1 Basic Concepts, Quality and Reliability Assurance of Complex Equipment and Systems

The purpose of *reliability engineering* is to develop methods and tools to *evaluate and demonstrate* reliability, maintainability, availability, and safety of components, equipment, and systems, as well as to *support* development and production engineers in *building in* these characteristics. In order to be cost and time effective, reliability engineering must be integrated in project activities, support quality assurance and concurrent engineering efforts, and be performed without bureaucracy. This chapter introduces basic concepts, shows their relationships, and discusses the tasks necessary to assure quality and reliability of complex equipment and systems with *high quality and reliability requirements.* A comprehensive list of definitions is given in Appendix A1. Standards for quality assurance (management) systems are discussed in Appendix A2. Refinements of management aspects are given in Appendices A3 - A5.

1.1 Introduction

Until the nineteen-sixties, quality targets were deemed to have been reached when the item considered was found to be free of *defects* or *systematic failures* at the time it left the manufacturer. The growing complexity of equipment and systems, as well as the rapidly increasing cost incurred by loss of operation as a consequence of failures, have brought to the forefront the aspects of *reliability, maintainability, availability*, and *safety.* The expectation today is that complex equipment and systems are not only *free from defects and systematic failures* at time $t = 0$ (when they are put into operation), but also *perform the required function failure free* for a stated time interval and *have a fail-safe behavior in case of critical or catastrophic failures.* However, the question of whether a given item will operate without failures during a stated period of time cannot be simply answered by *yes* or *no*, on the basis of a compliance test. Experience shows that *only a probability* for this occurrence can be given. This probability is a measure of the *item's*

A. Birolini, *Reliability Engineering*, 6th ed., DOI 10.1007/978-3-642-14952-8_1,
© Springer-Verlag Berlin Heidelberg 2010

reliability and can be *interpreted* as follows:

> *If n statistically identical items are put into operation at time $t = 0$ to perform a given mission and $\bar{v} \leq n$ of them accomplish it successfully, then the ratio $\bar{v} / n$ is a random variable which converges for increasing n to the true value of the reliability (Appendix A6.11).*

Performance parameters as well as *reliability, maintainability, availability,* and *safety* have to be *built in* during design & development and retained during production and operation of an item. After the introduction of some important concepts in Section 1.2, Section 1.3 gives basic tasks and rules for quality and reliability assurance of *complex equipment and systems with high quality and reliability requirements* (see Appendix A1 for a comprehensive list of definitions and Appendices A2 - A5 for a refinement of management aspects).

1.2 Basic Concepts

This section introduces important concepts used in reliability engineering and shows their relationships (see Appendix A1 for a more complete list).

1.2.1 Reliability

Reliability is a *characteristic* of an item, expressed by the *probability* that the item will perform its *required function* under *given conditions* for a *stated time interval.* It is generally designated by R. From a qualitative point of view, reliability can be defined as the *ability of the item to remain functional.* Quantitatively, reliability specifies the *probability that no operational interruptions* will occur during a stated time interval. This does not mean that *redundant* parts may not fail, such parts can fail and be repaired (without operational interruption at item (system) level). The concept of reliability thus applies to *nonrepairable* as well as to *repairable* items (Chapters 2 and 6, respectively). To make sense, a numerical statement of reliability (e. g. $R = 0.9$) must be accompanied by the definition of the *required function*, the *operating conditions,* and the *mission duration.* In general, it is also important to know whether or not the item can be considered new when the mission starts.

An *item* is a functional or structural *unit* of arbitrary complexity (e. g. component, assembly, equipment, subsystem, system) that can be considered as an *entity* for investigations. It may consist of hardware, software, or both and may also include human resources. Often, *ideal* human aspects and logistic support are assumed, even if (for simplicity) the term *system* is used instead of *technical system.*

The *required function* specifies the item's task. For example, for given inputs, the item outputs have to be constrained within specified tolerance bands (performance parameters should still be given with tolerances). The definition of the required function is the starting point for *any reliability analysis*, as it defines *failures*.

Operating conditions have an important influence on reliability, and must therefore be specified with care. Experience shows for instance, that the failure rate of semiconductor devices will double for operating temperature increase of $10-20\,^{\circ}\mathrm{C}$.

The required function and/ or operating conditions can be *time dependent*. In these cases, a *mission profile* has to be defined and all reliability figures will be related to it. A representative mission profile and the corresponding reliability targets should be given in the *item's specifications*.

Often the mission duration is considered as a parameter t, the *reliability function* is then defined by $\mathrm{R}(t)$. $\mathrm{R}(t)$ is the probability that no failure at item level will occur in the interval $(0, t]$. The item's condition at $t=0$ (new or not) influences final results. To consider this, in this book reliability figures at system level will have indices Si (e.g. $\mathrm{R}_{Si}(t)$), where S stands for system and i is the state entered at $t=0$ (Tab. 6.2). State *0*, with all elements new, is often assumed at $t=0$, yielding $\mathrm{R}_{S0}(t)$.

A distinction between *predicted* and *estimated* or *assessed* reliability is important. The first one is calculated on the basis of the item's reliability structure and the failure rate of its components (Sections 2.2 & 2.3), the second is obtained from a statistical evaluation of reliability tests or from field data by known environmental and operating conditions (Section 7.2).

The concept of reliability can be extended to processes and services as well, although *human aspects* can lead to modeling difficulties (see e.g. Section 1.2.7).

1.2.2 Failure

A *failure* occurs when the item stops performing its required function. As simple as this definition is, it can become difficult to apply it to complex items. The *failure-free time* (hereafter used as a synonym for *failure-free operating time*) is generally a *random variable*. It is often reasonably long, but it can be very short, for instance because of a failure caused by a transient event at turn-on. A general assumption in investigating failure-free times is that at $t=0$ the item is free of *defects* and *systematic failures*. Besides their *frequency*, failures should be classified (as far as possible) according to the mode, cause, effect, and mechanism:

1. *Mode*: The mode of a failure is the *symptom* (local effect) by which a failure is observed; e.g., opens, shorts, or drift for electronic components (Table 3.4); brittle rupture, creep, cracking, seizure, fatigue for mechanical components.
2. *Cause*: The cause of a failure can be *intrinsic*, due to weaknesses in the item and/or wearout, or *extrinsic*, due to errors, misuse or mishandling during the design, production, or use. Extrinsic causes often lead to *systematic failures,*

which are *deterministic* and should be considered like *defects* (dynamic defects in software quality). *Defects are present at* $t = 0$, even if often they can not be discovered at $t = 0$. *Failures appear always in time*, even if the time to failure is short as it can be with systematic or early failures.

3. *Effect*: The effect (consequence) of a failure can be different if considered on the item itself or at higher level. A usual classification is: *non relevant*, *partial*, *complete*, and *critical failure*. Since a failure can also cause further failures, distinction between *primary* and *secondary failure* is important.
4. *Mechanism*: Failure mechanism is the physical, chemical, or other process resulting in a failure (see Table 3.5 for some examples).

Failures can also be classified as *sudden* and *gradual*. In this case, sudden and complete failures are termed *cataleptic failures*, gradual and partial failures are termed *degradation failures*. As failure is not the only cause for an item being down, the general term used to define the down state of an item (not caused by a preventive maintenance, other planned actions, or lack of external resources) is *fault*. Fault is thus a state of an item and can be due to a *defect* or a *failure*.

1.2.3 Failure Rate

The *failure rate* plays an important role in reliability analysis. This Section introduces it heuristically, see Appendix A6.5 for an analytical derivation.

