# CHAPTER 7

# R&M AS A SYSTEM ENGINEERING DISCIPLINE

## CONTENTS

## 1. INTRODUCTION

1.1 Systems engineering is an interdisciplinary field of engineering focusing on how complex engineering projects should be designed and managed throughout their life cycles to achieve the most cost-effective solution possible whilst ensuring that the product is available for as high a proportion of time as possible. Systems engineering deals with work-processes and tools to manage risks throughout the life of such projects. One area of risk is Availability, Reliability and Maintainability (ARM), this chapter explains the integrated nature of ARM requirements and their relationship with functional and other requirements.

1.2 When investigating systems engineering, and looking for authoritative sources, it is widely accepted that, due to the enormous amounts of time, money, evaluation and research spent by NASA on the subject, their systems engineering handbook is one of the best guides available. Other guides such as the INCOSE systems engineering handbook and ISO-IEC 15288:2008 are available and offer similar advice but this chapter uses the NASA systems engineering handbook as its primary source.

1.3 **Availability Reliability Maintainability**

> 1.3.1 Availability can be defined as the ability to be in a state to perform as required, under given conditions, at a given instant, or over a given time interval.
>
> 1.3.2 Reliability can be defined as the ability of a system or component to perform its required functions under stated conditions for a specified period of time.

1.3.3 Maintainability can be defined as the probability that a given maintenance action, performed under stated conditions and using stated procedures and resources, can be carried out within a stated time interval.

## 2. RELATIONSHIPS AND DEPENDENCIES

2.1 Availability can be calculated using the formula: Availability = $\frac{\textbf{Uptime}}{\textbf{Uptime + Downtime}}$

2.1 Uptime can be, simplistically, defined as the amount of time the system is in a fully usable condition, this can be heavily influenced by the reliability of the system. Downtime is the amount of time when the system is not in a fully usable condition and can be heavily influenced by the number of instances when it is required to carry out scheduled maintenance and the amount of times faults or failures occur which make the system unusable requiring unscheduled maintenance tasks to be carried out.

2.3 It should be clear from these relationships and dependencies, coupled with the overall aim of systems engineering, that reliability and maintainability need to be addressed from as early in the project as possible and treated as ongoing concerns throughout the life of the project.

2.4 The NASA system engineering handbook defines system engineering thus: "*System engineering is a robust approach to the design, creation, and operation of systems. In simple terms, the approach consists of identification and quantification of system goals, creation of alternative system design concepts, performance of design trades, selection and implementation of the best design, verification that the design is properly built and integrated, and post-implementation assessment of how well the system meets (or met) the goals.*" In MOD projects the goals which are referred to would be the System Requirements, always remembering that the aim of systems engineering is to achieve these by the most cost-effective means.

2.5 It then goes on to identify only six areas as being specialty engineering disciplines, these are: Safety and Reliability, Quality Assurance, ILS, Maintainability, Producibility, and Human Factors. It offers an overview of these specialty engineering disciplines to give systems engineers a brief introduction. It should be noted that both Reliability and Maintainability are identified, meaning those two areas account for one third of specialty engineering disciplines.

2.6 In its attempt to demonstrate the importance of Reliability within the systems engineering environment the NASA handbook states: "*A reliable system ensures mission success by functioning properly over its intended life. It has a low and acceptable probability of failure, achieved through simplicity, proper design, and proper application of reliable parts and materials. In addition to long life, a reliable system is robust and fault tolerant, meaning it can tolerate failures and variations in its operating parameters and environments.*" One factor that should be pointed out here is that, within the MOD, we would not necessarily place the major emphasis on a low probability of failure, it is far more important that the risks are fully understood and an acceptable level of failure is achieved.

