GUIDE ON THE DESIGN FOR SAFETY AND RELIABILITY

Institution of MECHANICAL ENGINEERS

This document describes good Safety and Reliability engineering practice, which embeds the key factors and if followed should ensure that customers' expectations are met.

Improving the world through engineering

GUIDE ON DESIGN FOR SAFETY AND RELIABILITY

CONTENTS

SCOPE

This guide offers general guidance on how to plan for and meet the Safety and Reliability (S&R) requirements of a product, eg equipment, system, service. It aims to provide everyone associated with designing, manufacturing, operating or maintaining products with:

- Best practice for a cross-industry approach to Safety and Reliability
- A framework for engineers to recognise Continuing Professional Development (CPD) needs and a staged approach to the development of competence, particularly for developing engineers
- A Capability Maturity Model (CMM) that will allow an organisation to assess its (and its suppliers') level of maturity in Safety and Reliability engineering practices

The Safety and Reliability engineering disciplines are examined, including definitions, explaining their interrelationships and their importance, generally and at specific times during development, production, operation and maintenance phases of product life cycle.

In addition, the guide includes advice on the competence of personnel and methods of assessing the overall level of capability of the organisation.

FOREWORD

The IMechE code of conduct requires that all members "conduct their professional work and relationships with integrity and objectivity and with due regard for the welfare of the people, the organisations and the environment with which they interact" and "take reasonable steps to maintain appropriate professional competences".

Safety and Reliability are interdependent and fundamental aspects of engineering system behaviour and performance. They are part of the responsibility of everyone in the organisation. They are affected by all the decisions made throughout the life cycle.

Customers want products that work and go on working for a 'reasonable' period of time. There is also the expectation that products will not result in harm. If the customer's expectations are not met they may regard the equipment or service as 'unsafe' or 'unreliable'. Unsafe products are likely to lead to accidents resulting in injury, ill health, environmental or property damage, legal action, fines or even a criminal record. Dissatisfaction through poor reliability is likely to lead to lost business, which would then be difficult to recover. In today's highly competitive markets it is therefore worth recognising that it is not 'Safety' or 'Reliability' themselves that sell, but their benefits. Benefits of good Reliability include the need to keep fewer spares, carry out fewer inspections, reduced maintenance, increased availability, more marketable products, lower operating costs and ultimately increased profitability.

Minimum requirements for Safety are enshrined in law around the world. Safety and Reliability of specific types of equipment are contained within European and international standards. Clients, recognising the costs associated with poor Safety and Reliability, may also stipulate minimum requirements in procurement contracts.

Factors that have the greatest influence on Safety and Reliability are:

Design – ensuring a product is fit for purpose, relative to the required use and operating environment
Manufacture – ensuring a product is to as high and consistent a standard as appropriate to meet the requirements, and economically viable
Operation – ensuring adequate consideration is given to usability and foreseeable misuse
Maintenance – the remedial measures required to sustain the operation of the product must be achievable in an economic, safe and timely manner

This guide describes good Safety and Reliability engineering practice, which embeds these four factors and, if followed, should ensure that expectations are met. It provides an aide-mémoire to all personnel with experience in Safety and Reliability, and a primer of the essentials of what to expect for those who have no, or limited, experience.

Guidance is given about formal techniques which can establish and maintain confidence that the product will perform as designed when required to, and for as long as necessary. Management commitment to these techniques is vital, as is knowledge of the circumstances in which they should be applied.

Modern practices are tending towards a new term, 'dependability', taken to cover many activities associated with the Safety and Reliability engineering discipline.

Introduction: What are Safety and Reliability?

Safety and Reliability are defining characteristics of a product's performance and life cycle costs. In the context of this guide, it is understood that:

Safety is the visible and demonstrable absence of unacceptable risk of undesirable events affecting the health and safety of the workforce and the public at large.
Reliability is the ability of an item to perform a required function under stated conditions, including environment and usage, and for a stated time.

The aims of the Safety and Reliability engineering discipline, as part of an integrated team, are to:

- Specify and agree a product's Safety and Reliability requirements as appropriate
- Enable the assessment of the acceptability of design proposals from the point of view of Safety and Reliability
- Satisfy customer, operator, regulatory authority and legal requirements
- Co-ordinate and monitor the Safety and Reliability activities of suppliers
- Contribute to defining maintenance planning and logistic support functions
- Develop solutions to mitigate identified risks, which may lead to:
    1. Acceptance (because the risks are found to be tolerable)
    2. Recommending actions to eliminate the problem, or minimise its probability of occurrence (periodic checks, etc)
- Monitor in-service performance to ensure that Safety and Reliability requirements are being achieved, while cost of ownership is not adversely affected

When do we engineer for Safety and Reliability?

It is important to consider Safety and Reliability at all stages of the design process, and throughout the product life cycle. S&R characteristics should be included as an explicit design requirement, as consideration at the early stages of design contributes most significantly to the success or failure of the final product. It becomes increasingly difficult and costly to influence the Safety and Reliability of a product once the detail design stage has been reached. For maximum benefit, efforts should start as early in a product's life cycle as possible, noting that empirically the 1:10:100 rule applies (ie at each life cycle stage, final product costs increase by an order of magnitude).
Safety and Reliability of equipment cannot be enhanced by maintenance, only preserved.

How do we engineer for Safety and Reliability?

Engineering for Safety and Reliability requires:

- An overall integrated approach to the design process
- Interpretation of requirements
- Appropriate quantification of risk areas (including lessons learned from past experience)
- Development of appropriate engineering solutions
- Methods for assurance of achieving Safety and Reliability requirements
- Commitment and discipline from management, the team and the individual

Good, well-thought-out product requirements (including usage, environment, support) are an essential part of a robust, appropriate specification, which is in turn paramount for a successful product.

Both ‘Safety-related’ and ‘Reliability-related’ risks may be identified and managed using the same methods, although industry standards often split the two types for ease of handling in larger organisations. Pragmatism should be exercised to ensure preference is not given to managing one at the expense of the other to achieve an agreed and reasoned balance. Thus do only what is absolutely necessary, but what is necessary should be done absolutely.

APPLICATION OF PRINCIPLES FOR ENSURING SAFETY AND RELIABILITY IN DESIGN

Dependability Cycle Model

A company's maturity with regards to practices regarding safety and reliability in design can be separated into three indicators, with corresponding key processes, namely:

- Formal risk analysis and demonstration of reliability
- Implementation of reliability achievement and improvement strategy
- Longer term investments in reliability Management

Or more simply – "planning", "doing" and "sustaining". These can be arranged into a "dependability cycle" as shown in the model below.

