

The R&M Case - A Reasoned, Auditable Argument Supporting the Contention that a System Satisfies its R&M Requirements

Table of Contents

- Introduction
- The Basic Concept
- Building an R&M Assurance Case
- The Development of Claims
- R&M Case (Status) Reports
- The Evidence Framework
- Summary
- For Further Study
- About the Author
- Other START Sheets Available

Introduction

Today's customers demand reliable products. Obviously, such demands must be reflected in the product specification and requirements. Then the equipment suppliers must design products to perform reliably and also be capable of being maintained throughout the required product life. The suppliers must also provide evidence that their products will meet the reliability and maintainability (R&M) requirements. Recent thinking within the R&M community has led to a move away from the specification of a set of prescriptive methods that the supplier must undertake to a more cooperative approach.

Historically R&M methods have depended upon the availability of field data, experiential information, or learning through extensive and time consuming tests. Experience has shown that conformity to standards alone is insufficient justification for the reliability argument of the system – additional evidence is needed. This new approach known as “R&M Case,” requires the progressive exchange of information between the customer and the supplier in order to provide assurance that the product will meet the R&M requirements. Specifically the supplier must satisfy three objectives:

- Ascertain customer requirements

- Meet customer requirements
- Provide assurance that the customer requirements have been met

The primary advocate of the use of R&M case is the British Ministry of Defense (MOD) in the promulgation of **Defense Standard 00-42 Part 3** (Reference 1). Indeed, the second half of this START sheet is based primarily on that document. However, this “case” concept is also being adopted in the software reliability community (Reference 2), especially as it relates to Safety (Reference 3) and Supportability. It has some parallels with but is not identical to the “safety case” used in the nuclear industry. This “case” approach is documented in the release of some key new Society of Automotive Engineers (SAE) documents (References 4, 5, 6, 7, and 8). The concept of R&M Case now merits consideration for both military and commercial hardware and could be considered as a key criterion for product selection.

The Basic Concept

Under this new cooperative rather than prescriptive approach, the management of R&M is built around two key components: the R&M Plan and the R&M Case.

- The R&M Plan takes a forward view, it describes the activities together with any applicable success criterion that are to be undertaken to demonstrate that the R&M objectives have been achieved.
- The R&M Case provides a retrospective view e.g., a justification of the approach and documents evidence, throughout the project, which verifies that the system meets its R&M requirements. This includes evidence that the R&M requirements are achievable and are properly understood by the developing organization.

The R&M Plan and R&M Case may be seen as having variable purposes depending on whether they are used as contractual, developmental, or support mechanisms. In the contractual context, the plan and case can be used as formal deliverables to be jointly defined and approved between a

customer and supplier. The Plan and Case can contribute to any prospective development and may be requested during contract negotiations. In a developmental context, the Plan and Case may serve the internal needs of a development organization in meeting R&M objectives. Finally, for organizations involved in providing post-delivery support, the R&M Plan and R&M Case may be used to establish or validate cost and efficiency objectives.

The **R&M Plan** is the means through which activities and progress in satisfying customer R&M requirements are monitored and controlled. The plan provides clear traceability to original customer R&M requirements, and also shows activities together with any applicable success criterion relating to the generation of the associated R&M Case. The plan should be traceable to the broader planning activity for both system support and the acquisition/delivery arrangements for the overall fielded system. The plan should also be integrated appropriately with relevant system development and quality planning. The plan should be mutually agreed upon by the customer and the supplier before implementation, and subjected to appropriate management reviews during its period of use.

The core concept of the **R&M Case** is that this is the means by which suppliers can demonstrate that customer R&M requirements have been achieved for a particular product. An R&M Case should be a readable overview of the evidence, including references to more detailed evidence as appropriate, to support requirements satisfaction. Various types of information are possible. A Case document may be used both for the acceptance or assurance of new products and for substantiating R&M claims to potential new customers of proposed and existing products.

