GUIDE ON ACHIEVING RELIABILITY THROUGH THE DESIGN PROCESS

Institution of MECHANICAL ENGINEERS

This document describes good engineering practice, which embeds the key factors and, if followed, should ensure that customers' expectations are met **when it comes to operational performance.**

Improving the world through engineering

CONTENTS

SCOPE

This guide offers guidance on how to design and make a reliable product (e.g. equipment, system or service). It aims to provide everyone associated with designing, manufacturing, operating or maintaining products with:

- Best practice for a cross-industry approach to reliability
- A capability maturity model (CMM) that will allow an organisation to assess its (and its suppliers') level of maturity in reliability engineering practices

The reliability engineering discipline is examined, including definitions, explaining the interrelationships of activities and their importance, generally and at specific times during development, manufacturing,

installation, operational and maintenance phases of a products life cycle. The guide includes advice on the methods of assessing the overall level of capability of the organisation, along with references to example standards and publications, which offer additional guidance upon the subject.

FOREWORD

Customers want products that work and go on working for a ‘reasonable’ period of time. If the customer’s expectations are not met they may regard the equipment or service as ‘unreliable’. 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 ‘reliability’ that sells a product, but the benefits of having a reliable product. 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. Factors that have the greatest influence on reliability are:

Design – ensuring a product is fit for purpose, relative to the required use and operating environment

Manufacture – ensuring a product is made to as consistent a standard as appropriate to economically meet customer requirements

Installation / Integration – assimilating the product with all other associated products and the environment

Operation – ensuring adequate consideration is given to usability and foreseeable misuse

Maintenance – the measures required to sustain the operation of the product which must be achievable in an economic, safe and timely manner

This guide describes good 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 managing reliability, and a primer of the essentials of what to expect for those who have no, or limited, experience.

Guidance is given as to 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.

INTRODUCTION TO RELIABILITY IN DESIGN PRINCIPLES

Reliability is a defining characteristic of a product’s performance and life cycle costs. In the context of this guide, it is understood that reliability is the ability of an item to perform a required function under stated conditions, including environment and usage, for a stated time.

The aims of the reliability engineering discipline, as part of an integrated team, are to:

- Specify and agree a product’s reliability requirements
- Manage the focussed activities throughout the design of a product that will give confidence that reliability requirements can be met
- Co ordinate and monitor the reliability influencing activities within the supply chain
- Contribute to defining through-life activities for the product to preserve inherent reliability
- Risk management – assess, analyse and manage risks using techniques, e.g. failure mode and effects analysis, which either result in:

  - Acceptance, if risks are found to be tolerable

  - Mitigation, actions to eliminate the problem, reduce the probability of occurrence or minimise the consequences upon occurrence
- Monitor in service performance to ensure that reliability requirements are being achieved, while cost of ownership is not adversely affected
- Integrate through life cycle learning into design, manufacturing, installation, maintenance and operating processes
- Consider decommissioning and disposal

It is important to consider reliability at all stages of the product life cycle. Reliability 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 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 (i.e. at each life cycle stage, the cost of change increases by an order of magnitude). It is prudent at this stage to recognise that the reliability of a product cannot be enhanced by maintenance, only preserved.

Designing for reliability requires:

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

RELIABILITY IN DESIGN AS A BUSINESS GOAL

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

- Health and safety
- Environment
- Quality
- Economic factors

Reliable products support all of these business goals. Health and safety is supported as reliable products need fewer unplanned interventions, do not fail catastrophically or in an unintended manner. Such failures may also lead to releases of harmful or hazardous substances to the environment. Products that are reliable are more likely to meet customer requirements, hence quality is safeguarded; likewise, when reliability parameters are well understood and form the basis for engineering then product cost can be optimised as are through life costs. Compensation payments and rework costs may also be reduced through the same principles.

Why, therefore, is it usual to find that organisations have detailed policies and procedures for health, safety, environment and quality processes but not necessarily for reliability? It can be proposed that health, safety and environment are enshrined in regulations therefore such policies and procedures are mandatory. Certification to the ISO standards 45001 and 14001 allow companies to demonstrate compliance with requirements for managing occupational health and safety and environmental stewardship respectively.

The requirement for a quality policy and subordinate procedures is semi-mandatory as for many businesses a pre-requisite many customers demand, certainly for business-to-business transactions, is certification to a recognised quality assurance standard such as ISO 9001. It must be recognised that such certification does not necessarily assure a quality product, but demonstrates that a system is in place.

The format of the three standards so far mentioned – 9001, 14001 and 45001 – have all been harmonised under the ISO directives' annex SL, which dictates a common format for ISO management standards. This intent of this harmonisation is to remove much of the organisational burden in having a requirement to comply with many different standards which previously help disparate and sometimes conflicting requirements. The reason for the lengthy discussion on this topic is to draw the reader's attention to the fact that these principles, setting a policy and developing procedures in order to achieve a business goal, are very much aligned with the intent of this document.