THE KEY PROCESSES

A company's maturity with regards to practices regarding Safety and Reliability in design can be separated into three distinct categories, with corresponding Key Processes (KPs):

1. Formal risk analysis and demonstration of Reliability
2. Implementation of Reliability achievement and improvement strategy
3. Longer-term investments in Reliability management

Or more simply – 'planning', 'doing' and 'sustaining'. These Key Processes are summarised in Table 1, and described in detail in the subsequent sections.

Maturity characteristic	KP No	Key Processes
Formal risk analysis and demonstration of Reliability	1.	Setting and allocating Safety and Reliability requirements
	2.	Demonstration of Safety and Reliability in design
	3.	Process verification, validation and benchmarking
	4.	Safety and Reliability and risk reduction in design
Implementation of Reliability achievement and improvement strategy	5.	Safety and Reliability analysis and risk in design
	6.	Project risk management
	7.	Safety and Reliability testing in design and development
	8.	Failure reporting, analysis and corrective action system
	9.	Supply chain management
	10.	Management of change and life cycle transitions
	11.	Management of transition from development to production
Longer-term investments in Reliability management	12.	Feedback and organisational learning
	13.	Education and training in Safety and Reliability
	14.	Research and development in Safety and Reliability

Table 1 – Maturity characteristics and associated Key Processes

The implementation of Safety and Reliability through design centres on the deployment of core engineering design principles supported by the factors determined during the planning phase. This section focuses on Key Processes that should be deployed to support design activities to achieve the Safety and Reliability & Maintenance Cases. **See Annex 1 for details.**

WHY DESIGNING FOR SAFETY AND RELIABILITY IS IMPORTANT

Many industries require a minimum level of performance for Safety; this is covered by legislation and regulated by external bodies, such as the HSE in the UK. This should, by default, infer a level of Reliability performance, although it is by no means guaranteed. A safe system need not be a reliable system but a reliable system is usually a safe system, as there are fewer excursions from normal operating window, a reduced workload on operations and maintenance personnel, and more time for management to concentrate on proactive work. Defining and adhering to sensible engineering practices should mean that Safety and Reliability are relatively assured. Unlike Safety, a minimum level of Reliability is not usually required through legislation for most applications, but the more reliable the equipment the more successful the business will be – resulting in improved uptime, lower operating costs and more sales.

The principle of 'As Low As Reasonably Practicable' (ALARP) with regards to Safety risk is covered by UK legislation, and the same principle should also be applied to Reliability-related risk. Minimum detriments are set for managing Safety-related risk in many industries (eg the cost of a life), although the same cannot be said for Reliability-related risks. Those wishing to set levels for Reliability performance will have to determine the potential financial and reputational implications arising from their particular application.

Safety and Reliability of equipment, or a system, must be designed in from the start. Even at the concept stage, full knowledge of capability and performance requirements should be sought. This must include the intended usage, operational environment, expected life, type and frequency of use and experience and competence of end-users, support and maintenance plans and whole life costs. The potential effect of in-service design changes, updates and especially new technology must also be addressed. This is sometimes referred to as 'future proofing'.

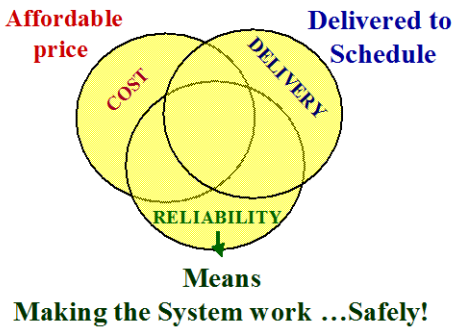
SAFETY AND RELIABILITY IN DESIGN AS BUSINESS GOALS

High-level organisational goals are defined by legal and corporate standards, customer requirements, business needs and ethical requirements. These core goals usually incorporate a combination of the following:

1. Health and Safety
2. Environment
3. Quality
4. Product cost

Delivery

The fact that the system must work safely and reliably in operation, while an obvious necessity, is not always articulated as a specific design requirement. In addition to the core business goals there are a large number of design, functional and operational goals. These goals are concerned with the way that the system will work in practice and must be achieved without compromising the core high-level business goals. Reliability essentially measures the probability that all these system requirements have been met.



The specific issue facing companies is how to achieve the combined goals of:
Reliability – to ensure sustained performance
Delivered to schedule
Acceptable cost
This is not an easy task. While most project teams can deliver a system to cost and schedule, only the best will be able to achieve all three, Reliability being an important characteristic of performance and whole life costs.

Figure 1: Project Goals

There are numerous factors to be considered in achieving Reliability, and hence Safety, some of which could be inadequately taken into account during design or emerge during life cycle. The life cycle must be considered to be 'cradle to grave', therefore both manufacture and dismantling/disposal of the equipment must be given as much thought as operation and maintenance. These influencing factors include, but are not limited to:

1. Environmental conditions
   - Temperature range
   - Cyclic temperature
   - Humidity
   - Atmospheric neutron radiation

2. Material changes due to global legislation
   - Lead-free solder – joint integrity
   - Plating materials (eg cadmium no longer allowed) – increased corrosion rates

3. Emergent technology developments
   - Shrinking device architectures and operating parameters
   - Silicon wear-out

4. Treatment and care of ancillary equipment
   - Protection from temperature, humidity, dust
   - Protection from various fluid mists

5. No Fault Found (NFF) events
   - Various technical, operational and management issues contribute to NFF events, especially in electronic equipment

6. Effects of ageing
   - Deterioration of electrical cable insulation
   - Wear
   - Corrosion
   - Structural fatigue

7. Other issues of note
    - Manufacturing techniques and 'built-in latent defects'
    - Obsolescence
    - Counterfeit components
    - Owner/operators remote from designer/manufacturer
    - Warranty periods

SAFETY VS RELIABILITY AND THE VALUE OF SAFETY AND RELIABILITY

In accordance with the definitions given in BS5760, there is a key differentiator between risk handled as 'Safety related' and that handled as 'Reliability related'. For a risk to be 'Safety related', the end consequence due to it being realised must be tangible harm, to equipment or more likely to people. Safety risks are generally subject to given boundaries of consequence, which are usually enshrined in regulation or industry good practice, whereas Reliability risks are generally not.

Figure 2 (below) depicts a typical Risk Assessment Matrix (RAM) for a fictitious company. RAMs may be used to correlate the consequences of an event with the probability of occurrence and can also help to differentiate if a Safety or a Reliability consequence would be more damaging to a company. Therefore, issues that may previously have been dismissed as being trivial due to low Safety consequences, may be reclassified as significant on a Reliability basis.