An R&M Case is compiled as design and development decisions are made. The approach to be applied for a particular product should be defined at the outset of planning, and implemented across the life-cycle through a suitable activity schedule.

Types of Evidence – An R&M Case may be based on a variety of types of evidence, but they must be within the bounds of the stated assumptions. The method used in a particular instance may be chosen at the supplier’s discretion, as appropriate to the nature of each requirement addressed. Suitable approaches are described as follows. These may be used in isolation, but more typically they will be used in combination to provide a more robust Case.

- Quantitative Evidence uses defined methods of analysis to generate metrics that demonstrate the required (or desirable) R&M features in the target product. This type of evidence also includes the results of any testing or demonstrations conducted as part of an R&M program.

- Qualitative Evidence focuses on the processes used for development and support of the system. It seeks to assure satisfaction of R&M requirements by inference, based on the demonstrable quality, maturity, and integrity of the underlying engineering and management processes.
- Historical or Comparative Evidence could be relevant for systems already in use and supported for other customers. Comparative evidence could be relevant for a system which is a variant of an existing product, or is similar to an existing product produced by the same supplier. The information provided might include both quantitative and qualitative aspects of the product and the associated support services.

Maintenance of the R&M Case – In general, the rationale for generating an R&M Case during development will apply similarly to maintenance of the case during later phases. The Case will provide the basis for assurance that the original R&M requirements continue to be met in the face of ongoing evolution and change to the system.

The R&M Plan and the R&M Case may be required as deliverables contracted between a supplier and customer. The Plan provides a forward view of intended processes and the Case looks back at decisions made. Therefore both of these key artifacts are created in the early stages of a project and it is to be expected that not only a Plan, but also a Case should form part of any proposal in order to justify design and process decisions upon which the proposal is based. The Case continues to be developed throughout a project and provides visibility of progress. Iterations of the Case may be linked to project and payment milestones. Where deliverables of one phase are used as discriminators for future contract awards, care should be taken to distinguish between acceptance of deliverables from one phase and claims about future intentions.

Building an R&M Assurance Case (Reference 9)

An assurance case is an argument that assures some set of facts. The concept is used widely in the safety industry, especially in Europe where it forms the basis of a large number of safety regulations. Any case-based argument must be based on the general principles of argument. “An argument is a connected series of statements intended to establish a definite proposition”. The statements used in the argument are generally statements about evidence that support the proposition (or claim) that the argument is attempting to put across. These statements can take a number of forms depending on the available evidence and the type of proposition being made. The statements in the argument take evidence and draw an inference from it and it is the pulling together of these inferences into an overall argument that support the proposition. Hence we have a simple model of “argument” as shown in Figure 1.

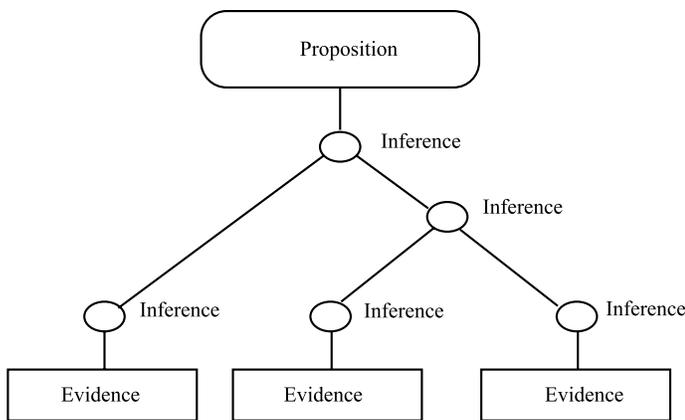


Figure 1. Argument Model as Used in an R&M Case

There are actually three types of inferences or arguments: a) Deterministic – arguments based upon axioms, proofs, logic, or prior research and experience, b) Probabilistic – arguments based upon failure rates, static analysis, and/or assumptions about independence, and c) Qualitative – arguments based on compliance with standards and industry practices.