2.7 It follows this with a description of where it sees Safety and Reliability engineering fitting into the system design process by stating: "*A focus on safety and reliability throughout the mission life cycle is essential for ensuring mission success. The fidelity to which safety and* *reliability are designed and built into the system depends on the information needed and the type of mission. It states that, for human-rated systems, safety and reliability is the primary objective throughout the design process, adding that for science missions, safety and reliability should be commensurate with the funding and level of risk a program or project is willing to accept, but stressing that, regardless of the type of mission, safety and reliability considerations must be an intricate part of the system design processes. To realise the maximum benefit from reliability analysis, it is essential to integrate the risk and reliability analysts within the design teams. The importance of this cannot be overstated. In many cases, the reliability and risk analysts perform the analysis on the design after it has been formulated. In this case, safety and reliability features are added on or outsourced rather than designed in. This results in unrealistic analysis that is not focused on risk drivers and does not provide value to the design. Risk and reliability analyses evolve to answer key questions about design trades as the design matures. Reliability analyses utilise information about the system, risk sources and drivers, and provide an important input for decision making."*

2.8 It then goes on to couple Reliability with Maintainability by referring to *NASA-STD-8729.1, Planning, Developing, and Maintaining an Effective Reliability and Maintainability (R&M) Program,* which outlines engineering activities that should be tailored for each specific project. The concept explained is to choose an effective set of reliability and maintainability engineering activities to ensure that the systems designed, built, and deployed will operate successfully for the required mission life cycle. In the early phases of a project, risk and reliability analyses help designers understand the interrelationships of requirements, constraints, and resources, and uncover key relationships and drivers so they can be properly considered. It further states: "*The analyst must help designers go beyond the requirements to understand implicit dependencies that emerge as the design concept matures, accepting that it is unrealistic to assume that design requirements will correctly capture all risk and reliability issues and "force" a reliable design*". Pointing further to the link between Reliability and systems engineering it explains the systems engineer should develop a system strategy mapped to the product breakdown structure on how to allocate and coordinate reliability, fault tolerance, and recovery between systems both horizontally and vertically within the architecture to meet the total mission requirements and that system impacts of designs must play a key role in the design, whilst stressing the importance of ensuring that designers are made aware of the fact that the impacts of their decisions on overall mission reliability is a key factor. It notes that as the design matures, reliability analysis occurs using established techniques, of which it offers the following, which form part of the R&M tool-set, as examples:

> 2.8.1 Event sequence diagrams/event trees are models that describe the sequence of events and responses to off-nominal conditions that can occur during a mission. See GR77 Pt C Ch 34
>
> 2.8.2 Failure Modes and Effects Analyses (FMEA) is a method of establishing the effect of failure within systems or processes; when applied to processes it is called a Process FMEA. This analysis can be performed at any level of an individual assembly. This may also be done together with a criticality analysis (CA). The combined exercise is then called a Failure Modes, Effects and Criticality Analysis (FMECA). See GR77 Pt C Ch 33

2.8.3 Qualitative top-down logic models identify how failures within a system can combine to cause an undesired event. See GR77 Pt A Ch 9

2.8.4 Quantitative logic models (probabilistic risk assessment) extend the qualitative models to include the likelihood of failure. These models involve developing failure criteria based on system physics and system success criteria, and employing statistical techniques to estimate the likelihood of failure along with uncertainty. See GR77 Pt A Ch 9

2.8.5 Reliability block diagrams are diagrams of the elements to evaluate the reliability of a system to provide a function. See GR77 Pt C Ch 30

2.8.6 Preliminary Hazard Analysis is performed early based on the functions performed during the mission. It is a “what if” process that considers the potential hazard, initiating event scenarios, effects, and potential corrective measures and controls. The objective is to determine if the hazard can be eliminated, and if not, how it can be controlled. See GR77 Pt B Ch 7

2.7.7 Hazard analysis evaluates the completed design using the principles and methods as preliminary hazard analysis. See GR77 Pt B Ch 7

2.8.8 Human reliability analysis is a method to understand how human failures can lead to system failure and estimate the likelihood of those failures. See GR77 Pt C Ch 31 & 32

2.8.9 Probabilistic structural analysis provides a way to combine uncertainties in materials and loads to evaluate the failure of a structural element. More information can be found at: http://www.tc.faa.gov/its/worldpac/techrpt/ar99-2.pdf

2.8.10 Sparing/logistics models provide a means to estimate the interactions of systems in time. These models include ground-processing simulations and mission campaign simulations. See JSP886 Vol7 Pt 8.10 Ch 2 Sect IV

2.9 The design and concept of operations should be thoroughly examined for accident initiators and hazards that could lead to mishaps. Conservative estimates of likelihood and consequences of the hazards can be used as a basis for applying design resources to reduce the risk of failures. The team should also ensure that the goals can be met and failure modes are considered and take into account the entire system and that, during the latter phases of a project, the team uses further risk assessments and reliability techniques to verify that the design is meeting its risk and reliability goals and to help develop mitigation strategies when the goals are not met or discrepancies/failures occur.