Consequence		Reliability International Co.				
Safety	**Cost**					
Result in a major safety incident affecting more than one person	Result in major financial losses leading to loss of jobs	**5**	**5**	**10**	**15**	**20**	**25**
Result in a major safety incident	Result in major financial losses	**4**	**4**	**8**	**12**	**16**	**20**
Result in a moderate safety incident	Result in moderate financial losses	**3**	**3**	**6**	**9**	**12**	**15**
Result in a minor safety incident	Result in minor financial losses	**2**	**2**	**4**	**6**	**8**	**10**
No concern	No concern	**1**	**1**	**2**	**3**	**4**	**5**
		Probability	**1**	**2**	**3**	**4**	**5**
Risk Assessment Matrix			Likely to happen once in ten years	Likely to happen once in five years	Likely to happen once in two years	Likely to happen once per year	Likely to happen more than once per year

Figure 2

Risks of all types are also generally subject to screening for credibility. Efforts are made to engineer tolerance to, or otherwise manage, reasonably foreseeable risks that have some probability of occurrence. Equipment tolerance to incredulous risks (ie high consequence yet extremely low frequency/probability, or those below the minimum consequence boundary) is generally achieved through adherence to industry good practice and use of proven, sound engineering practices. These would equate to the blue and green regions in the RAM above.

MEASURING RELIABILITY CAPABILITY

Reliability over the long term can be measured by observing the actual Reliability performance of suppliers' equipment in the field. In the short term however, measurement of an organisation's Reliability practices capability provides a valuable indicator of the future performance potential of equipment. A Capability Maturity Model (CMM) has been developed, therefore, to assess the Reliability capability of manufacturers (Figure 3). The characteristics which define the Reliability capability of an organisation are described below.

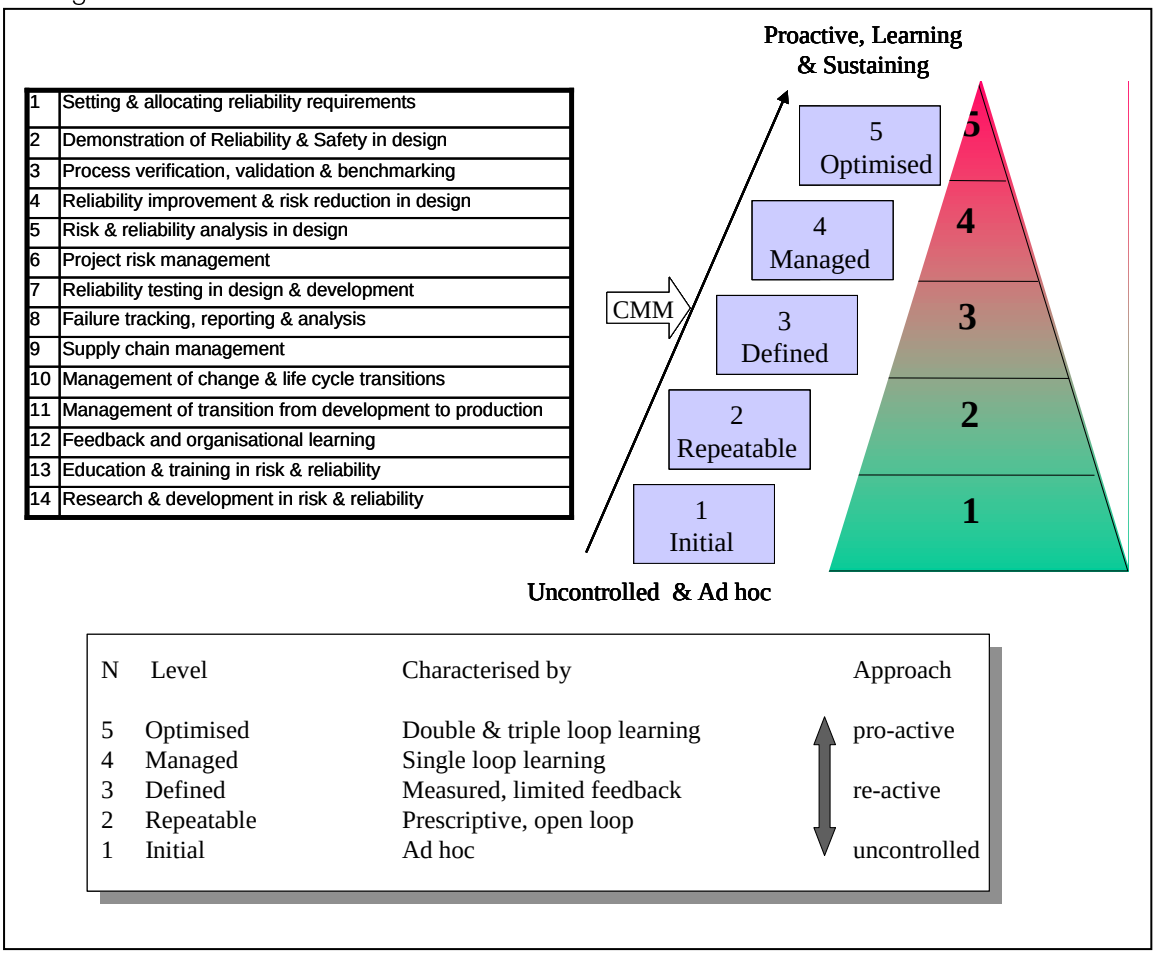


Figure 3: Reliability Capability Maturity Model and Key Processes

Five levels of Reliability capability have been defined:

1. Initial (no risk response)
2. Repeatable (immediate risk response)
3. Defined (risk response on product development)
4. Managed (risk response for product and processes)
5. Optimised (risk response for product, processes and organisation)

Research into the application of the CMM suggests that Reliability capability will be highly dependent on the degree to which the organisation invests effort in organisational learning and knowledge management. This in turn depends on a company's strategy for achieving its performance goals.

Management attention can focus on different aspects of its business. In general, these can be grouped into the following broad perspectives:

- Manufacture of product
- Processes (necessary for manufacturing)
- Preparedness to perform processes

Knowing this provides a basis for making judgements on the Safety and Reliability capability of an organisation. The most capable and sustainable organisations will be those adopting a balanced approach, investing effort at all steps through a product's life cycle. The highest levels of capability are awarded to those organisations investing effort, and adapting to information flows, at the level of process and organisational preparedness. The five levels are defined as follows and summarised in Figure 4.

Level 1: Initial

At this level the organisational approach to Reliability is reactive and ad hoc. There is no consistency in equipment Reliability, no formal Reliability processes and no knowledge of Reliability performance.

Level 2: Repeatable

This level is achieved when the manufacturing organisation has quality processes in place and is capable of generating a repeatable consistency, but without any knowledge of equipment Reliability and no specific processes to improve Reliability performance or reduce risk. The response to risk and failure is essentially open loop. Education and training and R&D are not focused on Reliability management or equipment Reliability improvements.