To be satisfied R&M requirements must first be fully understood and a suitable strategy with defined Project Management tasks developed (the R&M Plan). This strategy should include identifying R&M risk areas and considering how these risks will be managed. R&M activities are then undertaken in order to generate evidence. Hence it is comparable in many ways to building a legal case.

It is essential that the activity results (i.e., the evidence) be reviewed progressively against their defined “success criteria”, and also assessed in terms of meeting the ultimate target R&M measures. The strategy must be flexible in its approach to providing progressive R&M assurance, in that the results of R&M activities should be reviewed against the R&M requirements and the R&M Plan modified as necessary.

The R&M Case is a progressively expanding body of evidence. Starting with the initial statement of the requirements, the “R&M Case” also includes identified, perceived, and actual risks; strategies and an **Evidence Framework** referring to associated and supporting information; including R&M evidence and data from design activities; trials, etc.; through to in-service and field data as appropriate. It also records any subsequent changes. It thus becomes a top-level control document, summarized periodically through the issue of **R&M Case Reports** linked to the Evidence Framework. It records progress and remains with the equipment/system throughout its life.

The R&M Case is used throughout the procurement chain from prime contractor down to individual subcontractors and suppliers to provide live documentation that progresses and records achievements in an evidence framework set against the target R&M measures.

The R&M Case provides an audit trail of the engineering considerations starting with the requirements and continuing through to evidence of compliance. It provides traceability of why certain activities have been undertaken and how they can be judged as successful. It is initiated at the concept stage in accordance with the R&M Plan, and is revised progressively throughout the system life cycle. Typically it is summarized in R&M Case Reports at predefined milestones.

The Development of Claims

Figure 2 (taken from MOD Defense Standard 00-42 Part 3) (Reference 1) illustrates the concept of building and arguing claims in an R&M Case using evidence sources. It shows that the reasoned arguments in an R&M Case can combine different types of evidence and also build on assumptions.

In practice, the collation of all this documentation is likely to become unmanageable, particularly where there are many and diverse sources of evidence. Thus the R&M Case is typically derived from R&M Case Reports. These reports in turn then refer out to source evidence as illustrated in Figure 3.

The input to the R&M Case from an activity includes:

- Objective and Success Criteria (What the activity plans to achieve, and defines when the activity has been successful.)
- Outputs (These are the outputs from the activity.)
- Assumptions (Upon which the activity is based.)
- Evidence (How the outputs substantiate the claims in the R&M Case Report.)
- Development and Maintenance of Evidence (How will the results of the activity be maintained to reflect the latest design.)

R&M Case (Status) Reports

The R&M Case (Status) Report provides evidence at a specific stage within the R&M Case Evidence Framework. The reports present an argued claim, based on evidence and assumptions that the system will satisfy the R&M requirements. The report is not expected to contain all the evidence produced for at that stage, but it will summarize and act as a ‘signpost’, indicating where the detailed evidence can be found.

