2 Reliability Analysis During the Design Phase (Nonrepairable Elements up to System Failure)

Reliability analysis during the design and development of complex components, equipment, and systems is important to detect and eliminate *reliability weaknesses* as early as possible and to perform *comparative studies*. Such an investigation includes *failure rate* and *failure mode* analysis, verification of the adherence to *design guidelines*, and cooperation in *design reviews*. This chapter presents methods and tools for failure rate and failure mode analysis of complex equipment and systems considered as *nonrepairable* (up to system failure, apart from Eq. (2.48)). After a short introduction, Section 2.2 deals with series - parallel structures. Complex structures, elements with more than one failure mode, and parallel models with *load sharing* are investigated in Section 2.3. Reliability allocation is discussed in Section 2.4, stress / strength and drift analysis in Section 2.5. Section 2.6 deals with failure mode and causes-to-effects analyses. Section 2.7 gives a checklist for reliability aspects in design reviews. Maintainability is considered in Chapter 4 and repairable systems are investigated in Chapter 6 (including complex systems for which a reliability block diagram does not exist, imperfect switching, incomplete coverage, reconfigurable systems, common cause failures, as well as an introduction to network reliability, BDD, ET, dynamic FT, Petri nets, and computer-aided analysis). Design guidelines are in Chapter 5, qualification tests in Chapter 3, reliability tests in Chapters 7 & 8. Theoretical foundations for this chapter are in Appendix A6.

2.1 Introduction

An important part of the reliability analysis during the design and development of complex equipment and systems deals with failure rate and failure mode investigation as well as with the verification of the adherence to appropriate design guidelines for reliability. *Failure modes* and *causes-to-effects* analysis is considered in Section 2.6, *design guidelines* are given in Chapter 5. Sections 2.2 - 2.5 are devoted to *failure rate analysis.* Investigating the failure rate of a complex

A. Birolini, *Reliability Engineering*, 6th ed., DOI 10.1007/978-3-642-14952-8_2,

equipment or system leads to the calculation of the *predicted reliability*, i.e., that reliability which can be calculated from the structure of the item and the reliability of its elements. Such a prediction is necessary for an *early detection of reliability weaknesses*, for *comparative studies*, for *availability* investigation taking care of *maintainability* and *logistic support*, and for the definition of *quantitative reliability targets* for subcontractors. However, because of different kind of uncertainties, the predicted reliability can often be only given with a limited accuracy. To these uncertainties belong

- simplifications in the mathematical modeling (independent elements, complete and sudden failures, no flaws during design and manufacturing, no damages),
- insufficient consideration of faults caused by internal or external interference (switching, transients, EMC, etc.),
- inaccuracies in the data used for the calculation of the component failure rates.

On the other hand, the *true reliability* of an item can only be determined by *reliability tests,* performed often at the prototype's qualification tests, i.e., late in the design and development phase. Practical applications also shown that with an experienced reliability engineer, the predicted failure rate at equipment or system level often agree *reasonably well* (within a factor of 2) with field data. Moreover, relative values obtained by comparative studies generally have a much greater accuracy than absolute values. All these reasons support the efforts for a *reliability prediction* during the design of equipment and systems with specified reliability targets.

Besides theoretical considerations, discussed in the following sections, *practical aspects* have to be considered when designing reliable equipment or systems, for instance with respect to operating conditions and to the mutual influence between elements (input/output, load sharing, effects of failures, transients, etc.). Concrete possibilities for reliability improvement are

- reduction of thermal, electrical and mechanical stresses,
- correct interfacing of components and materials,
- simplification of design and construction,
- use of qualitatively better components and materials,
- protection against ESD and EMC,
- screening of critical components and assemblies,
- use of redundancy,

in that order. *Design guidelines* (Chapter 5) and *design reviews* (Tables A3.3, 2.8, 4.3, and 5.5, Appendix A4) are mandatory to support such improvements. This chapter deals with *nonrepairable* (up to system failure) equipment and systems. Maintainability is discussed in Chapter 4. Reliability and availability of repairable equipment and systems is considered carefully in Chapter 6.

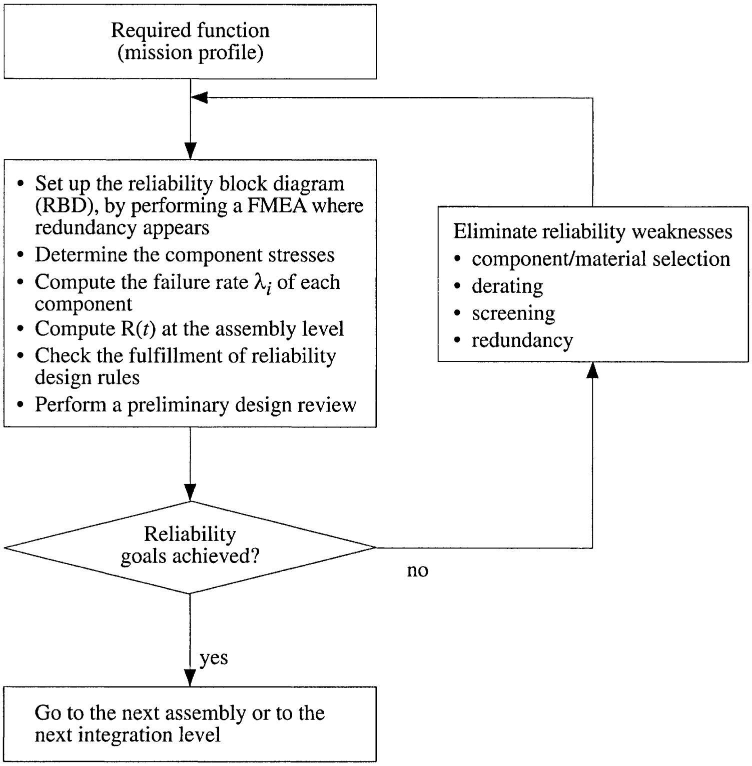

Required function
(mission profile)
• Set up the reliability block diagram (RBD), by performing a FMEA where redundancy appears
• Determine the component stresses
• Compute the failure rate λ_i of each component
• Compute R(t) at the assembly level
• Check the fulfillment of reliability design rules
• Perform a preliminary design review
Eliminate reliability weaknesses
• component/material selection
• derating
• screening
• redundancy
Reliability goals achieved?
no
yes
Go to the next assembly or to the next integration level

Figure 2.1 Reliability analysis procedure at assembly level

Taking account of the above considerations, Fig. 2.1 shows the reliability analysis procedure used in practical applications at assembly level. The procedure of Fig. 2.1 is based on the *part stress method* discussed in Section 2.2.4 (see Section 2.2.7 for the *part count method*). Also included are a failure modes and effect analysis (FMEA/FMECA), to check the validity of the assumed *failure modes*, and a verification of the adherence to *design guidelines for reliability in a preliminary design review* (Section 5.1, Appendices A3.3.5 & A4). Verification of the assumed failure modes is *mandatory where redundancy appears*, in particular because of the *series element* in the reliability block diagram (see for instance Example 2.6, Sections 2.3.6 for elements with more than one failure mode & 6.8.7 for common cause failures, and Figs. 2.8 - 2.9 & 6.17 - 6.18 for a comparative investigation). To simplify the notation, in the following *reliability* will be used for *predicted reliability* and *system* for *technical system* (i.e., for a system with ideal human factors and logistic support).

2.2 Predicted Reliability of Equipment and Systems with Simple Structure

Simple structures are those for which a reliability block diagram *exists* and can be reduced to a *series/parallel form* with *independent* elements. For such an item, the *predicted reliability* is calculated according to the following procedure, see Fig. 2.1:

1. Definition of the required function and of its associated mission profile.
2. Derivation of the corresponding reliability block diagram (RBD).
3. Determination of the operating conditions for each element of the RBD.
4. Determination of the failure rate for each element of the RBD.
5. Calculation of the reliability for each element of the RBD.
6. Calculation of the item (system) reliability function $\mathrm{R}_S(t)$.
7. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

This section discusses at some length steps 1 to 6, see Example 2.6 for the application to a simple situation. For the investigation of equipment or systems for which a reliability block diagram does not exist, one refers to Section 6.8.

2.2.1 Required Function

The *required function* specifies the item's task. Its definition is the starting point for any analysis, as it defines failures. For practical purposes, parameters should be defined with tolerances and not merely as fixed values.

In addition to the required function, *environmental conditions* at system level must also be defined. Among these, ambient temperature (e.g. +40°C), storage temperature (e.g. –20 to +60°C), humidity (e.g. 40 to 60%), dust, corrosive atmosphere, vibrations (e.g. $0.5 g_n$, at 2 to 60Hz), shocks, noise (e.g. 40 to 70dB), and power supply voltage variations (e.g. ±20%). From these global environmental conditions, the constructive characteristics of the system, and the internal loads, *operating conditions* (actual stresses) for each element of the system can be determined.

Required function and environmental conditions are often *time dependent*, leading to a *mission profile* (*operational profile* for software). A representative mission profile and the corresponding reliability targets should be defined in the system specifications (initially as a rough description and then refined step by step), see the remark on p. 38, as well as Section 6.8.6.2 for phased-mission systems.

2.2.2 Reliability Block Diagram

The *reliability block diagram* (RBD) is an *event* diagram. It answers the following question: *Which elements of the item under consideration are necessary for the*

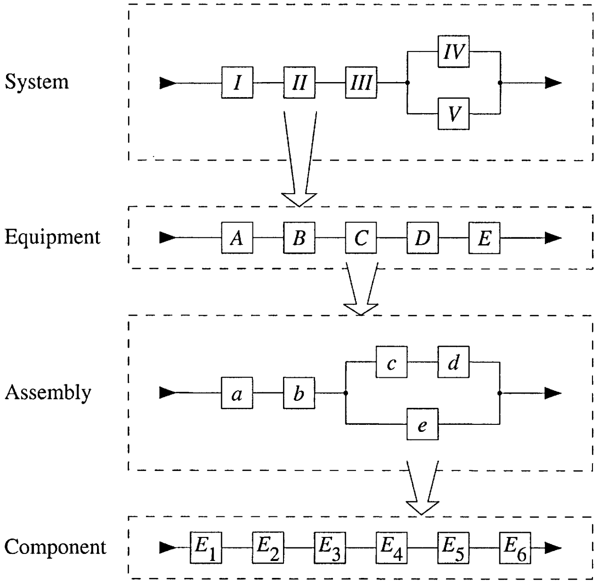


Figure 2.2 Procedure for setting up the reliability block diagram (RBD) of a system with four levels

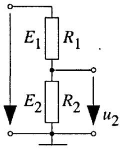
fulfillment of the required function and which can fail without affecting it? Setting up a RBD involves, at first, *partitioning* the item into elements with clearly defined tasks. The elements which are necessary for the required function are connected *in series*, while elements which can fail with no effect on the required function (redundancy) are connected *in parallel.* Obviously, the ordering of the series elements in the reliability block diagram can be arbitrary. Elements which are not relevant for (or used in) the required function under consideration are removed (put into a reference list), after having verified (FMEA) that their failure does not affect elements involved in the required function. These considerations make it clear that for a given system, *each required function has its own reliability block diagram.*

In setting up the reliability block diagram, care must be taken regarding the fact that only *two states* (good or failed) and *one failure mode* (e.g. opens or shorts) can be considered *for each element.* Particular attention must also be paid to the correct identification of the parts which appear *in series with a redundancy* (see e.g. Section 6.8). For large equipment or systems the reliability block diagram is derived top down as indicated in Fig. 2.2 (for 4 levels as an example). At each level, the corresponding required function is derived from that at the next higher level.

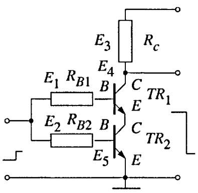
The technique of setting up reliability block diagrams is shown in the Examples 2.1 to 2.3 (see also Examples 2.6, 2.13, 2.14). One recognizes that a reliability block diagram basically differs from a *functional block diagram.* Examples 2.2, 2.3, 2.14 also show that one or more elements can appear *more than once* in a reliability block diagram, while the corresponding element is physically present *only once* in the item considered. To point out the *strong dependence* created by this fact, it is mandatory to use *a box form other than a square* for these elements (in Example 2.2, if E_2 fails the required function for mission 1 & 2 is fulfilled *only* if E_1, E_3, E_5 work). To avoid ambiguities, each physically different element of the item should bear its own number. The typical structures of reliability block diagrams are summarized in Table 2.1 (see Sect. 6.8 for cases in which a reliability block diagram does not exist).

Example 2.1

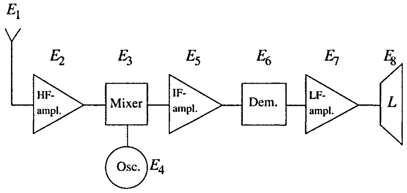
Set up the reliability block diagrams for the following circuits:



(i) Res. voltage divider



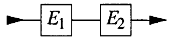
(ii) Electronic switch



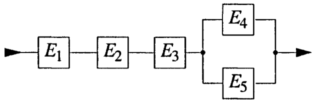
(iii) Simplified radio receiver

Solution

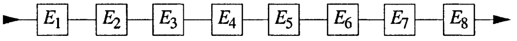
Cases (i) and (iii) exhibit no redundancy, i.e., for the required function (tacitly assumed here) all elements must work. In case (ii), transistors TR_1 and TR_2 are redundant if their failure mode is a *short* between emitter and collector (the failure mode for resistors is generally an open). From these considerations, the reliability block diagrams follows as



(i) Resistive voltage divider



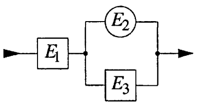
(ii) Electronic switch



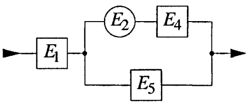
(iii) Simplified radio receiver

Example 2.2

An item is used for two different missions with the corresponding reliability block diagrams given in the figures below. Give the reliability block diagram for the case in which both functions are simultaneously required in a common mission.



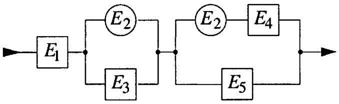
Mission 1



Mission 2

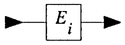
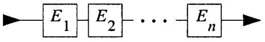
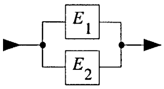
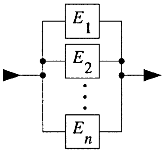
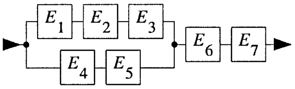
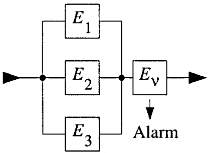
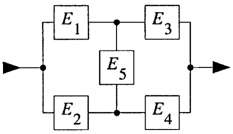
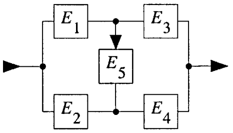
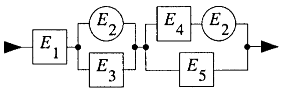
Solution

The simultaneous fulfillment of both required functions leads to the *series connection* of both reliability block diagrams. Simplification is possible for element E_1 but not for element E_2. A deeper discussion on phased-mission reliability analysis is in Section 6.8.6.2.



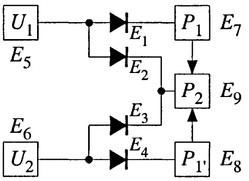
Mission 1 and 2

Table 2.1 Basic reliability block diagrams and associated reliability functions (nonrepairable up to system failure, new at $t=0$ ($R_{S0}(0)=1$), *independent elements* (except E_2 in 9), active redundancy; 7-9 are *complex structures* and cannot be reduced to a series-parallel structure with indep. elements)

Reliability Block Diagram	Reliability Function $(R_S = R_{S0}(t);\ R_i = R_i(t),\ R_i(0)=1)$	Remarks
 1	$R_S = R_i$	One-item structure, $\lambda(t)=\lambda \Rightarrow R_i(t)=e^{-\lambda_i t}$
 2	$R_S = \prod_{i=1}^{n} R_i$	Series structure, $\lambda_S(t)=\lambda_1(t)+\ldots+\lambda_n(t)$
 1-out-of-2 3	$R_S = R_1 + R_2 - R_1R_2$	1-out-of-2-redundancy, $R_1(t)=R_2(t)=e^{-\lambda t}$ $\Rightarrow R_S(t) = 2e^{-\lambda t} - e^{-2\lambda t}$
 k-out-of-n 4	$E_1 = \ldots = E_n = E$ $\rightarrow R_1 = \ldots = R_n = R$ $R_S = \sum_{i=k}^{n} \binom{n}{i} R^i (1-R)^{n-i}$	k-out-of-n redundancy for $k=1$ $\Rightarrow R_S = 1-(1-R)^n$
 5	$R_S = (R_1R_2R_3 + R_4R_5$ $- R_1R_2R_3R_4R_5)R_6R_7$	Series/parallel structure
 2-out-of-3 6	$E_1 = E_2 = E_3 = E$ $\rightarrow R_1 = R_2 = R_3 = R$ $R_S = (3R^2 - 2R^3)R_v$	Majority redundancy, general case $(n+1)$-out-of-$(2n+1)$, $n=1,2,\ldots$
 7	$R_S = R_5(R_1+R_2-R_1R_2)\cdot$ $(R_3+R_4-R_3R_4)+(1-R_5)\cdot$ $(R_1R_3+R_2R_4-R_1R_2R_3R_4)$	Bridge structure (bi-directional on E_5)
 8	$R_S = R_4[R_2+R_1(R_3+R_5-R_3R_5)$ $- R_1R_2(R_3+R_5-R_3R_5)]$ $+ (1-R_4)R_1R_3$	Bridge structure (unidirectional on E_5)
 9	$R_S = R_2R_1(R_4+R_5-R_4R_5)$ $+ (1-R_2)R_1R_3R_5$	The element E_2 appears twice in the reliability block diagram (not in the hardware)

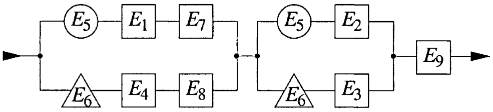
Example 2.3

Set up the reliability block diagram for the electronic circuit shown on the right. The required function asks for operation of P_2 (main assembly) and of P_1 or $P_{1'}$ (control cards).



