

Australian Standard[®]

**Equipment reliability—Reliability
assessment methods**



This Australian Standard® was prepared by Committee QR-005, Dependability. It was approved on behalf of the Council of Standards Australia on 16 June 2008. This Standard was published on 28 July 2008.

The following are represented on Committee QR-005:

- AirServices Australia
 - Australian Chamber of Commerce and Industry
 - Australian Electrical and Electronic Manufacturers Association
 - Australian Industry Group
 - Australian Nuclear Science & Technology Organisation
 - Australian Organisation for Quality
 - Certification Interests (Australia)
 - Department of Defence (Australia)
 - Energy Networks Association
 - Engineers Australia
 - The University of New South Wales
-

This Standard was issued in draft form for comment as DR 08033.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

Equipment reliability—Reliability assessment methods

First published as AS IEC 62308—2008.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 8830 0

PREFACE

This Standard was prepared by the Standards Australia Committee QR-005, Dependability.

The objective of this Standard is to describe methods for early reliability assessment of items based on field data and test data for components and modules and applicable to mission, safety and business critical high integrity and complex items. It includes guidance on related activities, management of the reliability assessment process, and reliability programme planning and monitoring.

This Standard is identical with, and has been reproduced from IEC 62308 Ed.1.0 (2006), *Equipment reliability—Reliability assessment methods*, which is part of a suite of Standards developed by the IEC Technical Committee IEC/TC 56, Dependability, and is suitable for use in conjunction with the AS IEC 60300 series of dependability management Standards.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.
- (b) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (c) A full point should be substituted for a comma when referring to a decimal marker.

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

	<i>Page</i>
INTRODUCTION	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	3
4 Abbreviations	3
5 Symbols	4
6 Introduction to reliability assessment	4
6.1 Introductory remarks	4
6.2 Description of reliability assessment	5
7 Management of reliability assessment process	8
7.1 Purpose of reliability assessment	8
7.2 Documentation	13
8 Data needs	14
8.1 Input data	14
8.2 Data sources and types	14
8.3 Data collection, storage, and retrieval	16
9 Reliability assessment methods	16
9.1 Introduction	16
9.2 Similarity analysis	17
9.3 Durability analysis	19
9.4 Sensitivity testing and analysis	20
9.5 Handbook predictions	22
9.6 Limitations of reliability assessment results	23
10 Considerations for selecting reliability assessment methods	24
11 Reliability assessment process improvement	25
11.1 General	25
11.2 Validating reliability assessment results	25
11.3 Improving the reliability assessment process	26
Annex A (informative) Similarity analysis examples	27
Annex B (informative) Durability analysis	38
Bibliography	45

INTRODUCTION

This International Standard describes procedures that are intended for use in assessing the reliability of items based on data from: the market of similar items; and field data and test data from suppliers of components and modules. The results of such assessments are intended for use as inputs to early equipment design decisions such as system architecture selection as well as business decisions such as estimating the cost of warranties or maintenance cost guarantees. Furthermore the results can be used as the initial estimate for input to safety analysis, for example FTA analysis. Modern electronic components and items are so reliable that estimating or verifying their reliability by testing is very difficult, therefore data from the field for previous similar items are often the only way to get an initial estimate of the reliability. Component manufacturers have used this method for years under the name of the “similarity principle”. By emphasising the use of data from previously marketed similar products, and requiring similarity to be documented, the method is a modern alternative to the classical but now obsolete handbook prediction.

Reliability assessment results should be viewed as an early estimate of the probability that the product reliability targets and goals can be satisfied using the chosen architecture, modules, components and maintenance policy. As such, they may be used, for example, to authorize advancement to the next step in product development, or to authorize progress payments, or to proceed with delivery and acceptance of products. Reliability assessment results should never be used to support a claim that the reliability targets, goals, or expectations have been satisfied. The only certain measure of reliability requirement having been met is from service/field performance. This standard describes the uses for reliability assessment results as well as providing a list of IEC standards that require such results as input.

The approach to reliability assessment in this International Standard

- encourages the equipment manufacturer to consider all relevant information regarding equipment reliability which may include the effects of design and manufacturing processes as well as component selection issues. This is in contrast to more traditional methods that focus on component reliability as the most significant contributor to the equipment reliability;
- encourages the equipment manufacturer to define and use the processes that are most effective for the manufacturer's own equipment;
- describes a continuous procedure in which a reliability assessment can be updated as more information becomes available during the life cycle of the equipment. This information may be used to improve both the reliability of the equipment and the effectiveness of the assessment process.