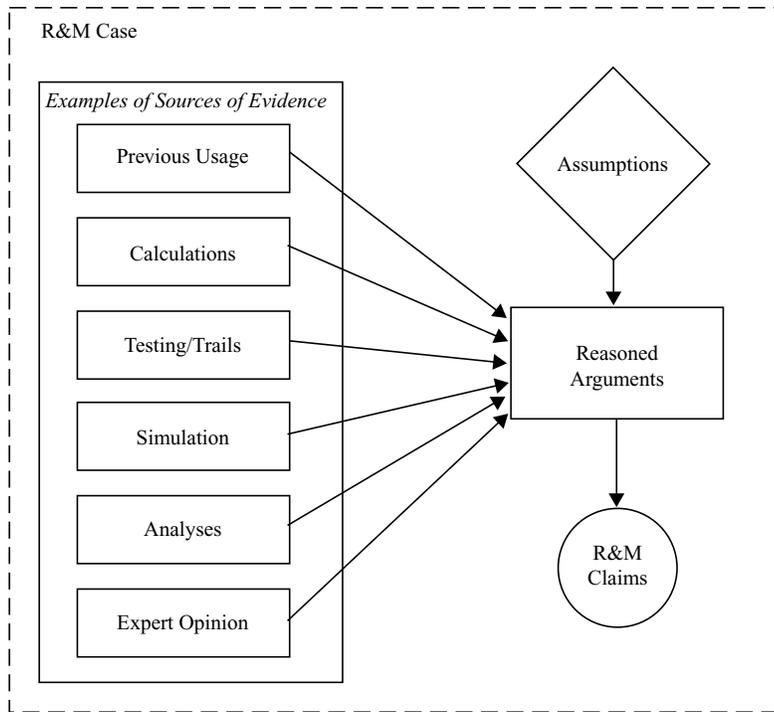


Figure 2. The Development of Claims

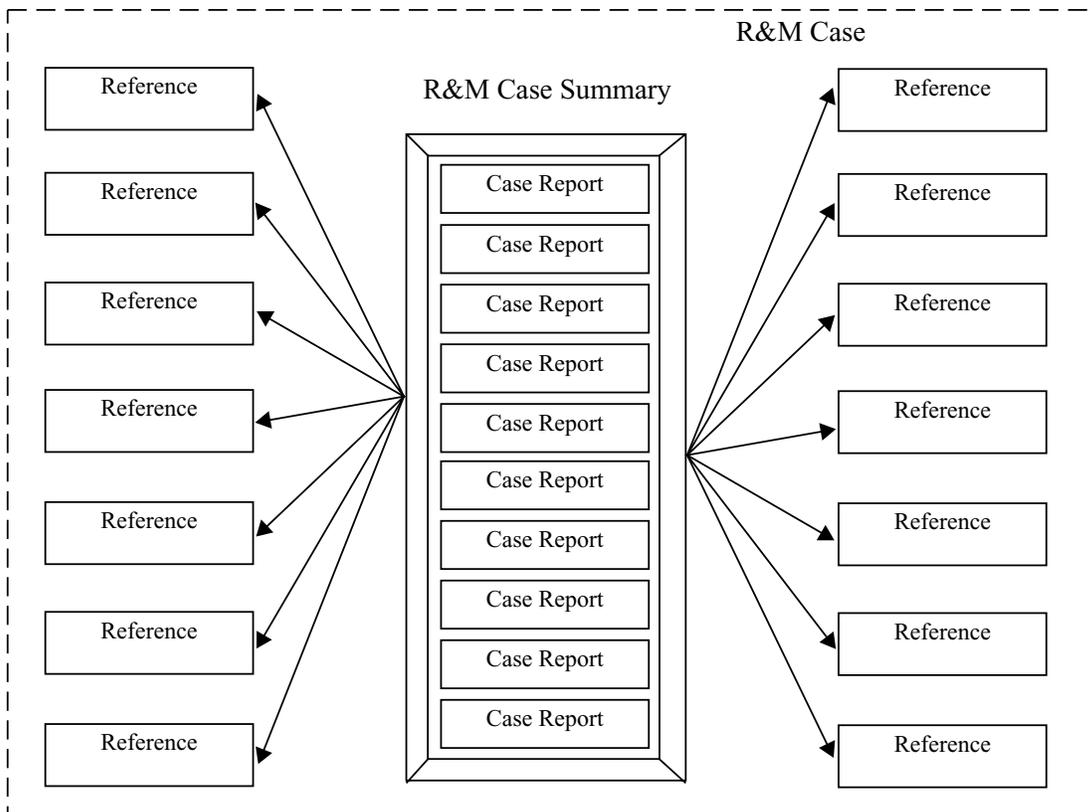


Figure 3. The Concept of the R&M Case

Each R&M Case (Status) Report lists and cross references the parent requirements in the Evidence Framework, against which the evidence is to be judged, and is traceable to the original Customer's requirement. The body of evidence traces the history of reviews and updates of the R&M design philosophy, targets, strategy and plan, which keep these in line with the changing status of the original risks, as well as any new/emerging risks. The status of the R&M assumptions, evidence, arguments, claims, and residual risks is then summarized and discussed.