Solution

This example is not as trivial as Examples 2.1 and 2.2. A good way to derive the reliability block diagram is to consider the mission "P_1 or $P_{1'}$ must work" *and* "P_2 must work" separately, and then to put both missions together as in Example 2.2 (see also Example 2.14).



Also given in Table 2.1 are the associated reliability functions for the case of *non-repairable elements* (up to system failure) with *active redundancy* and *independent elements* except case 9 (Sections 2.2.6, 2.3.1-2.3.4); see Section 2.3.5 for load sharing, Section 2.5 for mechanical systems, and Chapter 6 for repairable systems.

Table 2.2 Most important parameters influencing the failure rate of electronic components

Component	Ambient temp. (θ_A)	Junction temp. (θ_J)	Power stress (S)	Voltage stress (S)	Current stress (S)	Breakdown voltage	Technology	Complexity	Package	Application	Contact construction	Range	Production maturity	Environment (π_E)	Quality (π_Q)
Digital and linear ICs		D		x	x	x	x	x	x				x	x	x
Hybrid circuits	D	D	D	D	D	x	x	x	x	x	x	x	x	x	x
Bipolar transistors		D	D	x		x	x		x	x	x	x	x	x	x
FETs		D	D	x		x	x		x	x	x		x	x	x
Diodes		D	x	x	x	x	x		x	x	x	x	x	x	x
Thyristors		D	x	x	x	x	x		x		x	x	x	x	x
Optoelectronic components		D		x	x		x	x	x				x	x	x
Resistors	D		D				x					x	x	x	x
Capacitors	D			D			x		x	D		x	x	x	x
Coils, transformers	D		x	x			x						x	x	x
Relays, switches	D			x	x		x	x	x	x	D		x	x	x
Connectors	D				x		x		x	x	D	x	x	x	x

D denotes dominant, x denotes important

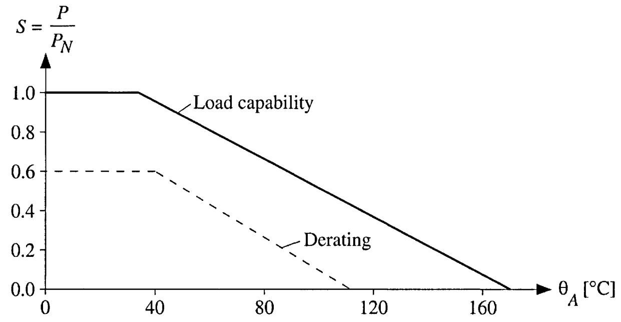


Figure 2.3 Load (power) capability and typical derating curve (dashed) for a bipolar Si-transistor as function of the ambient temperature θ_A (P = dissipated power, P_N = rated power (at 40 °C))

2.2.3 Operating Conditions at Component Level, Stress Factors

The *operating conditions* of each element in the reliability block diagram influence the item's reliability and have to be considered. These operating conditions are function of the *environmental conditions* (Section 3.1.1) and *internal loads*, in operating and dormant state. Table 2.2 gives an overview of the most important parameters influencing electronic component failure rates.

A basic assumption is that components are in no way *over stressed*. In this context it is important to consider that the *load capability* of many electronic components decreases with increasing *ambient temperature*. This in particular for power, but often also for voltage and current. As an Example, Fig. 2.3 shows the variation of the power capability as function of the ambient temperature θ_A for a bipolar Si transistor (with constant thermal resistance R_{JA}). The continuous line represents the *load capability*. To the right of the break point the junction temperature is nearly equal to 175°C (max. specified operating temperature). The dashed line gives a typical *derating curve* for such a device. *Derating* is the designed (intentional) non utilization of the full load capability of a component with the purpose to reduce its failure rate. The *stress factor* (stress ratio, stress) S is defined as

$$S = \frac{\text{applied load}}{\text{rated load at 40°C}} \,. \tag{2.1}$$

To give a touch, Figs. 2.4 - 2.6 show the influence of the temperature (ambient θ_A, case θ_C or junction θ_J) and of the stress factor S on the failure rate of some electronic components (from *IEC 61709* [2.22]). Experience shows that for a good design and $\theta_A \leq 40°\text{C}$ one should have $0.1 < S < 0.6$ for power, voltage, and current, $S \leq 0.8$ for fan-out, and $S \leq 0.7$ for U_{in} of lin. ICs (Table 5.1). $S < 0.1$ should also be avoided.

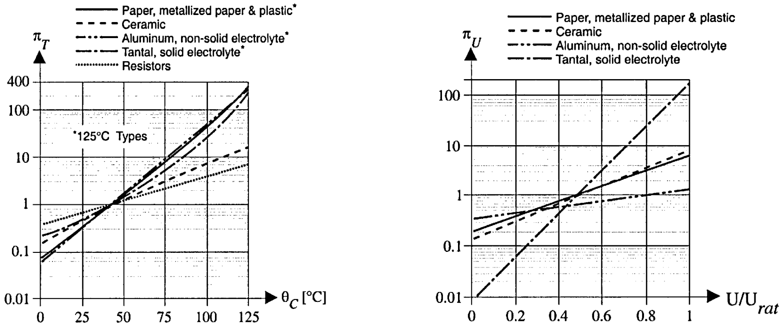


Figure 2.4 Factor π_T as function of the case temperature θ_C for capacitors and resistors, and factor π_U as function of the voltage stress for capacitors (examples from *IEC 61709* [2.22])

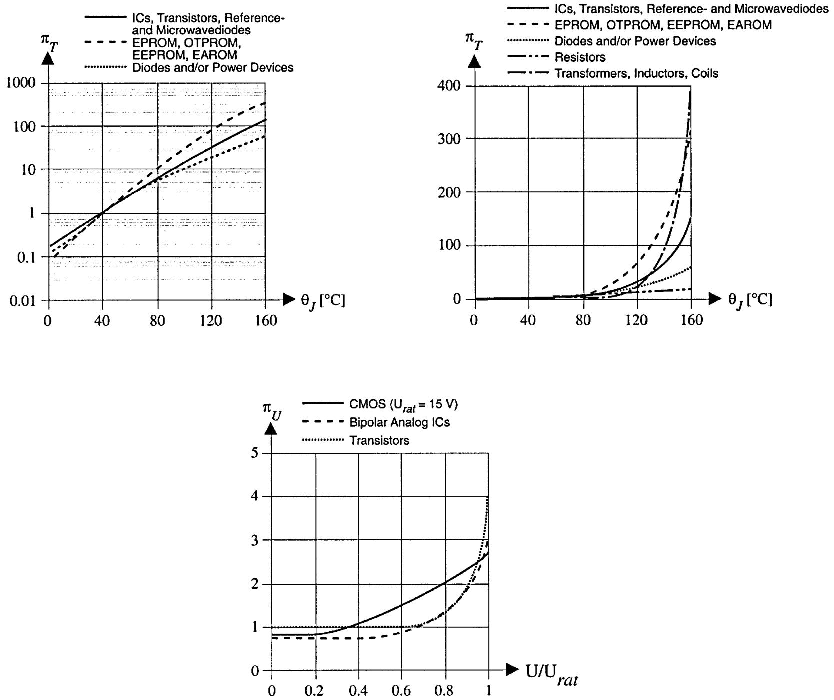


Figure 2.5 Factor π_T as function of the junction temperature θ_J (left, half log for semiconductors and right, linear for semiconductors, resistors, and coils) and factor π_U as function of the power supply voltage for semiconductors (examples from *IEC 61709* [2.22])

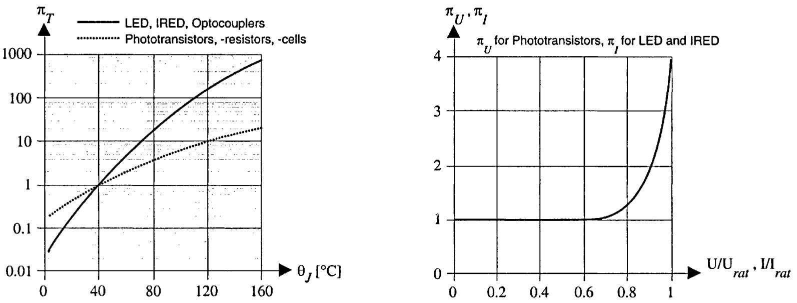


Figure 2.6 Factor π_T as function of the junction temperature θ_J and factors π_U and π_I as function of voltage and current stress for optoelectronic devices (examples from *IEC 61709* [2.22])

2.2.4 Failure Rate of Electronic Components

The *failure rate* $\lambda(t)$ of an item is the conditional probability referred to δt of a failure in the interval $(t, t + \delta t]$ *given that the item was new at* $t = 0$ *and did not fail in the interval* $(0, t]$, see Eqs. (1.5) & (A6.25). For a *large population of statistically identical and independent items*, $\lambda(t)$ exhibits often three successive phases: One of early failures, one with constant (or nearly so) failure rate and one involving failures due to wearout (Fig. 1.2). *Early failures* should be eliminated by a *screening* (Chapter 8). *Wearout failures* can be expected for some electronic components (electrolytic capacitors, power and optoelectronic devices, ULSI-ICs) as well as for mechanical and electromechanical components. They must be considered on a case-by-case basis in setting up a *preventive maintenance strategy* (Sections 4.6 & 6.8.2).

To simplify calculations, reliability prediction is often performed by assuming a *constant* (time independent) *failure rate* during the *useful life*

$$\lambda(t) = \lambda .$$

This approximation greatly simplify calculations, since a constant failure rate λ leads to a flow of failures described by a homogeneous *Poisson process* (process with *memoryless property*, Eqs. (A6.29) & (A6.87), Appendix A7.2.5). The failure rate of components can be assessed *experimentally* by accelerated reliability tests or from field data (if operating conditions are sufficiently well known) with appropriate data analysis (Chapter 7). For established electronic and electromechanical components, models and figures for λ are often given in *failure rate handbooks* [2.21-2.30]. Among these, *FIDES Guide 2009* [2.21], *IEC 61709*(1996) [2.22], *IEC TR 62380* (2004) [2.23], *IRPH 2003* [2.24], *MIL-HDBK-217G* (Draft 2009) [2.25], *RDF-96* [2.28], *RIAC-HDBK-217 Plus* (2008) [2.29], *Telcordia SR-332* (3 th Ed. planned) [2.30].

Table 2.3 Indicative figures for environmental conditions and corresponding factors π_E

	Stress					π_E factor			
Environment	Vibrations	Sand	Dust	RH (%)	Mech. shocks	ICs	DS	R	C
G_B (+5 to +45°C) (Ground benign)	2 – 200 Hz $\leq 0.1\ g_n$	l	l	40 – 70	$\leq 5\ g_n$ / 22 ms	1	1	1	1
G_F (-40 to +45°C) (Ground fixed)	2 – 200 Hz $1\ g_n$	m	m	5 – 100	$\leq 20\ g_n$ / 6 ms	2	2	3	3
G_M (-40 to +45°C) (Ground mobile)	2 – 500 Hz $2\ g_n$	m	m	5 – 100	$10\ g_n$ / 11 ms to $30\ g_n$ / 6 ms	5	5	7	7
N_S (-40 to +45°C) (Nav. sheltered)	2 – 200 Hz $2\ g_n$	l	l	5 – 100	$10\ g_n$ / 11 ms to $30\ g_n$ / 6 ms	4	4	6	6
N_U (-40 to +70°C) (Nav. unsheltered)	2 – 200 Hz $5\ g_n$	h	m	10–100	$10\ g_n$ / 11 ms to $50\ g_n$/ 2.3 ms	6	6	10	10

C=capacitors, DS=discrete semicond., R=resistors, RH=rel. humidity, h=high, m=medium, l=low, $g_n = 10\,\text{m/s}^2$
(G_B is *Ground stationary weather protected in* [2.24, 2.28,2.30] and is taken as reference value in [2.22, 2.23])

IEC 61709 gives *laws of dependency* of the failure rate on different stresses (temperature, voltage, etc.) and must be supported by a set of *reference failure rates* λ_{ref} for *standard industrial environment* (40°C ambient temperature θ_A, G_B as per Table 2.3, and steady-state conditions in field). *IRPH 2003* is based on *IEC 61709* and gives reference failure rates. Effects of thermal cycling, dormant state, and ESD are considered in *IEC TR 62380* and *RIAC-HDBK-217Plus*. Refined models are in *FIDES Guide 2009*. *MIL-HDBK217* was up to revision *F* the most common reference, it is possible that starting with revision *G* it will take back this position (see also p. 382). An international agreement on failure rate models for *reliability predictions at equipment and system level in practical applications* should be found to simplify comparative investigations (see e. g. [1.2 (1996)] and the remark on p. 38).

Failure rates are taken from one of the above handbooks or from *one's own field data* for the calculation of the predicted reliability. Models in these handbooks have often a simple structure, of the form

$$\lambda = \lambda_0\, \pi_T\, \pi_E\, \pi_Q\, \pi_A \tag{2.2}$$

or

$$\lambda = \pi_Q\, (C_1 \pi_T + C_2 \pi_E + C_3 \pi_L + \ldots), \tag{2.3}$$

with $\pi_Q = \pi_{Q\,\text{component}} \cdot \pi_{Q\,\text{assembly}}$, often further simplified to

$$\lambda = \lambda_{ref}\, \pi_T\, \pi_U\, \pi_I, \tag{2.4}$$

by taking $\pi_E = \pi_Q = 1$ because of the assumed standard industrial environment ($\theta_A = 40°\text{C}$, G_B as per Table 2.3, and steady-state conditions in field) and standard quality level. Indicative figures are in Tables 2.3, 2.4, A10.1, and in Example 2.4.

λ lies between $10^{-10}\,\text{h}^{-1}$ for passive components and $10^{-7}\,\text{h}^{-1}$ for VLSI ICs. The unit $10^{-9}\,\text{h}^{-1}$ is designated by *FIT* (failure(s) in time, failure(s) per 10^9 h).

Table 2.4 Reference values for the quality factors $\pi_{Q\ \text{component}}$

	Qualification		
	Reinforced	CECC $^{+)}$	no special
Monolithic ICs	0.7	1.0	1.3
Hybrid ICs	0.2	1.0	1.5
Discrete Semiconductors	0.2	1.0	2.0
Resistors	0.1	1.0	2.0
Capacitors	0.1	1.0	2.0

$^{+)}$ Reference value in [2.22-24,2.28], class II in [2.30] (corresponds to *MIL-HDBK-217F* classes B,JANTX,M)

For many electronic components, λ increases exponentially with temperature, doubling for an increase of 10 to 20°C. This is considered by the factor π_T, for which an *Arrhenius Model* is often used. In the case of *only one dominant failure mechanism*, Eq. (7.56) gives the ratio of π_T factors at two temperatures T_2 and T_1

$$\frac{\pi_{T_2}}{\pi_{T_1}} = A \approx e^{\frac{E_a}{k}\left(\frac{1}{T_1}-\frac{1}{T_2}\right)}, \qquad (2.5)$$

where A is the *acceleration factor*, k the Boltzmann constant ($8.6\cdot10^{-5}$ eV / K), T the temperature in Kelvin degrees (junction for semiconductor devices), and E_a the *activation energy* in eV. As given in Figs. 2.4 - 2.6, experience shows that a *global value* for E_a often lie between 0.3 eV and 0.6 eV for Si devices. The design guideline $\theta_J \le 100°\text{C}$, if possible $\theta_J \le 80°\text{C}$, given in Section 5.1 for semiconductor devices is based on this consideration (see π_T in linear scale on Fig. 2.5). Models in *IEC 61709* assumes for π_T *two dominant failure mechanisms* with activation energies E_{a_1} and E_{a_2} (about 0.3 eV for E_{a_1} and 0.6 eV for E_{a_2}). The corresponding equation for π_T takes in this case the form

$$\pi_T = \frac{a e^{zE_{a_1}} + (1-a)e^{zE_{a_2}}}{a e^{z_{ref}E_{a_1}} + (1-a)e^{z_{ref}E_{a_2}}}, \qquad (2.6)$$

with $0 \le a \le 1$, $z=(1/T_{ref}-1/T_2)/k$, $z_{ref}=(1/T_{ref}-1/T_1)/k$, and $T_{ref}=313\,\text{K}$ (40°C).

It can be noted that for $T_2=T_1+\Delta T$, Eq. (2.5) yields $A \approx e^{\Delta T E_a / k T_1^2}$ (straight line in Fig. 7.10). Assuming ΔT normally distributed (during operation), it follows from case (i) of Example A6.18 that the *acceleration factor A is lognormally distributed*; this can be used to refine failure rate calculations for missions with variable operating temperature, see also [3.57 (2005), 3.61] and remarks to Eqs. (7.55) & (7.56).