Let us assume that n *statistically identical*, new, and independent items are put into operation at time $t = 0$, under the same conditions, and at the time t a subset $\bar{\nu}(t)$ of these items have not yet failed. $\bar{\nu}(t)$ is a right continuous decreasing step function (Fig. 1.1). $t_1, ..., t_n$, measured from $t = 0$, are the *observed* failure-free times (times to failure) of the n items considered. They are independent realizations of a *random variable* τ (hereafter identified as failure-free time) and must not be confused with arbitrary points on the time axis ($t_1^*, t_2^*, ...$). The quantity

$$\hat{E}[\tau] = \frac{t_1 + \ldots + t_n}{n} \tag{1.1}$$

is the *empirical mean* (empirical expected value) of τ. Empirical quantities are statistical estimates, marked with ^ in this book. For $n \to \infty$, $\hat{E}[\tau]$ converges to the true mean of the failure-free time τ, $E[\tau] = MTTF$ given by Eq. (1.8) (Eq. (A6.147) and Appendix A8.1.1). The function

$$\hat{R}(t) = \frac{\bar{\nu}(t)}{n} \tag{1.2}$$

is the *empirical reliability function*. As shown in Appendix A8.1.1, $\hat{R}(t)$ converges to the reliability function $R(t)$ for $n \to \infty$.

For an arbitrary time interval $(t, t + \delta t]$, the *empirical failure rate* is defined as

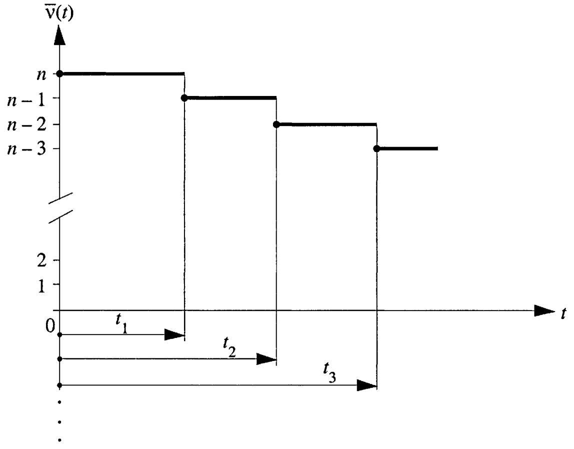


Figure 1.1 Number $\bar{\nu}(t)$ of (nonrepairable) items still operating at time t

$$\hat{\lambda}(t) = \frac{\bar{\nu}(t) - \bar{\nu}(t+\delta t)}{\bar{\nu}(t)\delta t}. \tag{1.3}$$

$\hat{\lambda}(t)\delta t$ is the ratio of the items failed in the interval $(t, t+\delta t]$ to the number of items *still operating* (or surviving) *at time t.* Applying Eq. (1.2) to Eq. (1.3) yields

$$\hat{\lambda}(t) = \frac{\hat{R}(t) - \hat{R}(t+\delta t)}{\delta t \hat{R}(t)}. \tag{1.4}$$

For R(t) derivable, $n \to \infty$ & $\delta t \to 0$, $\hat{\lambda}(t)$ converges to the (instantaneous) *failure rate*

$$\lambda(t) = \frac{-d\,R(t)/dt}{R(t)}. \tag{1.5}$$

Considering $R(0) = 1$ (at $t = 0$ all items are new), Eq. (1.5) leads to

$$R(t) = e^{-\int_0^t \lambda(x)dx}. \tag{1.6}$$

The failure rate $\lambda(t)$ given by Eqs. (1.3)-(1.5) applies in particular to *nonrepairable items* (Figs. 1.1 & 1.2). However, considering Eq. (A6.25) it can also be defined for *repairable items which are as-good-as-new after repair* (renewal), taking instead of t the variable *x starting by* $x = 0$ *at each renewal* (see e. g. Fig. 4.5). If a repairable system cannot be restored to be as-good-as-new after repair (with respect to the state considered), i. e., if at least one element with time dependent failure rate has not been renewed at every repair, *failure intensity* z(t) has to be used (see pp. 370, 418, 516 for comments). The use of *hazard rate* for $\lambda(t)$ should also be avoided.

In many practical applications, $\lambda(t)=\lambda$ can be assumed. Eq. (1.6) then yields

$$\mathrm{R}(t)=e^{-\lambda t}, \qquad \text{for} \quad \lambda(t)=\lambda, \tag{1.7}$$

and the failure-free time $\tau>0$ is *exponentially distributed* ($\mathrm{F}(t)=\Pr\{\tau \le t\}=1-e^{-\lambda t}$, Eq. (A6.81)). For this case, and only in this case, the failure rate λ can be estimated by $\hat{\lambda}=k/T$, where T is a given (fixed) cumulative operating time and k the total number of failures during T (Eqs. (7.28) and (A8.46)).

The *mean* (expected value) of the failure-free time $\tau>0$ is given by (Eq.(A6.38))

$$MTTF = E[\tau] = \int_0^\infty \mathrm{R}(t)\,dt, \tag{1.8}$$

where *MTTF* stands for *mean time to failure*. For $\lambda(t)=\lambda$ it follows that $\mathrm{E}[\tau]=1/\lambda$.

Constant (time independent) failure rate λ is often assumed also for repairable items. For the case of only 2 states (good/failed), the item is *considered as-good-as-new after each repair*, and successive failure-free times are *independent random variables*, *exponentially distributed with the same parameter* λ and mean

$$MTBF = 1/\lambda, \qquad \text{for} \quad \lambda(x)=\lambda. \tag{1.9}$$

MTBF stands for *mean operating time between failures*. Also because of the statistical estimate $\hat{MTBF}=T/k$ used in practical applications (Eq. (7.28)), *MTBF* should be confined to the case of repairable items with *constant failure rate* (p. 372). For systems with more than 2 states, based on Markov models, MUT_S is used (Eq. (6.291)).

For an item with 2 states, the only possibility to have successive *statistically identical and independent operating times* after each repair, giving a sense to a mean operating time between failures $MTBF = \mathrm{E}$ [operating time between failures], is to replace at each repair also *all not failed parts with time dependent failure rate*, to reestablish an *as-good-as-new* item (system).

The failure rate of a *large population* of *statistically identical and independent items* exhibits often a typical bathtub curve (Fig. 1.2) with the following 3 phases:

1. *Early failures*: $\lambda(t)$ decreases (in general) rapidly with time; failures in this phase are attributable to *randomly* distributed weaknesses in materials, components, or production processes.
2. *Failures with constant (or nearly so) failure rate*: $\lambda(t)$ is approximately constant; failures in this period are *Poisson distributed* and often cataleptic.
3. *Wearout failures*: $\lambda(t)$ increases with time; failures in this period are attributable to aging, wearout, fatigue, etc. (e.g. corrosion, electromigration).

Early failures are *not deterministic* and appear in general randomly distributed in time and over the items. During the early failure period, $\lambda(t)$ must not necessarily decrease as in Fig. 1.2, in some cases it can oscillate. To eliminate early failures, *burn-in* or *environmental stress screening* is used (Chapter 8). Early failures must be distinguished from *systematic failures*, which are deterministic and caused by *errors*

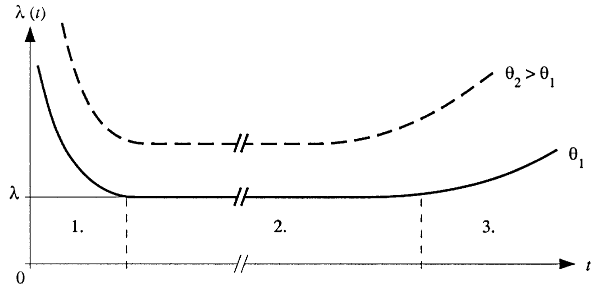


Figure 1.2 Typical shape for the failure rate of a *large population of statistically identical and independent* (nonrepairable) *items* (dashed is a possible shift for a higher stress, e. g. ambient temperature)

or *mistakes*, and whose elimination requires a *change* in design, production process, operational procedure, documentation or other. Length of early failure period varies greatly in practice, from some few to some 1'000 h. The presence of a period with *constant* (or nearly so) *failure rate* $\lambda(t)=\lambda$ is realistic for many equipment & systems, and useful for calculations. The *memoryless property,* which characterizes this period, leads to exponentially distributed failure-free times (times to failure) and to a (time homogeneous) *Markov process* for the time behavior of a repairable item if also *constant repair rates* can be assumed (Chapter 6). An *increasing failure rate* after a given operating time (> 10 years for many electronic equipment) is *typi-cal for* most items and appears because of degradation phenomena due to wearout.

