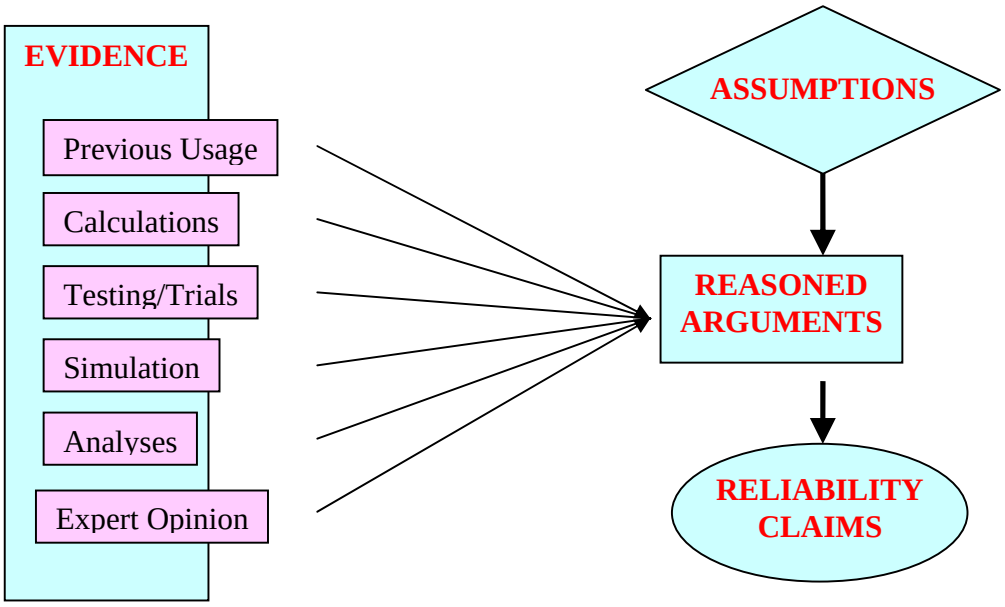

Figure 1. The Reliability Case (UK MOD, 1999)

The interaction and synergy between different tools and methods serves three purposes:

- The different sources of information complement each other, thus giving more solid basis to the reliability assessment and better addressing the uncertainties and limitations of each separate tool.
- Feedback from one tool to the other helps design a more effective demonstration process (see following example).
- The combined use of all available information allows wiser distribution of resources, and allows overall cost & schedule to be reduced.

One such example of combined methods is the explicit connection between:

- Failure modes analysis, risk and uncertainty analysis.
- Testing.
- Modeling and simulation.

The connection is described in figure 2.

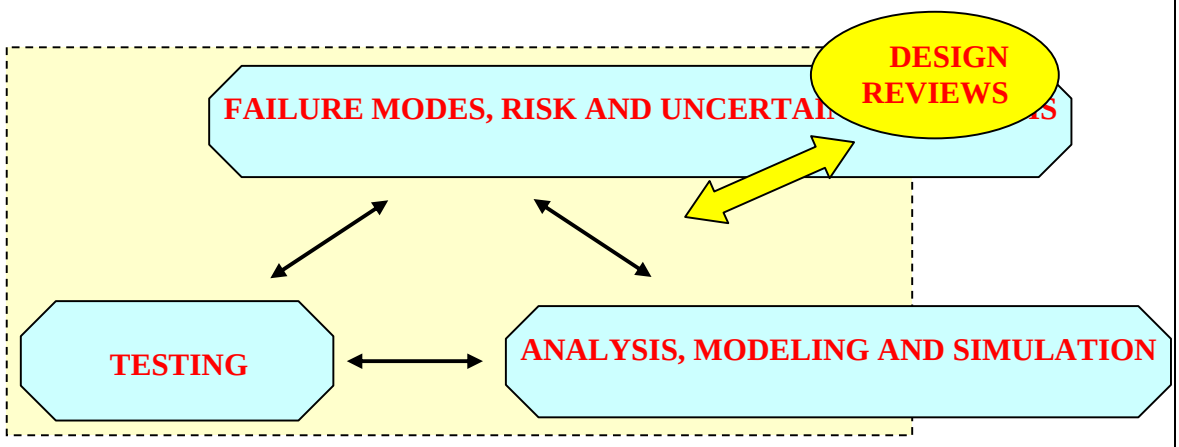

Figure 2. Combining Methods in Reliability Demonstration

The failure mode, risk and uncertainty analyses serve as the basis for generating he list of tests and models needed.