2.10 Maintainability engineering is another major specialty discipline that contributes to the goal of a supportable system. This is primarily accomplished in the systems engineering process through an active role in implementing specific design features to facilitate safe and effective maintenance actions in the predicted physical environments, and through a central role in developing the ILS system. Example tasks of the maintainability engineer include: developing and maintaining a system maintenance concept, establishing and allocating maintainability requirements, performing analysis to quantify the system’s maintenance resource requirements, and verifying the system’s maintainability requirements.

2.11 More information on the importance of Maintainability can be found in GR77 Pt G Lflt 4

2.12 There may be limitations on the use of reliability analysis. The engineering design team must understand that reliability is expressed as the probability of mission success and that, as most will already know, probability is a mathematical measure expressing the likelihood of occurrence of a specific event. Therefore, probability estimates should be based on engineering and historical data, and any stated probabilities should include some measure of the uncertainty surrounding that estimate. Uncertainty expresses the degree of belief analysts have in their estimates and uncertainty decreases as the quality of data and understanding of the system improve. Initial estimates of failure rates or failure probability might be based on comparison to similar equipment, historical data (heritage), failure rate data from handbooks, or expert elicitation. Possible limitations when utilising reliability analysis are:

2.12.1 Reliability estimates express probability of success.

2.12.2 Uncertainty should be included with reliability estimates.

2.12.3 Reliability estimates combined with FMEAs provide additional and valuable information to aid in the decision making process.

2.13 It can be seen from the information above, that factors affecting reliability and maintainability, if not addressed early enough in the project life cycle, will impact greatly upon other all other areas of the project leading, potentially, to an equipment performing, and delivering, to less than optimum standards and failing to meet the requirements unless substantially more resources, in terms of manpower, cost and time, are expended at a later date.

2.14 Given the statement that Systems Engineering is an interdisciplinary field of engineering focusing on how complex engineering projects should be designed and managed throughout their life cycles to achieve the most cost-effective solution possible, the following paragraphs highlight how R&M can impact costs:

2.14.1 Lower R&M leading to higher equipment costs – equipment that fails more frequently and with less predictability will be unavailable for a greater percentage of time. In order to meet the system requirements, in simplistic terms, the only way to overcome this would be to acquire larger numbers of ineffective equipment.

2.14.2 Lower R&M leading to higher maintenance costs – equipment that fails more frequently and with less predictability will require longer and more repetitive periods of unscheduled maintenance. This will necessitate either the same number of personnel, each performing more of the same task, or a higher number of personnel performing a reduced number of the same task each. Either of these options means a higher number of man-hours spent on maintenance. Both of these options will incur additional cost.

2.14.3 Lower R&M leading to higher spares costs – equipment that fails more frequently and with less predictability will need more spares available in order to maintain the required levels of availability. This will be seen in both the initial provisioning of spares and the number of spares required to support the equipment throughout its life cycle. This will have knock-on effects impacting on the logistics footprint of the equipment which could be further highlighted if, for example, the equipment was used in multiple, wide spread locations or was a piece of mobile, deployable equipment.

2.14.4 Lower R&M leading to higher mission/purpose failure rates – equipment that fails more frequently and with less predictability is less likely to be able to successfully complete any tasks placed upon it. This could lead to the need to employ a higher number of equipments to achieve the stated goal or drive the necessity to accept a higher mission failure rate.

2.14.5 Lower R&M leading to increased safety risk – safety is another area where reliability can have an enormous impact, highlighted by the fact that in the NASA systems engineering handbook they classify it as safety and reliability engineering. Equipment that fails more frequently and less predictably, which is in any way safety related, will lead to unacceptably high risk.

## 3. CONCLUSIONS

3.1 If R&M disciplines are not included within the tool-set available to system engineers, from the earliest phase of the project, there is a very low probability that the equipment designed will be able to meet any requirements set by the purchasing authority.

3.2 Failure to address R&M adequately, from the earliest possible point in the program, will undoubtedly cause poor reliability which will, in turn, lead to poor availability which will cause inevitable increases in expenditure of resources regardless of whether that increase is measured in terms of performance, cost or time.