For components of good commercial quality, and using $\pi_E = \pi_Q = 1$, failure rate calculations lead to figures which for practical applications in *standard industrial environments* ($\theta_A = 40°\text{C}$, G_B as per Table 2.3, and steady-state conditions in field) *often agree reasonably well with field data* (up to a factor of 2). This holds at *equipment & system level,* although deviations can occur at component level, depending on the failure rate catalog used (Example 2.4). There my be differences if field conditions are severe or not sufficiently well known. However, discussion over comparison with obsolete data should be dropped and it would seem to be opportune to *unify models and data*, taking from each model the "good part" and putting them together for "better" models (strategy of wide applicability). Models for prediction in practical applications should remain *reasonably simple*, laws for *dominant failure mechanisms* should be given in *standards*, and the list of *reference failure rates* λ_{ref} should be yearly updated. Models based on *failure mechanisms* have to be used as a basis for simplified models. The assumption of $\lambda < 10^{-9}\,h^{-1}$ should be confined to components with stable production process and a reserve to technological limits.

Calculation of the failure rate at system level often requires considerations on the *mission profile*. If the mission can be partitioned in time spans with almost homogeneous stresses, switching effects are negligible, and the failure rate is time independent (between successive state changes of the system), the contribution of each time span can be added linearly, as often assumed for *duty cycles*. With these assumptions, investigation of *phased-mission* systems is possible (Section 6.8.6.2).

Estimation and demonstration of component's and system's failure rates are considered in Section 7.2.3, accelerated tests in Section 7.4.

Example 2.4

For indicative purpose, following table gives failure rates calculated according to some different data bases [2.30 (2001), 2.24, 2.23] for *continuous operation* in non interface application; $\theta_A = 40°C$, $\theta_J = 55°C$, $S = 0.5$, G_B, and $\pi_Q = 1$ as for CECC certified and class II Telcordia; Pl is used for plastic package; λ in $10^{-9}\,h^{-1}$ (FIT), *quantified* at $1 \cdot 10^{-9}\,h^{-1}$ (see also Tab. A10.1).

	Telcordia 2001	*IRPH 2003*	*IEC* ++) *62380 2004*	λ_{ref} +)
DRAM, CMOS, 1 M, Pl	32	10	6	10
SRAM, CMOS, 1 M, Pl	60	30	11	30
EPROM CMOS, 1 M, Pl	53	30	20	20
16 BitμP(10^5 *TR*), CMOS, Pl	18	60	(10)	40
Gate array, CMOS, 30,000 gates , 40 Pins, Pl	17	35	17	25
Lin, Bip, 70 Tr, Pl	33	7	21	10
GP diode, Si, 100 mA, lin, Pl	4	1	1	2
Bip. transistor, 300 mW, switching, Pl	6	3	1	3
JFET, 300 mW, switching, Pl	28	5	1	4
Ceramic capacitor, 100 nF, 125°C, class 1	1	1	1	1
Foil capacitor, 1 μF	1	1	1	1
Ta solid (dry) capacitor, herm., 100 μF, 0.3Ω / V	1	1	1	2
MF resistor, 1/4 W, 100 kΩ	1	1	1	1
Cermet pot, 50 kΩ, < 10 annual shaft rot.	20	(30)	1	6

+) *Indicative* values for computations as per *IEC 61709* [2.22], $\theta_A = 40°C$; ++) Production year 2001 for ICs

2.2.5 Reliability of One-Item Structures

A *one-item nonrepairable structure* is characterized by the distribution function $F(t) = \Pr\{\tau \le t\}$ of its *failure-free time* τ, assumed > 0 ($F(0) = 0$), hereafter used as a synonym for *failure-free operating* time. The *reliability function* $R(t)$, i.e., the probability of no failure in the interval $(0, t]$, follows as (Eq. (A6.24))

$$R(t) = \Pr\{\text{no failure in } (0, t] \mid \text{new at } t=0\} = \Pr\{\tau > t\} = 1 - F(t), \qquad R(0) = 1. \quad (2.7)$$

In Eq. (2.7), the condition *new at* $t = 0$ follows from $F(0) = 0$, yielding $R(0) = 1$, and is often tacitly assumed. The mean (expected value) of the failure-free time τ, designated as *MTTF* (*mean time to failure*), can be calculated from Eq. (A6.38) as

$$MTTF = E[\tau] = \int_0^\infty R(t)\,dt. \quad (2.8)$$

Should the one-item structure exhibit a *useful life* limited to T_L, Eq. (2.8) yields

$$MTTF_L = \int_0^{T_L} R(t)\,dt, \qquad R(t) = 0 \text{ for } t > T_L.$$

In the following, $T_L = \infty$ will be assumed (except in Example 6.25).

Equation (2.8) is an important relationship. It is valid not only for a one-item structure, often considered as an indivisible entity, but it also holds for a one-item structure of arbitrary complexity. $R_{Si}(t)$ & $MTTF_{Si}$ is used to emphasize this

$$MTTF_{Si} = \int_0^\infty R_{Si}(t)\,dt. \quad (2.9)$$

Thereby, S stands for *system* and i for the *state entered at* $t = 0$ (Table 6.2); $i = 0$ holds for *system new at* $t = 0$, yielding $R_{S0}(0) = 1$. For clarity, this notation will be consequently used starting with the next section, in particular in Chapter 6.

Back to the one-item structure, considered in this section as an indivisible entity, and assuming $R(t)$ derivable, the *failure rate* $\lambda(t)$ *of* a *nonrepairable one-item structure new at* $t = 0$ is given by (Eq. (A6.25))

$$\lambda(t) = \lim_{\delta t \downarrow 0} \frac{1}{\delta t} \Pr\{t < \tau \le t + \delta t \mid \tau > t\} = -\frac{d\,R(t)/dt}{R(t)}, \quad (2.10)$$

with $R(t)$ as per Eq. (2.7). Considering $R(0) = 1$, Eq. (2.10) yields

$$R(t) = e^{-\int_0^t \lambda(x)dx}, \quad (2.11)$$

from which, for $\lambda(t) = \lambda$,

$$R(t) = e^{-\lambda t}. \quad (2.12)$$

The mean time to failure in this case is equal to $1/\lambda$. In practical applications

$$1/\lambda = MTBF \tag{2.13}$$

(or $1/\lambda_S = MTBF_S$ for systems) is often used, where *MTBF* stands for *mean operating time between failures*, expressing thus a figure applicable to *repairable* one-item structures. To avoid misuses, and also because of the often used estimate $M\hat{T}BF = T/k$ (Eq. (7.28), p. 310), *MTBF* should be confined to *repairable items with constant* (time independent) *failure rate* which are as-good-as-new after each repair (see also remarks on pp. 6 and 372).

As shown by Eq. (2.11), the reliability function of a nonrepairable one-item structure new at $t=0$ is *completely defined* by its failure rate $\lambda(t)$. In the case of electronic components, $\lambda(t) = \lambda$ can often be assumed. The failure-free time τ then exhibits an *exponential distribution* ($\mathrm{F}(t) = \Pr\{\tau \le t\} = 1 - e^{-\lambda t}$). For a time dependent failure rate, the distribution function of the failure-free time can often be approximated by the weighted sum (Eq. (A6.34)) of a Gamma distribution (Eq. (A6.97)) with $\beta < 1$ and a shifted Weibull distribution (Eq. (A6.96)) with $\beta > 1$.

Equations (2.7) - (2.12) implies that the nonrepairable one-item structure is *new at time* $t = 0$. Also of interest in, some applications, is the probability of failure-free operation during an interval $(0, t]$ *under the condition that the item has already operated without failure for* x_0 *time units before* $t = 0$. This quantity is a conditional probability, designated by $\mathrm{R}(t, x_0)$ and given by (Eq. (A6.27))

$$\mathrm{R}(t,x_0) = \Pr\{\tau > t + x_0 \mid \tau > x_0\} = \frac{\mathrm{R}(t+x_0)}{\mathrm{R}(x_0)} = e^{-\int_{x_0}^{t+x_0} \lambda(x)dx}, \qquad \mathrm{R}(0)=1. \tag{2.14}$$

For $\lambda(x)=\lambda$, Eq. (2.14) reduces to Eq. (2.12). This *memoryless property* occurs only with *constant* (time independent) *failure rate*. Its use greatly simplify calculations, in particular in Chapter 6 for repairable systems. $\mathrm{R}(t, x_0)$ has to be distinguished from the interval reliability $\mathrm{IR}_{S0}(t, t+\theta)$ (Eq. 6.26), which applies to repairable items.

Equations (2.8) and (2.9) can also be used for *repairable items*. In fact, assuming that at failure the item is replaced by a statistically equivalent one, or repaired *as-good-as-new*, a new independent failure-free time τ with the *same distribution function* as the former one is started after repair (replacement), yielding the same expected value. However, for these cases the variable x starting by $x = 0$ after each repair has to be used instead of t (as for interarrival times). With this, $MTTF_{Si}$ can be used for the mean time to failure of a given system, independently of whether it is repairable or not. The only assumption is that the system is *as-good-as-new* after repair, with respect to the state i considered (Tab. 6.2). At system level, this occurs only if all nonrepaired (renewed) elements in the system have constant failure rates. If the failure rate of one nonrenewed element is not constant, difficulties can arise, even if the assumption of an *as-bad-as-old* situation (pp. 419 & 511) applies.

In some applications, it can appear that elements of a population of similar items exhibits different failure rate. Considering as an example the case of components delivered from two manufacturer with proportion p & $(1-p)$ and failure rates λ_1 & λ_2, the reliability function of an arbitrarily selected component is (Eq. (A6.34))

$$\mathrm{R}(t) = p\mathrm{R}_1(t) + (1-p)\mathrm{R}_2(t) = pe^{-\lambda_1 t} + (1-p)e^{-\lambda_2 t}.$$

According to Eq. (2.10), it follows for the failure rate that

$$\lambda(t) = \frac{p\lambda_1 e^{-\lambda_1 t} + (1-p)\lambda_2 e^{-\lambda_2 t}}{pe^{-\lambda_1 t} + (1-p)e^{-\lambda_2 t}}. \qquad (2.15)$$

From Eq. (2.15) one recognizes that the failure rate decrease monotonically from $p\lambda_1 + (1-p)\lambda_2$ at $t=0$ to the minimum of $\{\lambda_1, \lambda_2\}$ as $t \to \infty$.

2.2.6 Reliability of Series - Parallel Structures

For nonrepairable items (up to item failure), reliability calculation at equipment and system level can often be performed using models of Table 2.1. The one-item structure has been introduced in Section 2.2.5. Series, parallel, and series - parallel structures are considered in this Section. Section 2.3 deals then with the last three models of Table 2.1. To unify notation, *system* will be used for the *item investigated*, and it is assumed that at $t=0$ the system in new (yielding $\mathrm{R}_{S0}(t)$, with $\mathrm{R}_{S0}(0)=1$).

2.2.6.1 Systems without Redundancy

From a reliability point of view, a system has *no redundancy* (series model) if all elements must work in order to fulfill the required function. The reliability block diagram consists in this case of the series connection of all elements (E_1 to E_n) of the system (row 2 in Table 2.1). For calculation purposes it is often assumed that each element operates and fails *independently* from every other element (p. 52). For series systems, this assumption must not (in general) be verified, because the first failure is a system failure for reliability purposes. Let e_i be the event

$$\{e_i\} \equiv \{\text{element } E_i \text{ works without failure in the interval } (0, t] \mid \text{new at } t=0\}.$$

The probability of this event is the reliability function $\mathrm{R}_i(t)$ of the element E_i, i.e.

$$\Pr\{e_i\} = \Pr\{\tau_i > t\} = \mathrm{R}_i(t), \qquad \mathrm{R}_i(0) = 1. \qquad (2.16)$$

The system does not fail in the interval $(0, t]$ if and only if all elements, $E_1, \ldots, E_n$ do not fail in that interval, thus

$$\mathrm{R}_{S0}(t) = \Pr\{e_1 \cap \ldots \cap e_n\}.$$

Here and in the following, S stands for system and 0 specifies that the system is new at $t = 0$. Due to the assumed independence among the elements $E_1, \ldots, E_n$ and thus among $e_1, \ldots, e_n$, it follows (Eq. (A6.9)) that for the *reliability function* $\mathrm{R}_{S0}(t)$

$$\mathrm{R}_{S0}(t) = \prod_{i=1}^{n} \mathrm{R}_i(t), \qquad \mathrm{R}_i(0) = 1. \tag{2.17}$$

The *failure rate* of the system can be calculated from Eq. (2.10)

$$\lambda_S(t) = \sum_{i=1}^{n} \lambda_i(t), ^{+)} \tag{2.18}$$

Equation (2.18) leads to the following important conclusion:

> *The failure rate of a series system (system without redundancy), consisting of independent elements (p.52), is equal to the sum of the failure rates of its elements.*

The system's *mean time to failure* follows from Eq. (2.9). The special case in which all elements have a *constant failure rate* $\lambda_i(t) = \lambda_i$ leads to

$$\mathrm{R}_{S0}(t) = e^{-\lambda_S t}, \qquad \lambda_S(t) = \lambda_S = \sum_{i=1}^{n} \lambda_i^{+)}, \qquad MTTF_{S0} = \frac{1}{\lambda_S}. \tag{2.19}$$

2.2.6.2 Concept of Redundancy

High reliability, availability, and / or safety at equipment or system level can often only be reached with the help of redundancy. *Redundancy* is the existence of more than one means (in an item) for performing the required function. Redundancy does not just imply a *duplication of hardware*, since it can be implemented at the software level or as a *time redundancy*. However, to avoid *common mode* and *single-point failures*, redundant elements should be realized (designed and manufactured) *independently* from each other. Irrespective of the *failure mode* (e. g. shorts or opens), redundancy still appears in *parallel on the reliability block diagram*, not necessarily in the hardware (Example 2.6). In setting up the reliability block diagram, particular attention must be paid to the *series* element to a redundancy. An FMEA (Section 2.6) is generally *mandatory* for such a decision. Should a redundant element fulfill only a part of the required function a *pseudo redundancy* exist. From the operating point of view, one distinguishes between active, warm, and standby redundancy:

+) In Eq. (2.18) and in the following, $\lambda_S(t)$ is used instead of $\lambda_{S0}(t)$ also to point out that for considerations on the failure rate, the item (system) is generally assumed new at $t = 0$ (Eq. (2.10)).

1. *Active Redundancy* (parallel, hot): Redundant elements are subjected from the beginning to the *same load* as operating elements; *load sharing* is possible, but is not considered in the case of *independent elements* (Section 2.2.6.3).
2. *Warm Redundancy* (lightly loaded): Redundant elements are subjected to a *lower load* until one of the operating elements fails; *load sharing is* present; however, the failure rate is lower in reserve than in operation (Section 2.3.5).
3. *Standby Redundancy* (cold, unloaded): Redundant elements are subjected to *no load* until one of the operating elements fails; no *load sharing* is possible, and the failure rate in reserve state is *assumed* to be zero (Section 2.3.5).

Important redundant structures with *independent elements in active redundancy* are considered in Sections 2.2.6.3 to 2.3.4. Warm and standby redundancies are investigated in Section 2.3.5 and Chapter 6 (repair rate $\mu = 0$).

2.2.6.3 Parallel Models

A parallel model consists of n (often statistically identical) elements in *active redundancy*, of which k $(1 \le k < n)$ are necessary to perform the required function and the remaining $n-k$ are in reserve. Such a structure is designated as a *k-out-of-n* (or *k-out-of-n: G*) *redundancy*. Investigation assumes, in general, independent elements (see Sections 2.3.5 & 6.5 for load sharing and Section 6.8 for further refinements like imperfect switching, common cause failures etc.).

Let us consider at first the case of an active *1-out-of-2 redundancy* as given in Table 2.1 (row 3). The required function is fulfilled if at least one of the elements E_1 or E_2 works without failure in the interval $(0, t]$. With the same notation as for Eq. (2.16) it follows that (Eq. (A6.13))

$$\mathrm{R}_{S0}(t) = \Pr\{e_1 \cup e_2\} = \Pr\{e_1\} + \Pr\{e_2\} - \Pr\{e_1 \cap e_2\}; \qquad (2.20)$$

from which, due to the assumed independence among the elements E_1 & E_2 and thus among the events e_1 & e_2 (Eqs. (A6.8), (2.16))

$$\mathrm{R}_{S0}(t) = \mathrm{R}_1(t) + \mathrm{R}_2(t) - \mathrm{R}_1(t)\,\mathrm{R}_2(t), \qquad \mathrm{R}_1(0) = \mathrm{R}_2(0) = 1. \qquad (2.21)$$

The *mean time to failure* $MTTF_{S0}$ can be calculated from Eq. (2.9). For two identical elements with constant failure rate λ $(\mathrm{R}_1(t) = \mathrm{R}_2(t) = e^{-\lambda t})$ it follows that

$$\mathrm{R}_{S0}(t) = 2e^{-\lambda t} - e^{-2\lambda t}, \quad \lambda_S(t) = 2\lambda \frac{1-e^{-\lambda t}}{2-e^{-\lambda t}}, \quad MTTF_{S0} = \frac{2}{\lambda} - \frac{1}{2\lambda} = \frac{3}{2\lambda}. \qquad (2.22)$$

Equation (2.22) shows that in the presence of redundancy, the system failure rate $\lambda_S(t)$ is a function of time (strictly increasing from 0 to λ), even if the element's failure rate λ is constant. However, the stochastic behavior of the system is still described by a Markov process (Section 2.3.5). This time dependence becomes negligible in the case of *repairable systems* (see Eq. (6.94) for const. failure & repair rates).