A possible explanation for the shape of $\lambda(t)$ given in Fig. 1.2 is that the population of n statistically identical and independent items contains $n\,p_f$ weak elements and $n(1-p_f)$ good ones. The distribution of the failure-free time can then be expressed by a *weighted sum* of the form $\mathrm{F}(t)=p_f\,\mathrm{F}_1(t)+(1-p_f)\mathrm{F}_2(t)$. For calculation or simulation purposes, $\mathrm{F}_1(t)$ can be a gamma distribution with $\beta<1$ and $\mathrm{F}_2(t)$ a shifted Weibull distribution with $\beta>1$ (Eqs. (A6.34), (A6.96), (A6.97)).

The failure rate strongly depends upon the item's *operating conditions*, see e.g. Figs. 2.5 & 2.6 and Table 2.3. Typical figures for λ are 10^{-10} to $10^{-7}\,\mathrm{h}^{-1}$ for electronic components at 40°C, doubling for a temperature increase of 10 to 20°C.

The concept of failure rate also applies to humans and a shape similar to that depicted in Fig. 1.2 can be obtained from a mortality table.

From Eqs. (1.3) - (1.5) one recognizes that for an *item new at* $t=0$ and $\delta t \to 0$, $\lambda(t)\delta t$ is the *conditional* probability for failure in $(t, t+\delta t]$ *given that the item has not failed in* $(0, t]$. Thus, $\lambda(t)$ is *not a density* as defined by Eq. (A6.23) and must be clearly distinguished from the density $\mathrm{f}(t)$ of the failure-free time ($\mathrm{f}(t)\delta t$ is the *unconditional* probability for failure in $(t, t+\delta t]$), from the *failure intensity* $\mathrm{z}(t)$ of an arbitrary point process, and form the *intensity* $\mathrm{h}(t)$ or $\mathrm{m}(t)$ of a renewal or Poisson process (Eqs. (A7.228), (A7.18), (A7.193)); this also in the case of a homogeneous Poisson process, see pp. 370, **418**, 458, 516 for deeper considerations.

1.2.4 Maintenance, Maintainability

Maintenance defines the set of activities performed on an item to *retain* it in or to *restore* it to a specified state. Maintenance is thus subdivided into *preventive maintenance,* carried out at predetermined intervals to reduce wearout failures, and *corrective maintenance,* carried out after failure detection and intended to put the item into a state in which it can again perform the required function. Aim of a preventive maintenance is also to detect and repair *hidden failures*, i.e., failures in redundant elements not detected at their occurrence. Corrective maintenance is also known as *repair*, and can include any or all of the following steps: *detection*, *localization* (isolation), *correction*, *checkout*. *Repair* is used in this book as a synonym for *restoration*, by neglecting delays (logistic & administrative). To simplify calculations, it is generally assumed that *the element in the reliability block diagram* for which a maintenance action has been performed is *as-good-as-new* after maintenance. This assumption is *valid for the whole equipment or system in the case of constant failure rate* for all elements which have not been repaired or replaced.

Maintainability is a *characteristic* of an item, expressed by the *probability* that a *preventive maintenance* or a *repair* of the item will be performed within a stated *time interval* for given *procedures and resources* (skill level of personnel, spare parts, test facilities, etc.). From a qualitative point of view, maintainability can be defined as the *ability of an item to be retained in or restored to a specified state.* The *mean* (expected value) of the repair time is denoted by *MTTR* (mean time to repair (restoration)), that of a preventive maintenance by *MTTPM.* Maintainability has to be *built into* complex equipment or systems *during design and development* by realizing a *maintenance concept.* Due to the increasing maintenance cost, maintainability aspects have grown in importance. However, maintainability achieved in the field largely depends on the resources available for maintenance (human and material), as well as on the correct installation of the equipment or system, i. e. on the *logistic support* and *accessibility*.

1.2.5 Logistic Support

Logistic support designates all activities undertaken to provide effective and economical use of an item during its operating phase. To be effective, logistic support should be integrated into the *maintenance concept* of the item under consideration and include after-sales service.

An emerging aspect related to maintenance and logistic support is that of *obsolescence management,* i.e., how to assure functionality over a long operating period (e. g. 20 years) *when technology is rapidly evolving* and components need for maintenance are no longer manufactured. Care has to be given here to *design aspects,* to assure *interchangeability* during the equipment's useful life without important redesign (standardization has been started [1.5, 1.11, A2.5 (IEC 62402)]).

1.2.6 Availability

Availability is a broad term, expressing the ratio of delivered to expected service. It is often designated by A and used for the stationary & steady-state value of the point and average availability ($PA = AA$). *Point availability* (PA(t)) is a characteristic of an item expressed by the *probability* that the item will perform its *required function* under *given conditions* at a stated *instant of time t*. From a qualitative point of view, *point availability* can be defined as the *ability of the item to perform its required function under given conditions at a stated instant of time* (*dependability*).

Availability evaluations are often difficult, as *logistic support* and *human factors* should be considered in addition to reliability and maintainability. *Ideal* human and logistic support conditions are thus often assumed, yielding to the *intrinsic* (inherent) *availability*. In this book, *availability* is used as a synonym for *intrinsic availability*. Further assumptions for calculations are continuous operation and *complete renewal of the repaired element* in the reliability block diagram (assumed as-good-as-new after repair). For a given item, the point availability $\mathrm{PA}(t)$ rapidly converges to a *stationary & steady-state value*, given by (Eq. (6.48))

$$PA = \frac{MTTF}{MTTF + MTTR} . \tag{1.10}$$

PA is also the stationary & steady-state value of the *average availability* (AA) giving the *mean* (expected value) of the *percentage of the time* during which the item performs its required function. PA_S and AA_S is used for considerations at system level. Other availability measures can be defined, e.g. *mission availability*, *work-mission availability*, *overall availability* (Sections 6.2.1.5, 6.8.2). Application specific figures are also known, see e.g. [6.12]. In contrast to reliability analyses for which *no failure at item (system) level* is allowed (only redundant parts can fail and be repaired on line), availability analyses *allow failures at item (system) level.*

1.2.7 Safety, Risk, and Risk Acceptance

Safety is the ability of the item not to cause injury to persons, nor significant material damage or other unacceptable consequences during its use. Safety evaluation must consider the following two aspects: Safety when the item functions and is operated correctly and safety when the item or a part of it has failed. The first aspect deals with *accident prevention*, for which a large number of national and international regulations exist. The second aspect is that of *technical safety* which is investigated using similar tools as for reliability. However, a distinction between technical safety and reliability is necessary. While safety assurance examines measures which allow the item to be brought into a *safe state* in the case of failure (*fail-safe behavior*), reliability assurance deals more generally with measures for minimizing the total number of failures. Moreover, for technical safety the effects of *external influences* like human errors, catastrophes, sabotage, etc. are of great importance and must be considered carefully. The safety level of an item influences the number of *product liability claims*. However, increasing in safety can reduce reliability.

Closely related to the concept of (technical) safety are those of *risk, risk management,* and *risk acceptance*; including risk analysis & assessment [1.9, 1.21, 1.26, 1.28]. Risk problems are often *interdisciplinary* and have to be solved in *close cooperation between engineers and sociologists* to find common solutions to controversial questions. An appropriate weighting between *probability of occurrence* and *effect* (consequence) of a given accident is important. The *multiplicative rule* is one among different possibilities. Also it is necessary to consider the different *causes* (machine, machine & human, human) and *effects* (location, time, involved people, effect duration) of an accident. Statistical tools can support *risk assessment*. However, although the behavior of a homogenous human population is often known, experience shows that the reaction of a *single person* can become unpredictable. Similar difficulties also arise in the evaluation of *rare events* in complex systems. Risk analysis is basically performed with tools used for failure modes analysis (Section 2.6). However, for high-risk systems, refinements are often necessary, for instance, using the *risk priority number concept* with logarithmic scale [2.82].