A relative newcomer to the ISO management standards, ISO 55001 was developed with the intent of driving sound asset management practices through implementation of an organisational management system. Unlike the previously mentioned standards, however, certification to ISO 55001 is not widely seen as a requirement for doing business. Many organisations that rely on public funding or whose finances are government regulated (e.g. utilities and transport) have been set targets by government in the UK to achieve certification. There is some movement from investor organisations such as venture capitalists who recognise that having a system in place for stewardship of capital assets, i.e. their investment, is actually a good idea.

Asset management is becoming a boardroom topic, and as such a recognition of the fact that taking a longer term life cycle cost approach as opposed to a shorter term focus on minimising (as opposed to optimising) capital expenditure will help to meet overall business goals. Certification to ISO 55001 may not necessarily be seen to be mandatory for such organisations, but the practices and ideas held therein are looked upon as a recognised good practice as a basis for organisational processes and systems.

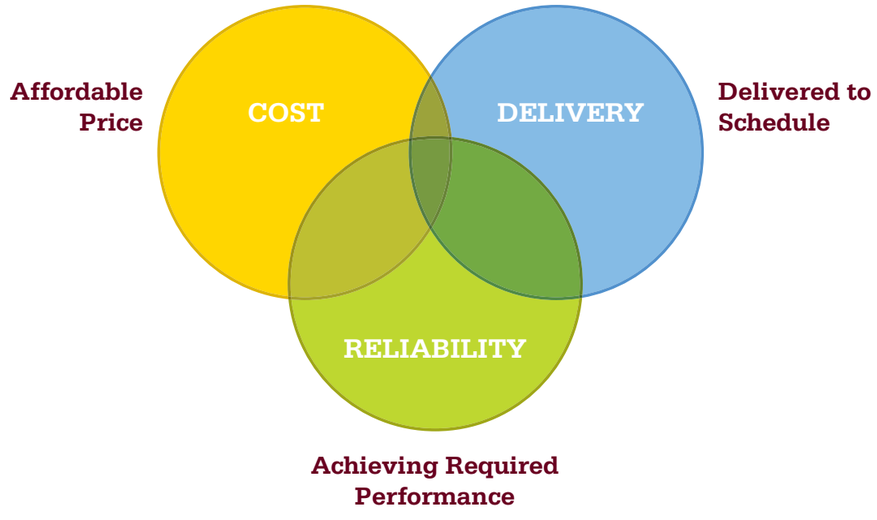
Now bringing the topic back to designing for reliability. If we recognise that reliability needs to be seen as a business goal, and a framework exists that can be used for the achievement of such a goal, then attention naturally turns to how we deliver.

DESIGNING FOR RELIABILITY

The specific issue facing companies is how to achieve the combined goals of:

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.

First the organisation needs to set performance targets. This is where opinions can diverge, as operations people will often make statements such as "it just needs to work" and designers may make statements like "why wouldn't it work, so long as you don't go outside of the window of design".



If we return back to our definition of reliability, neither of these statements are time-bound and the likelihood that something will just work is rather absurd. The measurement of reliability can, to some, be a little abstract as it can involve statistical distributions – suffice to say, at this juncture, that someone who has a good understanding of how reliability can be measured and how that relates to the real world should be engaged in helping to define targets and the measurement system.

Back to the point our fictitious designer made, the next basic step is defining the window of design. There are numerous factors to be considered in achieving reliability, some of which could be inadequately taken into account during design or emerge during the 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:

- **Environmental conditions**
  1. Temperature – range and cycles
  2. Pressures
  3. Humidity
  4. Arduousness of duty
  5. Altitude/Submersed depth
  6. Dusts, mists and other environmental contaminants

- **Effects of age and use**
  1. Deterioration of electrical cable insulation
  2. Wear
  3. Corrosion
  4. Fatigue
  5. Misuse

- **Material changes due to global legislation,** e.g.
  1. Lead-free solder – joint integrity
  2. Plating materials (e.g. cadmium no longer allowed)

- **Emergent technology developments**
  1. Industrial 'internet of things' – connectivity, data collection requirements
  2. Shrinking device architectures
  3. Obsolescence

- **Serviceability**
  1. Susceptibility to no fault found (NFF) events
  2. Location
  3. Training and technical skill levels
  4. Information and documentation
  5. Modular design

- **Other issues of note**
  1. Manufacturing techniques and 'built-in latent defects'
  2. Counterfeit components
  3. Owner/operators remote from designer/ manufacturer
  4. Warranty periods

Best endeavours should be made during product specification to identify all of the aspects that make up the window of design, to ensure that adequate design considerations are made that will allow the product to meet expectations, i.e. achieve the set reliability target.

RISK MANAGEMENT

Here we mention another ISO management standard, ISO 31000. This standard presents a framework that organisations can use to help manage risk. Do not expect to find organisations certified to this standard however, as it is not a "certifiable standard". The principles may be used to audit your own, or other, organisations' practices for risk management. ISO 31010 presents an overview, and the applicability of, various risk management techniques and as such is an excellent primer for individuals who are starting on a journey as a risk management practitioner. It is unlikely that one individual will become an expert in all of the risk management techniques.