Level 3: Defined

The level 3 organisation is defined and measured. It has key procedures and practices in place to define Reliability such as:

- The setting of Reliability requirements
- The performance of risk and Reliability analysis in design
- Reporting, tracking and analysis of Reliability data

However, at this level the processes for the management of risk and Reliability improvement are limited to immediate project issues. There is some learning by

individuals exposed to failures and performance information, but it is not fully organised knowledge. There is a little feedback to equipment but the response is largely reactive and limited to equipment on current projects. The mode of organisational learning is, therefore, characterised as reactive, single-loop learning. The approach to risk is via a phased audit and review with quantification at component failure level. Education and training and R&D processes are limited to those needed to support immediate project issues.

Level 4: Managed

At level 4, organisations should have procedures in place to manage Reliability. These should include all processes and practices listed in level 3, but they should be performed to a higher standard and used to inform other processes. A level 4 organisation should have a capability to perform:

- Formal Reliability demonstration to customers
- Reliability improvement
- Project risk management
- Supply chain management
- Management of change and lifecycle transitions
- Reliability testing

At level 4, Reliability is well defined and analytical tools are more disciplined than at level 3. The learning mode is still single loop in that actions are taken to correct identified faults in the equipment families, but there is little or no effort to adapt organisational processes to bring about Reliability improvements. The approach to risk is essentially phased risk management. Formal analysis is used to inform risk reduction and Reliability improvement strategy. There is a very disciplined approach to Reliability analysis, involving specialist tools for systems Reliability and availability analysis. Education and training and R&D are aimed at equipment improvement, but not targeted on processes.

Level 5 Optimised

The organisation has procedures in place to optimise risk and Reliability.
At this level, additional processes are in place for:

- Feedback and organisational learning
- Verification, validation and benchmarking

Reliability is well defined. Programmes are in place to sustain long-term continuous Reliability improvement and risk reduction. The learning mode is double and triple loop in that actions are taken, not only to adapt equipment but also to adapt the organisation (double loop) and inform education and training (triple loop) to bring about Reliability improvements. Level 2, 3 and 4 processes are also in place at this level, but operated to a higher standard. The approach to risk is concurrent risk management, whereby risks are identified and assessed by team members at the point of design continuously and as a normal part of the design process. All design team members are highly skilled and knowledgeable about risk and reliability.

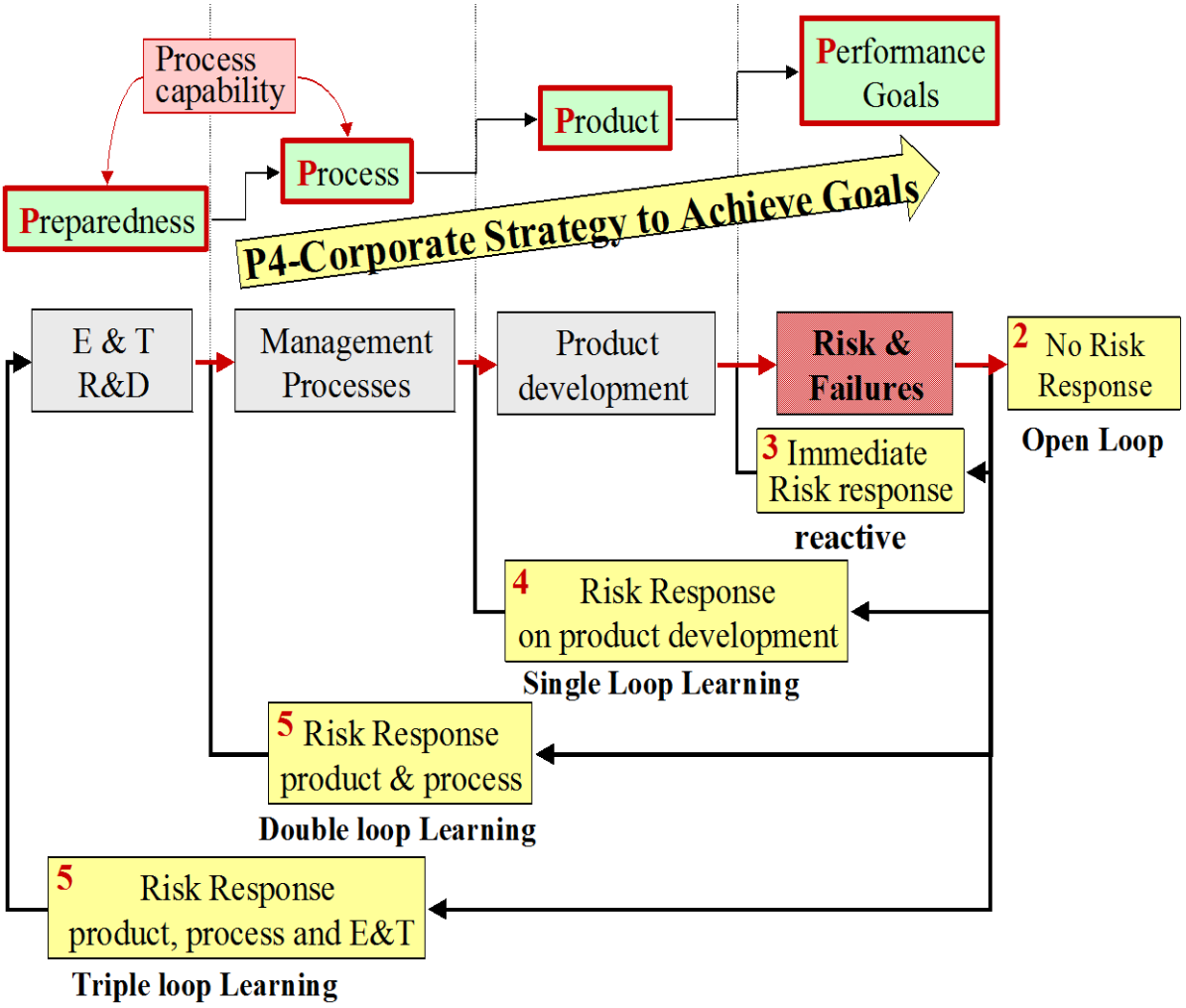


Figure 4: Characteristics of the Reliability Capability Maturity Model

COMPETENCE AND TRAINING

In today's world, it is important that persons are deemed to be 'competent'. A general definition of 'competent' is 'able to do something successfully or efficiently'. More specifically, for UK engineers, this means:

- Develop an appreciation of engineering processes and practices which would be regarded in the appropriate industry as sound engineering practice
- Appreciation and practical application of judgements made on tolerability of risk in terms of Safety and Reliability
- An appreciation of the tools and processes available for the assessment and management of risk
- Understanding of the aspects of Safety and Reliability that are required during the design, manufacture, fabrication and construction programmes
- Understanding of the aspects of Safety and Reliability that are required during operation and maintenance activities

- Understanding the equipment, manufacturing processes and their interaction in order to be able to appreciate how through-life issues may affect safe and commercial operation

A high-Reliability organisation will have a training and competence framework that incorporates sound understanding of these principles, not only for engineers but for individuals working at all levels of the organisation.