Quite generally, considerations on risk and risk acceptance should take into account that the probability p_1 for a given accident which can be caused by one of n statistically identical and *independent* items, each of them with occurrence probability p, is for np small nearly equal to np as per

$$p_1 = n\,p(1-p)^{n-1} \approx n\,p\,e^{-np} \approx n\,p(1-n\,p) \approx n\,p. \tag{1.11}$$

Equation (1.11) follows from the binomial distribution and the Poisson approximation (Eqs. (A6.120) & (A6.129)). It also applies with $n\,p = \lambda_{tot} T$ to the case in which one assumes that the accident occurs randomly in the interval $(0, T]$, caused by one of n *independent* items (systems) with failure rates $\lambda_1, \ldots, \lambda_n$, where $\lambda_{tot} = \lambda_1 + \ldots + \lambda_n$. This is because the *sum of n independent Poisson processes is again a Poisson process* (Eq. (7.27)) and the probability $\lambda_{tot} T e^{-\lambda_{tot} T}$ for one failure in the interval $(0, T]$ is nearly equal to $\lambda_{tot} T$. Thus, for $n\,p \ll 1$ or $\lambda_{tot} T \ll 1$ it holds that

$$p_1 \approx n\,p \approx (\lambda_1 + \ldots + \lambda_n)\,T. \tag{1.12}$$

Also by assuming a reduction of the individual occurrence probability p (or failure rate λ_i), one recognizes that in the future it will be necessary either to *accept greater risks* p_1 or to keep the spread of high-risk technologies under *tighter control*. Similar considerations apply to *environmental stresses* caused by mankind. Aspects of *ecologically acceptable* production, use, disposal, and *recycling* or *reuse* of products should become subject for international regulations, in the general context of *sustainable development*.

In the context of a *product development,* risks related to *feasibility* and *time to market* within the given cost constraints must also be considered during all development phases (*feasibility checks* in Fig. 1.6 and Tables A3.3 & 5.3).

Mandatory for *risk management* are psychological aspects related to *risk awareness* and *safety communication.* As long as a *danger for risk* is not perceived, people often do not react. Knowing that a *safety behavior* presupposes a risk awareness, *communication* is an important tool to avoid that the risk related to a given system will be underestimated, see e.g. [1.26].

1.2.8 Quality

Quality is understood as the *degree to which a set of inherent characteristics fulfills requirements.* This definition, given now also in the ISO 9000 family [A1.6], follows closely the traditional definition of quality, expressed by *fitness for use*, and applies to products and services as well.

1.2.9 Cost and System Effectiveness

All previously introduced concepts are interrelated. Their relationship is best shown through the concept of cost effectiveness, as given in Fig. 1.3. *Cost effectiveness* is a measure of the ability of the item to meet a service demand of stated quantitative characteristics, with the best possible usefulness to life-cycle cost ratio. It is often referred also to as *system effectiveness.* Figure 1.3 deals essentially with technical and cost aspects. Some management aspects are considered in Appendices A2 - A5. From Fig. 1.3, one recognizes the central role of *quality assurance,* bringing together all assurance activities (Section 1.3.3), and of *dependability* (collective term for availability performance and its influencing factors).

As shown in Fig. 1.3, *life-cycle cost* (LCC) is the sum of cost for acquisition, operation, maintenance, and disposal of the item. For complex systems, higher reliability leads in general to higher acquisition cost and lower operating cost, so that the optimum of life-cycle cost seldom lies at extremely low or high reliability figures. For such a system, per year operating & maintenance cost often exceeds 10% of acquisition cost, and experience shows that up to 80% of the life-cycle cost is frequently generated by decisions early in the design phase. To be complete, life-cycle cost should also take into account *current and deferred damage to the environment* caused by production, use, and disposal of the item. Life-cycle cost optimization falls within the framework of *cost effectiveness* or *systems engineering*. It can be positively influenced by *concurrent engineering* [1.16, 1.22]. Figure 1.4 shows an example of the influence of the attainment level of quality and reliability targets on the sum of cost of quality and operational availability assurance for two systems with different mission profiles [2.2 (1986)], see Example 1.1 for an introduction.

Example 1.1

An assembly contains n independent components each with a *defective probability* p. Let c_k be the cost to replace k defective components. Determine (i) the mean (expected value) $C_{(i)}$ of the total replacement cost (no defective components are allowed in the assembly) and (ii) the mean of the total cost (test and replacement) $C_{(ii)}$ if the components are submitted to an incoming inspection which reduces defective percentage from p to p_0 (test cost c_t per component).

Solution

(i) The solution makes use of the *binomial distribution* (Appendix A6.10.7) and question (i) is also solved in Example A6.19. The probability of having exactly k defective components in a lot of size n is given by (Eq. (A6.120))

$$p_k = \binom{n}{k} p^k (1-p)^{n-k}. \qquad (1.13)$$

The mean $C_{(i)}$ of the total cost (deferred cost) caused by the defective components follows then from

$$C_{(i)} = \sum_{k=1}^{n} c_k p_k = \sum_{k=1}^{n} c_k \binom{n}{k} p^k (1-p)^{n-k}. \qquad (1.14)$$

(ii) To the cost caused by the defective components, calculated from Eq. (1.14) with p_0 instead of p, one must add the incoming inspection cost $n\,c_t$

$$C_{(ii)} = nc_t + \sum_{k=1}^{n} c_k \binom{n}{k} p_0^k (1-p_0)^{n-k}. \qquad (1.15)$$

The difference between $C_{(i)}$ and $C_{(ii)}$ gives the gain (or loss) obtained by introducing the incoming inspection, allowing thus a *cost optimization* (see also Section 8.4 for a deeper discussion).

Using Eq. (A7.42) instead of (A6.120), similar considerations to those in Example 1.1 yield for the *mean* (expected value) of the total repair cost C_{cm} during the cumulative operating time T of an item with failure rate λ and cost c_{cm} per repair

$$C_{cm} = \lambda\, T\, c_{cm} = \frac{T}{MTBF} c_{cm}. \qquad (1.16)$$

(In Eq. (1.16), the term λT gives the mean value of the number of failures during T (Eq. (A7.42)), and $MTBF$ is used as $MTBF = 1/\lambda$.)

From the above considerations, the following equation expressing the *mean* C of the sum of the cost for quality assurance and for the assurance of reliability, maintainability, and logistic support of a system can be obtained

$$C = C_q + C_r + C_{cm} + C_{pm} + C_l + \frac{T}{MTBF_S} c_{cm} + (1 - OA_S) T c_{off} + n_d c_d. \qquad (1.17)$$

Thereby, q is used for quality, r for reliability, cm for corrective maintenance, pm for preventive maintenance, l for logistic support, *off* for down time & d for defects.