Generalization to an active *k-out-of-n redundancy (k-out-of-n: G)* with n identical ($\mathrm{R}_1(t) = \ldots = \mathrm{R}_n(t) = \mathrm{R}(t)$) and independent elements follows from the *binomial distribution* (Eq. (A6.120)) by setting $p = \mathrm{R}(t)$

$$\mathrm{R}_{S0}(t) = \sum_{i=k}^{n} \binom{n}{i} \mathrm{R}^i(t)(1-\mathrm{R}(t))^{n-i}, \qquad \mathrm{R}(0) = 1. \tag{2.23}$$

$\mathrm{R}_{S0}(t)$ is the sum of the probabilities for $0, 1, \ldots, n-k$ failures ($i = n, n-1, \ldots, k$) and can be interpreted as the probability of observing at least k successes in n Bernoulli trials with $p = \mathrm{R}(t)$. The case $k = 1$ yields (with $R = \mathrm{R}(t)$ and $\mathrm{R}(0) = 1$)

$$\mathrm{R}_{S0}(t) = \sum_{i=1}^{n} \binom{n}{i} R^i(1-R)^{n-i} = \sum_{i=0}^{n} \binom{n}{i} R^i(1-R)^{n-i} - (1-R)^n = 1-(1-R)^n. \tag{2.24}$$

The mean time to failure $MTTF_{S0}$ can be calculated from Eq. (2.9), yielding

$$\mathrm{R}_{S0}(t) = 1-(1-e^{-\lambda t})^n \qquad \text{and} \qquad MTTF_{S0} = \frac{1}{\lambda}(1+\frac{1}{2}+\ldots+\frac{1}{n}) \tag{2.25}$$

for $k = 1$ and $\mathrm{R}(t) = e^{-\lambda t}$. The improvement in $MTTF_{S0}$ shown by Eq. (2.25) becomes much greater when *repair* without interruption of operation at system level is possible ($\mu / 2\lambda$ instead of $3/2$ for an active 1-out-of-2 redundancy, where $\mu = 1/MTTR$ is the constant repair rate, see Tables 6.6 & 6.8). However, as shown in Fig. 2.7, the increase of the reliability function $\mathrm{R}_{S0}(t)$ caused by redundancy is *important* for *short missions* ($t \ll 1/\lambda$), even in the nonrepairable case.

If the elements of a k-out-of-n active redundancy are independent but different, computation must consider all $\binom{n}{i}$ subsets with exactly i elements up and $n-i$ elements down, and sum from $i = k$ to n (for $k = 1$, Eq.(2.24) applies as $R_{S0} = 1 - \prod(1-R_i)$).

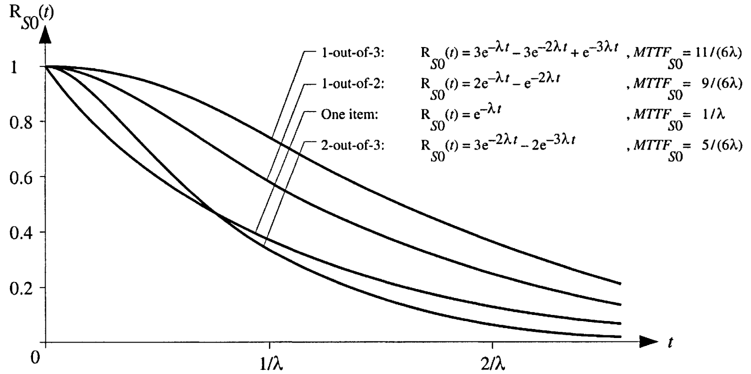


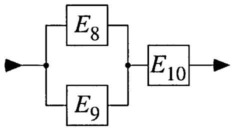
Figure 2.7 Reliability function for the one-item structure (as reference) and for some active redundancies (nonrepairable up to system failure, constant failure rates, identical and independent elements, no load sharing; see Section 2.3.5 for load sharing)

In addition to the k-out-of-n redundancy described by Eq. (2.23), of interest in some applications are cases in which the fulfillment of the required function asks that *not more* than $n-k$ *consecutive* elements fail (in linear or circular arrangement). Such a structure can allow more than $n-k$ failures and is thus at least as reliable as the corresponding k-out-of-n redundancy. For a 3-out-of-5 redundancy it holds e.g. $R_{S0} = R^5 + 5R^4(1-R) + 10R^3(1-R)^2 + 7R^2(1-R)^3 + R(1-R)^4$ for linear and $R_{S0} = R^5 + 5R^4(1-R)$ $+10R^3(1-R)^2 + 5R^2(1-R)^3$ for circular arrangement ($R_{S0} = R^5 + 5R^4(1-R) + 10R^3(1-R)^2$ according to Eq. (2.23)). The model considered here differs from the so called *consecutive k-out-of-n: F system,* in which the system is failed if k or more consecutive elements are failed [2.31, 2.38, 2.42]. Examples for consecutive k-out-of-n structures are conveying systems and relay stations. However, for this kind of application it is important to verify that all elements are *independent*, in particular with respect to common cause failures, load sharing, etc. (of course, for $k=1$ the *consecutive k-out-of-n: F system* reduces to a series model).

2.2.6.4 Series - Parallel Structures

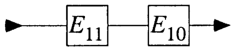
Series - parallel structures can be investigated through successive use of the results for series and parallel models. This holds in particular for *nonrepairable* systems with *active redundancy* and *independent* elements (p. 52). To demonstrate the procedure, let us consider row 5 in Table 2.1:

1st step: The series elements E_1 - E_3 are replaced by E_8, E_4 & E_5 by E_9, and E_6 & E_7 by E_{10}, yielding



with
$$R_8(t) = R_1(t)R_2(t)R_3(t)$$
$$R_9(t) = R_4(t)R_5(t)$$
$$R_{10}(t) = R_6(t)R_7(t)$$

2nd step: The 1-out-of-2 redundancy E_8 and E_9 is replaced by E_{11}, giving



with $R_{11}(t) = R_8(t) + R_9(t) - R_8(t)R_9(t)$

3rd step: From steps 1 and 2, the *reliability function* of the system follows as (with $R_S = R_{S0}(t)$, $R_i = R_i(t)$, $R_i(0)=1$, $i=1,...,7$)

$$R_S = R_{11}R_{10} = (R_1 R_2 R_3 + R_4 R_5 - R_1 R_2 R_3 R_4 R_5) R_6 R_7. \tag{2.26}$$

The mean time to failure can be calculated from Eq. (2.9). Should all elements have a constant failure rate (λ_1 to λ_7), then

$$R_{S0}(t) = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7)t} + e^{-(\lambda_4+\lambda_5+\lambda_6+\lambda_7)t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7)t}$$

and

$$MTTF_{S0} = \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7} + \frac{1}{\lambda_4+\lambda_5+\lambda_6+\lambda_7} - \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7}. \qquad (2.27)$$

Under the assumptions of active redundancy, nonrepairable (up to system failure), independent elements (p. 52), and constant failure rates, the *reliability function* $R_{S0}(t)$ of a system with series-parallel structure is given by a *sum of exponential functions*. The *mean time to failure* $MTTF_{S0}$ follows then directly from the exponent terms of $R_{S0}(t)$, see Eq. (2.27) for an example.

The use of *redundancy* implies the introduction of a *series element* in the reliability block diagram which takes into account the parts which are common to the redundant elements, creates the redundancy (Example 2.5), or assumes a control and/or *switching function*. For a design engineer it is important to *evaluate the influence of the series element* in a redundant structure. Figures 2.8 and 2.9 allow such an evaluation to be made for the case in which *constant failure rates*, *independent elements*, and *active redundancy* can be assumed. In Fig. 2.8, a one-item structure (element E_1 with failure rate λ_1) is compared with a 1-out-of-2 redundancy with a series element (element E_2 with failure rate λ_2). In Fig. 2.9, the 1-out-of-2 redundancy with a series element E_2 is compared with the structure which would be obtained if a 1-out-of-2 redundancy for element E_2 with a series element E_3 would become necessary. Obviously $\lambda_3<\lambda_2<\lambda_1$ (the limiting cases $\lambda_1=\lambda_2$ for Fig. 2.8 and $\lambda_1=\lambda_2=\lambda_3$ for Fig. 2.9 have an indicative purpose only). The three cases are labeled a, b, and c. The upper part of Figs. 2.8 and 2.9 depict the reliability functions and the lower part the ratios $MTTF_{S0b}/MTTF_{S0a}$ and $MTTF_{S0c}/MTTF_{S0b}$, respectively. The comparison between case a of Fig. 2.8 and case c of Fig. 2.9, given as $MTTF_{S0c}/MTTF_{S0a}$ on Fig. 2.8, shows a lower dependency on λ_2/λ_1. From Figs. 2.8 and 2.9 following *design guideline* can be formulated:

> *The failure rate λ_2 of the series element in a nonrepairable (up to system failure) 1-out-of-2 active redundancy should not be larger than 10% of the failure rate λ_1 of the redundant elements; the 10% rule applies also for the case of λ_3 in Fig. 2.9, i. e.*

$$10\lambda_3 < \lambda_2 < 0.1\lambda_1. \qquad (2.28)$$

The investigation of the structures given in Figs. 2.8 and 2.9 for the repairable case ($\mu = 1/MTTR$ as constant repair rate) leads in Section 6.6 to more severe conditions ($\lambda_2<0.01\lambda_1$ in general, and $\lambda_2<0.002\lambda_1$ for $\mu/\lambda_1>500$), see Figs. 6.17, 6.18.

Influence of imperfect switching, as well as incomplete coverage, common cause failures, and other more, are investigated for the repairable case in Section 6.8.

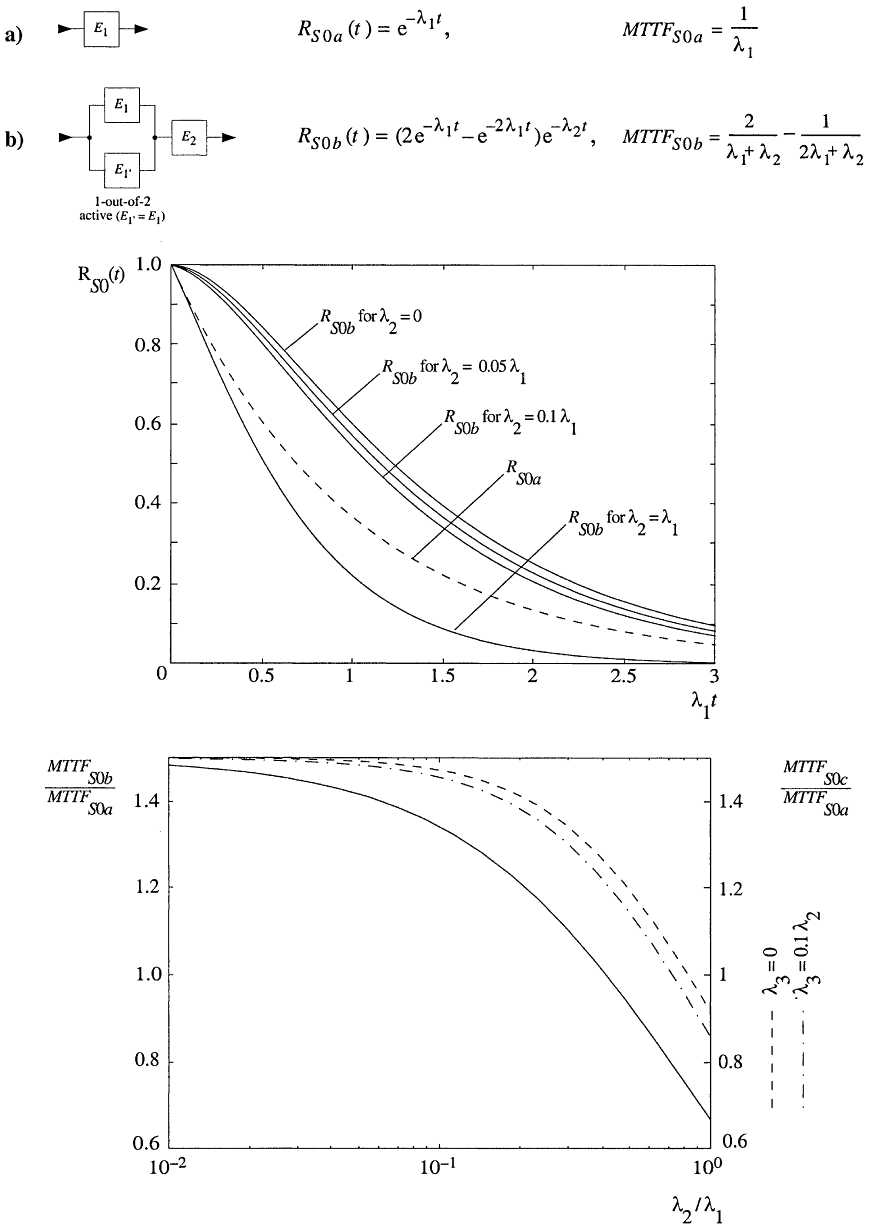
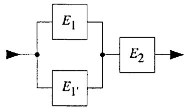


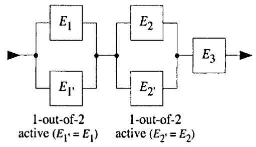
Figure 2.8 Comparison between the one-item structure and a 1-out-of-2 active redundancy with series element (nonrepairable up to system failure, independent elements, constant failure rates λ_1 & λ_2, λ_1 remains the same in both structures; equations according to Table 2.1; given on the right-hand side is $MTTF_{S0c} / MTTF_{S0a}$ with $MTTF_{S0c}$ from Fig. 2.9; see Fig. 6.17 for the repairable case)

b)



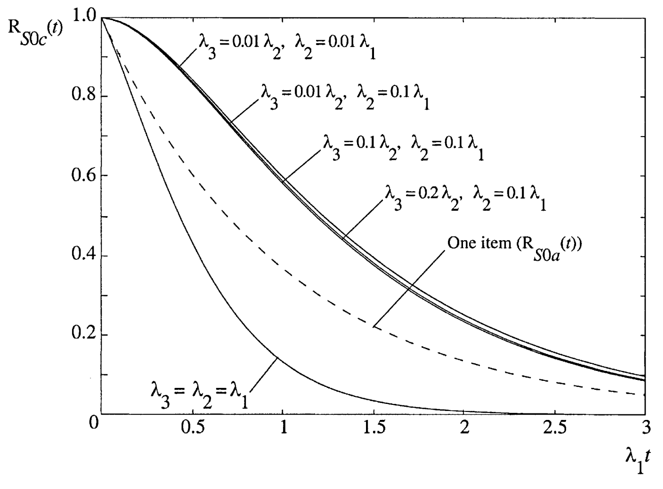
$$R_{S0b}(t) = (2e^{-\lambda_1 t} - e^{-2\lambda_1 t})e^{-\lambda_2 t}, \quad MTTF_{S0b} = \frac{2}{\lambda_1 + \lambda_2} - \frac{1}{2\lambda_1 + \lambda_2}$$

c)


E_1
$E_{1'}$
E_2
$E_{2'}$
E_3
1-out-of-2 active ($E_{1'} = E_1$)
1-out-of-2 active ($E_{2'} = E_2$)

$$R_{S0c}(t) = (2e^{-\lambda_1 t} - e^{-2\lambda_1 t})(2e^{-\lambda_2 t} - e^{-2\lambda_2 t})e^{-\lambda_3 t},$$

$$MTTF_{S0c} = 4\,/\,(\lambda_1 + \lambda_2 + \lambda_3) - 2\,/\,(\lambda_1 + 2\lambda_2 + \lambda_3) - 2\,/(2\lambda_1 + \lambda_2 + \lambda_3) + 1\,/\,(2\lambda_1 + 2\lambda_2 + \lambda_3)$$



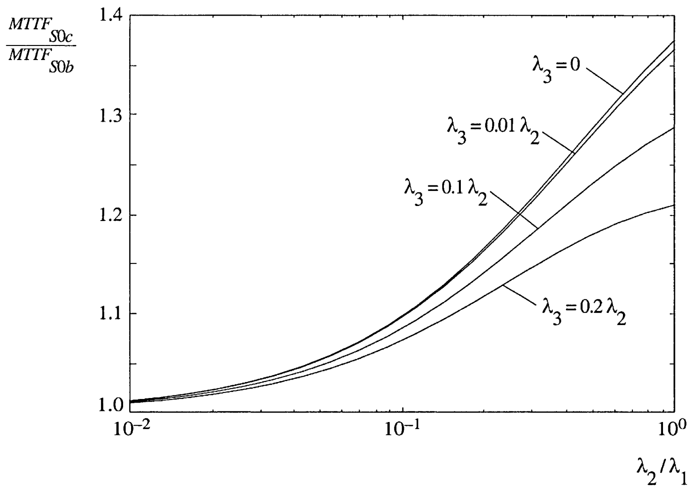


Figure 2.9 Comparison between basic series - parallel structures (nonrepairable up to system failure, active redundancy, independent elements, constant failure rates λ_1 to λ_3, λ_1 and λ_2 remain the same in both structures; equations according to Table 2.1; see Fig. 6.18 for the repairable case)

2.2.6.5 Majority Redundancy

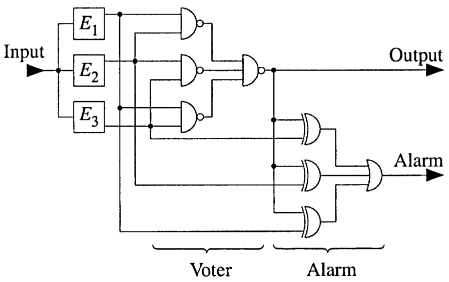
Majority redundancy is a special case of a k-out-of-n redundancy, frequently used in, but not limited to, redundant digital circuits. $2n+1$ outputs are fed to a *voter* whose output represents the majority of its $2n+1$ input signals (*N-modular redundancy*). The investigation is based on the previously described procedure for series - parallel structures, see for example the case of $n=1$ (active redundancy 2-out-of-3 in series with the voter E_v) given in row 6 of Table 2.1. The majority redundancy realizes in a simple way a *fault-tolerant structure without the need for control or switching elements*. The required function is performed with no operational interruption up to the time point of the second failure, while the first failure is automatically masked by the majority redundancy. In digital circuits, the *voter* for a majority redundancy with $n=1$ consists of three two-input NAND and one three-input NAND gate, for one bit solution. An *alarm circuit* is also simple to realize, and can be implemented with three two-input EXOR and one three-input OR gates (Example 2.5). A similar structure as for the alarm circuit can be used to realize a second alarm circuit giving a pulse at the second failure, expanding thus the 2-out-of-3 active redundancy to a 1-out-of-3 active redundancy (Problem 2.6 in Appendix A11). A majority redundancy can also be realized with software (*N-version programming*). Without loss of generality, majority redundancy applies to serial or parallel n bit words (bytes). See e.g. [6.75 (Chapter 4)] for a deeper discussion.