The reason for the introduction of this standard is that robust risk management forms the bulk work of organisational reliability engineering practices. The core reason for risk management is to uncover potential problems as early as possible and present the facts in a somehow weighted manner to allow quality decision making at the right time. Such decisions will involve developing mitigating actions, including appropriate contingency planning.

A best practice to be considered is the introduction of a central risk register at a reasonably early point in product development. This register collects all of the project and product risks identified through other discrete risk management techniques, providing a master list which in turn can be used to drive action, decision or acceptance. This can be considered a list of 'lessons learnt' for subsequent projects, storing and preserving organisational

knowledge. Likewise, incorporation of lessons learned from within the particular industry or from the use of similar products can present opportunities to prevent unwanted consequences.

Risks of all types should be subjected to screening for credibility in this master list, as the techniques used to define and (as far as is possible) measure risks will undoubtedly do so in different ways. This presents a difficulty in assessing different types of risk against each other to allow prioritisation of effort. Organisations may employ a unified risk assessment matrix example see Figure 1, to ensure a consistent and reasoned approach to risk management. As with the development of reliability measurement, this can be an abstract system to relate to the real world therefore individuals with the understanding and experience of risk management should be involved in its development.

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	Low	Medium	High	Very High	Very High
Result in a major safety incident	Result in major financial losses	4	Low	Medium	Medium	High	Very High
Result in a moderate safety incident	Result in moderate financial losses	3	Low	Low	Medium	Medium	High
Result in a minor safety incident	Result in minor financial losses	2	Negligible	Low	Low	Medium	Medium
No concern	No concern	1	Negligible	Negligible	Low	Low	Low
Probability			Once in a thousand years or less	Once in a hundred years	Once in ten years	Once per year	Greater than once per year
Risk Assessment Matrix			1	2	3	4	5

Figure 1

MEASURING ORGANISATIONAL RELIABILITY CAPABILITY

Reliability over the long term can be measured by observing the actual reliability performance of products in the field. In the short term, however, observation of an organisation's systems and processes related to reliability provides a valuable indicator of the capability/likelihood of producing a reliable product. A capability maturity model (CMM), is a useful tool to assess the reliability capability of manufacturers. The characteristics which define the reliability capability of an organisation can be described as:

Level 1: Initial - no risk response

Level 2: Repeatable - immediate risk response

Level 3: Defined - risk response on product development

Level 4: Managed - risk response for product and processes

Level 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 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.

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, training, and research and design (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 design, 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 process with quantification at component failure level. Education, 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 life cycle 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; 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, 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. Programs 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 and inform education and training 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, and organisational goals, policies and procedures are updated to ensure that learning is embedded.

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 that 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 reliability
- An appreciation of the tools and processes available for the assessment and management of risk
- Understanding of the aspects of reliability that are required during the design, manufacture, fabrication and construction programmes
- Understanding of the aspects of reliability that are required during operation and maintenance activities
- Understanding the equipment and manufacturing processes, and their interactions, in order to appreciate how through-life issues may effect safe and prosperous operation

Incorporated and chartered engineers, in accordance with UK Engineering Council criteria, may demonstrate engineering competence. There needs to be a recognition of discipline, industry or product specific competence. Therefore, a high reliability organisation will have a training and competence framework that incorporates sound understanding of reliability engineering principles, not only for engineers but for individuals working at all levels of the organisation.

APPLICATION OF PRINCIPLES FOR ENSURING RELIABILITY IN DESIGN

In order to define the activities to ensure reliability is "built in" during design, let us first consider a basic design process (see Figure 2). Recognising the varied approaches that can be taken, and the iterative nature of design, this may be either overly simplified or complicated, but it is useful to consider such a model to define the "reliability enablers" at each stage.