This International Standard describes the application of three approaches to reliability assessment, namely: similarity analysis, durability analysis, and handbook predictions. This standard does not, however, provide information on assessing the reliability of software systems but can be used for assessing the reliability of hardware systems containing embedded software.

STANDARDS AUSTRALIA

Australian Standard**Equipment reliability—Reliability assessment methods****1 Scope**

This International Standard describes early reliability assessment methods for items based on field data and test data for components and modules. It is applicable to mission, safety and business critical, high integrity and complex items. It contains information on why early reliability estimates are required and how and where the assessment would be used. Finally, it details methods for reliability assessment and the data required to support the assessment. To estimate durability (life time or wear-out), the physics-of-failure method is used.

Three types of assessment are discussed in detail:

- the similarity approach;
- models for durability analysis;
- handbook methods.

Clause 6 provides an introduction to reliability assessment and Clause 7 the management of the process. Clause 8 describes the data needs, sources and types for assessments and Clause 9 provides details of the assessment methods.

Annexes A and B provide additional information to aid understanding of the similarity analysis and durability analysis.

This standard is applicable to making reliability estimates for specifications, design, design modification and support engineering.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

References to international standards that are struck through in this clause are replaced by references to Australian or Australian/New Zealand Standards that are listed immediately thereafter and identified by shading. Any Australian or Australian/New Zealand Standard that is identical to the International Standard it replaces is identified as such.

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

~~IEC 60300-1, Dependability management—Part 1: Dependability management systems~~

AS IEC 60300.1, *Dependability management— Dependability management systems*

~~IEC 60300-3-1:2003, Dependability management—Part 3-1: Application guide—Analysis techniques for dependability—Guide on methodology~~

AS IEC 60300.3.1, *Dependability management—Application guide—Analysis techniques for dependability—Guide on methodology*

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

~~IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*~~

AS IEC 60300.3.3, *Dependability management—Application guide—Life cycle costing*

IEC 60300-3-4:1996, *Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements*

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

~~IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*~~

AS/NZS 3931, *Risk analysis of technological systems—Application guide*

~~IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*~~

AS IEC 60300.3.11, *Dependability management—Application guide—Reliability centred maintenance*

~~IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*~~

AS IEC 60300.3.12, *Dependability management—Application guide—Integrated logistic support*

~~IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*~~

AS IEC 60812, *Analysis techniques for system reliability—Procedure for failure mode and effects analysis (FMEA)*

~~IEC 61025, *Fault tree analysis (FTA)*~~

AS IEC 61025, *Fault tree analysis (FTA)*

~~IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*~~

AS IEC 61078, *Analysis techniques for dependability—Reliability block diagram and Boolean methods*

~~IEC 61160, *Design review*~~

AS IEC 61160, *Design review*

~~IEC 61165, *Application of Markov techniques*~~

AS IEC 61165, *Application of Markov techniques*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61649, *Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data*

IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61713, *Software dependability through the software life-cycle processes – Application guide*

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

IEC 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191, together with the following, apply.

3.1

durability analysis

analysis of the equipment's responses to the stresses imposed by operational use, maintenance, shipping, storage and other activities throughout its specified life-cycle in order to estimate its predicted reliability and expected life

3.2

life-cycle

time interval between a product's conception and its disposal

3.3

similarity analysis

structured comparison of the elements of the equipment being assessed with those of predecessor equipment for which in-service reliability data are available

4 Abbreviations

ASIC	Application specific integrated circuit
BITE	Built in test equipment
COTS	Commercial off the shelf
FEA	Finite element analysis
FFOP	Failure free operating period
FITS	Failure per thousand million hours
FMEA	Failure mode and effects analysis
FMECA	Failure mode, effects and criticality analysis
FRACAS	Failure reporting, analysis and corrective action system
FTA	Fault tree analysis
HALT	Highly accelerated life test
IC	Integrated circuit
LCC	Life cycle costs
LRU	Line replaceable unit
MCTF	Mean cycles to failure
MTBF	Mean time between failures