Example 2.5

Realize a majority redundancy for $n=1$ with voter and alarm signal at the first failure of a redundant element (one bit solution with "1" for operating and "0" for failure).

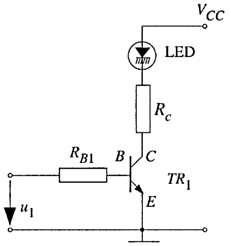
Solution

Using the same notation as for Eq. (2.16), the 2-out-of-3 active redundancy can be implemented by $(e_1 \cap e_2) \cup (e_1 \cap e_3) \cup (e_2 \cap e_3)$. With this, the functional block diagram of the voter for a majority redundancy with $n=1$ is obtained as realization of the logic equation related to the above expression. The alarm circuit giving a logic 1 at the occurrence of the first failure is also easy to implement. Also it is possible to realize a second alarm circuit to detect the second failure, expanding the 2-out-of-3 to a 1-out-of-3 redundancy (Problem 2.6 in Appendix A11).



Example 2.6

Compute the predicted reliability for the following circuit, for which the required function asks that the LED must light when the control voltage u_1 is high. The environmental conditions correspond to G_B in Table 2.3, with ambient temperature $\theta_A = 50°C$ inside the equipment and 30°C at the location of the LED; quality factor $\pi_Q = 1$ as per Table 2.4.



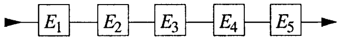
u_1	:	0.1 V and 4 V
V_{CC}	:	5 V
LED	:	1 V at 20 mA, $I_{max} = 100$ mA
R_C	:	150 Ω, 1/2 W, MF
TR_1	:	Si, 0.3 W, 30 V, β > 100, plastic
R_{B1}	:	10 kΩ, 1/2 W, MF

Solution

The solution is based on the procedure given in Fig 2.1.

1. The required function can be fulfilled since the transistor works as an electronic switch with $I_C \approx 20\,\text{mA}$ and $I_B \approx 0.33\,\text{mA}$ in the on state (saturated) and the off state is assured by $u_1 = 0.1\,\text{V}$.

2. Since all elements are involved in the required function, the reliability block diagram consists of the series connection of the five items E_1 to E_5, where E_5 represents the printed circuit with soldering joints.



$E_1 \triangleq$ LED, $E_2 \triangleq R_C$, $E_3 \triangleq R_{B1}$, $E_4 \triangleq TR_1$
$E_5 \triangleq$ PCB and solder joints

3. The stress factor of each element can be easily determined from the circuit and the given rated values. A stress factor 0.1 is assumed for all elements when the transistor is off. When the transistor is on, the stress factor is 0.2 for the diode and about 0.1 for all other elements. The ambient temperature is 30°C for the LED and 50°C for the remaining elements.

4. The failure rates of the individual elements is determined (approximately) with data from Section 2.2.4 (Example 2.4, Figs. 2.4 - 2.6, Tables 2.3 and 2.4 with $\pi_E = \pi_Q = 1$). Thus,

LED	:	$\lambda_1 \approx 1.3 \cdot 10^{-9}\,\text{h}^{-1}$
Transistor	:	$\lambda_4 \approx 3 \cdot 10^{-9}\,\text{h}^{-1}$
Resistor	:	$\lambda_2 = \lambda_3 \approx 0.3 \cdot 10^{-9}\,\text{h}^{-1}$,

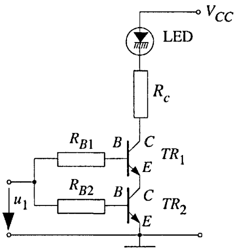
   when the transistor is on. For the printed circuit board and soldering joints, $\lambda_5 = 2 \cdot 10^{-9}\,\text{h}^{-1}$ is assumed. The above values for λ remain practically unchanged when the transistor is off due to the low stress factors (the stress factor in the off state was set at 0.1).

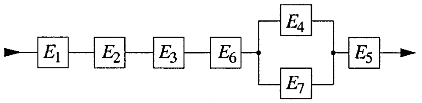
5. Based on the results of Step 4, the reliability function of each element can be determined as $\text{R}_i(t) = e^{-\lambda_i t}$

6. The reliability function $\text{R}_{S0}(t)$ for the whole circuit can now be calculated. Equation (2.19)

yields $R_S(t) = e^{-6.9\cdot10^{-9}t}$. For 10 years of continuous operation, for example, the predicted reliability of the circuit is > 0.999.

7. ***Supplementary result:*** To discuss this example further, let us assume that the failure rate of the transistor is too high (e. g. for safety reasons) and that no transistor of better quality can be obtained. Redundancy should be implemented for this element. Assuming as *failure modes* *short* between emitter and collector for transistors and *open* for resistors, the resulting circuit and the corresponding reliability block diagram are





E_1 to E_5 as in point 2
$E_6 \triangleq R_{B2} \triangleq R_{B1}$, $E_7 \triangleq TR_2 \triangleq TR_1$

Due to the very small stress factor, calculation of the individual element failure rates yields the same values as without redundancy. Thus, for the reliability function of the circuit one obtains (assuming independent elements)

$$R_{S0}(t) = e^{-4.2\cdot10^{-9}t}(2e^{-3\cdot10^{-9}t} - e^{-6\cdot10^{-9}t}),$$

from which it follows that

$$R_{S0}(t) \approx e^{-4.2\cdot10^{-9}t} \qquad \text{for } t \le 10^6\,\text{h}.$$

Circuit reliability is then practically no longer influenced by the transistor. This agrees with the discussion made with Fig. 2.7 for $\lambda t << 1$. If the *failure mode* of the transistors were an open between collector and emitter, both elements E_4 and E_7 would appear in series in the reliability block diagram; redundancy would be a *disadvantage* in this case. The intention to put R_{B1} and R_{B2} in parallel (redundancy) or to use just one basis resistor is wrong, the functionality of the circuit would be compromised because of the saturation voltage of TR_2.

2.2.7 Part Count Method

In an early development phase, for logistic purposes, or in some particular applications, a *rough estimate* of the predicted reliability can be required. For such an analysis, it is generally assumed that the system under consideration is *without redundancy* (series structure as in Section 2.2.6.1) and the calculation of the failure rate at component level is made either using *field data* or by considering technology, environmental, and quality factors only. This procedure is known as *part count method* [2.25] and differs basically from the *part stress method* introduced in Section 2.2.4. Advantage of a part count prediction is the great simplicity, but its usefulness is often limited to specific applications.

2.3 Reliability of Systems with Complex Structure

Complex structures arise in many applications, e.g. in power, telecommunications, defense, and aerospace systems. In the context of this book, a structure is *complex* when the reliability block diagram either cannot be reduced to a series-parallel structure with independent elements or does not exist. For instance, a reliability block diagram does not exist if more than two states (good / failed) or one failure mode (e.g. short or open) must be considered for an element. Moreover, the reduction of a reliability block diagram to a series - parallel structure with independent elements is in general not possible with distributed structures or when elements appear in the diagram more than once (cases 7, 8, 9 in Table 2.1). The term *independent elements* refers to *independence up to the system failure*, in particular *without load sharing* between redundant elements (load sharing is considered in Section 2.3.5 and Chapter 6). For comparative investigations in Chapter 6, the term *totally independent elements* will be used to indicate for, repairable systems, *independence with respect to operation and repair* (each element in the reliability block diagram operates and fails *independently* from every other element and has its own repair crew).

Analysis of complex structures can become difficult and time-consuming. However, methods are well developed, should the reliability block diagram *exist* and the system satisfy the following requirements:

1. Only active (parallel) redundancy is considered.
2. Elements can appear more than once in the reliability block diagram, but different elements are independent (totally independent for Eq. (2.48)).
3. On / off operations are either 100% reliable, or their effect has been considered in the reliability block diagram according to the above restrictions.

Under these assumptions, analysis can be performed using Boolean models. However, for practical applications, simple heuristically oriented methods apply well. *Heuristic methods* are given in Sections 2.3.1-2.3.3, *Boolean models* in Section 2.3.4.

Section 2.3.5 deals then with *warm redundancy*, allowing for *load sharing*. Section 2.3.6 considers elements with *two failure modes*. Stress / strength analysis are discussed in Section 2.5. Further aspects, as well as situations in which the reliability block diagram does not exist, are considered in Section 6.8 (see also Section 6.9 for an introduction to BDD, dynamic FT, Petri nets & computer-aided analysis).

As in the previous sections, reliability figures have the indices $S0$, where S stands for *system* and 0 specifies *system new at* $t=0$.

2.3.1 Key Item Method

The *key item method* is based on the theorem of *total probability* (Eq. (A6.17)). Assuming the item is new at $t=0$, the event $\{$item operates failure free in $(0, t]\}$, or $\{$system *up* in $(0, t]\}$, can be split into the following two complementary events

$$\{\text{Element } E_i \textit{ up} \text{ in } (0, t] \cap \text{system } \textit{up} \text{ in}(0, t]\}$$

and

$$\{\text{Element } E_i \text{ fails in } (0, t] \cap \text{system } \textit{up} \text{ in}(0, t]\}.$$

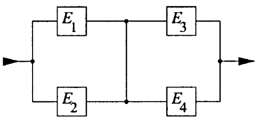
From this it follows that, for the *reliability function* $\mathrm{R}_{S0}(t)$,

$$\begin{aligned}\mathrm{R}_{S0}(t) &= \mathrm{R}_i(t)\Pr\{\text{system } \textit{up} \text{ in } (0,t] \mid (E_i \textit{ up} \text{ in } (0, t] \cap \text{system new at } t = 0)\}\\ &+ (1-\mathrm{R}_i(t))\Pr\{\text{system } \textit{up} \text{ in } (0,t] \mid (E_i \textit{ failed} \text{ in } (0, t] \cap \text{system new at } t = 0)\},\end{aligned} \tag{2.29}$$

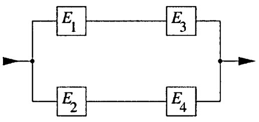
where $\mathrm{R}_i(t) = \Pr\{E_i \textit{ up} \text{ in}(0,t] \mid \text{system new at } t = 0\} = \Pr\{E_i \textit{ up} \text{ in } (0,t] \mid E_i \text{ new at } t = 0\}$ as in Eq. (2.16). Element E_i must be chosen in such a way that a series-parallel structure is obtained for the reliability block diagrams conditioned by the events $\{E_i \textit{ up} \text{ in } (0, t]\}$ and $\{E_i \text{ failed in } (0, t]\}$. Successive application of Eq. (2.29) is also possible (Examples 2.9 and 2.14). Sections 2.3.1.1 and 2.3.1.2 present two typical situations. In the context of Boolean functions, the above decomposition is known as a *Shannon decomposition* (Eq. (2.38)) and leads in particular to *binary decision diagrams* (Section 6.9.3).

2.3.1.1 Bridge Structure

The reliability block diagram of a *bridge structure* with a bi-directional connection is shown in Fig. 2.10 (row 7 in Table 2.1). Element E_5 can work with respect to the required function in *both directions*, from E_1 via E_5 to E_4 and from E_2 via E_5 to E_3. It is therefore in a *key position* (key element). This property is used to calculate the reliability function by means of Eq. (2.29) with $E_i = E_5$. For the conditional probabilities in Eq. (2.29), the corresponding reliability block diagrams are



E_5 did not fail in $(0, t]$



E_5 failed in $(0, t]$

From Eq. (2.29), it follows that (with $R_S = R_{S0}(t)$, $R_i = R_i(t)$, and $R_i(0) = 1$, $i = 1, \ldots, 5$)

$$R_S = R_5(R_1 + R_2 - R_1 R_2)(R_3 + R_4 - R_3 R_4) + (1-R_5)(R_1 R_3 + R_2 R_4 - R_1 R_2 R_3 R_4). \tag{2.30}$$

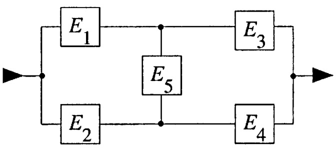


Figure 2.10 Reliability block diagram of a bridge circuit with a bi-directional connection on E_5

Same considerations apply to the bridge structure with a directed connection (row 8 in Table 2.1). Here, E_i must be E_1, E_2, E_3, or E_4 (preferably E_1 or E_4), yielding

$$R_S = R_4 [R_2 + R_1(R_3 + R_5 - R_3R_5) - R_2R_1(R_3 + R_5 - R_3R_5)] + (1 - R_4)R_1R_3 , \qquad (2.31)$$

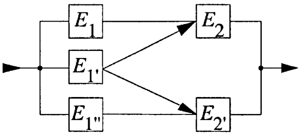
when choosing $E_i = E_4$, and to the same result

$$R_S = R_1 [R_3 + R_4(R_2 + R_5 - R_2R_5) - R_3R_4(R_2 + R_5 - R_2R_5)] + (1 - R_1)R_2R_4 ,$$

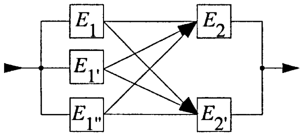
when choosing E_1. Example 2.7 shows a further application of the key item method.

Example 2.7

Give the reliability of the item according to case a) below. How much would the reliability be improved if the structure were be modified according to case b)? (Assumptions: nonrepairable up to system failure, active redundancy, independent elements, $\mathrm{R}_{E1}(t) = \mathrm{R}_{E1'}(t) = \mathrm{R}_{E1''}(t) = \mathrm{R}_1(t)$ and $\mathrm{R}_{E2}(t) = \mathrm{R}_{E2'}(t) = \mathrm{R}_2(t)$).



Case a)



Case b)

Solution

Element $E_{1'}$ is in a key position in case a). Thus, similarly to Eq. (2.30), one obtains $R_a = R_1(2R_2 - R_2^2) + (1 - R_1)(2R_1R_2 - R_1^2R_2^2)$ with $R_a = \mathrm{R}_{0a}(t)$, $R_i = \mathrm{R}_i(t)$, $\mathrm{R}_i(0) = 1$, $i = 1, 2$. Case b) represents a series connection of a 1-out-of-3 redundancy with a 1-out-of-2 redundancy. From Sections 2.2.6.3 and 2.2.6.4 it follows that $R_b = R_1R_2(3 - 3R_1 + R_1^2)(2 - R_2)$, with $R_b = \mathrm{R}_{0b}(t)$, $R_i = \mathrm{R}_i(t)$, $\mathrm{R}_i(0) = 1$, $i = 1, 2$. From this,

$$R_b - R_a = 2R_1R_2(1 - R_2)(1 - R_1)^2 . \qquad (2.32)$$

The difference $R_b - R_a$ reaches as maximum the value $2/27$ for $R_1 = 1/3$ and $R_2 = 1/2$, i.e. $R_b = 57/108$ and $R_a = 49/108$ ($R_b - R_a = 0$ for $R_1 = 0$, $R_1 = 1$, $R_2 = 0$, $R_2 = 1$); the advantage of case b) is small, as far as reliability is concerned.

2.3.1.2 Reliability Block Diagram in Which at Least One Element Appears More than Once

In practice, situations often occur in which an element appears more than once in the reliability block diagram, although, physically, there is only one such element in the system considered. These situations can be investigated with the *key item method* introduced in Section 2.3.1.1, see Examples 2.8, 2.9, and 2.14.

Example 2.8

Give the reliability for the equipment introduced in Example 2.2.