The case report should provide a balanced review of the body of evidence in terms of its completeness, timeliness, and acceptability with regard to the criteria contained in the Evidence Framework. Conclusions are drawn with regard to the status of the progressive assurance and the activities necessary to mitigate the residual risks. Recommendations are based on current shortfalls in the evidence available and proposed changes, as appropriate, to the R&M design philosophy, targets, strategy, and plan in order to maximize the progress towards assuring that the system will satisfy each of the R&M Requirements.

The Evidence Framework

The R&M Evidence Framework is a matrix of the R&M risks, requirements for evidence to mitigate the risks, activities necessary to obtain the required evidence, the evidence acceptance criteria, references to the evidence actually provided and confirmation of its acceptance (or rejection). Thus the R&M Case provides traceability of the process throughout the life of the system. Both the Customer's and Supplier's risks need to be addressed.

The Evidence Framework captures the current set of mitigation activities (including their success criteria) to address the R&M risks. Typically it is presented in the form of a matrix. The number, content, objectives, and timescales of the R&M Case (Status) Reports are determined and prescribed by the Evidence Framework. Initial work starts with the R&M Strategy & Plan and is updated throughout the project. Each R&M Case (Status) Report reflects the latest state of the Evidence Framework as shown in Figure 4. This element of the R&M Case contains details of the initial (justified) requirement and reasons for implementing the proposed solution.