MTBUR	Mean time between unit repair
MTTF	Mean time to failure
MTTR	Mean time to restoration/recovery/repair
MTTSC	Mean time to service call
MTTSI	Mean time to service interruption
MTTWC	Mean time to warranty claim
RBD	Reliability block diagram
RCM	Reliability centred maintenance
RET	Reliability enhancement test
SRU	Shop replaceable unit

5 Symbols

λ	Constant failure rate of the exponential distribution
t	Time period of interest
$f(t)$	Probability density function
$F(t)$	Cumulative distribution function
$R(t)$	Reliability function
T^*	Accumulated exposure time

6 Introduction to reliability assessment

6.1 Introductory remarks

The reliability of an item will often have to be assessed for a range of reasons including the following:

- a) setting targets and specifications;
- b) comparing options;
- c) identifying and prioritising problems;
- d) indicating fitness for purpose;
- e) optimizing support (e.g. spares);
- f) to give input to other analysis (e.g. safety analysis);
- g) to prioritise areas for improvement with the greatest cost-effectiveness improvement potential.

This reliability may be quoted in a number of ways, including for example

- accumulated percentage of failures;
- call rate;
- probability of survival;
- failure intensity;
- instantaneous failure rate;
- MTTF;
- MTBF.

The procedure outlined in this standard is aimed at providing reliability analysts, project managers, risk management engineers, designers, safety and reliability engineers, and logistic support engineers with an assessment method for an early estimate of an item's instantaneous failure rate. The process for estimating life for items with a wear-out failure characteristic is also included.

6.2 Description of reliability assessment

6.2.1 General information

Reliability is not an attribute that can be assigned or measured for a single item. It is a stochastic or probabilistic parameter and therefore it cannot be measured exactly and repeatedly. It therefore has to be estimated from information on the amount of usage (e.g. running hours, cycles of operation, etc.) and the number of failures observed. It should be presented in the form of a confidence statement such as "80 % confidence that the true probability of successfully completing the mission lies between X and Y" or "period of time of interest without failure is between 0,963 and 0,995". An explanation of confidence and confidence intervals can be found in IEC 61649.

The classical definition of reliability is the probability of providing a specified performance level for a specified duration in a specified environment. Although such a probability is a useful measure for mission-oriented, low-volume products such as spacecraft, it is rarely a suitable measure for most high-volume products for which reliability relates more to product population than the performance of a single system or a mission. Specifying a single characteristic such as mean time to failure (MTTF) is not sufficient for a product that exhibits a time-dependent failure rate (i.e. non-constant failure rate).

6.2.2 Constant failure rate reliability measures

The general expression for reliability, $R(t)$, is given by

$$R(t) = \exp\left(-\int_t^{\infty} \lambda(t) dt\right) \quad (1)$$

where $\lambda(t)$ is the instantaneous failure rate.

Another very useful (general) expression is

$$f(t) = -\frac{dR(t)}{dt} = \frac{dF(t)}{dt} \quad (2)$$

where $f(t)$ is the probability density function of times to failure. In terms of these quantities the instantaneous failure rate is given by

$$\lambda(t) = \frac{f(t)}{R(t)} \quad (3)$$

Yet another fundamental general expression is that for MTTF. This quantity is given by

$$\text{MTTF} = \int_0^{\infty} R(t) dt \quad (4)$$

Now when $\lambda(t)$ is constant with time, it should simply be written as λ . Under these circumstances, times to failure follow an exponential distribution and the following relationships hold:

$$R(t) = \exp(-\lambda t) \quad (5)$$

$$f(t) = \lambda \exp(-\lambda t) \quad (6)$$

$$\lambda(t) = \lambda \quad (7)$$

$$\text{MTTF} = \frac{1}{\lambda} \text{ often denoted by the symbol } \theta \quad (8)$$

This only holds when λ is constant.

Another useful but problematic quantity is the total accumulated number of product-hours, sometimes denoted by T^* . Under the assumption of constant failure rate there is no difference from a statistical point of view between accumulating 1 000 000 h by one product, or 1 h by 1 000 000 products. In either case a point estimate of the population failure rate if there is one failure would be 10^{-6} failures per product-hour.

The parameter λ being independent of time is referred to as the constant failure rate. A constant failure rate has many useful properties, one of which is that the mean value of the distribution of the product's time to failure is $1/\lambda$. For non-repaired items (components), this mean value represents the statistically expected average length of time until product failure, commonly called the mean life or MTTF. This means that 63 % of the items can be expected to fail from time 0 until MTTF and 37 % after the MTTF. Another useful property of the constant failure rate is that it can be estimated from a population as the fractional decrease in the number of surviving items per unit time. However, it should be noted that the exponential distribution is the only distribution for which the failure rate is a constant and that the mean life is not $1/\lambda(t)$ when the failure rate is not constant.