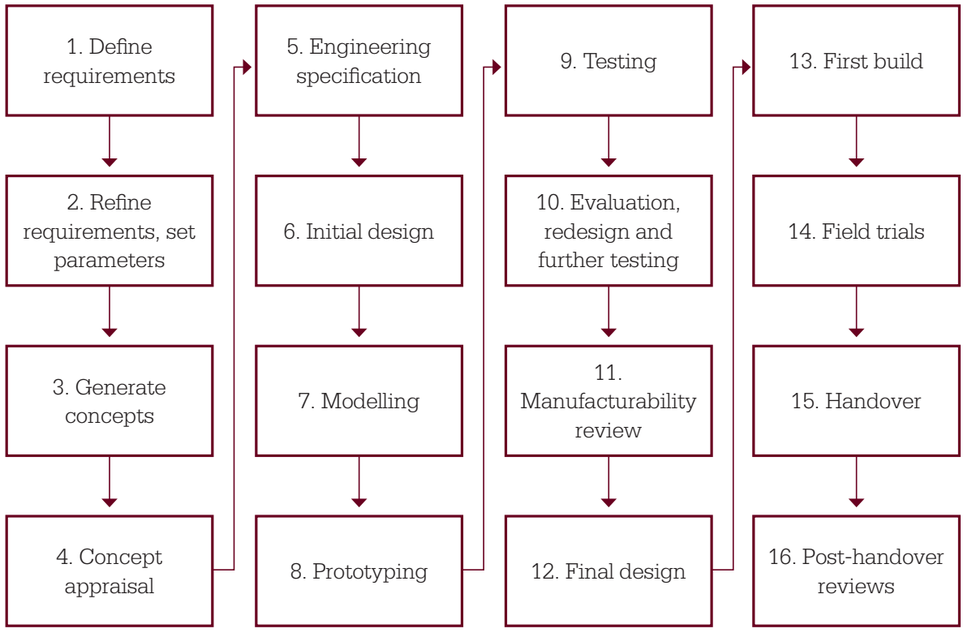


Figure 2

However, it must also be recognised that the design process must fit into the overall organisational management system and therefore it is useful to think of activities or organisational aspects – 'key processes' – and how they influence the design for reliability process.

THE KEY PROCESSES

A company's maturity with regards to practices regarding reliability in design can be separated into three distinct categories, with corresponding key processes (KPs):

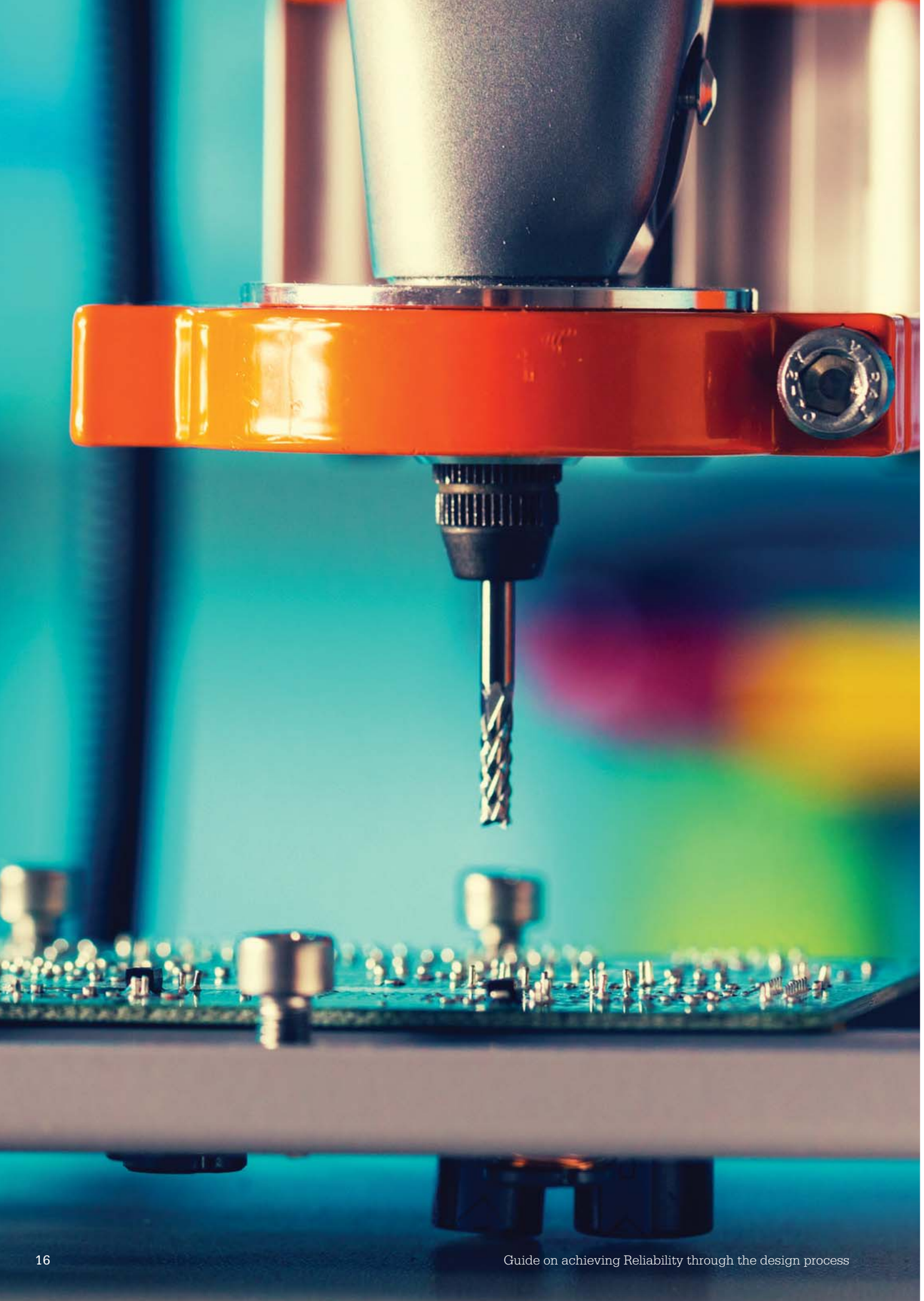
1. Formal risk analysis and demonstration of reliability
2. Implementation of reliability achievement and improvement strategy
3. Longer-term investments in reliability management