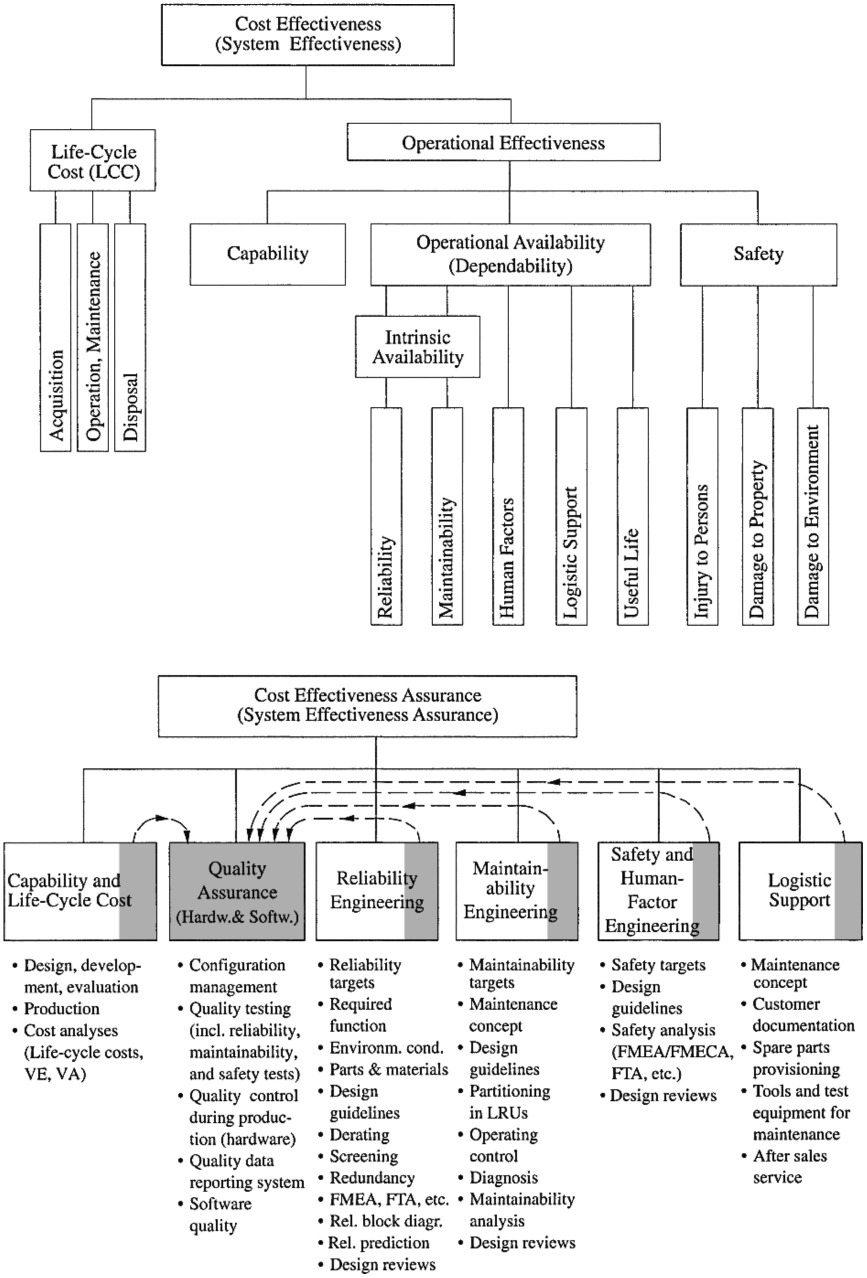


Figure 1.3 Cost Effectiveness (System Effectiveness) for *complex equipment & systems with high quality and reliability requirements* (see Appendices A1 - A5 for definitions and management aspects; dependability can be used instead of operational availability, for a qualitative meaning)

$MTBF_S$ and OA_S are the system mean operating time between failures (assumed here $= 1/\lambda_S$) and the system steady-state *overall availability* (Eq. (6.196) with T_{pm} instead of T_{PM}). T is the total system operating time (useful life) and n_d is the number of *hidden defects* discovered (and eliminated) in the field. C_q, C_r, C_{cm}, C_{pm}, and C_l are the cost for quality assurance and for the assurance of reliability, repairability, serviceability, and logistic support, respectively. c_{cm}, c_{off}, and c_d are the cost per repair, per hour down time, and per hidden defect, respectively (preventive maintenance cost are scheduled cost, considered here as a part of C_{pm}). The first five terms in Eq. (1.17) represent a part of the *acquisition cost*, the last three terms are *deferred cost* occurring during field operation. A model for investigating the cost C according to Eq. (1.17) was developed in [2.2 (1986)], by assuming C_q, C_r, C_{cm}, C_{pm}, C_l, $MTBF_S$, OA_S, T, c_{cm}, c_{off}, and c_d as parameters and investigating the variation of the total cost expressed by Eq. (1.17) as a function of the level of attainment of the specified targets, i.e., by introducing the variables $g_q = QA/QA_g$, $g_r = MTBF_S / MTBF_{Sg}$, $g_{cm} = MTTR_{Sg}/MTTR_S$, $g_{pm} = MTTPM_{Sg} / MTTPM_S$, and $g_l = MLD_{Sg} / MLD_S$, where the subscript g denotes the specified target for the corresponding quantity. A power relationship

$$C_i = C_{ig}\, g_i^{\,m_i} \tag{1.18}$$

was assumed between the actual cost C_i, the cost C_{ig} to reach the specified target (goal) of the considered quantity, and the *level of attainment* of the specified target ($0 < m_l < 1$ and all other $m_i > 1$). The following relationship between the number of hidden defects discovered in the field and the ratio C_q / C_{qg} was also included in the model

$$n_d = \frac{1}{(C_q / C_{qg})^{m_d}} - 1 = \frac{1}{g_q^{\,m_q m_d}} - 1. \tag{1.19}$$

The final equation for the cost C as function of the variables g_q, g_r, g_{cm}, g_{pm}, and g_l follows then as (using Eq. (6.196) for OA_S)

$$C = C_{qg} g_q^{\,m_q} + C_{rg} g_r^{\,m_r} + C_{cmg} g_{cm}^{\,m_{cm}} + C_{pmg} g_{pm}^{\,m_{pm}} + C_{lg} g_l^{\,m_l} + \frac{T c_{cm}}{g_r MTBF_{Sg}}$$
$$+ \Big(1 - \frac{1}{1 + \frac{1}{g_r g_{cm}} \cdot \frac{MTTR_{Sg}}{MTBF_{Sg}} + \frac{1}{g_r g_l} \cdot \frac{MLD_{Sg}}{MTBF_{Sg}} + \frac{MTTPM_{Sg}}{g_{pm} T_{pm}}}\Big) T c_{off} + \Big(\frac{1}{g_q^{\,m_q m_d}} - 1\Big) c_d . \tag{1.20}$$

The relative cost C / C_g given in Fig. 1.4 is obtained by dividing C by the value C_g form Eq. (1.20) with all $g_i = 1$. Extensive analyses with different values for m_i, C_i, $MTBF_S$, OA_S, T, c_{cm}, c_{off}, and c_d have shown that the value C / C_g is only moderately sensitive to the parameters m_i.

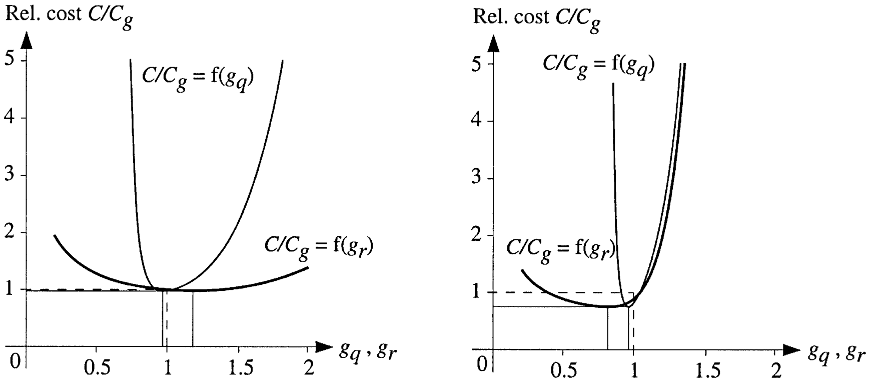


Figure 1.4 Basic shape of the relative cost C/C_g per Eq. (1.20) as function of $g_q = QA/QA_g$ and $g_r = MTBF_S/MTBF_{S_g}$ (quality assurance and reliability assurance as in Fig. 1.3) for two complex systems with different mission profiles (the specified targets $g_q = 1$ and $g_r = 1$ are dashed)

1.2.10 Product Liability

Product liability is the onus on a manufacturer (producer) or others to compensate for losses related to injury to persons, material damage, or other unacceptable consequences caused by a product (item). The manufacturer *has to specify a safe operational mode* for the product (user documentation). In legal documents related to product liability, the term *product* often indicates *hardware* only and the term *defective product* is in general used instead of *defective* or *failed product.* Responsible in a product liability claim are all those people involved in the design, production, sale, and maintenance of the product (item), inclusive suppliers. Often, *strict liability* is applied (the manufacturer has to demonstrate that the product was free from defects). This holds in the USA and increasingly in Europe [1.10]. However, in Europe the causality between damage and defect has still to be demonstrated by the user.