For repaired items, MTTF is sometimes misunderstood to be the life of the product rather than the reciprocal of the constant failure rate. If a product has an MTTF of 1 000 000 h, it does not mean that the product will last that long (longer than the average human lifetime). Rather, it means that, on average, one of the products will fail for every 1 000 000 product-hours of operation, i.e. if there are 1 000 000 products in the field on average, one of them will fail in 1 h on average. In this case, if product failures are truly exponentially distributed, then on average 63 % of the products will have failed after 1 000 000 h of operation. Products with truly exponentially distributed failures over their entire lifetime almost never occur in practice, but a constant failure rate and MTTF may in some cases be a good approximation to product failure behaviour.

Table 1 – Example of constant rate reliability measures

Constant rate measure	Mean life equivalent	Definition	Use
Constant failure rate using time	MTTF (mean time to failure)	Total failures divided by total population operating time	Standard measure for reliability predictions when time is the relevant parameter
Constant failure rate using cycles or distance instead of time	Mean cycles/km MCTF	Total failures divided by total population number of product cycles or distance, e.g. kilometres	Standard measure for reliability predictions when usage is more relevant than time. These measures are sometimes converted to time-based measures by specifying an operating profile or duty ratio
Constant restoration/repair rate	MTTR (mean time to restoration/repair)	Total restorations/repairs divided by total population operating time	Useful for sizing a repair depot or manufacturing repair line
Constant replacement rate	MTTR (mean time to replacement)	Total replacements divided by total population operating time	Used as surrogate for constant failure rate when no failure analysis is available; useful for warranty analysis
Constant service or customer call rate	MTTSC (mean time to service call)	Total service/customer calls divided by total population operating time	Customer perception of constant failure rate; useful for sizing support needs
Constant warranty claim rate	MTTWC (mean time to warranty claim)	Total warranty claims divided by warranted population operating time	Useful for pricing warranties and setting warranty reserves
Constant service interruption rate	MTTSI (mean time to service interruption)	Total service interruptions divided by total population operating time	Customer perception of constant failure rate; may be an availability measure

There are several equivalent ways of expressing the constant rate measures in Table 1. For example, a constant failure rate of 1 % per year is equivalent to $1,1 \cdot 10^{-6} \text{ h}^{-1}$, 1 100 FITs, 0,01 failures per unit per year, 1,1 failures per million hours, and 10 failures per 1 000 products per year (assuming replacement, 9,95 failures per 1 000 products per year without replacement).

6.2.3 Repaired and non-repaired item concepts

Specifying a single value, such as MTTF, is not sufficient for a product that exhibits a time-dependent failure rate.

This standard considers similarity analysis for the constant failure rate case as well as for non-constant failure rate. IEC 61649, IEC 61710 and IEC 60300-3-5 give details on statistical methods for non-constant failure rate, including Weibull analysis.

Situations may also occur when repaired items, which are restored to functionality after failure, are not repaired to a 'good-as-new' condition and so exhibit a non-constant failure intensity. IEC 60300-3-5 provides guidance on non-constant failure rate and non-constant failure intensity. MTTF should be used in case of non-repairable items and MTBF should be used in case of repairable items.

Generally it is recommended to state the failure probability, $F(t)$, of the item instead of stating MTBF or MTTR; however, if MTTF is used it should be used for non-repaired items and MTBF used for repaired items.

6.2.4 Methods for estimating reliability

The following is a list of methods commonly used for assessing reliability:

- similarity analysis;
- durability analysis;
- handbook methods.

The main benefit of a reliability assessment is the identification of the major contributions to system failure, rather than the accuracy of the absolute prediction. The identification of the sources of unreliability supports the prioritisation of actions and allows modifications to be made to the design at an early stage. This is especially important if components, modules or design solutions are reused from previous products. In this case the assessment method estimates the failure rate to be expected if improvement activities are not made. The accuracy of any prediction is determined by the quality of the data and their similarity to the proposed design and its usage and environment.