ANNEX 1: KEY PROCESSES

KP1: Setting and Allocating Safety and Reliability Requirements

Customers will set system-level requirements, and expect suppliers and design contractors (system integrators) to be capable of interpreting and allocating Safety and Reliability requirements to system components and subsystems as an input to design. However, projects can vary from a simple device or machine to a complex process plant, the failure characteristics of which can be vastly different. It is an inherent fact that simple machine systems are more reliable than complex ones. The first step in any design and development project is to consider if the required Safety and Reliability goals are realistic and achievable given the intent and complexity of the system.

The Safety and Reliability goals should form a key element of the system requirement document and include:

1. Probability of system failure at a given life
2. System availability at different stages throughout the life cycle, split by probability of failure and expected downtime for restorative maintenance
3. Expected operating environment and stresses
4. Operational usage
5. Technical and maintenance support
6. Acceptance criteria
7. Definition of failure
8. Total life cycle costs (or expectation that this is to be developed)

Each requirement will be specified by a target value to a given level of confidence, or some other measurable performance characteristic.

It is suggested that provision of relevant assurances is best achieved by means of an R&M Case. Based on the principle of a Safety Case (for example Defence Standard 00-56), the R&M Case (ie Defence Standard 00-42 part 3) should contain an overview of the design philosophy used and justification of the design and manufacturing processes relevant to the achievement of the R&M requirements. At the beginning of a project, it should provide confidence, before committing significant resources, that there is minimal risk of failing to meet the R&M requirements. During the design, development and manufacturing processes, the R&M Case will be a living document and proceed through a number of stages of increasing detail. During in-service use, it should provide confidence that the system remains reliable and maintainable in its operational role. In summary, it will form an audit trail and a dossier of all evidence supporting the claim that the Safety and Reliability requirements have been met.

Typical Activities

Purchaser	Supplier
1. Define operational requirements 2. Set system-level requirements 3. Define the R&M policy/strategy 4. Define high-level R&M goals and link these to the business risks 5. Define maintenance and technical support requirements 6. Initiate R&M Case and define deliverables	1. Provide supplier R&M organisational structure 2. Define the R&M philosophy 3. Advise relevant legislation 4. Assist in R&M strategy and plans 5. Develop R&M Case

KP2: Demonstration of Safety and Reliability in Design

As well as meeting the Safety and Reliability requirements set by customers, suppliers will be expected to provide documentary evidence that the required Safety and Reliability will be met. As per KP1, it is suggested that this is best provided by a Safety Case and an R&M Case (other examples, set by legislation, may include Offshore Safety Case, COMAH report). These documents would accompany the design documentation for the system.

To recap on the Safety Case and the R&M Case – these are reasoned, auditable arguments created to support the contention that a defined system satisfies (or will satisfy) Safety and Reliability requirements. It requires a strategy and will contain evidence based on three objectives:

1. The purchaser's Safety and Reliability requirements shall be determined and understood by both the purchaser and supplier.

2. A programme of activities shall be planned and implemented to deliver the requirements, with regard to mitigating risks identified during analysis.

3. Demonstration via progressive assurance that the requirements are being, have been or will be met.

Progress reports will give a summary of evidence to support programme milestones. They should provide sufficient detail to allow a decision on whether to proceed from one phase of the project to the next.

The concept and techniques of 'progressive assurance' are intended to provide a logical 'roadmap' through development, identifying and solving problems as they occur. This allows for revision to original design if necessary to effect a solution keeping with the original core and project goals.

Acceptable evidence of achievement of the Safety Case and R&M Case will include calculations, results of tests, simulations, trials, demonstration, analysis, plus interpretation of any relevant historical evidence from like systems, or even expert opinion or best practice.

Typical Activities

Purchaser	Supplier
1. Define operational requirements and expectations 2. Review supplier progress and output 3. Review/revise strategy in response to deviations from expectations	1. Define and plan a strategy to demonstrate achievement of Safety and R&M Cases 2. Review progress against plan 3. Revise plans 4. Produce Safety and R&M Case Reports

KP3: Process Verification, Validation and Benchmarking

Suppliers with the highest levels of capability will have developed standard processes for the verification, validation and benchmarking of Safety and Reliability design tasks, namely to:

a) Check that all design assumptions, Safety and Reliability models, collected supporting data and system stresses are valid
b) Verify that all required processes and activities have been carried out
c) Benchmark the capability of the organisation to perform key processes

There may be greater confidence in the validity of this key process if carried out by an independent body, and some industry sectors legally require 'third-party' certification, eg aerospace.

Typical Activities

Purchaser	Supplier
1. Agree acceptability of plans and results expected 2. Review and agree interpretation of progress 3. Determine any third-party verification requirements 4. Review subsequent plans	1. Define methods and plans for demonstration 2. Report on progress and any problems 3. Work with third parties as required 4. Revise plans if required 5. Produce Case Reports

KP4: Safety and Reliability Risk Reduction in Design

Where outputs from analyses or tests indicate that Safety and Reliability is unacceptable, actions must be taken to improve. The efforts expended to improve Safety and/or Reliability need to be proportionate to the consequential risks of failure, bearing in mind ethical and legal commitments. There are a number of strategies that can be adopted in design to enhance Safety and Reliability, and these can be broken down into the following three broad categories:

1. Actions to increase inherent Safety and Reliability at equipment level:
a) Change technology to remove a Failure Mode (FM)
b) Remove or reduce faults introduced during manufacturing and assembly
c) Perform Environmental Stress Screening (ESS) and burn-in tests
d) Reduce or adequately separate design and operational stresses – thermal, mechanical, chemical, etc – and consider stress/strength distributions
e) Increase tolerance to corrosion, fatigue, erosion and wear damage
f) Select components or materials less susceptible to damaging factors
g) Control the environment

2. Actions to increase Safety and Reliability at the system level:
a) Active redundancy
b) Passive redundancy

3. Actions to increase maintainability:
a) Predictive technologies
b) Reduce time to repair and replace

Thought must be given to changes made to the design, and it may be necessary to revisit KP1-3 after redefinition or redesign takes place.