The rapid increase of product liability claims (alone in the USA, 50,000 in 1970 and over one million in 1990) cannot be ignored by manufacturers. Although such a situation has probably been influenced by the peculiarity of US legal procedures, *configuration management* and *safety analysis* (in particular *causes-to-effects* analysis, i.e., FMEA/FMECA or FTA as introduced in Section 2.6) as well as considerations on risk management should be performed to *increase safety* and avoid product liability claims (see Sections 1.2.7 & 2.6, and Appendix A.3.3).

1.2.11 Historical Development

Methods and procedures of quality assurance and reliability engineering have been developed extensively over the last 50 years. For indicative purpose, Table 1.1 summarizes the major steps of this development and Fig. 1.5 shows the approximate distribution of the relative effort between quality assurance and reliability engineering during the same period of time. Because of the rapid progress of microelectronics, considerations on *redundancy*, *fault-tolerance*, *test strategy*, and *software quality* have increased in importance. A skillful, allegorical presentation of the *story of reliability* (as an *Odyssey*) is given in [1.25].

Table 1.1 Historical development of quality assurance (management) and reliability engineering

before 1940	Quality attributes and characteristics are defined. In-process and final tests are carried out, usually in a department within the production area. The concept of *quality of manufacture* is introduced.
1940 - 50	Defects and failures are systematically collected and analyzed. *Corrective actions* are carried out. *Statistical quality control* is developed. It is recognized that quality must be *built into* an item. The concept *quality of design* becomes important.
1950 - 60	*Quality assurance* is recognized as a means for developing and manufacturing an item with a specified quality level. *Preventive measures* (actions) are added to tests and corrective actions. It is recognized that correct short-term functioning does not also signify *reliability*. *Design reviews* and systematic analysis of failures (failure data and failure mechanisms), performed often in the research & development area, lead to important reliability improvements.
1960 - 70	Difficulties with respect to reproducibility and change control, as well as interfacing problems during the integration phase, require a refinement of the concept of *configuration management*. Reliability engineering is recognized as a means of developing and manufacturing an item with specified reliability. R*eliability estimation methods and demonstration tests* are developed. It is recognized that reliability cannot easily be demonstrated by an *acceptance test*. Instead of a reliability figure (λ or $MTBF = 1/\lambda$), the contractual requirement is for a *reliability assurance program*. *Maintainability*, *availability*, and *logistic support* become important.
1970 - 80	Due to the increasing complexity and cost for maintenance of equipment and systems, the aspects of *man-machine interface* and *life-cycle cost* become important. Terms like *product assurance*, *cost effectiveness* and *systems engineering* are introduced. *Product liability* becomes important. Quality and reliability assurance activities are made *project specific* and carried out in *close cooperation* with all engineers involved in a project. Customers require demonstration of reliability and maintainability during the warranty period.
1980 - 90	The aspect of *testability* gains in significance. *Test and screening strategies* are developed to reduce testing cost and warranty services. Because of the rapid progress in microelectronics, greater possibilities are available for *redundant* and *fault tolerant structures*. The concept of *software quality* is introduced.
after 1990	The necessity to further shorten the development time leads to the concept of *concurrent engineering*. *Total Quality Management* (*TQM*) appears as a refinement to the concept of quality assurance as used at the end of the seventies.

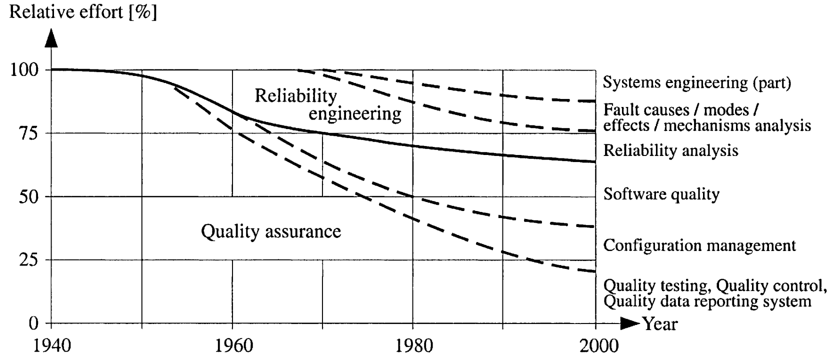


Figure 1.5 Approximate distribution of the relative effort between quality assurance and reliability engineering for *complex equipment and systems*

1.3 Basic Tasks & Rules for Quality and Reliability Assurance of Complex Systems

This section deals with some important considerations on the organization of quality and reliability assurance in the case of *complex equipment and systems with high quality and reliability requirements.* This minor part of the book aims to support managers in answering the question of *how to specify and realize high reliability targets for complex equipment and systems when tailoring is not mandatory.* Refinements are in Appendices A1 - A5, with considerations on *quality management* and *total quality management* (*TQM*) as well. As a general rule, quality assurance and reliability engineering must avoid bureaucracy, be integrated in project activities, and support quality management and *concurrent engineering* efforts, as per *TQM.*

1.3.1 Quality and Reliability Assurance Tasks

Experience shows that the development and production of complex equipment and systems with *high* reliability, maintainability, availability, and / or safety targets requires *specific activities* during all life-cycle phases of the item considered. For complex equipment and systems, Fig. 1.6 shows the *life-cycle phases* and Table 1.2 gives *main tasks* for quality and reliability assurance. Depicted in Table 1.2 is also the period of time over which the tasks have to be performed. Within a project, the tasks of Table 1.2 must be refined in a project-specific quality and reliability *assurance program* (Appendix A3).

Table 1.2 Main tasks for quality and reliability assurance of *complex equipment and systems with high quality and reliability requirements* (the bar height is a measure of the relative effort)

Main tasks for quality and reliability assurance of *complex equipment and systems*, conforming to TQM (see Table A3.2 for more details and for task assignment)	Project-independent	Specific during					
		Conception	Definition	Design & Devel.	Evaulation	Production	Use
1. Customer and market requirements	▂	█	▁	▁	▁	▁	▁
2. Preliminary analyses		▄	█	▁	▁	▁	
3. Quality and reliability aspects in specs, quotations, contracts, etc.		▄	█	▁	▁	▁	
4. Quality and reliability assurance program		▂	▆	▂	▆	▂	
5. Reliability and maintainability analyses			▂	█	▂	▁	▁
6. Safety and human factor analyses			▂	█	▄	▁	▁
7. Selection and qualification of components and materials			▂	▆	▄	▂	
8. Supplier selection and qualification			▁	▄	▆	▄	
9. Project-dependent procedures and work instructions			▄	▆	▁	▆	
10. Configuration management		▁	▂	▆	▂	▆	▂
11. Prototype qualification tests			▁	▂	█		
12. Quality control during production				▄	▄	█	
13. In-process tests				▂	▄	█	
14. Final and acceptance tests		▁	▁	▁	▄	█	▂
15. Quality data reporting system					▂	█	▂
16. Logistic support		▂	▂	▆	▂	▂	▄
17. Coordination and monitoring	▄	▁	▁	▄	▁	▄	▁
18. Quality costs	▁	▁	▁	▄	▂	▆	▁
19. Concepts, methods, and general procedures (quality and reliability)	█			▂	▂	▂	
20. Motivation and training	█			▄	▁	▄	