Unless new technology is being considered, a reliability assessment should be based on appropriate in-service data that are available. Data may be obtained from a number of sources. In order of preference, they are as follows:

- the same or similar equipment used in the same or similar operational, physical and support environment;
- data derived from physical and engineering analysis across the range of environmental conditions in which it will be used;
- test data or field data from component or module suppliers;
- data from industry or generic sources. Generic data sources need to be used with great caution and with lower confidence in the reliability assessment until such time as they can be replaced with better data.

There are many generic and industry specific data sources to support reliability assessments.

This standard describes a number of alternative reliability assessment methods that can provide failure rate data from an equipment level down to a functional or piece part level. When selecting a particular methodology for a specific application, a review of the accuracy and limitations of the approach to provide a justification for its usage should be documented. This justification should include the uncertainty and confidence factors associated with the results of the assessment method.

This standard does not address software issues but only covers methods for hardware items. However, it can be used for hardware items that contain embedded software. Reliability of the embedded software and its interaction with the hardware must be addressed, which may change the original reliability information.

7 Management of reliability assessment process

7.1 Purpose of reliability assessment

7.1.1 General

There are numerous reasons for assessing reliability of an item. Figure 1 illustrates some examples of the activities that require a reliability assessment as an input. For example, to calculate the spares provision for an item in the field, knowledge of the item's failure rate and exposure time would be necessary.

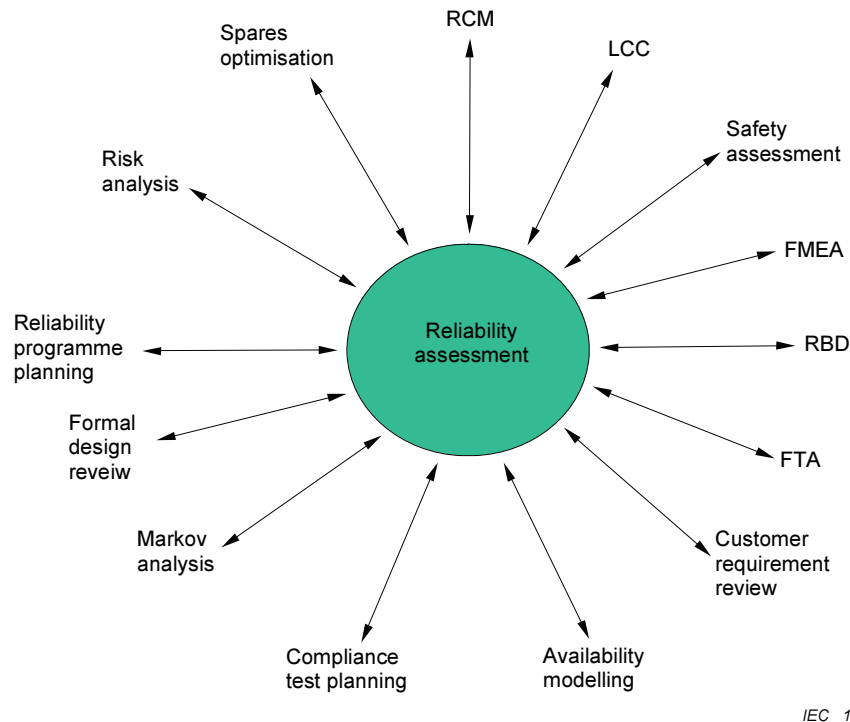


Figure 1 – Methods requiring a reliability assessment as input

Table 2 presents the IEC references for standards on the methods that require reliability assessment as an input.

Table 2 – IEC Standards providing guidance on methods

Method	IEC standard
Analysis techniques for dependability – Guide on methodology	IEC 60300-3-1
FTA	IEC 61025
FMEA	IEC 60812
RBD	IEC 61078
Requirements	IEC 60300-3-4
Design review	IEC 61160
Availability modelling	IEC 61078
Spares provision	IEC 60300-3-12
R&M programme plan	IEC 60300-1
Risk analysis	IEC 60300-3-9
Reliability Centred Maintenance	IEC 60300-3-11
Software dependability	IEC 61713
LCC	IEC 60300-3-3
Safety assessment	IEC 61882
Markov techniques	IEC 61165
Functional safety	IEC 61508
Reliability prediction	IEC 62380

A reliability assessment may be needed to fulfil the following tasks:

- a) Reliability goal assessment – Reliability assessments are used to help assess the probability that the system can satisfy its reliability goals (feasibility study).