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	Key processes
Formal risk analysis and assurance of reliability	1	Setting and allocating reliability requirements
	2	Assurance of reliability in design
	3	Process verification, validation and benchmarking
	4	Reliability and risk analysis in design
Implementation of reliability achievement and improvement strategy	5	Reliability and risk reduction in design
	6	Project risk management
	7	Reliability testing
	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 reliability
	14	Research and development in reliability

Table 1 - Maturity characteristics and associated key processes

The implementation of 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, when deployed in support of design activities, can help achieve the required reliability level.



KP1

SETTING AND ALLOCATING RELIABILITY REQUIREMENTS

Customers set system-level requirements and expect suppliers and design contractors (system integrators) to be capable of interpreting and allocating 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 maturity of suppliers and design contractors in their ability to interpret and meet reliability requirements will also vary, and some attention needs to be given to how this is managed throughout the design cycle.

The first step in any design and development project is to consider if the required reliability goals are realistic and achievable given the intent and complexity of the system, and the maturity of the design and manufacturing supply chain.

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

- Probability of system failure at a given life
- System availability at different stages throughout the life cycle, split by probability of failure and expected downtime for restorative maintenance
- Expected operating environment and stresses
- Operational usage
- Technical and maintenance support
- Acceptance criteria
- Definition of failure
- 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.

Typical activities

Purchaser	Supplier
1. Define operational requirements	1. Provide supplier R&M organisational structure
2. Set system-level requirements	2. Define the R&M philosophy
3. Define the reliability and maintainability (R&M) policy/strategy	3. Advise relevant legislation
4. Define high-level R&M goals and link these to the business risks	4. Assist in R&M strategy and plans

Related basic design stages: define requirements, refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, evaluation, re-design and further testing.

KP2

ASSURANCE OF RELIABILITY IN DESIGN

It is suggested that provision of relevant assurances that the required reliability can be met is best achieved by means of a reliability & maintainability (R&M) case. Based on the principle of a safety case the R&M case (e.g. in accordance with BS EN 62741) 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 reliability requirements have been met. The R&M case presents reasoned, auditable arguments to support the contention that a defined system satisfies (or will satisfy) reliability requirements. It requires a strategy and will contain evidence based on three objectives:

1. The purchaser's 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 documented 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.

Acceptable evidence of achievement of the 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. Develop R&M case	1. Define and plan a strategy to demonstrate achievement of R&M case
2. Review supplier progress and output	2. Manage progress against plan
3. Review/revise strategy in response to deviations from expectations	3. Produce R&M case reports
4. Produce R&M case reports	

Related basic design stages: refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design.

KP3

PROCESS VERIFICATION, VALIDATION AND BENCHMARKING

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

- Check that all design assumptions, reliability models, collected supporting data and system stresses are valid
- Verify that all required processes and activities have been carried out
- 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, e.g. aerospace.

Typical activities

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

Related basic design stages: concept appraisal, evaluation, re-design and further testing, handover, post-handover reviews.

KP4

RELIABILITY AND RISK ANALYSIS IN DESIGN

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

- Model the system and interfaces (e.g. reliability block diagram)
- Identify potential system failure modes and mechanisms and assess probability and consequences of occurrence (failure mode and effects analysis, FMEA)
- Simulation of the system, e.g. Monte Carlo analysis, Weibull, fault tree analysis

These will be applied during the design process and will be used to inform where 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/failure
- Tolerance to predicted damage/failure
- Human factors in manufacture, installation, operation or maintenance
- Common cause and common mode failures
- Single-point failures

A risk register with reasons, assumptions and mitigation proposals should be created to identify and control risks. This usually forms part of the FMEA and would include reasons for, and benefits of, particular mitigating actions. An evidence framework can then be produced to show how requirements have been or are being achieved to be included in the R&M case.

Typical activities

Purchaser	Supplier
1. Conduct or commission analyses	1. Interpret requirements and prepare strategy to deliver
2. Review supplier outputs	2. Establish an R&M programme
3. Revise strategy	3. Produce case reports
4. Review case reports	4. Participation in analyses
5. Update risk register	5. Update risk register

Related basic design stages: concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review.