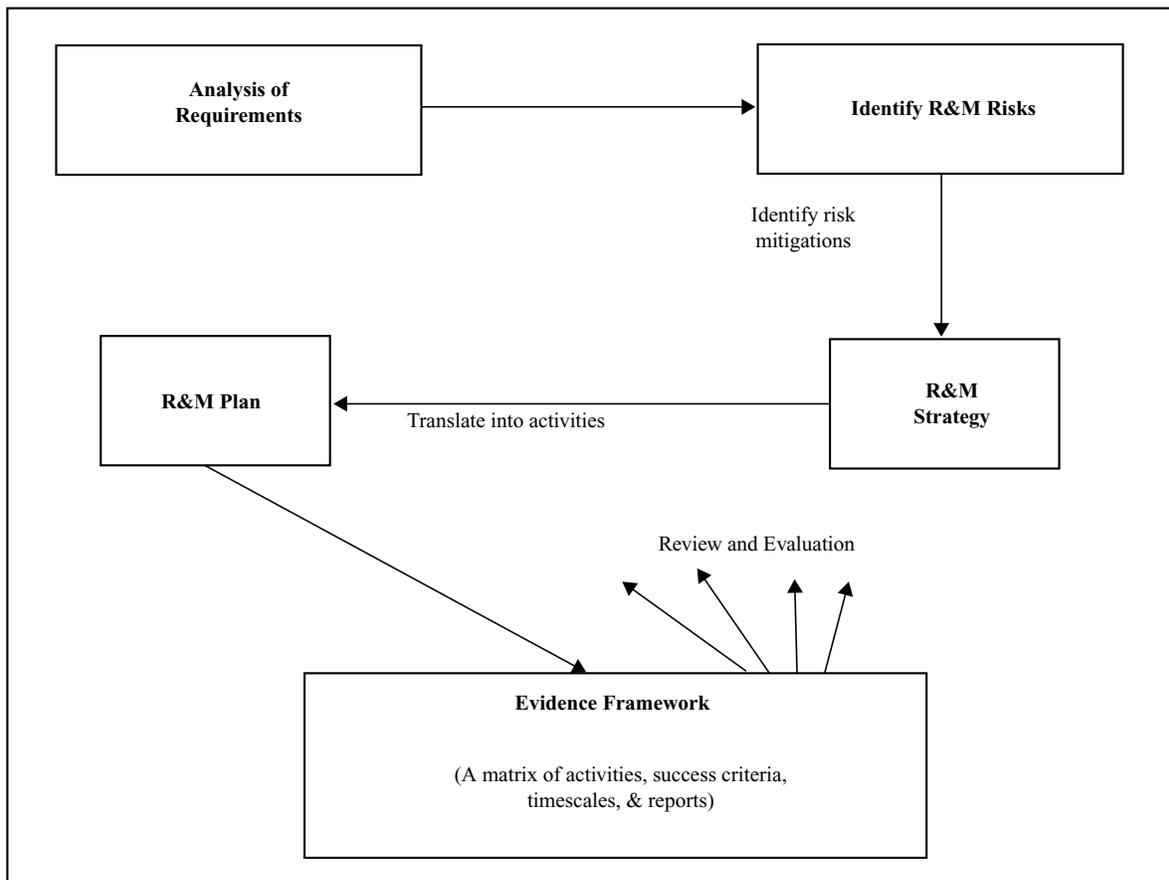


Figure 4. Establishing and Developing the Evidence Framework

The objective of developing a strategy is to provide confidence to both the Supplier and the Customer that the risk of failing to meet the R&M requirements has been minimized, before they commit resources to the program.

In every project there will be some potential for shortfalls in R&M performance. The recognition of these R&M risks should thus prompt the selection of a program of specific R&M Activities as well as the core design proving activities, which can mitigate these risks. The objective is to build up a body of evidence, which provides assurance that the R&M requirements are being achieved.

The risks of not achieving the R&M requirements is evaluated at each step and is managed by the application and practice of risk management. This typically involves “scoring” of each risk in accordance with a set of criteria which were defined at the start of the project. The risk management process commences at the bidding stage and continues throughout the development, manufacture and in-service stages. Thus it is an active process, which reacts to changing levels of risk, and the emergence of new risks as the project progresses.

There are occasions when the selection of a different design option, technology insertion or mid-life improvement will render a proportion of the previously collected evidence obsolete, thus fresh evidence will need to be generated. Also, there will be some periods when no evidence is being provided, e.g., during testing, prior to the release of the test results.

The adequacy of evidence is primarily a function of its practical impact on the reduction of R&M risks, i.e., progressive assurance. Some principal criteria for assessing the adequacy of evidence are:

- Is the evidence, as a whole, clearly derived from a closed loop R&M Risk Reduction process such as shown in Figure 5?
- Is the origin of any specific item of evidence unambiguously linked to specific R&M Practice(s) and/or Control process(es)?
- Are the links between any specific item of evidence and the R&M Risk Register, Strategy, and R&M Plan clearly shown?
- Is the status of each item of evidence readily identified in the Evidence Framework in terms of its relevance, completeness, accuracy, and how it has been used to influence the system and reduce risk?

Summary

The R&M Case approach represents a cooperative approach in stark contrast to the historic R&M prescriptive approach, heavily reliant upon the use of “hard-line standards”. An R&M Case is closely linked with the R&M Plan and is the sum total of all the R&M evidence that is generated by the engineering design activities, trials and testing, and in-service or field data.

To meet the R&M requirements, the R&M Case, in conjunction with the R&M Plan, provides the evidence by which the following objectives are demonstrated:

- The R&M requirements of the customer are determined and demonstrated to be understood by both the customer and the supplier.
- Strategies are developed in the R&M Plan resulting in a program of R&M activities together with applicable success criterion, which demonstrate that their implementation will satisfy the R&M requirements.
- The customer is provided with progressive assurance that the R&M requirements will be satisfied.
- The R&M Risks and management strategy are clearly identified in meeting the R&M requirements.
- The creation of R&M Case (Status) Reports which record how the R&M requirements are met through all stages of procurement through to in-service operation.