- b) Comparisons of designs and products – Most systems have design implementation options. Tradeoffs have to be made among the various options, and reliability assessment is an important input to these tradeoffs. These options may even affect the system architecture, e.g. the amount and level of redundancy. Since tradeoffs often have to be made early in the design process, the reliability assessment may be very preliminary. However, it is still useful since the important information may be the relative reliability and ranking of design choices rather than a precise quantitative value.
- c) Method to identify and prioritise potential reliability improvement opportunities – Reliability improvement activities should generally focus on the areas with the greatest opportunity for improvement. A reliability assessment quantifies the opportunity by identifying the relative reliability of various units and by predicting the reliability improvement obtained from a reliability improvement activity.
- d) Logistics support – Reliability assessments are a key to deciding on spare part provisioning policy and estimating the costs of a warranty policy. They can also be used for the first estimate of life cycle costs.
- e) Determining the interval for 'failure finding' and 'function testing' types of maintenance tasks.
- f) Mission reliability estimation – Missions may have multiple phases with different equipment configurations, and system reliability models can be used for a first estimate of the potential reliability for the entire mission.

One further important factor when assessing reliability is 'when', i.e. at what stage in the product life cycle. To assess item reliability it is crucial to start estimating early in the product life cycle and update such assessments as more information becomes available, e.g. from test. Similarly if the assessed reliability is not acceptable, then improvement activities have to be started as early as possible in the product life cycle to ensure reliability improvements. Thus, reliability assessment and monitoring reliability growth (see IEC 61014) is crucial to the correct use of reliability assessments.

Reliability assessment results are typically used for:

- business decisions;
- system architecture decisions;
- equipment design decisions;
- safety analyses;
- reliability programme planning and monitoring.

7.1.2 Business decisions

Examples of business decisions that rely heavily upon the results of reliability assessment include warranty decisions, maintenance cost guarantees and profit sharing agreements, planned design updates, spares provisioning, maintenance scheduling, budgeting and staffing. Applicable measures may be expressed in cost of ownership terms such as service delay and cancellation or operator maintenance burden.

Since business decisions often involve proprietary, sensitive or confidential cost information, reliability assessment reports for these decisions should be carefully controlled and may be maintained separately from results for other purposes. Furthermore, the degree that this information is shared between business entities (e.g. customer, supplier, user) should be the subject of business or contractual agreements.

Prior to the selection of a reliability assessment method a number of criteria have to be considered; these include

- the desired uses of the assessment (*why*);
- the appropriate time in the system life cycle to perform the assessment (*when*);
- which business entity can most capably perform the reliability assessment (*who*);

- the item(s) for which the reliability assessment is to be performed (*what*); and
- the factors that should be considered in selecting the appropriate reliability assessment method (*how*).

7.1.3 System architecture decisions

System architecture is the high-level description, in functional terms, of the structure chosen to satisfy the design specification. This high-level description ensures that system objectives are understood by all interested parties, all relevant factors are considered in the design, all elements of the design are defined and understood at the appropriate level, all elements of the design are evaluated correctly, and alternative solutions are considered.

Examples of system architecture decisions that can be supported by assessment results are as follows:

- fault tolerant design and built-in test; e.g. test method, coverage, or frequency;
- top level hardware and/or software functional partitioning;
- functional partition between modules (block diagram);
- redundancy needs; and
- maintenance support for prognostics.

7.1.4 Equipment design decisions

Examples of equipment design decisions that should be based upon reliability assessment include, but are not limited to”

- system design, comparing hardware technologies, e.g. digital processor, digital logic array versus analogue;
- comparing circuit architecture alternatives;
- comparing utilization, duty cycle, or electrical stress derating alternatives;
- selecting or eliminating certain components;
- deciding on the level of component integration (ASIC-discrete);
- comparing packaging and assembly technology, e.g. surface mount versus through-hole;
- comparing environmental management techniques, e.g. vibration damping and cooling; and
- identifying and correcting design deficiencies in a timely manner based on field and test data of similar components, modules and design.

As with system architecture decisions, the reliability assessment results should be used to substantiate equipment design decisions.

7.1.5 Safety assessment

Safety assessment is the disciplined approach to identifying system hazards and their causes, and to assessing their risks. Safety assessment relates to the reliability assessment of safety-related functions and components. An output of reliability assessment is failure rate, which is often used in various analyses for safety assessment, for example

- fault tree analysis (FTA);
- Markov analysis;
- event tree analysis;
- FMEA; and
- FMECA.