3.3 R&M impacts upon many, if not all, other disciplines within the system engineering environment. As explained above these will include, but are not limited to, safety, logistic planning, logistic support and associated costs, initial and ongoing equipment costs, manpower costs and success rates.

3.4 It is worth noting in the diagram below, detailing the components contributing to system effectiveness, taken from the NASA systems engineering handbook, that the only factor mentioned twice is reliability.

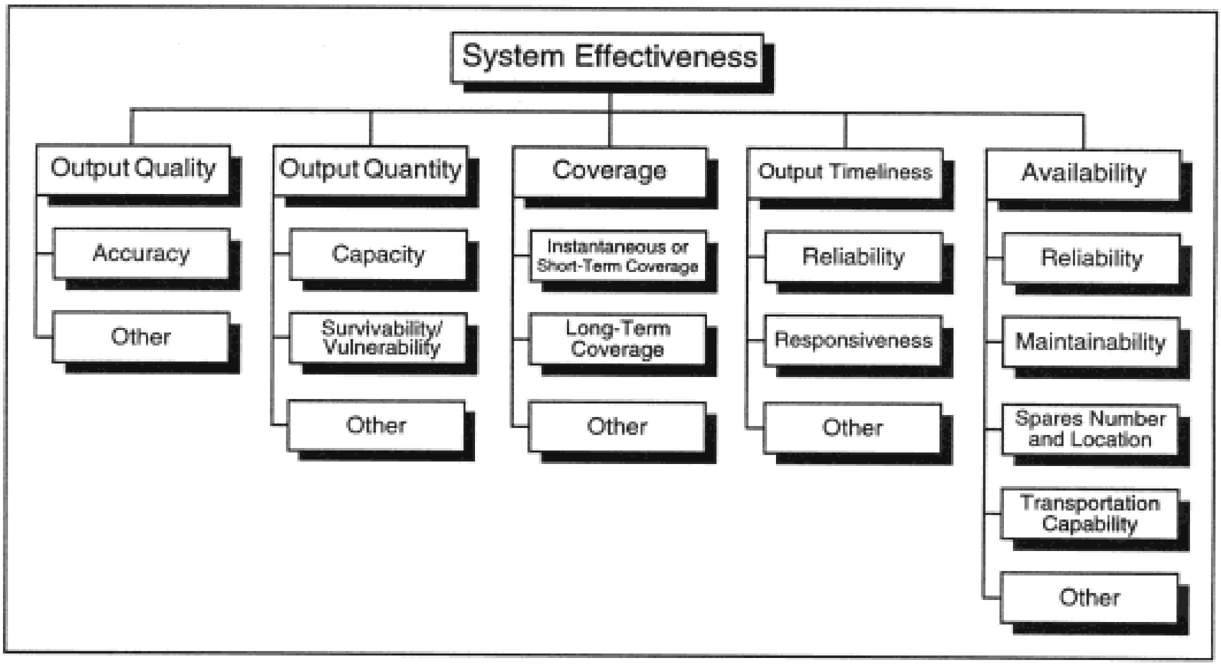

Figure 26 — System Effectiveness Components (Generic).

## 4. RECOMMENDATIONS

4.1 The R&M tool-set should be highlighted to system engineering practitioners as one of the more important areas within the discipline.

4.2 The R&M tool-set should be fully utilised within the project from the earliest possible opportunity.

4.3 The R&M tool-set should be used to ensure a robust through-life reliability and maintainability plan is produced as early as possible in the project. This should feed directly into the Project Management Plan.

4.4 The overarching project risk register should include at least one entry relating to R&M as one of the main project risks which may be referred to as a Key User Requirements.

4.5 It is important to note that, whilst systems engineering, with particular reference to R&M, may well be carried out at all levels within a system it is imperative to ensure that the constituent parts are not only looked at in a stand alone way. They should also be looked at with an overarching systems engineering approach to ensure matters such as interfaces and integration are taken into consideration from the earliest possible point in the project. This may be particularly relevant in COTS projects aiming to combine various elements from a range of suppliers.

## 5. REFERENCES

DefStan 00-49 issue 2
NASA System Engineering Handbook