For Future Study

1. Def Stan 00-42 (PART 3) “Reliability and Maintainability Assurance Guide Part 3: R&M Case” (Issue 2 06-Jun-03).
2. Herrmann, Peercy D. “Software Reliability Cases: The Bridge Between Hardware, Software and System Safety and Reliability”, 1999 R&M Symposium, Page 398-402.
3. Def Stan 00-55 “Safety Critical Software” (Issue 2).
4. SAE JA1002 “Software Reliability Program Standard” (January 2004).
5. SAE JA1003, “Software Reliability Program Implementation Guide” (January 2004).
6. SAE JA1004 “Software Supportability Program Standard” (January 2004).
7. SAE JA1005 “Software Supportability Program Implementation Guide” (January 2004).
8. SAE JA 1010-1 “Maintainability Program Standard Implementation Guide” (to be published).

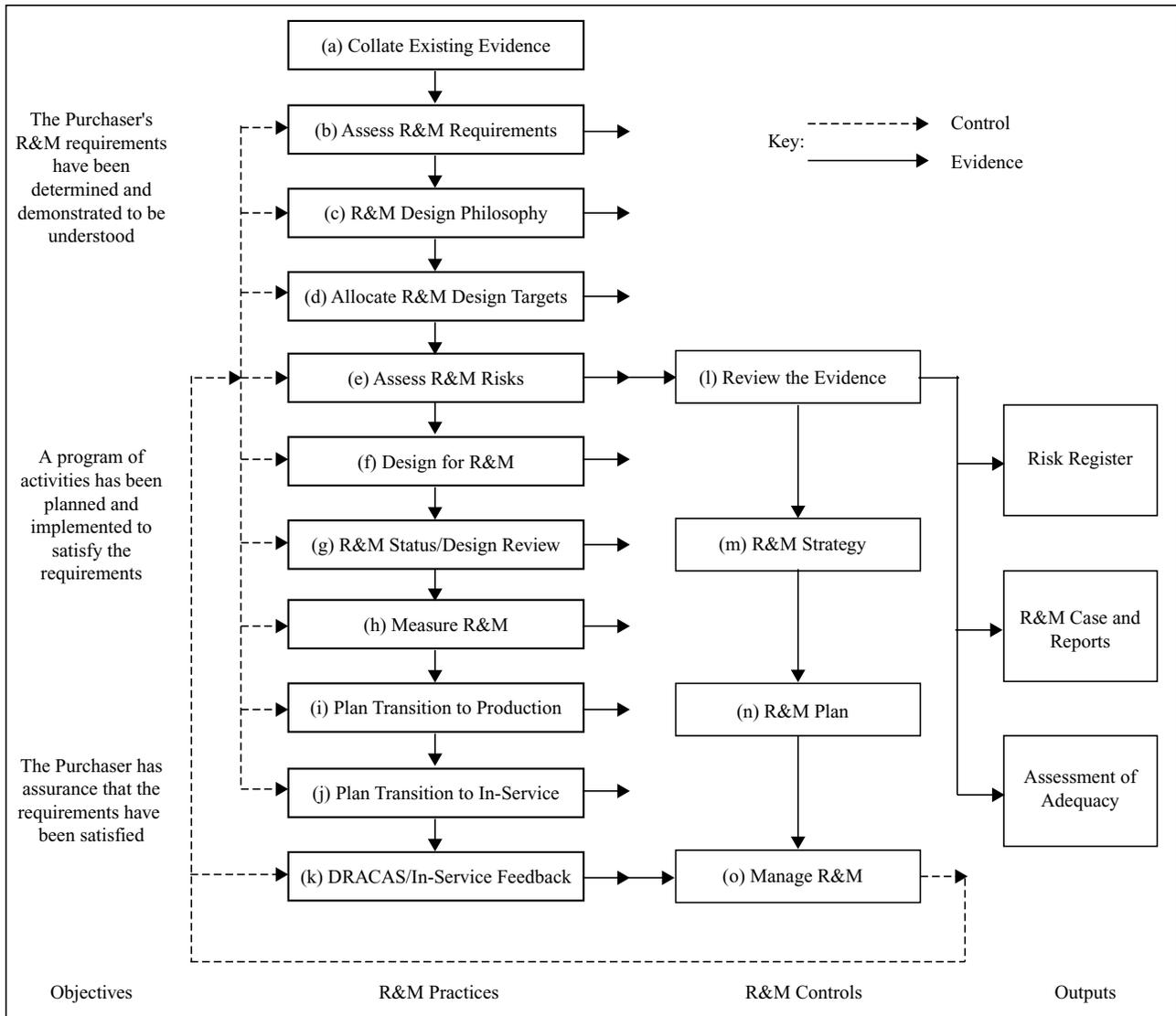


Figure 5. Risk Reduction Process

- Jones J.A., Marshall J., Newman R. "The Reliability Case In The REMM Methodology" Annual R&M Symposium (January 2004).

About the Author

Norman B. Fuqua is a Senior Engineer with Alion Science and Technology. He has 44 years of varied experience in the field of dependability, reliability, and maintainability and has applied these principles to a variety of military, space and commercial programs. At Alion Science and Technology, and its predecessor IIT Research Institute (IITRI), he has been responsible for reliability and maintainability training and for the planning and

implementation of various dependability, reliability, and maintainability study programs.

Mr. Fuqua developed unique distance learning Web-based and Windows™-based computer-aided reliability training courses. He is the developer and lead instructor for the Reliability Analysis Center's (RAC) popular Electronic Design Reliability Training Course. This three-day course has been presented over 200 times to some 7,000 students in the US, England, Denmark, Norway, Sweden, Finland, Germany, Israel, Canada, Australia, Brazil, and India. Audiences have included space, military, industrial, and commercial clients.

He was also the lead developer and instructor for a two-day Dependability Training Course for an Automotive Supplier and a three-day Robust Circuit Design Training Course. These courses enable mechanical and electronic design engineers and reliability engineers to utilize advanced software-based tools in producing designs that exhibit minimum sensitivity to both internal and external variations.