Typical Activities

Purchaser	Supplier
1. Advise areas of particular interest for expansion of operational and performance requirements 2. Advise any particular perceptions for extreme operation of equipment 3. Agree acceptance criteria for Safety Case and R&M Case	1. Suggest potential opportunities for improvement in design 2. Advise plans for controlling and minimising risk during design and development 3. Demonstrate achievement of Safety Case and R&M Case through design

KP5: Safety and Reliability Analysis and Risk in Design

System suppliers will be expected to possess a high level of competence in their ability to:

a) Initial system modelling (RBD)
b) Identify potential system failure modes and mechanisms (FMEA and FMECA)
c) Forecast the Safety and Reliability consequences of equipment failure
d) Predict and assess system Safety and Reliability (FTA)
e) Simulation of system availability, eg Monte Carlo Analysis, Weibull

These will be applied during the design process, and will be used to inform decision-making on where Safety and Reliability improvements are required at component or system level. The process should also follow the principle of 'designing for manufacture' to simplify both assembly and subsequent maintenance of equipment. Analyses should be capable of identifying and assessing:

- Susceptibility to forms of damage
- Tolerance to predicted damage
- Human factors in manufacture, installation, operation or maintenance
- Common cause and common mode failures
- Single-point failures

Minimising manufacturing/maintenance operations – ie 'lowest replaceable assembly' concept

A risk register with reasons, assumptions and mitigation proposals should be created to identify and control risks. This usually forms part of the FMEA/FMECA and would include reasons for, and benefits of, particular ideas and decisions. An evidence framework can then be produced to show how requirements have been or are being achieved.

Typical Activities

Purchaser	Supplier
1. Review operational requirements with respect to analysis results 2. Review supplier outputs 3. Revise strategy 4. Review Case Reports 5. Participation in analyses	1. Interpret requirements and prepare strategy to deliver 2. Establish an R&M programme 3. Review risks (possibly covered by KP5) 4. Produce Case Reports 5. Participation in analyses

KP6: Project Risk Management

The majority of equipment is developed, manufactured, assembled and installed within a project environment. Project goals are generally focused on the delivery of equipment within a specified time and to a pre-agreed budget, and are often in conflict with the goal of developing reliable equipment. Primary causes of the conflict are (a) the uncertainty in resources (time, tools and man-hours) required to achieve task goals and (b) unplanned project delays, which reduce the time available to perform key Safety and Reliability assurance activities.

Project risk management is a key process which provides some assurance that equipment Safety and Reliability will not be compromised in order to meet project goals. Suppliers will be required to demonstrate a strong project risk management capability to ensure that equipment reliability as well as project requirements are achieved.

In the context of a Safety and Reliability management capability, project risk management activities will typically involve:

a) Identification of project tasks
b) Identification of resources required to successfully achieve the task goal
c) Identification of risks to each task (eg likelihood of delays, increase in required task resources)
d) Identification of risks to equipment from less-than-thorough attention to the task (eg likelihood of failures, increased equipment costs)
e) Ensuring that sufficient resources are available to carry out each task needed to achieve Safety and Reliability goals
f) Review of the design risk register to aid control and mitigation
g) Review to ensure that action taken is mitigating and hence reducing risks
h) Consideration of future obsolescence and supportability

Typical Activities

Purchaser	Supplier
1. Review areas of potential risk based on past experiences 2. Review supplier's risk assumptions	1. Review and advise areas of potential risk, eg new techniques, components 2. Produce comprehensive risk register and propose a plan for reduction

KP7: Safety and Reliability Testing in Design and Development

The purpose of Safety and Reliability testing is to explore and validate performance characteristics and failure processes. This is quite distinct from qualification testing, where the goal is to confirm that a specified performance requirement can be met. Safety and Reliability testing is carried out to reveal weaknesses, which are then corrected, and has several goals:

a) Identification of failure modes in equipment
b) Verification of failure modes (or lack of) identified in FMECA activities
c) Model validation (for physics of failure models)
d) Learning about physical failure mechanisms where the mechanism is poorly understood
e) Demonstrating Safety and Reliability improvements from design changes
f) Generation of Safety and Reliability and equipment life data

Due to cost, Safety and Reliability testing of machinery is usually with a few samples and a limited testing period, but even with limited results, it is still possible to estimate failure characteristics such as infant mortality, ageing, characteristic life.

To improve accuracy, the data sets can be adjusted by one of a selection of procedures such as Bernard's equation, median ranking, Nelson's hazard analysis. The development data sets can then be analysed according to the Weibull, Duane or Crow-AMSAA procedures. These techniques are covered in various sources. The ability to obtain such results will enable the risk of not meeting the Safety and Reliability goals to be assessed.

Safety and Reliability testing can also include a number of highly specialised methods for Accelerated Life Testing (ALT), Highly Accelerated Life Testing (HALT), Safety and Reliability Environmental Testing (RET), Reliability Growth Trials (RGT), Test Automation Framework (TAF), Environmental Stress Screening (ESS), Step Stress Testing (SST), etc.

HALT and similar techniques must be properly considered and designed to avoid introducing or causing additional non-representative problems, which can disguise the real issues.

A robust FRACAS [defined overleaf] is an essential part of this activity (see below).

Typical Activities

Purchaser	Supplier
1. Specify testing requirement 2. Validate results 3. Agree corrective actions	1. Propose testing methods 2. Analyse results 3. Propose corrective actions

KP8: Failure Reporting, Analysis and Corrective Action System

Failure Tracking, Reporting and Analysis is the sensing arm of a closed-loop circuit, which enables the organisation to implement organisational learning and improve Safety and Reliability. When combined with corrective action, it is also known as FRACAS or DRACAS[1]. Failure tracking and reporting must involve communication between the customer and the suppliers.

The difficulties of communication can be reduced by the establishment of a failure analysis team involving both customer and equipment supplier.

Good data on operational performance is essential evidence to assess Safety and Reliability, as is a good system to capture and use it for improvement. Turning data into useful information is the key to making critical equipment reliable. However, good data is difficult to define, it needs to be relevant to the particular concern, eg reliability, collected over a period and sorted out from non-relevant data.

Central to the good management of an effective FRACAS is the operation of a Failure Review Board. This should also, where possible, involve the customer.

Typical Activities

Purchaser	Supplier
1. Agree proposed methods of monitoring and control 2. Review and accept or debate reports of progress	1. Define methods and techniques to be adopted 2. Report on progress and any problems 3. Produce analyses of results and any recovery plans if required 4. Produce Case Reports

[1]FRACAS: failure reporting, analysis and corrective action system; DRACAS: data reporting, analysis and corrective action system

KP9: Supply Chain Management

It is often found that high-level system failures with significant consequences originate from the failure of minor components in the system. Systems designers/integrators must understand the significance of the risk potential of all components, including minor components supplied by second and third-tier suppliers. Safety and Reliability requirements should be allocated, where appropriate, down to all components (ie piece-part level) including Commercial Off The Shelf (COTS) and bought-in items. All suppliers will be expected to be capable of managing the various interfaces between the customers and suppliers down the supply chain, including recognition of likely obsolescence issues.

Integration and compatibility issues must be checked by each supplier as appropriate and confirmed to ensure that no undesirable influences occur between components or subsystems. They must also be compatible with the intended operational environment.

The Prime Contractor should understand his responsibility for considering the system as a whole, not just its constituent parts.