KP5

RELIABILITY RISK REDUCTION IN DESIGN

Where outputs from analyses or tests indicate that reliability is unacceptable, actions must be taken to improve. The efforts expended to improve 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 reliability, and these can be broken down into the following three broad categories:

- Actions to increase inherent reliability at equipment level, e.g.:
  1. Change technology or item to remove a failure mode
  2. Remove or reduce faults introduced during manufacturing and assembly (process FMEA)
  3. Perform highly accelerated stress screening (HASS) to eliminate early life failure inducing defects
  4. Reduce or adequately separate design and operational stresses such as thermal, mechanical, chemical, etc. Consider stress/strength distributions – finite element analysis (FEA)
  5. Increase tolerance to corrosion, fatigue, erosion and wear damage
  6. Select components or materials less susceptible to damaging factors
  7. Control the environment
- Actions to increase reliability at the system level, e.g.:
  1. Active redundancy
  2. Passive redundancy
- Actions to increase maintainability e.g.:
  1. Predictive technologies
  2. Reduce time to repair and replace

Thought must be given to changes made to the design, and it may be necessary to revisit KPs 1-4 after mitigating actions or redesigns are undertaken.

Typical activities

Purchaser	Supplier
1. Assessment of analyses results	1. Suggest potential opportunities for improvement in design
2. Development of mitigating actions	2. Advise plans for controlling and minimising risk during design and development
3. Agree acceptance criteria for the R&M case	3. Update risk register
4. Update risk register	

Related basic design stages: concept appraisal, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials.

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 set budget. These goals can be in conflict with the goal of developing reliable equipment due to the increased cost from commissioning studies or purchasing higher specification equipment or materials.

Project risk management provides some assurance that equipment reliability will not be compromised in order to meet project goals, or as a minimum where compromises are made the effects of such compromises are understood. 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 reliability management capability, project risk management activities will typically involve:

- Identification of project tasks
- Identification of resources required to successfully achieve the task goal
- Identification of threats to the successful execution of each task (e.g. lead time to purchase, availability of labour or resources, cost pressures from material price fluctuations)
- Identification of consequences of each threat (e.g. catastrophic failure, increased equipment cost)
- Determining the probability of each consequence occurring (qualitative or quantitative)
- Assessment of overall risk and underlying risk drivers
- Creation of a risk register to aid control and mitigation
- Periodic review to ensure that actions taken are mitigating risk

Typical activities

Purchaser	Supplier
1. Review areas of potential risk based on past experiences	1. Review and advise areas of potential risk, e.g. new techniques or components
2. Determine supply chain risk management protocols	2. Update risk register
3. Document process in a risk management procedure	
4. Create risk register	

Related basic design stages: define requirements, refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, handover, post-handover reviews.

KP7

RELIABILITY TESTING

The purpose of 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. Reliability testing is carried out to reveal weaknesses, which are then corrected, and has several goals:

- Verification of failure modes (or lack of) identified in FMEA activities
- Identification of unpredicted physical failure modes
- Model and simulation validation
- Learning about physical failure mechanisms where the mechanism is poorly understood
- Demonstrating reliability improvements from design changes
- Generation of reliability and equipment life data

Due to cost and practicality, reliability testing is usually conducted with a small sample population and a limited testing period. Even with limited results, it is still possible to estimate failure characteristics such as infant mortality, ageing and characteristic life. The data set can be analysed according to the Weibull, Duane or Crow-AMSAA procedures. These techniques are covered in various sources, and the results of the analysis will enable the ability to meet the reliability goals to be assessed.

Reliability testing can also include a number of highly specialised methods, for example accelerated life testing (ALT), highly accelerated life testing (HALT), reliability environmental testing (RET), reliability growth trials (RGT), test automation framework (TAF), step stress testing (SST).

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. Expert advice from experienced test personnel should be sought.

A robust FRACAS (see KP 8) is an essential and integral part of this activity.

Typical activities

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

Related basic design stages: modelling, prototyping, testing, evaluation, redesign and further testing, first build, field trials.

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 reliability. When combined with corrective action, it is also known as FRACAS or DRACAS. Failure tracking and reporting must involve communication between the customer and the suppliers. These difficulties can be reduced by the establishment of a failure analysis team involving both customer and equipment supplier, and modern communication and shared computing technology is very conducive to such a collaborative approach.

Good data regarding operational performance is essential evidence to assess 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, e.g. reliability, collected over a period and sorted out from non-relevant data. Some thought and energy should be expended up front to determine what type of data will be collected, how it will be collected, where it will be stored, how it will be structured, who is going to use it, and for what purpose.

There are some industry specific published standards such as ISO 14224 for oil & gas and petrochemical assets and KKS RDS-PP for power generation, which offer a taxonomy for structuring such data. The ORDEA handbook is an example of an industry publication, following the structured principles of ISO 14224, containing failure modes and data.

Typical activities

Purchaser	Supplier
1. Agree proposed methods of monitoring and control	1. Define methods and techniques to be adopted
2. Monitor performance	2. Report on progress and any problems
3. Review corrective actions	3. Produce analyses of results and any recovery plans if required
4. Update risk register	4. Produce case reports

Related basic design stages: testing, evaluation, re-design and further testing, first build, field trials, post-handover reviews.

1 FRACAS: failure reporting, analysis and corrective action system; DRACAS: defect 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. Reliability requirements should be allocated, where appropriate, down to all components (i.e. 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 throughout the supply chain, including recognition of likely obsolescence issues.