Tests are used not only to verify system operation, but mainly to verify the models. As it is usually impossible to cover the entire operational parameter space experimentally, the models allow us to "connect the dots" between the conditions in which actual testing was performed.

The results of tests and models bring out new unpredicted failure modes, risk or uncertainties.

The explicit correlation between the three processes, and the completeness of the reliability case based on this correlation, is verified through the review process: every failure mode, risk or uncertainty is answered for through either testing or modeling; every model is validated, through testing if necessary; the models and tests put together cover the entire operation parameter space.

Integrating Reliability Demonstration into the Design Process. In our view, demonstrating the product's reliability is an inherent part of the design Verification and Validation (V&V) process, as both are aimed to show that the product will perform as expected without failure (Maymon & Benyamini, 2002). The immediate conclusion is that the reliability demonstration process should be integrated into the design testing and V&V process, rather than artificially separated from it.

In one aspect, testing and analyses performed during design phases should be planned with

reliability demonstration in mind, rather than designed for verifying performance in a single point in the operational space. Examples include:

- Parametric recording of results, rather than pass/fail tests, may be used to quantitatively estimate variation, and verify sufficiency of safety margins. High instrumentation and comprehensive measurements, in at least some of the test articles, may yield much information usable for model calibration and verification.
- Test conditions including significant safety margins, preferably testing up to failure for critical parameters, rather than testing "just-to-spec" or with minimal safety margins.
- Designing test conditions and measurements with the intent of finding failures and exciting failure modes ("find and fix", "failures are welcome"), rather attempting to accumulate "successful" tests. HALT (Highly Accelerated Life Testing) methodology is an example of such testing.

All of these methods may greatly decrease the time and number of articles which are required for demonstrating the product's reliability, and at the same time increase the confidence (from engineering, not just statistical, point of view) in the reliability of the product.

From another aspect, the demonstration process should incorporate all relevant information not only from dedicated testing, but also from design testing and from analyses. Not only does this result in saving time and money on dedicated testing, but it also allows management and control of system reliability, assuring reliability growth and narrowing of uncertainty bounds throughout the development process (see figure 3). Note that we refer to managing uncertainty in a broad context (including for example model uncertainty), such as through enhanced modeling capabilities and scientific understanding or increasing design margins and their verification, and not only to the aspect of decreasing statistical errors through increased sampling.

A Balanced and Realistic Quantitative Approach. The ability to accurately quantify the reliability of complex systems, with variable operation conditions, high performance and reliability requirements, and a limited amount of test data is inherently limited (see, for example, (Kleyner and Boyde 2004)). Nevertheless, all classical reliability demonstration methods are entirely focused on the quantitative aspect of statistical and probabilistic estimation. An effective reliability demonstration method must acknowledge and address both the strengths and the limitations of the quantitative tools.

We believe, that the quantitative framework should be used as a guidance tool for decision-making, rather than be the main, if not only, aspect of the demonstration process. Quantitative models can and should be used, in order to give an overall view of needs, priorities, alternative selection etc. However, these tools should be used selectively, in cases where their underlying assumptions are indeed applicable, and where the results can be applied directly to engineering or managerial decisions and can be justified by engineering or managerial arguments.

The depth, complexity and precision of the models should be justified according to the decisions to be supported, and be in accordance with the fidelity of the data available. Illusions of precise models, using highly uncertain data, should be avoided. All aspects of uncertainty, and not just statistical sampling "confidence levels", should be addressed and presented in order to avoid misinterpretation. Finally, one must acknowledge that complete quantification cannot be achieved in highly complex, difficult-to-test systems.