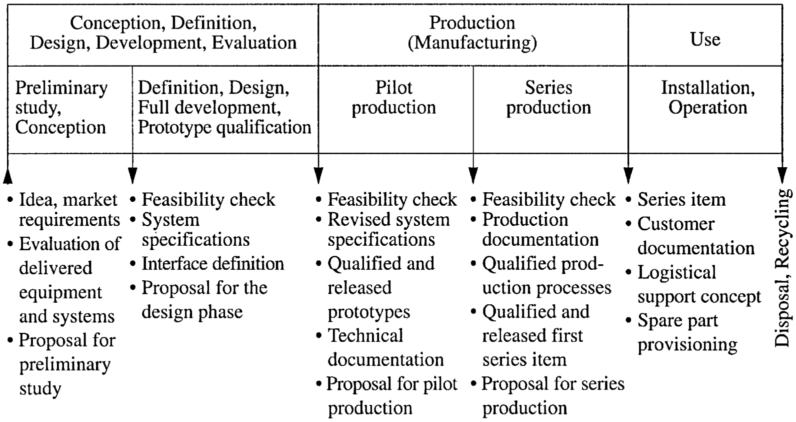

Conception, Definition, Design, Development, Evaluation
Production (Manufacturing)
Use
Preliminary study, Conception
Definition, Design, Full development, Prototype qualification
Pilot production
Series production
Installation, Operation
• Idea, market requirements
• Evaluation of delivered equipment and systems
• Proposal for preliminary study
• Feasibility check
• System specifications
• Interface definition
• Proposal for the design phase
• Feasibility check
• Revised system specifications
• Qualified and released prototypes
• Technical documentation
• Proposal for pilot production
• Feasibility check
• Production documentation
• Qualified production processes
• Qualified and released first series item
• Proposal for series production
• Series item
• Customer documentation
• Logistical support concept
• Spare part provisioning
Disposal, Recycling

Figure 1.6 Basic life-cycle phases of *complex equipment and systems* (the output of a given phase is the input to the next phase; see Tab. 5.3 for software)

1.3.2 Basic Quality and Reliability Assurance Rules

Performance, dependability, cost, and time to market are key factors for today's products and services. Taking care of the considerations in Section 1.3.1, the *basic rules* for a quality and reliability assurance optimized by considering cost and time schedule aspects (conforming to *TQM*) can be summarized as follows:

1. Quality and reliability targets should be just as high as necessary to satisfy real customer needs

   → *Apply the rule "as-good-as-necessary".*

2. Activities for quality & reliability assurance should be performed continuously throughout *all project phases*, from definition to operating phase (Table 1.2)

   → *Do not change the project manager before ending the pilot production.*

3. Activities must be performed in close cooperation between all engineers involved in the project (Table A3.2)

   → *Use TQM and concurrent engineering approaches.*

4. Quality and reliability assurance activities should be monitored by a central quality & reliability assurance department (Q & RA), which cooperates a*ctively* in all project phases (Fig. 1.7 and Table A3.2)

   → *Establish an efficient and independent quality & reliability assurance department* (Q & RA) *active in the projects.*

Figure 1.7 shows a basic organization which could embody the above rules and satisfy requirements of *quality management standards* (Appendix A2). As shown in Table A3.2, the assignment of quality and reliability assurance tasks should be such, that every engineer in a project *bears his/her own responsibilities* (as per *TQM*). A design engineer should for instance be responsible for all aspects of his/her own product (e. g. an assembly) including reliability, maintainability & safety, and the production department should be able to manufacture and test such an item within its own competence. The *quality & reliability assurance department* (Q & RA in Fig. 1.7) can be for instance responsible for (see also Tab. A3.2)

- setting targets for reliability and quality levels,
- preparation of guidelines and working documents (quality and reliability aspects),
- coordination of the activities belonging to quality and reliability assurance,
- reliability analyses at system level,
- qualification, testing, and screening of components and material (quality and reliability aspects),
- release of manufacturing processes (quality and reliability aspects),
- development and operation of the quality data reporting system,
- acceptance testing.

This central quality and reliability department should not be too small (credibility) nor too large (sluggishness).

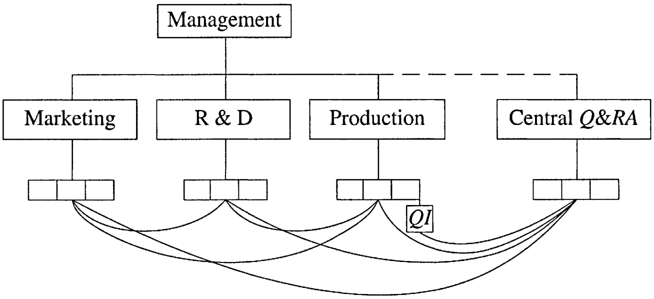


Figure 1.7 Basic organizational structure for quality & reliability assurance in a company producing *complex equipment and systems with high quality (Q), reliability (R), and / or safety requirements* (connecting lines indicate close cooperation; *A* denotes assurance, *I* inspection)

1.3.3 Elements of a Quality Assurance System

As stated in Sections 1.3.1, many of the tasks associated with *quality assurance* (here in the sense of *quality management* as per *TQM*) are *interdisciplinary* in nature. In order to have a minimum impact on cost and time schedules, their solution requires the *concurrent efforts* of *all engineers involved in a project.* To improve coordination, it can be useful to group the quality assurance activities into the following basic areas (Fig. 1.3):

1. *Configuration Management*: Procedure used to specify, describe, audit & release the configuration of the item, as well as to control it during modifications or changes. Configuration management is an important tool for quality assurance. It can be subdivided into configuration *identification*, *auditing (design reviews)*, *control*, and *accounting* (Appendix A3.3.5).
2. *Quality Tests*: Tests to verify whether the item conforms to specified requirements. Quality tests include incoming inspections, as well as qualification tests, production tests, and acceptance tests. They also cover reliability, maintainability, safety, and software aspects. To be cost effective, quality tests must be coordinated and integrated into a *test strategy*.
3. *Quality Control During Production*: Control (monitoring) of the production processes and procedures to reach a stated quality of manufacturing.
4. *Quality Data Reporting System* (*QDS, FRACAS*): A system to collect, analyze, and correct all defects and failures (faults) occurring during the production and test of an item, as well as to evaluate and feedback the corresponding quality and reliability data. Such a system is generally computer assisted. Analysis of failures and defects must be traced to the *cause*, to *avoid repetition* of the same problem.
5. *Software quality*: Special procedures and tools to specify, develop, and test software (Section 5.3).

Configuration management spans from the definition up to the operating phase (Appendices A3 & A4). Quality tests encompasses technical and statistical aspects (Chapters 3, 7, and 8). The concept of a quality data reporting system is depicted in Fig. 1.8 (see Appendix A5 for basic requirements). Table 1.3 shows an example of data reporting sheets for PCBs evaluation.

The quality and reliability assurance system must be described in an appropriate *quality handbook* supported by the company management. A possible content of such a handbook for a company producing *complex equipment and systems with high quality & reliability requirements* can be: • General, • Project Organization, • Quality Assurance (Management) system, • Quality & Reliability Assurance Program, • Reliability Engineering, • Maintainability Engineering, • Safety Engineering, • Software Quality Assurance, • Logistic Support, • Motivation & Training.