Integration and compatibility must be checked at each stage of the supply chain to ensure that no undesirable influences occur between components or subsystems. They must also be compatible with the intended operational environment.

The organisation responsible for final build should understand his responsibility for considering the system as a whole, not just its constituent parts.

Typical activities

Purchaser	Supplier
1. Define desired methods and plans for support requirements	1. Confirm understanding of requirements
2. Review and agree proposals	2. Ensure design and development plans will meet compliance requirements
	3. Report on progress and impact of any problems
	4. Revise plans if required
	5. Produce case reports

Related basic design stages: define requirements, refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, handover, post-handover reviews.

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 may affect factors such as performance, compatibility or manufacturing procedures. Companies will be expected to develop change control processes which include procedures for:

- Monitoring - identification of change
- Assessing risks from the change
- Managing the effects of change - change control follow-up and risk reduction
- Monitoring and benchmarking changes and follow-up actions

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

- 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.

Typical activities

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

Related basic design stages: define requirements, refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, handover, post-handover reviews.

MANAGEMENT OF TRANSITION FROM DEVELOPMENT TO PRODUCTION

Due to the differences between development and production facilities, the transition phase between the two 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 implement changes. This causes frustration; from increased costs and risk of reduced reliability compared to that anticipated.

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:

1. Demonstration of manufacturing and assembly techniques
2. Proving of production-standard tooling and associated equipment
3. confirmation of test methods
4. Confirmation of associated instructions and publications
5. quality control procedures

No design scheme should be issued as finalised unless it has been accepted by manufacturing. Similarly, 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. Develop, or manage development of, build procedures and quality control plans	1. Design for manufacture/maintenance
2. Monitor progress to confirm capability of manufacturer	2. Early involvement of production engineering
3. Accept standard of manufactured items	3. Implement appropriate systems and procedures to ensure smooth transition

Related basic design stages: concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build.

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 reliability. Good 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.

Organisational learning is concerned with the transformation of data and information into the intellectual capital of the organisation. Intellectual capital takes three main forms:

- Human capital – knowledge of individuals in the organisation
- Structural capital – knowledge structured in policies, procedures, databases and knowledge bases
- Customer capital – knowledge of the value to customers

Typical activities

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

Related basic design stages: initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, handover, post-handover reviews.

EDUCATION AND TRAINING IN RELIABILITY

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 organisational and human factors lead to errors and mistakes in design of components and systems. Technical training will also be needed in reliability engineering and risk management to enable design teams to understand the meaning of reliability, how it is affected by design and to become familiar and proficient with the tools.

Typical activities

Purchaser	Supplier
1. Identify the necessary reliability related skills for the type of organisation	1. Develop and deliver appropriate training for staff
2. Develop and deliver appropriate training for project staff and advisers	

Related basic design stages: define requirements, refine requirements and set parameters, generate concepts, concept appraisal, engineering specification, initial design, modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, handover, post-handover reviews.