Mr. Fuqua holds a Bachelor of Science degree in Electrical Engineering from the University of Illinois, Urbana Illinois, is a Registered Professional Engineer (Quality Engineer) in California (retired), and a Senior Member of the IEEE and the IEEE Group on Reliability.

He is a former Member of the Editorial Board, "Electrical and Electronics Series", for Marcel Dekker Inc., and the Education and Training Editor for the "SAE Communications in Reliability, Maintainability and Supportability Journal". He is also a former Member of the EOS/ESD Association, and Chairman of three different EOS/ESD Association Standards Committees.

He is the author of a number of technical papers, twenty RAC publications and a reliability college textbook published by Marcel Dekker Inc.

Other START Sheets Available

Many Selected Topics in Assurance Related Technologies (START) sheets have been published on subjects of interest in reliability, maintainability, quality, and supportability. START sheets are available on-line in their entirety at <<http://rac.alionscience.com/rac/jsp/start/startsheet.jsp>>.

For further information on RAC START Sheets contact the:

Reliability Analysis Center
201 Mill Street
Rome, NY 13440-6916
Toll Free: (888) RAC-USER
Fax: (315) 337-9932

or visit our web site at:

<<http://rac.alionscience.com>>



About the Reliability Analysis Center

The Reliability Analysis Center is a Department of Defense Information Analysis Center (IAC). RAC serves as a government and industry focal point for efforts to improve the reliability, maintainability, supportability and quality of manufactured components and systems. To this end, RAC collects, analyzes, archives in computerized databases, and publishes data concerning the quality and reliability of equipments and systems, as well as the microcircuit, discrete semiconductor, and electromechanical and mechanical components that comprise them. RAC also evaluates and publishes information on engineering techniques and methods. Information is distributed through data compilations, application guides, data products and programs on computer media, public and private training courses, and consulting services. Located in Rome, NY, the Reliability Analysis Center is sponsored by the Defense Technical Information Center (DTIC). Alion, and its predecessor company IIT Research Institute, have operated the RAC continuously since its creation in 1968. Technical management of the RAC is provided by the U.S. Air Force's Research Laboratory Information Directorate (formerly Rome Laboratory).