Typical Activities

Purchaser	Supplier
1. Advise on likely areas and environments for maintenance and support activities 2. Define desired methods and plans for support requirements 3. Review and agree proposals	1. Confirm understanding of requirements and ensure design and development plans will allow compliance 2. Report on progress and impact of any problems 3. Revise plans if required 4. Produce Case Reports

KP10: Management of Change and Life Cycle Transitions

Many failures originate from changes made during the life cycle of the equipment or occur at life cycle transitions. Such changes of an engineering/design nature may affect performance, compatibility, manufacturing procedures, etc. Companies will be expected to develop systems for change control which include procedures for:

a) Monitoring (identification of change)
b) Assessing (identification and assessment of change risks)
c) Managing change (change control follow-up and risk reduction)
d) Monitoring and benchmarking changes and follow-up actions

The system should be applied throughout the whole equipment life cycle, eg:

- Conceptual design
- Detail design
- Manufacture
- Assembly
- Shipping
- Installation
- Operation
- Disposal

Actual cycles will vary with each industry but there will be specific stages, which all need to be managed and recorded.

Change management requires a sound configuration and change control system, which should also include updates to relevant publications, training requirements for operators and maintainers, plus implications for stores.

This is a separate consideration to that of transfer from one phase to another, eg from development to production, where problems can occur through differing processes or facilities. These can be significant in maintaining integrity of the designed objectives (see KP11).

Typical Activities

Purchaser	Supplier
1. Ascertain procedures for identification and control of changes required during the equipment life cycle 2. Monitor associated risk aspects and configuration control procedures 3. Review implications for training and documentation, etc	1. Advise or devise procedures for configuration and control of changes during the equipment life cycle 2. Advise methods or rationale for defining levels where changes affect Build Standard and interchangeability 3. Advise implications for training and documentation, etc

KP11: Management of Transition from Development to Production

Due to different constraints on development and production facilities, the transition phase can reveal unforeseen problems, unless manufacturing techniques and procedures have been given due regard during the design process. Various engineering procedures routinely used to overcome problems during development, are often difficult or even not possible in the production environment. At this stage it is too late and thus expensive and time-consuming to effect changes. This causes frustration, increased costs and risk of reducing Safety and Reliability from that anticipated from earlier trials and forecasts.

Wherever possible all development manufacture and certainly final production standard prototypes (where applicable/possible) should be manufactured using (and proving) production standard tooling and techniques.

Key aspects to be considered include:

- Demonstration of manufacturing, assembly and testing capability and techniques
- Proving of production-standard tooling and associated equipment
- Demonstration of various processes and confirmation of test methods
- Confirmation of associated instructions and publications
- Maintenance of quality control procedures and hence Safety and Reliability

No design scheme should be issued as finalised unless it has been accepted by Manufacturing. Similarly, Safety and Reliability concerns should be addressed and vetted as providing at least the minimum requirements before any scheme is released to the next stage.

NB: Production Engineering and Manufacturing should be involved as early as possible in the design and development process.

Typical Activities

Purchaser	Supplier
1. Monitor progress to confirm capability of manufacturer 2. Accept standard of manufactured items	1. Design for manufacture/maintenance, early involvement of Production Engineering 2. Implement appropriate systems and procedures to ensure smooth transition

KP12: Feedback and Organisational Learning

The tracking and analysis of data has limited value unless the information is converted into organisational knowledge and ultimately used to improve equipment Safety and Reliability. Good Safety and Reliability management will provide resources to ensure that information is fed back to the whole organisation involved in design and system integration, to understand the lessons to be learned from failure.
The organisational learning is concerned with the transformation of data and information into intellectual capital of the organisation. Intellectual capital takes three main forms:

- Human Capital: knowledge of individuals in the organisation
- Structural Capital: knowledge structured in databases and knowledge bases (lessons learned)
- Customer Capital: knowledge of the value to customers

Typical Activities

Purchaser	Supplier
1. Organise regular progress review sessions to analyse and understand progress 2. Assist as appropriate with any resulting revisions required to the programme	1. Advise procedures for monitoring and analysis of accumulating data and results 2. Advise methodologies for feedback of information produced into the programme 3. Produce reports accordingly

KP13: Education and Training in Safety and Reliability

Safety and Reliability improvement will require in-depth knowledge of how design and the design processes can prevent failure. Training should be targeted both at understanding technical failure mechanisms, and at how the organisation and human factors cause errors and mistakes in design of components and systems at root cause level. Education and training will also be needed in Safety and Reliability engineering and risk management, to enable design teams to understand the meaning of Safety and Reliability, how it is affected by design and to become familiar and proficient with the tools.

This should also include maintainability and quality, plus operator competence and understanding.

Typical Activities

Purchaser	Supplier
1. Develop and deliver appropriate training for Project staff and advisers	1. Develop and deliver appropriate training for all Design and Development staff and advisers

KP14: Research and Development in Safety and Reliability

Leading organisations with high Safety and Reliability management capabilities will include R&D programmes to support and inform the Safety and Reliability strategy of the organisation.

Research and development programmes will be dictated by the company's overall business strategy. However, the most capable organisations will use research and development as a key input to both equipment and process development. Key areas where research is currently necessary in the Safety and Reliability field include:

- Development of Safety and Reliability assessment tools
- Predictive tools linking design, manufacture, usage and environment to equipment Safety and Reliability
- Development of improved data and data collection methods
- Development of Safety and Reliability testing methods/tools
- Development of novel equipment with high levels of fault and damage tolerance and reliability
- End-of-life management

This also requires an efficient and comprehensive data management and usage system in order to maintain and gain maximum advantage of information from records of usage and relevant experiences. Appropriate historical information is of great benefit when reviewing designs or developing new equipment.

Typical Activities

Purchaser	Supplier
1. Develop, introduce and monitor programmes to record equipment operational performance and identify particular effects, eg frequency and environment 2. Debate during review meetings	1. Discuss relevant previous performance of similar equipment and advise information which would be useful 2. Research other sources of useful information and debate with purchaser

BIBLIOGRAPHY

NB: This bibliography is just a selection of the many books and publications that are available on the subject, and should not therefore be regarded as definitive.

The Reliability of Mechanical Systems (2nd Edition). John Davidson. IMechE Guides for the Process Industry. Published by Wiley-Blackwell. 1994. ISBN 0852988818.

Mechanical Reliability. ADS Carter. Published by Macmillan Education. Second edition. 1986. ISBN 0333405870.

Mechanical Reliability and Design. ADS Carter. Published by Wiley-Blackwell. 1997. ISBN 0470237198.

How Did It Happen? Engineering Safety and Reliability. W Wong. Published by PEP. 2002. ISBN 1860583598.

Practical Reliability Engineering (4th Edition). PDT O'Connor. Published by Wiley-Blackwell. 2002. ISBN 0470844639.