KP14

RESEARCH AND DEVELOPMENT IN RELIABILITY

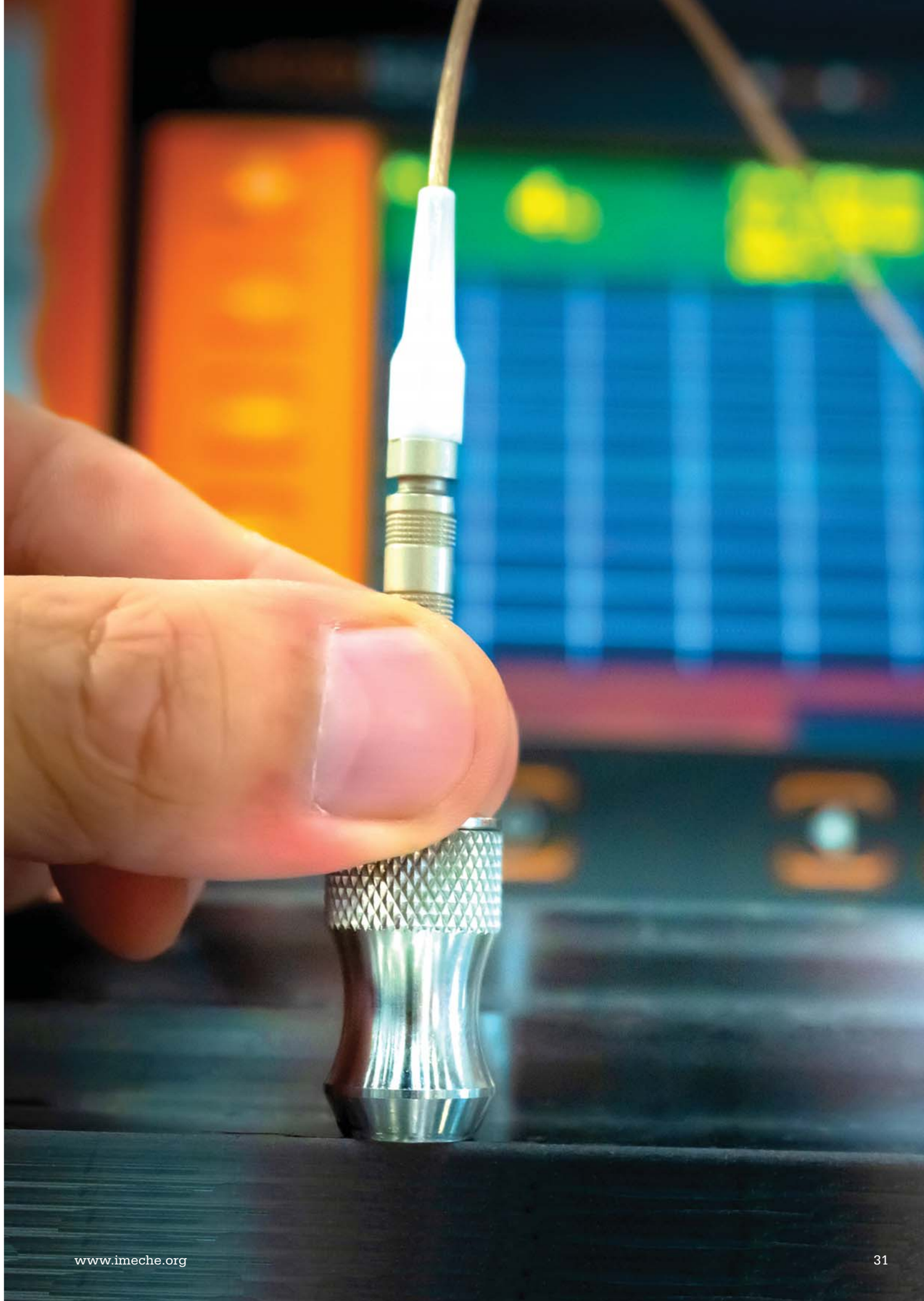
Organisations with high reliability capabilities will include R&D programmes to support and inform the reliability strategy of the organisation.

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. 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, e.g. frequency and environment	1. Discuss relevant previous performance of similar equipment and advise information which would be useful
2. Inform the company R&D strategy according to where value from reliability improvement can be gained	2. Research other sources of useful information and debate with purchaser

Related basic design stages: modelling, prototyping, testing, evaluation, re-design and further testing, manufacturability review, final design, first build, field trials, post-handover reviews.



BIBLIOGRAPHY

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

Andrews, J. D. and Moss, T. R.; 2002, ***Reliability and Risk Assessment,*** Wiley-Blackwell. ISBN 1860582907

Carter, A.; 1986, ***Mechanical Reliability*** (2nd edition), Macmillan Education. ISBN 0333405870

Carter, A.; 1997 ***Mechanical Reliability and Design,*** Wiley-Blackwell. ISBN 0470237198

Davidson, J.; 1994, ***The Reliability of Mechanical Systems*** (2nd edition); IMechE Guides for the Process Industry, Wiley-Blackwell. ISBN 0852988818.

Hecht, H.; 2003, ***Systems Reliability & Failure Prevention,*** Artech House. ISBN 1580533728

Kleyner, A. and O'Connor, P. D. T; 2012, ***Practical Reliability Engineering*** (5th edition), Wiley-Blackwell. ISBN 047097981x.

Moubray, J.; 1999, ***Reliability Centred Maintenance,*** Butterworth-Heinemann. ISBN 0750633581

O'Connor, P. D. T.; 2002, ***Practical Reliability Engineering*** (4th edition), Wiley-Blackwell. ISBN 0470844639

Smith, D. J.; 2011, ***Reliability, Maintainability & Risk,*** Butterworth-Heinemann. ISBN 008096902x

Thompson, G.; 1999, ***Improving Maintainability and Reliability Through Design,*** Wiley-Blackwell. ISBN 1860581358

Wong, W.; 2002, ***How did it Happen? Engineering Safety and Reliability,*** PEP. ISBN 1860583598

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

Restricted availability (i.e. not on the ISBN system) – UK source:

Reliability: a Practitioner's Guide, Intellect/Relex Software Corporation, 2003.

British Standard 5760. Part 0.R Reliability of Systems, Equipment and Components. Introductory Guide to Reliability. BSI, 1986; R reissued in 2014.

Restricted availability (i.e. not on the ISBN system) – US source:

RIAC (reliability information analysis centre) has a very good range of publications at reasonable prices.

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 reliability

There are numerous and various accepted definitions of 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".

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 performance is an absence of undesired effects. Although reliability failures can be measured, the absence of data does not prove that the system has achieved its 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 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:

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 collectively as reliability, are core aspects of risk management in engineering.

IMECHE POSITION STATEMENT ON SAFETY AND RELIABILITY

Government has encouraged 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 collectively 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:

> 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 they continue 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.

Institution of Mechanical Engineers

1 Birdcage Walk
Westminster
London SW1H 9JJ

imeche.org

Issue 3 - March 2019