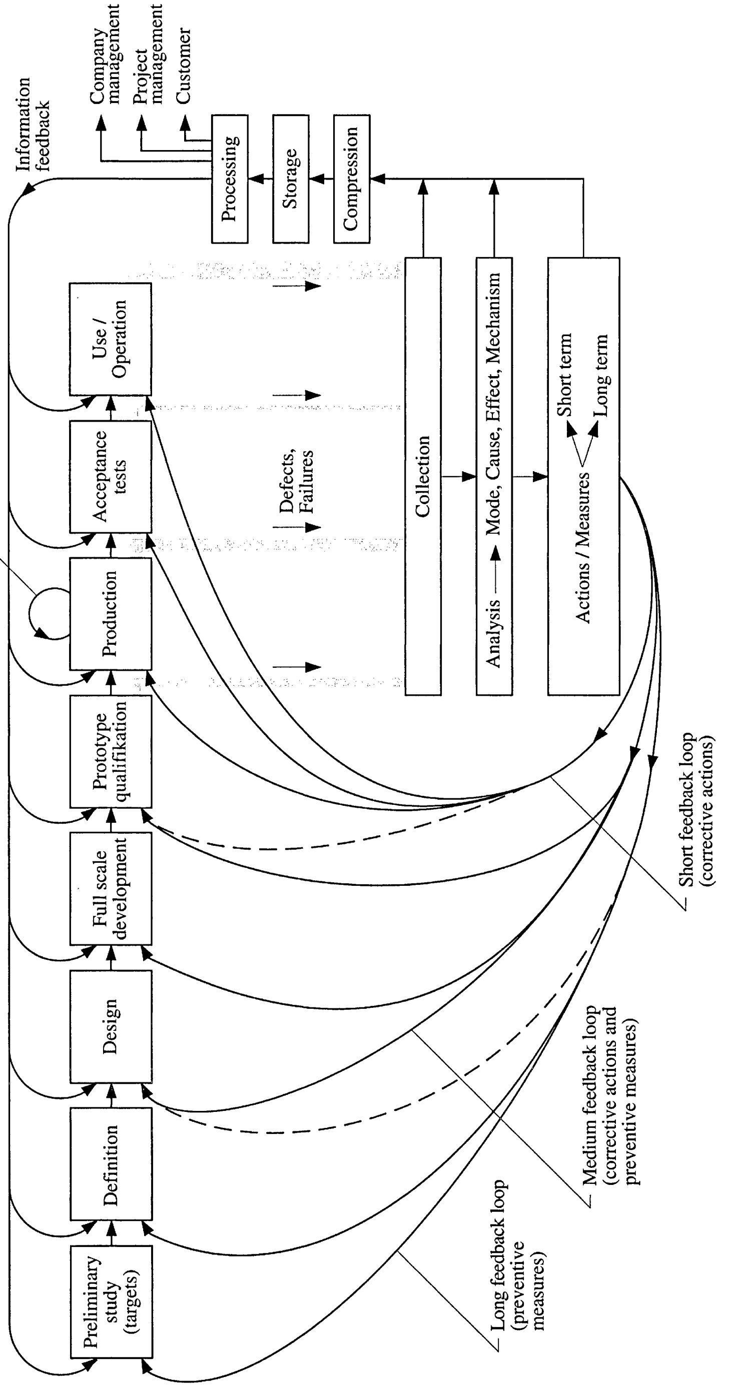


Figure 1.8 Basic concept for a quality data reporting system

Table 1.3 Example of information status for PCBs (populated printed circuit board's) from a quality data reporting system

a) Defects and failures at PCB level

Period: . . . .

PCB	No. of PCBs			Rough classification				No. of faults		Measures		Cost		
	tested	with faults	%	assembling	soldering	board	component	total	per PCB	short term	long term	production	Q A	other areas

b) Defects and failures at component level

Period: . . . .   PCB: . . . .   No. of PCBs: . . . .

Component	Manufacturer	No. of components		Number of faults	%	No. of faults per place of occurrence			
		Same type	Same application			incoming inspection	in-process test	final test	warranty period

c) Cause analysis for defects and failures due to components

Period: . . . .

Component	PCB	Cause			Percent defective (%)		Failure rate ($10^{-9}\,h^{-1}$)		Measures	
		systematic	inherent failure	not identified	observed	predicted	observed	predicted	short term	long term

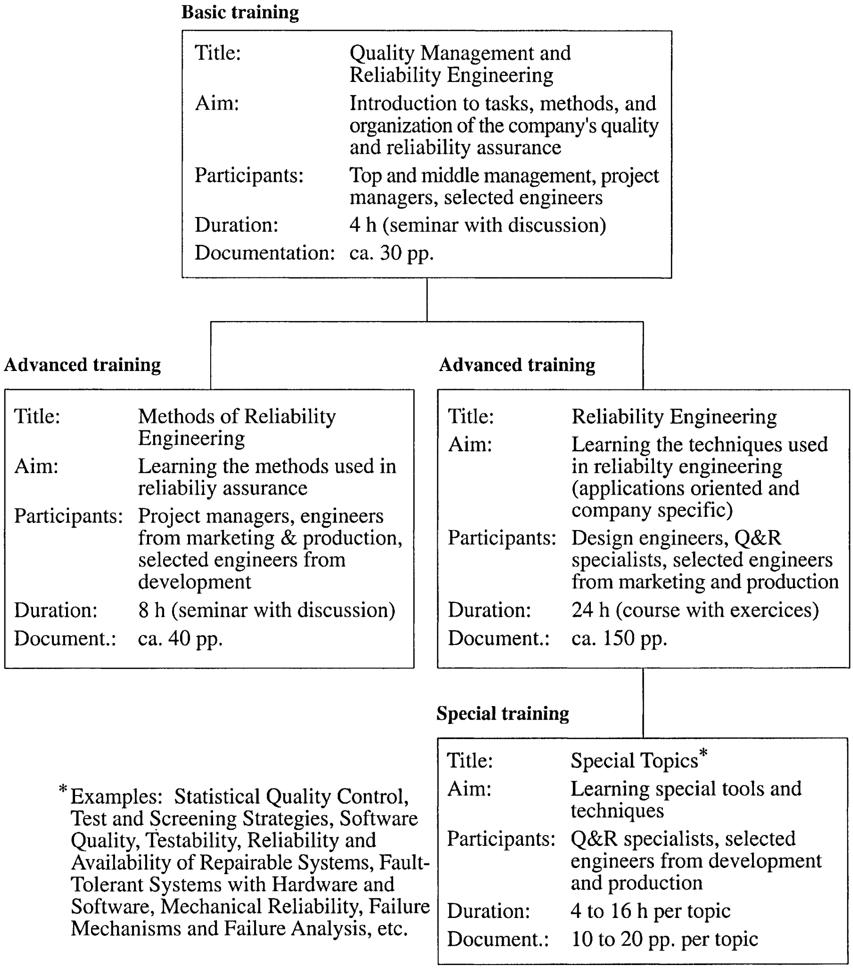
d) Correlation between components and PCBs

Period: . . . .

PCB Component					

1.3.4 Motivation and Training

Cost effective quality and reliability assurance (management) can be achieved if every engineer involved in a project is made responsible for his / her assigned activities (e. g. as per Table A3.2). Figure 1.9 shows a comprehensive, practice oriented, *motivation and training* program in a company producing *complex equipment and systems with high quality & reliability requirements.*



Basic training

Title:	Quality Management and Reliability Engineering
Aim:	Introduction to tasks, methods, and organization of the company's quality and reliability assurance
Participants:	Top and middle management, project managers, selected engineers
Duration:	4 h (seminar with discussion)
Documentation:	ca. 30 pp.

Advanced training

Title:	Methods of Reliability Engineering
Aim:	Learning the methods used in reliabiliy assurance
Participants:	Project managers, engineers from marketing & production, selected engineers from development
Duration:	8 h (seminar with discussion)
Document.:	ca. 40 pp.

Advanced training

Title:	Reliability Engineering
Aim:	Learning the techniques used in reliabilty engineering (applications oriented and company specific)
Participants:	Design engineers, Q&R specialists, selected engineers from marketing and production
Duration:	24 h (course with exercices)
Document.:	ca. 150 pp.

Special training

Title:	Special Topics*
Aim:	Learning special tools and techniques
Participants:	Q&R specialists, selected engineers from development and production
Duration:	4 to 16 h per topic
Document.:	10 to 20 pp. per topic

*Examples: Statistical Quality Control, Test and Screening Strategies, Software Quality, Testability, Reliability and Availability of Repairable Systems, Fault-Tolerant Systems with Hardware and Software, Mechanical Reliability, Failure Mechanisms and Failure Analysis, etc.

Figure 1.9 Example for a practical oriented training and motivation program in a company producing *complex equipment and systems with high quality (Q) & reliability (R) requirements*