Solution

In the reliability block diagram of Example 2.2, element E_2 is in a key position. Similarly to Eq. (2.30) it follows that

$$R_S = R_2 R_1 (R_4 + R_5 - R_4 R_5) + (1 - R_2) R_1 R_3 R_5, \tag{2.33}$$

with $R_S = \mathrm{R}_{S0}(t)$ and $R_i = \mathrm{R}_i(t)$, $\mathrm{R}_i(0) = 1$, $i = 1, ..., 5$.

Example 2.9

Give the reliability for the redundant circuit of Example 2.3.

Solution

In the reliability block diagram of Example 2.3, U_1 and U_2 are in a key position. Using the method introduced in Section 2.3.1 successively on U_1 and U_2, i.e. on E_5 and E_6, yields.

$$R_S = R_9 \{R_5 [R_6 (R_1 R_7 + R_4 R_8 - R_1 R_4 R_7 R_8)(R_2 + R_3 - R_2 R_3) + (1 - R_6) R_1 R_2 R_7]$$
$$+ (1 - R_5) R_3 R_4 R_6 R_8 \}.$$

With $R_1 = R_2 = R_3 = R_4 = R_D$, $R_5 = R_6 = R_U$, $R_7 = R_8 = R_I$, $R_9 = R_{II}$ it follows that

$$R_S = R_U R_{\mathrm{II}} [R_U (2 R_D R_{\mathrm{I}} - R_D^2 R_{\mathrm{I}}^2)(2 R_D - R_D^2) + 2(1 - R_U) R_D^2 R_{\mathrm{I}}], \tag{2.34}$$

with $R_S = \mathrm{R}_{S0}(t)$, $R_U = \mathrm{R}_U(t)$, $R_D = \mathrm{R}_D(t)$, $R_I = \mathrm{R}_I(t)$, $R_{II} = \mathrm{R}_{II}(t)$, $\mathrm{R}_i(0) = 1$ $(i = 1, ..., 9)$.

2.3.2 Successful Path Method

In this and in the next section, two general (closely related) methods are introduced. For simplicity, considerations will be based on the reliability block diagram given in Fig. 2.11. As in Section 2.2.6.1, e_i stands for the *event*

$$\{\text{element } E_i \textit{ up} \text{ in the interval } (0, t] \mid \text{new at } t = 0\},$$

hence $\Pr\{e_i\} = \mathrm{R}_i(t)$ with $\mathrm{R}_i(0) = 1$, as in Eq. (2.16), and $\Pr\{\bar{e}_i\} = 1 - \mathrm{R}_i(t)$. The *successful path method* is based on the following concept:

> *The system fulfills its required function if there is at least one path between the input and the output upon which all elements perform their required function.*

Paths must lead from left to right and may not contain any loops. Only the given direction is possible along a directed connection. The following successful paths exist in the reliability block diagram of Fig. 2.11

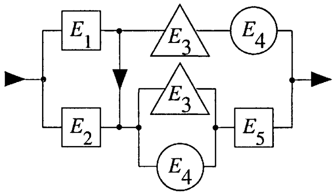


Figure 2.11 Reliability block diagram of a complex structure (elements E_3 and E_4 appear each twice in the RBD, the directed connection has reliability 1)

$$e_1 \cap e_3 \cap e_4, \quad e_1 \cap e_3 \cap e_5, \quad e_1 \cap e_4 \cap e_5, \quad e_2 \cap e_3 \cap e_5, \quad e_2 \cap e_4 \cap e_5.$$

Consequently it follows that

$$\mathrm{R}_{S0}(t) = \Pr\{(e_1 \cap e_3 \cap e_4) \cup (e_1 \cap e_3 \cap e_5) \cup (e_1 \cap e_4 \cap e_5) \\ \cup (e_2 \cap e_3 \cap e_5) \cup (e_2 \cap e_4 \cap e_5)\};$$

from which, using the addition theorem of probability theory (Eqs. (A6.14), (A6.15)),

$$R_S = R_1 R_3 R_4 + R_1 R_3 R_5 + R_1 R_4 R_5 + R_2 R_3 R_5 + R_2 R_4 R_5 - 2 R_1 R_3 R_4 R_5 \\ - R_1 R_2 R_3 R_5 - R_1 R_2 R_4 R_5 - R_2 R_3 R_4 R_5 + R_1 R_2 R_3 R_4 R_5, \qquad (2.35)$$

with $R_S = R_{S0}(t)$, $R_i = R_i(t)$, and $R_i(0) = 1$, $i = 1, ..., 5$. Equation (2.35) follows also (directly) using the key item method (Section 2.3.1) successively on E_3 and E_5 ($R_S = R_3 [R_5 (R_1 + R_2 - R_1 R_2) + (1 - R_5) R_1 R_4] + (1 - R_3) R_4 R_5 (R_1 + R_2 - R_1 R_2)$).

2.3.3 State Space Method

This method is based on the following concept:

Every element E_i is assigned an indicator $\zeta_i(t)$ with the following property: $\zeta_i(t) = 1$ as long as E_i does not fail, and $\zeta_i(t) = 0$ if E_i has failed ($\zeta_i(0) = 1$). For every given (fixed) $t \geq 0$, the vector with components $\zeta_i(t)$ determines the system state. Since each element in the interval $(0, t]$ functions or fails independently of the others, 2^n states are possible for an item with n elements. After listing the 2^n possible states at time t, all those states are determined in which the system performs the required function. The probability that the system is in one of these states is the reliability function $\mathrm{R}_{S0}(t)$ of the system considered (with $\mathrm{R}_{S0}(0) = 1$).

The 2^n possible conditions at time t for the reliability block diagram of Fig. 2.11 are

E_1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
E_2	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
E_3	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
E_4	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
E_5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S	1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

A "1" in this table means that the element or item considered has not failed in $(0, t]$ (see footnote on p. 58 for fault tree analysis). For Fig. 2.11, the event

$$\{\text{system } up \text{ in the interval } (0, t] \mid \text{new at } t=0\}$$

is equivalent to the event

$$\begin{aligned}\{&(e_1 \cap e_2 \cap e_3 \cap e_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap e_3 \cap e_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap e_4 \cap e_5)\\ &\cup (e_1 \cap e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap \bar{e}_3 \cap e_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap \bar{e}_3 \cap e_4 \cap e_5)\\ &\cup (e_1 \cap e_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \cup (\bar{e}_1 \cap e_2 \cap e_3 \cap \bar{e}_4 \cap e_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5)\\ &\cup (e_1 \cap e_2 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap e_4 \cap \bar{e}_5)\}.\end{aligned}$$

After appropriate simplification, this reduces to

$$\begin{aligned}\{&(e_2 \cap e_3 \cap e_5) \cup (e_1 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5)\\ &\cup (e_1 \cap \bar{e}_2 \cap e_4 \cap e_5) \cup (e_2 \cap \bar{e}_3 \cap e_4 \cap e_5)\},\end{aligned}$$

from which

$$\begin{aligned}\mathrm{R}_{S0}(t) = \Pr\{&(e_2 \cap e_3 \cap e_5) \cup (e_1 \cap e_3 \cap e_4 \cap \bar{e}_5) \cup (e_1 \cap \bar{e}_2 \cap e_3 \cap \bar{e}_4 \cap e_5)\\ &\cup (e_1 \cap \bar{e}_2 \cap e_4 \cap e_5) \cup (e_2 \cap \bar{e}_3 \cap e_4 \cap e_5)\}. \qquad (2.36)\end{aligned}$$

Evaluation of Eq. (2.36) leads to Eq. (2.35). Note that all events in the state space method (columns in state space table & terms in Eq. (2.36)) are *mutually exclusive.*

2.3.4 Boolean Function Method

The *Boolean function method* generalizes & formalizes the methods based on the reliability block diagram (Section 2.2) and those introduced in Sections 2.3.1 - 2.3.3. For this analysis, besides the 3 assumptions given on p. 52, it is supposed that the system considered is *coherent* (see Eq. (2.37) for a definition); i.e., basically, that the state of the system depends on the states of all of its elements and the structure function (Eq. (2.37)) is monotone (implying in particular, that for a system down no additional failure of any element can bring it in an up state and, for a repairable system, if the system is up it remains up if any element is repaired). Almost all systems in practical applications are coherent. In the following, *up* is used for *system in operating state* and *down* for *system in a failed state* (in repair if repairable).

A system is *coherent* if its state can be described by a *structure function* ϕ

$$\phi = \phi(\zeta_1, \ldots, \zeta_n) = \begin{cases} 1 & \text{for system up} \\ 0 & \text{for system down}^{+)} \end{cases} \qquad (2.37)$$

of the *indicators* $\zeta_i = \zeta_i(t)$, defined in Section 2.3.3 [++)] ($\zeta_i = 1$ if element E_i is *up* and $\zeta_i = 0$ if element E_i is *down*), for which the following applies:

1. ϕ depends on all the variables ζ_i $(i = 1, \ldots, n)$.
2. ϕ is non decreasing in all variables ($\phi = 0$ for all $\zeta_i = 0$, $\phi = 1$ for all $\zeta_i = 1$).

ϕ is a Boolean function and can thus be written as (Shannon decomposition)

$$\begin{aligned} \phi(\zeta_1, \ldots, \zeta_n) = {} & \zeta_i \, \phi(\zeta_1, \ldots, \zeta_{i-1}, 1, \zeta_{i+1}, \ldots, \zeta_n) \\ & + (1 - \zeta_i) \, \phi(\zeta_1, \ldots, \zeta_{i-1}, 0, \zeta_{i+1}, \ldots, \zeta_n), \qquad i = 1, \ldots, n. \end{aligned} \qquad (2.38)$$

Equation (2.38) is similar to Eq. (2.29). Successive Shannon decompositions leads to *Binary Decision Diagrams* (BDD), see Section 6.9.3.

Since the indicators ζ_i and the structure function ϕ take only values 0 and 1, it follows that $\mathrm{E}[\zeta_i(t)] = 1 \cdot \Pr\{\zeta_i(t) = 1\} + 0 \cdot \Pr\{\zeta_i(t) = 0\} = \Pr\{\zeta_i(t) = 1\}$; thus,

$$\mathrm{R}_i(t) = \Pr\{\zeta_i(t) = 1\} = \mathrm{E}[\zeta_i(t)], \qquad \mathrm{R}_i(0) = 1, \; i = 1, \ldots, n, \qquad (2.39)$$

applies for the *reliability function* $\mathrm{R}_i(t)$ of element E_i [++)], and

$$\mathrm{R}_{S0}(t) = \Pr\big\{\phi(\zeta_1(t), \ldots, \zeta_n(t)) = 1\big\} = \mathrm{E}[\phi(\zeta_1(t), \ldots, \zeta_n(t))], \quad \mathrm{R}_S(0) = 1, \qquad (2.40)$$

applies for the *reliability function* $\mathrm{R}_{S0}(t)$ of the system (calculation of $\mathrm{E}[\phi]$ is often easier than calculation of $\Pr\{\phi = 1\}$).

The Boolean function method transfers thus the problem of calculating $\mathrm{R}_{S0}(t)$ to that of the determination of the structure function $\phi(\zeta_1, \ldots, \zeta_n)$. Two methods with a great intuitive appeal are available for this purpose (for coherent systems):

1. *Minimal Path Sets* approach: A set $\mathcal{P}_i$ of elements is a *minimal path set* if the system is up when $\zeta_j = 1$ for all $E_j \in \mathcal{P}_i$ and $\zeta_k = 0$ for all $E_k \notin \mathcal{P}_i$, but this does not apply for any subset of $\mathcal{P}_i$ (for the bridge in Fig. 2.10, {1,3}, {2,4}, {1,5,4}, and {2,5,3} are the minimal path sets). The elements E_j within $\mathcal{P}_i$ form a *series model* with structure function

$$\phi_{\mathcal{P}_i} = \prod_{E_j \in \mathcal{P}_i} \zeta_j \, . \qquad (2.41)$$

If for a given system there are r minimal path sets, these form an *active 1-out-of-r redundancy*, yielding (see also Eq. (2.24))

[+)] In fault tree analysis (FTA), "0" for up and "1" for down is often used [A2.5 (IEC 61025)].

[++)] No distinction is made here between *Boolean random variable* ζ_i and *Boolean variable* (realization of ζ_i); equations with $\zeta_i(t), \mathrm{R}_i(t), \mathrm{R}_{S0}(t)$ are intended to apply for every given (fixed) $t \geq 0$; considering that each ζ_i takes values 0 & 1 and appears only in linear form, addition, subtraction & multiplication can be used (in particular $\zeta_i \wedge \zeta_j = \zeta_i \zeta_j$).

$$\phi = \phi(\zeta_1, \ldots, \zeta_n) = 1 - \prod_{i=1}^{r} (1 - \phi_{\mathcal{P}_i}) = 1 - \prod_{i=1}^{r} (1 - \prod_{E_j \in \mathcal{P}_i} \zeta_j). \tag{2.42}$$

2. *Minimal Cut Sets* approach: A set C_i is a *minimal cut* set if the system is down when $\zeta_j = 0$ for all $E_j \in C_i$ and $\zeta_k = 1$ for all $E_k \notin C_i$, but this does not apply for any subset of C_i (for the bridge in Fig. 2.10, {1,2}, {3,4}, {1,5,4}, and {3,5,2} are the minimal cut sets). The elements E_j within C_i form a *parallel model* (*active redundancy with* $k = 1$) with structure function (Eq. (2.24))

$$\phi_{C_i} = 1 - \prod_{E_j \in C_i} (1 - \zeta_j). \tag{2.43}$$

If for a given system there are m minimal cut sets, these form a *series model*, yielding (see also Eq. (2.17))

$$\phi = \phi(\zeta_1, \ldots, \zeta_n) = \prod_{i=1}^{m} \phi_{C_i} = \prod_{i=1}^{m} (1 - \prod_{E_j \in C_i} (1 - \zeta_j)). \tag{2.44}$$

A series model with elements $E_1, \ldots, E_n$ has one path set and n cut sets, a parallel model (1-out-of-n) has one cut set and n path sets. Algorithms for finding all minimal path sets and all minimal cut sets are known, see e.g. [2.34 (1975)].

For coherent *nonrepairable systems* (up to system failure) with structure function $\phi(\zeta_1, \ldots, \zeta_n)$ per Eq. (2.42) or (2.44), the reliability function $R_{S0}(t)$ follows (for any given (fixed) $t > o$, $R_{S0}(0) = 1$) from Eq. (2.40) or directly from

$$R_{S0}(t) = \Pr\{\phi_{\mathcal{P}_1} = 1 \cup \ldots \cup \phi_{\mathcal{P}_r} = 1\} = 1 - \Pr\{\phi_{C_1} = 0 \cup \ldots \cup \phi_{C_m} = 0\}. \tag{2.45}$$

Equation (2.45) has a great intuitive appeal. For practical applications, the following bounds for the reliability function $R_{S0}(t)$ can often be used [2.34 (1975)]

$$\prod_{i=1}^{m} \Pr\{\phi_{C_i} = 1\} \le R_{S0}(t) \le 1 - \prod_{i=1}^{r} \Pr\{\phi_{\mathcal{P}_i} = 0\}. \tag{2.46}$$

If the minimal path sets have no common elements, the right-hand inequality of Eq. (2.46) becomes an equality, similar is for the minimal cut sets (left-hand inequality).

For coherent *nonrepairable systems* (up to system failure) with *independent elements*, the reliability function $R_{S0}(t)$ can also be obtained, considering $\zeta_i \, \zeta_i = \zeta_i$,

> *directly from the structure function* $\phi(\zeta_1, \ldots, \zeta_n)$ *given by Eqs. (2.42) or (2.44), by substituting* $R_i(t)$ *for* ζ_i (Eqs. (2.39), (2.40), (A6.69)).

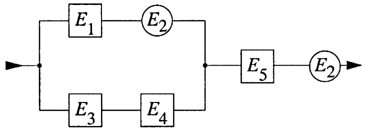
Also it is possible to use the *disjunctive normal form* $\phi_D(\zeta_1, \ldots, \zeta_n)$ or *conjunctive normal form* $\phi_L(\zeta_1, \ldots, \zeta_n)$ of the structure function $\phi(\zeta_1, \ldots, \zeta_n)$, yielding

$$R_{S0}(t) = \phi_D(R_1, \ldots, R_n) = \phi_L(R_1, \ldots, R_n), \quad R_i = R_i(t), R_i(0) = 1, i = 1, \ldots, n. \tag{2.47}$$

The path sets given on p. 56 are the minimal path sets for the reliability block diagram of Fig. 2.11. Equation (2.35) follows then from Eq. (2.40), using Eq. (2.42) for $\phi(\zeta_1,...,\zeta_5) = 1-(1-\zeta_1\zeta_3\zeta_4)(1-\zeta_1\zeta_3\zeta_5)(1-\zeta_1\zeta_4\zeta_5)(1-\zeta_2\zeta_3\zeta_5)(1-\zeta_2\zeta_4\zeta_5)$, simplified by considering $\zeta_i\zeta_i=\zeta_i$, and substituting $\mathrm{R}_i(t)$ for ζ_i in the final $\phi(\zeta_1,...,\zeta_5)$, see also the footnote on p. 58. Investigation of the block diagram of Fig. 2.11 by the method of minimal cut sets is more laborious. Obviously, minimal path sets and minimal cut sets deliver the same structure function, with different effort depending on the structure of the reliability block diagram considered (structures with many series elements can be treated easily with minimal path sets).