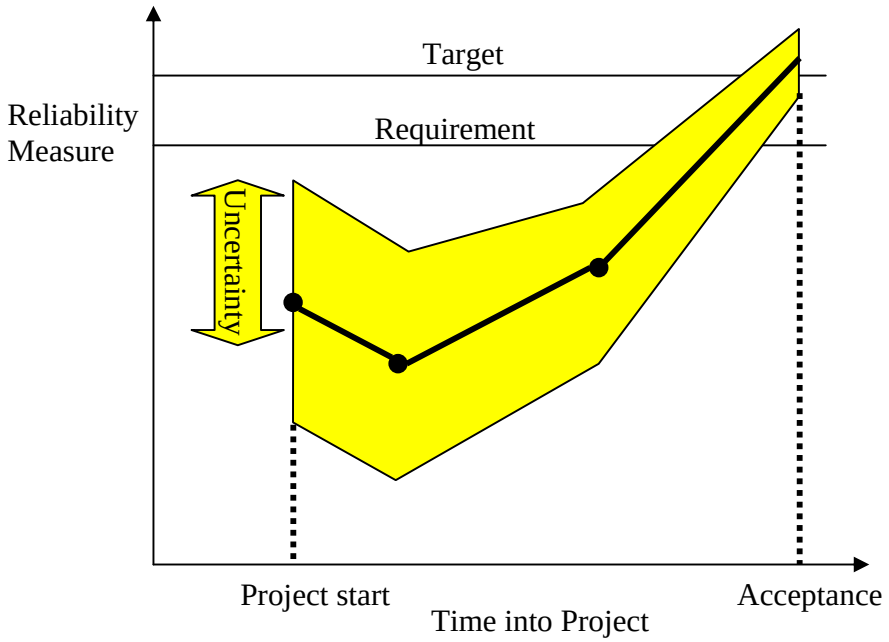

Figure 3. Managing Reliability & Uncertainty Throughout the Development Process (UK MOD, 1999).

SUMMARY

Reliability demonstration is an integral part of the project development process. The system engineering environment of today, from both technical and project management aspects, differs from that for which classical reliability demonstration models were originally developed. These changes cause the need to re-examine and re-tailor reliability demonstration concepts.

In order to be effective, a reliability demonstration method must be:

- Integrated throughout the development process.
- Based on the use of a combination of methods, from a joint and overall point of view, with emphasis on cost-effectiveness.
- Tailored to the technical and managerial properties of the project.

The practice and application of reliability is slowly but constantly changing. The methods presented in this paper are gradually implemented successfully in a growing number of projects in RAFAEL.

REFERENCES

A. Kleyner and J. Boyle, Reliability Demonstration Tools: Advantages and Limitations, *Proceedings of the Applied Reliability Symposium*, 2004.

Maymon, G. and Benyamini, Z., Foundations of a Methodology for Integrating Reliability

Demonstration into the Development Process, internal report MA-DT-2002/24, 2002.
MIL-HDBK-781D, Reliability Design Qualification and Production Acceptance Tests.
M. Modarres, M. Kaminskiy, and V. Krivtsov, *Reliability Engineering and Risk Analysis: A Practical Guide*, Marcel Dekker, New York, N.Y., 1998.
UK MOD, DEF-STAN –00-42 (part 3/1): Reliability and Maintainability (R&M) Assurance Guidance, Part 3: R&M Case, 1999.

BIOGRAPHY

Mr. Zvi Benyamini Earned his B.Sc. in Mathematics and Physics from the Hebrew University in Jerusalem (1992), and his M.Sc. in Statistics and Operations Research from Tel Aviv University (1997). His Experience is in the field of Operations Research, System Engineering and Analysis and RAMS. He was a reliability engineer and system engineer on several major projects in RAFAEL, and as of 2002 is the Head of RAFAEL's Reliability & Systems Center.

Dr. Avigdor Zonnenshain is currently the Deputy for Operations, ordnance systems Division, at RAFAEL – the Armament Development Authority of Israel. Dr. Zonnenshain is a Ph.D. for Systems Engineering from the University of Arizona, Tucson. Formerly, Dr. Zonnenshain held several major positions in the Quality and System Engineering arena:

- Director for Quality & Productivity of RAFAEL.
- Director of the Quality of Excellence Center, in the Prime Minister's Office.
- Director of Quality & Certification Department, in the Standards' Institute of Israel.
- The first president of the World Quality Council (WQC).
- Director of Systems Department

He is also an active member of the Israel Society for Quality (ISQ), and INCOSE_IL.