Generic and industry data sources are often used to provide the base failure rate data in system safety assessment. However, this document describes a number of alternative reliability assessment methods that can provide failure rate data from equipment level down to functional or piece part level. (For system safety analysis, the ability to assess the reliability of specific functions is particularly important.)

NOTE IEC 61508 deals with functional safety issues.

7.1.6 Reliability programme planning and monitoring

Reliability assessment results may be used as deliverables at various milestone points in the product design, development, production, and service life cycle. Reliability programme planning should include reliability assessments based on various activities carried out at different stages in the cycle (examples include assembly screening planning, reliability development test planning and reliability verification test planning). Quantitative reliability measures such as MTTF, MTBF, failure-free operating period, time to failure, reliability growth management goals and reliability acceptance requirements should also be identified. Documentation should be produced to ensure that sufficient analysis and/or testing is conducted so that these measures can be produced with the accuracy and confidence required to support reliability programme planning decisions and update estimates in a timely manner. Bayesian statistics may be used to reduce required test sample sizes if the basis of the prior distribution is considered acceptable from an engineering point of view.

Figure 2 shows the stages of the product life cycle and how a reliability assessment may be required at each stage of the process both as an input and as an output.

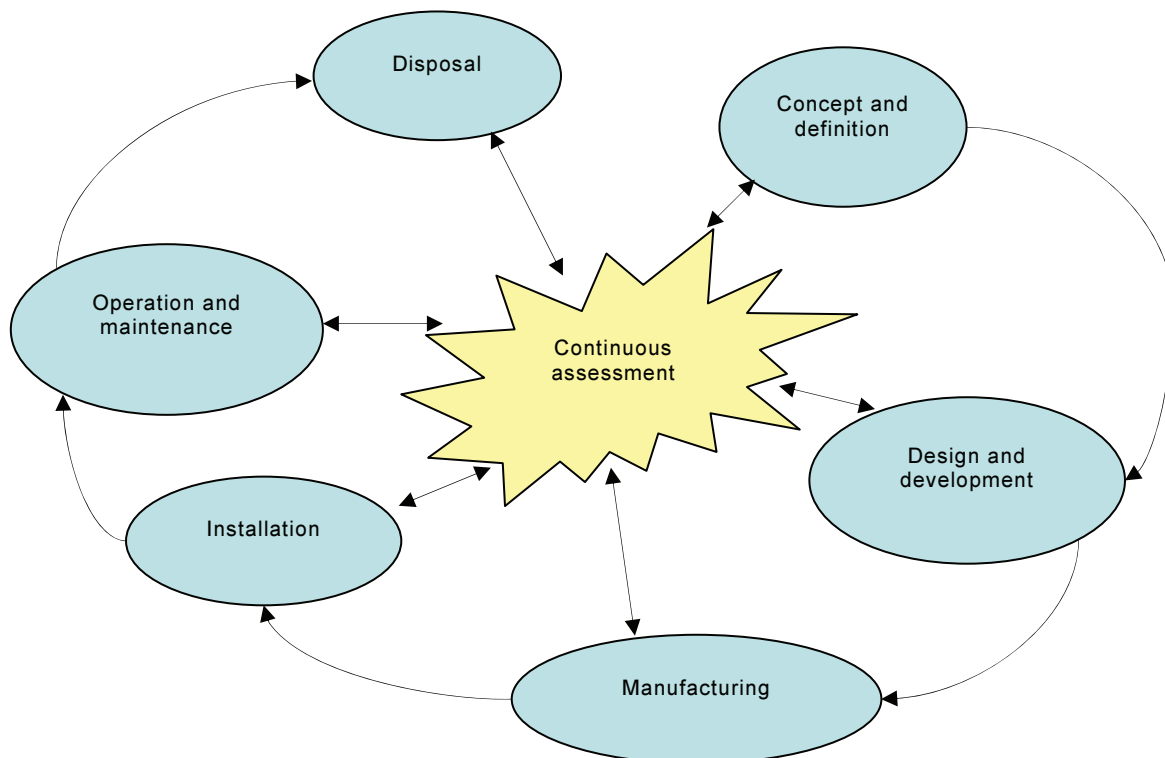


Figure 2 – Stages of product life cycle