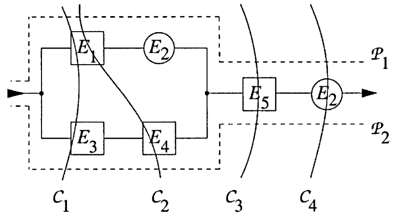
Example 2.10

Give the structure function according to the minimal path sets and the minimal cut sets approach for the following reliability block diagram, and calculate the reliability function assuming independent elements and active redundancies.



Solution

For the above reliability block diagram, there exist 2 minimal path sets $\mathcal{P}_1$, $\mathcal{P}_2$ and 4 minimal cut sets $C_1,...,C_4$, as given below.



The structure function follows then from Eq. (2.42) for the minimal path sets

$$\phi(\zeta_1,...,\zeta_5) = 1-(1-\zeta_1\zeta_2\zeta_5)(1-\zeta_2\zeta_3\zeta_4\zeta_5) = \zeta_1\zeta_2\zeta_5+\zeta_2\zeta_3\zeta_4\zeta_5-\zeta_1\zeta_2\zeta_3\zeta_4\zeta_5$$

or from Eq. (2.44) for the minimal cut sets (in both cases by considering $\zeta_i\zeta_i=\zeta_i$, $\zeta_i\zeta_j=\zeta_j\zeta_i$)

$$\begin{aligned}\phi(\zeta_1,...,\zeta_5) &= [1-(1-\zeta_1)(1-\zeta_3)][1-(1-\zeta_1)(1-\zeta_4)][1-(1-\zeta_5)][1-(1-\zeta_2)] \\ &= (\zeta_1+\zeta_3-\zeta_1\zeta_3)(\zeta_1+\zeta_4-\zeta_1\zeta_4)\zeta_2\zeta_5 \\ &= \zeta_1\zeta_2\zeta_5+\zeta_2\zeta_3\zeta_4\zeta_5-\zeta_1\zeta_2\zeta_3\zeta_4\zeta_5.\end{aligned}$$

Assuming independence for the (different) elements, it follows for the reliability function (for both cases and with $R_S=R_{S0}(t)$, $R_i=R_i(t)$, and $R_i(0)=1$, $i=1, ..., 5$)

$$R_S = R_1R_2R_5+R_2R_3R_4R_5-R_1R_2R_3R_4R_5.$$

Supplementary results: Calculation with the key item method leads directly to

$$R_S = R_2(R_1+R_3R_4-R_1R_3R_4)R_5+(1-R_2)\cdot 0.$$

For *coherent repairable systems* with elements which are *as-good-as-new* after repair and *totally independent* (every element operates and is repaired independently from each other element, i. e., has its own repair crew and continues operation during the repair of a failed element), expressions for $\mathrm{R}_{S0}(t)$ can be used to calculate the *point availability* $\mathrm{PA}_{S0}(t)$, substituting $\mathrm{R}_i(t)$ with $\mathrm{PA}_{i0}(t)$. For Eq. (2.47) this leads to

$$\mathrm{PA}_{S0}(t) = \phi_D(PA_1, \ldots, PA_n) = \phi_L(PA_1, \ldots, PA_n), \tag{2.48}$$

with $PA_i = \mathrm{PA}_{i0}(t)$ for the general case (Eq. (6.17)) or $PA_i = MTTF_i / (MTTF_i + MTTR_i)$ for steady-state or $t \to \infty$ (Eq. (6.48)). However, in many practical applications, a repair crew for each element in the reliability block diagram of a system is not available and not failed elements often stop to operate during the repair of a failed element. Nevertheless, Eq. (2.48) can be used as an *approximation* (upper bound in general) for $\mathrm{PA}_{S0}(t)$. For *repairable* elements, the indicator $\zeta_i(t)$ given in Section 2.3.3 is defined as $\zeta_i(t)=1$ for element E_i *operating* (up) and $\zeta_i(t)=0$ for E_i *in repair* (down), yielding $\mathrm{E}[\zeta_i(t)] = \mathrm{PA}_{i0}(t)$. In practical applications, it is often preferable to compute the *unavailability* $1-\mathrm{PA}_{S0}(t)$.

2.3.5 Parallel Models with Const. Failure Rates & Load Sharing

In the redundancy structures investigated in the previous sections, all elements were operating under the same conditions. For this type of redundancy, called *active* (parallel) *redundancy*, the assumed statistical independence of the elements implies in particular that there is *no load sharing*. This assumption does not arise in many practical applications, for example, at component level or in the presence of power elements. The investigation of the reliability function in the case of load sharing or of other kinds of dependency involves the use of *stochastic processes*. The situation is simple if one can assume that the failure rate of each element changes *only* when a failure occurs. In this case, the general model for a *k-out-of-n redundancy* is a *death process* as given in Fig. 2.12 (birth and death process as in Fig. 6.13 for the repairable case with constant failure & repair rates). $Z_0, \ldots, Z_{n-k+1}$ are the states of the process. In state Z_i, i elements are down. At state Z_{n-k+1} the system is down.

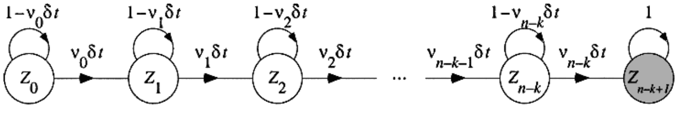


Figure 2.12 Diagram of the transition probabilities in $(t, t+\delta t]$ for a k-out-of-n redundancy (nonrepairable, constant failure rates *during the sojourn time in each state* (not necessarily at a state change, e. g. because of load sharing), t arbitrary, $\delta t \to 0$, Markov process, Z_{n-k+1} down state)

Assuming

$$\lambda = \text{failure rate of an element in the } \textit{operating state} \tag{2.49}$$

and

$$\lambda_r = \text{failure rate of an element in the } \textit{reserve state} \quad (\lambda_r \le \lambda), \tag{2.50}$$

the model of Fig. 2.12 considers in particular the following cases:

1. Active redundancy without load sharing (independent elements)

   $$\nu_i = (n-i)\,\lambda, \qquad i = 0, \ldots, n-k, \tag{2.51}$$

   λ is the same for all states.

2. Active redundancy with *load sharing* $(\lambda = \lambda(i))$

   $$\nu_i = (n-i)\,\lambda(i), \qquad i = 0, \ldots, n-k, \tag{2.52}$$

   $\lambda(i)$ increases at each state change.

3. Warm (lightly loaded) redundancy $(\lambda_r < \lambda)$

   $$\nu_i = k\lambda + (n-k-i)\,\lambda_r, \qquad i = 0, \ldots, n-k, \tag{2.53}$$

   λ and λ_r are the same for all states.

4. Standby (cold) redundancy $(\lambda_r \equiv 0)$

   $$\nu_i = k\lambda, \qquad i = 0, \ldots, n-k, \tag{2.54}$$

   λ is the same for all states.

For a *standby redundancy, it is assumed* that the failure rate in the reserve state is $\equiv 0$ (the reserve elements are switched on when needed). *Warm redundancy* is somewhere between active and standby $(0 < \lambda_r < \lambda)$. It should be noted that the k-out-of-n active, warm, or standby redundancy is only the *simplest* representatives of the general concept of redundancy. Series - parallel structures, voting techniques, bridges, and more complex structures are frequently used (see Sections 2.2.6, 2.3.1 - 2.3.4, and 6.6 - 6.8 with repair rate $\mu = 0$, for some examples). Furthermore, redundancy can also appear in other forms, e.g. at software level, and the benefit of redundancy can be limited by the involved *failure modes* as well as by *control and switching elements* (see Section 6.8 for some examples).

For the analysis of the model shown in Fig. 2.12, let

$$\mathrm{P}_i(t) = \Pr\{\text{ the process is in state } Z_i \text{ at time } t\,\} \tag{2.55}$$

be the *state probabilities* $(i = 0, \ldots, n-k+1)$. $\mathrm{P}_i(t)$ is obtained by considering the process at two adjacent time points t and $t + \delta t$ and by making use of the *memoryless property* resulting from the *constant failure rate assumed between consecutive state changes* (Appendix A7.5). The function $\mathrm{P}_i(t)$ thus satisfies the following *difference equation*

$$\mathrm{P}_i(t+\delta t)=\mathrm{P}_i(t)(1-\nu_i\,\delta t)+\mathrm{P}_{i-1}(t)\,\nu_{i-1}\delta t+\mathrm{o}\delta t,\qquad i=1,\dots,n-k,\tag{2.56}$$

where $\mathrm{o}(\delta t)$ denotes a quantity having *an order higher than that of* δt. For $\delta t\to 0$, there follows then a system of differential equations describing the *death process*

$$\begin{aligned}&\dot{\mathrm{P}}_0(t)=-\nu_0\,\mathrm{P}_0(t)\\&\dot{\mathrm{P}}_i(t)=-\nu_i\,\mathrm{P}_i(t)+\nu_{i-1}\,\mathrm{P}_{i-1}(t),\qquad i=1,\dots,n-k,\\&\dot{\mathrm{P}}_{n-k+1}(t)=\nu_{n-k}\,\mathrm{P}_{n-k}(t).\end{aligned}\tag{2.57}$$

Assuming the initial conditions $\mathrm{P}_i(0)=1$ and $\mathrm{P}_j(0)=0$ for $j\neq i$ at $t=0$, the solution (generally obtained using the Laplace transform) leads to $\mathrm{P}_i(t)$, $i=0,\dots,n-k+1$. Knowing $\mathrm{P}_i(t)$, one can evaluate the *reliability function* $\mathrm{R}_S(t)$

$$\mathrm{R}_S(t)=\sum_{i=0}^{n-k}\mathrm{P}_i(t)=1-\mathrm{P}_{n-k+1}(t)\tag{2.58}$$

and the *mean time to failure* from Eq. (2.9). Assuming for instance $\mathrm{P}_0(0)=1$ as initial condition, one obtains for the Laplace transform of $\mathrm{R}_{S0}(t)$,

$$\tilde{\mathrm{R}}_{S0}(s)=\int_0^{\infty}\mathrm{R}_{S0}(t)\,e^{-s\,t}dt,\tag{2.59}$$

(using $\tilde{\mathrm{P}}_{n-k+1}(s)$ obtained recursively from Eq. (2.57)) the expression

$$\tilde{\mathrm{R}}_{S0}(s)=\frac{(s+\nu_0)\dots(s+\nu_{n-k})-\nu_0\dots\nu_{n-k}}{s(s+\nu_0)\dots(s+\nu_{n-k})}.\tag{2.60}$$

The *mean time to failure* follows then from

$$MTTF_{S0}=\tilde{\mathrm{R}}_{S0}(0)\tag{2.61}$$

and (using $dy/ds=y\cdot d(\ln y)/ds$ with $\mathrm{y}=(\mathrm{s}+\nu_0)\cdots(s+\nu_{n-k})$) leads to

$$MTTF_{S0}=\sum_{i=0}^{n-k}\frac{1}{\nu_i}.\tag{2.62}$$

Thereby, S stands for system and 0 specify the initial condition $\mathrm{P}_0(0)=1$ (Table 6.2).

For a k-out-of-n *standby redundancy* (Eq. (2.54)), it follows that

$$\mathrm{R}_{S0}(t)=\sum_{i=0}^{n-k}\frac{(k\lambda t)^i}{i!}e^{-k\lambda t}\tag{2.63}$$

and

$$MTTF_{S0}=\frac{n-k+1}{k\lambda}.\tag{2.64}$$

Equation (2.63) gives the probability for up to $n-k$ failures $(0,1,\dots,n-k)$ in $(0,t]$ by constant failure rate $k\lambda$, and shows the relation existing between the *Poisson distribution* and the occurrence of *exponentially* distributed events (Appendix A7.2.5).

For the case of a k-out-of-n *active redundancy* without load sharing, it follows from Eqs. (2.62) and (2.51) that

$$MTTF_{S0} = \frac{1}{\lambda}\left(\frac{1}{k} + \ldots + \frac{1}{n}\right), \tag{2.65}$$

see also Table 6.8 with $\mu = 0$, and $\lambda_r = \lambda$. Some examples for $\mathrm{R}_{S0}(t)$ with different values for n and k are given in Fig. 2.7.

2.3.6 Elements with more than one Failure Mechanism or one Failure Mode

In the previous sections, it was assumed that each element exhibits only one dominant *failure mechanism,* causing one dominant *failure mode*; for example intermetallic compound causing a short, or corrosion causing an open, for integrated circuits. However, in practical applications, components can have some failure mechanisms and fail in different manner (see e.g. Table 3.4). A simple way to consider more than one failure mechanism is to *assume* that each failure mechanism is *independent* of each other and causes a failure at item level. In this case, a *series model* can be used by assigning a failure rate to each failure mechanism, and Eq. 2.18 or Eq. 7.57 delivers the total failure rate of the item considered. More sophisticated models are possible. A mixture of failure rates and / or mechanisms has been discussed in Section 2.2.5 (Eq. (2.15)). This section will consider as an example the case of a diode exhibiting two failure modes. Let

$$\mathrm{R}(t) = \Pr\{\text{no failure in } (0, t] \mid \text{diode new at } t=0\}$$

$$\overline{\mathrm{R}}(t) = 1 - \mathrm{R}(t) = \Pr\{\text{failure in } (0, t] \mid \text{diode new at } t=0\}$$

$$\overline{\mathrm{R}}_U(t) = \Pr\{\text{open in } (0, t] \mid \text{diode new at } t=0\}$$

$$\overline{\mathrm{R}}_K(t) = \Pr\{\text{short in } (0, t] \mid \text{diode new at } t=0\}.$$

Obviously (Example 2.11)

$$1 - \mathrm{R}(t) = \overline{\mathrm{R}}(t) = \overline{\mathrm{R}}_U(t) + \overline{\mathrm{R}}_K(t). \tag{2.66}$$

The series connection of two diodes exhibits a circuit failure if either one open or two shorts occur. From this,

$$\overline{R}_S = 1-(1-\overline{R}_U)^2 + \overline{R}_K^2 = 2\,\overline{R}_U - \overline{R}_U^2 + \overline{R}_K^2, \tag{2.67}$$

with $R_S = \mathrm{R}_{S0}(t)$, $\overline{R}_K = \overline{\mathrm{R}}_K(t)$, $\overline{R}_U = \overline{\mathrm{R}}_U(t)$.

Example 2.11

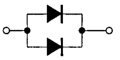
In an accelerated test of 1000 diodes, 100 failures occur, of which 30 are opens and 70 shorts. Give an estimate for $\overline{R}$, $\overline{R}_U$, and $\overline{R}_K$.

Solution

The maximum likelihood estimate of an unknown probability p is, according to Eq. (A8.29), $\hat{p} = k/n$. Hence, $\hat{\overline{R}} = 0.1$, $\hat{\overline{R}}_U = 0.03$, and $\hat{\overline{R}}_K = 0.07$.

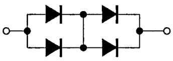
Similarly, for two diodes in parallel (Example 2.12),

$$\overline{R}_S = 2\overline{R}_K - \overline{R}_K^2 + \overline{R}_U^2. \qquad (2.68)$$



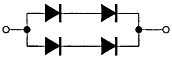
To be *simultaneously* protected against at *least one* failure of *arbitrary mode* (short or open), a *quad redundancy* is necessary. Depending upon whether opens or shorts are more frequent, a quad redundancy with or without a bridge connection is used. For both these cases it follows that

$$\overline{R}_S = 2\overline{R}_U^2 - \overline{R}_U^4 + (2\overline{R}_K - \overline{R}_K^2)^2, \qquad (2.69)$$



and

$$\overline{R}_S = 2\overline{R}_K^2 - \overline{R}_K^4 + (2\overline{R}_U - \overline{R}_U^2)^2. \qquad (2.70)$$



Equations (2.67) to (2.70) can be obtained using the *state space method* introduced in Section 2.3.3, however with *three states* for every element (good, open (U), and short (K) leading to a *state space* with 3^n elements in each line, see Example 2.12).

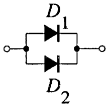
Example 2.12

Using the state space method, give the reliability of two parallel connected diodes, assuming that opens and shorts are possible.

Solution

Considering the three possible states (good (1), open (U), and short (K)), the state space for two parallel connected diodes is

D_1	1	1	1	U	U	U	K	K	K
D_2	1	U	K	1	U	K	1	U	K
S	1	1	0	1	0	0	0	0	0



From the above table, it follows that

$$\overline{R}_S = \Pr\{S=0\} = 2R\,\overline{R}_K + \overline{R}_U^2 + 2\overline{R}_U\,\overline{R}_K + \overline{R}_K^2$$

$$= 2(1 - \overline{R}_U - \overline{R}_K)\overline{R}_K + \overline{R}_U^2 + 2\overline{R}_U\,\overline{R}_K + \overline{R}_K^2 = 2\overline{R}_K - \overline{R}_K^2 + \overline{R}_U^2.$$

The linear superposition of the two failure modes, appearing in the final result for $\overline{R}_S$, do not apply necessarily to arbitrary structures.

2.3.7 Basic Considerations on Fault Tolerant Structures

In applications with *high* reliability, availability or safety requirements, equipment and systems must be *designed* to be *fault tolerant.* This means that without external help (autonomously) the item considered should be able to *recognize a fault* (failure or defect) and quickly *reconfigure* itself in such a way as to remain *safe* and possibly continue to operate with minimal performance loss (*fail-sale, graceful degradation*).