Practical Reliability Engineering (5th Edition). PDT O'Connor & Andre Kleyner. Published by Wiley-Blackwell. 2012. ISBN 047097981X

Reliability and Risk Assessment. JD Andrews and TR Moss. Published by Wiley-Blackwell. 2002. ISBN 1860582907.

Systems Reliability & Failure Prevention. H Hecht. Published by Artech House. 2003. ISBN 1580533728.

Improving Maintainability and Reliability Through Design. G Thompson. Published by Wiley-Blackwell. 1999. ISBN 1860581358.

Reliability, Maintainability & Risk. David J Smith. Published by Butterworth-Heinemann. 2011. ISBN 008096902X.

Reliability Centred Maintenance. John Moubray. Published by Butterworth-Heinemann. 1999. ISBN 0750633581.

Of the above publications, Carter is out of print but new or used copies are available from, or via, www.Amazon.co.uk. Cost is generally around £60-£100 each.

b) Restricted availability (ie not on the ISBN system) – UK source

Reliability: A Practitioner's Guide. Published by Intellect/Relex Software Corporation. 2003.

British Standard 5760. Part 0. Reliability of Systems, Equipment and Components. Introductory Guide To Reliability. Published by BSI. 1986. Reissued in 2014.

c) Restricted availability (ie not on the ISBN system) – US source

RIAC (Reliability Information Analysis Centre) has a very good range of publications at reasonable prices. They can be sourced in the UK from certain specialist booksellers, but ordering direct from RIAC is quite easy.

Reliability Toolkit: Commercial Practices Edition

System Reliability Toolkit

Maintainability Toolkit

Supportability Toolkit

Quality Toolkit

Mechanical Applications in Reliability Engineering

Applied Reliability Engineering (Vols I and II)

FRACAS Application Guidelines

APPENDICES

Definitions

Definitions of Safety and Reliability

There are numerous and various accepted definitions of Safety and Reliability. For example ISO 8402 Quality Vocabulary defines Reliability as "the ability to perform a stated function under stated conditions for a stated period of time". IEC Guide 51 defines Safety as "freedom from unacceptable risk".

Reliability is an operational parameter; simply, it is sustained performance. The achievement of Reliability results, in the first instance, from a structured, coherent and knowledgeable approach to the initial derivation of the level of Reliability demanded by the operational requirement. Subsequently, the design and development of the equipment to meet that need must be underpinned by a contract strategy that delivers and demonstrates that the requirement has been satisfied.

Successful Safety performance is an absence of effects. Although Safety and Reliability failures can be measured, the absence of data does not prove that the system has achieved its Safety aims. As previously stated, when new projects are initiated, there is a large number of design, functional and operability requirements set by the customer and imposed on the project contractors and system suppliers. So how will companies interpret Safety and Reliability? It is the function of the design and engineering teams to provide an engineering solution which best meets the technical requirements without compromising the core business values identified above.

However, for this guide, we accept and work with the following definitions, that:

Safety is the visible and demonstrable absence of unacceptable risk of undesirable events affecting the health and safety of the workforce and the public at large (HSE definition).
Reliability is the ability of an item to perform a required function under stated conditions, including environment and usage, and for a stated time.
Maintainability is the ability of an item, under stated conditions of use, to be retained in, or restored to, a state in which it can perform its required functions, when maintenance is performed under stated conditions and using prescribed procedures and resources.
Availability is the ability of an item (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated instant of time or over a stated time.
Dependability is the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance.

Generally, these and other aspects, referred to as Safety and Reliability, are core aspects of risk management in engineering.

Quality versus Reliability – Are they the same thing?

A definition of 'quality' in the sense meant by the various management systems standards used in commerce and industry reads something like "*The characteristics of*

equipment or a service that bear on its ability to satisfy stated or implied needs" (1). ISO9001. The widely adopted management system standard is slightly more succinct: *"Degree to which a set of inherent characteristics fulfils requirements"* (2). Both of these definitions embody the concept that the 'quality' of a product or service is a measure of its ability to meet its requirements. Thus 'quality' is comparative – it compares the ability of a 'product' with its requirements. This is in contrast with the everyday meaning of the word, which implies that 'quality equipment' is in some sense excellent, superior or better than average.

Likewise, the term 'reliability' has evolved a specific technical definition, which is perhaps different from its everyday meaning. The designer of equipment understands 'reliability' as the probability that the equipment or system will perform its intended function(s) for a given period of time or under specified circumstances. Reliability in this sense is simply a measure of an attribute of equipment expressed as a probability. Thus a system that demonstrably achieves a quoted probability of failure can be deemed to be 'reliable' (3). This is in contrast with the everyday meaning of reliable equipment as being 'unlikely to fail'.

In both cases, the technical definitions of 'quality' and 'reliability' imply a comparison between a requirement and a measure of the ability of equipment to meet that requirement. In contrast, the everyday definitions imply an absolute standard. 'Quality' spans all attributes of equipment whereas 'reliability' is limited to the probability of equipment failing to fulfil specified functions. Thus reliability is but one dimension of quality.

For example, a car will be perceived to be 'reliable' if it starts and runs as and when required without breaking down. However, a 'quality' car is seen as much more than this. The quality of car will be determined by the degree of fulfilment of a host of other requirements (however expressed) such as the ride comfort, level of interior noise.

References

1. Definition provided by the American Institute of Quality.
2. ISO 9001.
3. Paraphrased from 'Statistical Methods for Reliability Data', Meeker and Escobar, Chapter 1. John Wiley and Sons. 1998.

IMechE Position Statement on Safety and Reliability

Government has encouraged the Engineering Institutions and academia to promote the achievement of Safety and Reliability. A statement has been prepared to present the Institution of Mechanical Engineers' current views on Safety and Reliability issues.

For the purposes of the statement, the following have been agreed:

Safety is the visible and demonstrable absence of unacceptable risk of undesirable events affecting the health and safety of the workforce and the public at large.

Reliability is the ability of an item to perform a required function under stated conditions, including environment and usage, and for a stated time.

Generally, these and other aspects, such as maintainability and availability, referred to as ‘Safety and Reliability’, are considered to be core aspects of risk management in engineering.

In addition to this, practitioners of Safety and Reliability activities are expected to follow a code of conduct, such as that defined by IMechE, namely:

“In order to facilitate the advancement of the science of mechanical engineering by preserving the respect in which the community holds persons who are engaged in the profession of mechanical engineering, every member shall, for as long as he continues to be a member, comply with By-laws 29 to 31 and the Code of Conduct Regulations. All members are ambassadors of the Institution and must therefore conduct themselves in a manner that upholds and enhances the reputations of the Institution, the profession of mechanical engineering and the Institution’s members. All members shall conduct their professional work and relationships with integrity and objectivity and with due regard for the welfare of the people, the organisations and the environment with which they interact. All members shall take reasonable steps to maintain appropriate professional competences.”