Methods to investigate *fault tolerant* items have been introduced in Sections 2.2.6.2 through 2.3.6, in particular Sections 2.2.6.5 (*majority redundancy*) and 2.3.6 (*quad redundancy*). The latter is one of the few structures which can support *at least one failure of any mode*, the price paid is four devices instead of one. Other possibilities are known to implement fault tolerance at component level, e. g. [2.41].

Repairable fault tolerant systems are considered carefully in Chapter 6, in particular in Section 6.8 for *non ideal reconfiguration* (imperfect switching, incomplete coverage, etc.). It is shown, that the stochastic processes introduced in Appendix A7 can be used to investigate reliability and availability of *fault tolerant systems* for cases in which a reliability block diagram does not exist as well.

To avoid *common cause* or *single-point failures*, redundant elements should be designed and produced *independently* from each other, in critical cases with different technology, tools, and personnel. Investigation of all possible *failure (fault) modes* during the design of fault tolerant equipment or systems is mandatory. This is generally done using *failure modes and effects analysis* (FMEA/FMECA), *fault tree analysis* (FTA), *causes-to-effects diagrams* or similar tools (Sections 2.6 & 6.9), supported by appropriate investigation models (see e.g. Examples 6.15 & 6.17). Failure modes analysis is essential where *redundancy* appears, among other to identify the parts which are in series to the ideal redundancy (in the reliability block diagram), to discover *interactions* between elements of the given item, and to find appropriate measures to avoid *failure propagation* (secondary failures).

Protection against *secondary failures* can be realized, at component level, with *decoupling elements* such as diodes, resistors, capacitors (diodes E_1 - E_4 in Example 2.3). Other possibilities are the introduction of *standby elements* which are activated at failure of active elements, the use of basically different technologies for redundant elements, etc. Quite generally, all parts which are essential for basic functions (e. g. interfaces and monitoring circuits) have to be designed with care. Adherence to appropriate *design guidelines* is important (Chapter 5). Recognition and localization of *hidden failures* as well as avoidance of *false alarms* (caused e. g. by *synchronization problems*) is mandatory. These and similar considerations applies in particular for equipment and systems with high reliability and/or safety requirements, as used e.g. in aerospace, automotive, and nuclear applications.

In digital systems, fault tolerance can often be obtained using error correction techniques (see e.g.[4.22] for an advanced application). Basic possibilities for redundancy in software are *N-version programming* and *N self configuring programming.*

2.4 Reliability Allocation

With complex equipment and systems, it is important to allocate reliability goals at subsystem and assembly levels early in the design phase. Such an allocation motivates the design engineer to consider reliability aspects at all system levels.

Allocation is simple if the item (system) has no redundancy and its components have constant failure rates. The system's failure rate λ_S is then constant and equal to the sum of the failure rates of its elements (Eq. (2.19)). In such a case, the allocation of λ_S can be done as follows:

1. Break down the system into elements $E_1, \ldots, E_n$.
2. Define a complexity factor k_i for each element ($0 \leq k_i \leq 1$, $k_1 + \ldots + k_n = 1$).
3. Determine the *duty cycle* d_i for each element (d_i = operating time of element E_i / operating time of the system).
4. Allocate the system's failure rate λ_S among elements $E_1, \ldots, E_n$ according to

$$\lambda_i = \lambda_S \, k_i \, / \, d_i \, , \qquad \lambda_S = \sum_i \lambda_i d_i . \tag{2.71}$$

Should all elements have the same complexity ($k_1 = \ldots = k_n = 1/n$) and the same duty cycle ($d_1 = \ldots = d_n = 1$), then

$$\lambda_i = \lambda_S \, / \, n . \tag{2.72}$$

In addition to the above, cost, technology risks, and failure effects should also be considered. A case-by-case *optimization* is often possible.

Should the individual element failure rates not be constant and/or the system contain redundancy, allocation of reliability goals is more difficult. Results of Sections 2.2 & 2.3 can support this effort. If *repairable* series - parallel structures appear, one can often assume that the failure rate at equipment or system level is fixed by the series elements (Section 6.6), for which Eqs. (2.71) and (2.72) can be used. For a deeper investigation, related also to *reliability optimization*, one may refer e. g. to [2.34, 2.47].

2.5 Mechanical Reliability, Drift Failures

As long as the reliability is considered to be the probability R for a mission success (without relation to the distribution of the failure-free time), the reliability *analysis procedure* for mechanical equipment or systems is similar to that used for electronic equipment or systems and is based on the following steps:

1. Definition of the system and of its associated mission profile.
2. Derivation of the corresponding reliability block diagram.

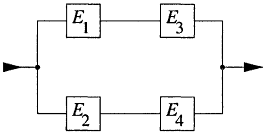
3. Determination of the reliability for each element of the reliability block diagram.
4. Calculation of the system reliability R_S (R_{S0} to point out system new at $t=0$).
5. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

Such a procedure is currently used in practical applications and is illustrated by Examples 2.13 and 2.14.

Example 2.13

The fastening of two mechanical parts should be easy and reliable. It is done by means of two flanges which are pressed together with 4 clamps E_1 to E_4 placed 90° to each other. Experience has shown that the fastening holds when at least 2 opposing clamps work. Set up the reliability block diagram for this fixation and compute its reliability (each clamp is news at $t=0$ and has reliability $R_1 = R_2 = R_3 = R_4 = R$).

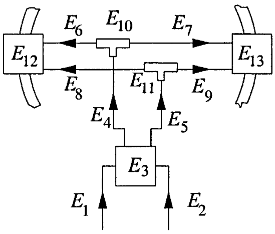
Solution



Since at least two opposing clamps (E_1 and E_3 or E_2 and E_4) have to function without failure, the reliability block diagram is obtained as the series connection of E_1 and E_3 in parallel with the series connection of E_2 and E_4, see graph on the right. Under the assumption that clamp is independent from every other one, the item reliability follows from $R_{S0} = 2R^2 - R^4$.

Supplementary result: If two arbitrary clamps were sufficient for the required function, a 2-out-of-4 active redundancy would apply yielding (Tab. 2.1) $R_{S0} = 6R^2 - 8R^3 + 3R^4$.

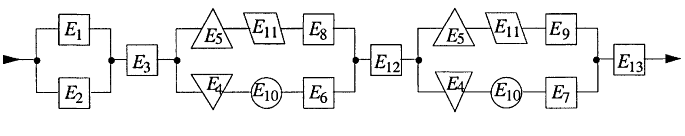
Example 2.14



To separate a satellite's protective shielding, a special electrical-pyrotechnic system described in the block diagram on the right is used. An electrical signal comes through the cables E_1 and E_2 (redundancy) to the electrical-pyrotechnic converter E_3 which lights the fuses. These carry the pyrotechnic signal to explosive charges for guillotining bolts E_{12} and E_{13} of the tensioning belt. The charges can be ignited from two sides, although one ignition will suffice (redundancy). For fulfillment of the required function, both bolts must be exploded simultaneously. Give the reliability of this separation system as a function of the reliability $R_1, \ldots, R_{13}$ of its elements (news at $t=0$).

Solution

The reliability block diagram is easily obtained by considering first the ignition of bolts E_{12} & E_{13} separately and then connecting these two parts of the reliability block diagram in series.



Elements E_4, E_5, E_{10}, and E_{11} each appear twice in the reliability block diagram. Repeated application of the *key item method* (successively on E_5, E_{11}, E_4, and E_{10}, see Section 2.3.1 and Example 2.9), by assuming that the elements $E_1, \ldots, E_{13}$ are independent, leads to

$$\begin{aligned} R_{S0} &= R_3 R_{12} R_{13} (R_1 + R_2 - R_1 R_2) \{ R_5 \langle R_{11} [R_4 \{ R_{10} (R_6 + R_8 - R_6 R_8)(R_7 + R_9 - R_7 R_9) \\ &\quad + (1 - R_{10}) R_8 R_9 \} + (1 - R4) R_8 R_9] + (1 - R_{11}) R_4 R_6 R_7 R_{10} \rangle + (1 - R_5) R_4 R_6 R_7 R_{10} \} \\ &= R_3 R_{12} R_{13} (R_1 + R_2 - R_1 R_2) \{ R_4 R_5 R_{10} R_{11} (R_6 + R_8 - R_6 R_8)(R_7 + R_9 - R_7 R_9) \\ &\quad + (1 - R_4 R_{10}) R_5 R_8 R_9 R_{11} + (1 - R_5 R_{11}) R_4 R_6 R_7 R_{10} \}. \end{aligned} \qquad (2.73)$$

More complicated is the situation when the reliability function $R(t)$ is required. For electronic components it is possible to operate with the failure rate, since models and data are often available. This is generally not the case for mechanical parts, although failure rate models for some parts and units (bearings, springs, couplings, valves, etc.) have been developed [2.26]. If no information about failure rates is available, a general approach based on the *stress-strength method*, often supported by *finite element analysis*, can be used. Let $\xi_L(t)$ be the *stress* (load) and $\xi_S(t)$ the *strength*, a failure occurs at the time t for which $|\xi_L(t)| > |\xi_S(t)|$ holds for the first time. Often, $\xi_L(t)$ and $\xi_S(t)$ can be considered as deterministic values and the ratio $\xi_S(t) / \xi_L(t)$ is the *safety factor*. In many practical applications, $\xi_L(t)$ and $\xi_S(t)$ are random variables, often stochastic processes. A practical oriented *procedure* for the reliability analysis of mechanical systems in these cases is:

1. Definition of the system and of its associated mission profile.
2. Formulation of *failure hypotheses* (buckling, bending, etc.) and validation of them using an FMEA / FMECA (Section 2.6); failure hypotheses are often correlated, this dependence must be identified and considered.
3. Evaluation of the stresses applied with respect to the critical failure hypotheses.
4. Evaluation of the strength limits by considering also dynamic stresses, notches, surface condition, etc.
5. Calculation of the system reliability (Eqs. (2.74) – (2.80)).
6. Elimination of reliability weaknesses and return to step 1 or 2, as necessary.

Reliability calculation often leads to one of the following situations:

1. One failure hypothesis, stress and strength are > 0: The *reliability function* is given by

$$R_{S0}(t) = \Pr\{\xi_S(x) > \xi_L(x), \quad 0 < x \le t\}, \qquad R_{S0}(0) = 1. \qquad (2.74)$$

2. More than one (n >1) failure hypothesis that can be correlated, stresses and strength are > 0: The *reliability function* is given by

$$\mathrm{R}_{S0}(t) = \Pr\{((\xi_{S_1}(x) > \xi_{L_1}(x)) \cap (\xi_{S_2}(x) > \xi_{L_2}(x)) \cap \ldots$$
$$\cap (\xi_{S_n}(x) > \xi_{L_n}(x)), \quad 0 < x \le t\}, \qquad \mathrm{R}_{S0}(0) = 1. \qquad (2.75)$$

Equation (2.75) can take a complicated form, according to the degree of dependence encountered.

The situation is easier when stress and strength can be assumed to be *independent and positive random variables*. In this case, $\Pr\{\xi_S > \xi_L \mid \xi_L = x\} = \Pr\{\xi_S > x\} = 1 - \mathrm{F}_S(x)$ and the theorem of total probability leads to

$$\mathrm{R}_{S0}(t) = R_{S0} = \Pr\{\xi_S > \xi_L\} = \int_0^{\infty} \mathrm{f}_L(x)(1 - \mathrm{F}_S(x))dx. \qquad (2.76)$$

Examples 2.15 and 2.16 illustrate the use of Eq. (2.76).

Example 2.15

Let the stress ξ_L of a mechanical joint be normally distributed with mean $m_L = 100\,\mathrm{N/mm^2}$ and standard deviation $\sigma_L = 40\,\mathrm{N/mm^2}$. The strength ξ_S is also normally distributed with mean $m_S = 150\,\mathrm{N/mm^2}$ and standard deviation $\sigma_S = 10\,\mathrm{N/mm^2}$. Compute the reliability of the joint.

Solution

Since ξ_L and ξ_S are normally distributed, their difference is also normally distributed (Example A.6.16). Their mean and standard deviation are $m_S - m_L = 50\,\mathrm{N/mm^2}$ and $\sqrt{\sigma_S^2 + \sigma_L^2} \approx 41\,\mathrm{N/mm^2}$, respectively. The reliability of the joint is then given by (Table A9.1)

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \Pr\{\xi_S - \xi_L > 0\} = \frac{1}{41\sqrt{2\pi}} \int_0^{\infty} e^{-\frac{(x-50)^2}{2 \cdot 41^2}} dx = \frac{1}{\sqrt{2\pi}} \int_{-50/41}^{\infty} e^{-y^2/2} dy \approx 0.89.$$

Example 2.16

Let the strength ξ_S of a rod be normally distributed with mean $m_S = 450\,\mathrm{N/mm^2} - 0.01\,t\,\mathrm{N/mm^2\,h^{-1}}$ and standard deviation $\sigma_S = 25\,\mathrm{N/mm^2} + 0.001\,t\,\mathrm{N/mm^2\,h^{-1}}$. The stress ξ_L is constant and equal $350\,\mathrm{N/mm^2}$. Calculate the reliability of the rod at $t = 0$ and $t = 10^4\,\mathrm{h}$.

Solution

At $t = 0$, $m_S = 450\,\mathrm{N/mm^2}$ and $\sigma_S = 25\,\mathrm{N/mm^2}$. Thus,

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \frac{1}{\sqrt{2\pi}} \int_{\frac{350-450}{25}}^{\infty} e^{-y^2/2} dy \approx 0.99997.$$

After 10,000 operating hours, $m_S = 350\,\mathrm{N/mm^2}$ and $\sigma_S = 35\,\mathrm{N/mm^2}$. The reliability is then

$$R_{S0} = \Pr\{\xi_S > \xi_L\} = \frac{1}{\sqrt{2\pi}} \int_{\frac{350-350}{35}}^{\infty} e^{-y^2/2} dy = \frac{1}{\sqrt{2\pi}} \int_0^{\infty} e^{-y^2/2} dy = 0.5.$$

Equation (2.76) holds for a one-item structure. For a series model, i.e., in particular for the *series* connection of two independent elements one obtains:

1. Same stress $\xi_L \quad (\xi_L, \xi_{S_i} > 0)$

$$R_{S0} = \Pr\{\xi_{S_1} > \xi_L \cap \xi_{S_2} > \xi_L\} = \int_0^{\infty} \mathrm{f}_L(x)(1 - \mathrm{F}_{S_1}(x))(1 - \mathrm{F}_{S_2}(x))dx. \tag{2.77}$$

2. Independent stresses ξ_{L_1} and $\xi_{L_2} \quad (\xi_{L_i}, \xi_{S_i} > 0)$

$$\begin{aligned} R_{S0} &= \Pr\{\xi_{S_1} > \xi_{L_1} \cap \xi_{S_2} > \xi_{L_2}\} = \Pr\{\xi_{S_1} > \xi_{L_1}\}\Pr\{\xi_{S_2} > \xi_{L_2}\} \\ &= (\int_0^{\infty} \mathrm{f}_{L_1}(x)(1 - \mathrm{F}_{S_1}(x))dx)(\int_0^{\infty} \mathrm{f}_{L_2}(x)(1 - \mathrm{F}_{S_2}(x))dx) \hat{=} R_1 R_2. \end{aligned} \tag{2.78}$$

For a parallel model, i.e., in particular for the *parallel* connection of two non repairable independent elements it follows that:

1. Same stress $\xi_L \quad (\xi_L, \xi_{S_i} > 0)$

$$R_{S0} = 1 - \Pr\{\xi_{S_1} \le \xi_L \cap \xi_{S_2} \le \xi_L\} = 1 - \int_0^{\infty} \mathrm{f}_L(x)\mathrm{F}_{S_1}(x)\mathrm{F}_{S_2}(x)dx. \tag{2.79}$$

2. Independent stresses ξ_{L_1} and $\xi_{L_2} \quad (\xi_{L_i}, \xi_{S_i} > 0)$

$$R_{S0} = 1 - \Pr\{\xi_{S_1} \le \xi_{L_1}\}\Pr\{\xi_{S_2} \le \xi_{L_2}\} \hat{=} 1-(1-R_1)(1-R_2) = R_1 + R_2 - R_1 R_2. \tag{2.80}$$

As with Eqs. (2.78) and (2.80), the results of Table 2.1 can be applied in the case of *independent* stresses and elements. However, this *ideal situation* is seldom true for mechanical systems, for which Eqs. (2.77) and (2.79) are often more realistic. Moreover, the *uncertainty* about the *exact form* of the distributions for stress and strength far from the mean value, *severely reduce the accuracy* of the results obtained from the above equations in practical applications. For mechanical items, *tests* are thus often the only way to evaluate their reliability. Investigations into new methods are in progress, paying particular attention to the *dependence between stresses* and to a *realistic truncation* of the stress and strength densities (Eq. (A6.33)). Other approaches are possible for mechanical systems, see e. g. [2.61-2.77].

For electronic items, Eqs. (2.76) and (2.77) - (2.80) can often be used to investigate *drift failures*. Quite generally, all considerations of Section 2.5 could be applied to electronic items. However, the method based on the failure rate, introduced in Section 2.2, is easier to be used and works reasonably well in many practical applications dealing with electronic and electromechanical equipment and systems.

2.6 Failure Modes Analysis

Failure rate analysis (Sections 2.1-2.5) basically do not account for the *mode* and *effect* (consequence) of a failure. *To understand the mechanism of system failures and in order to identify potential weaknesses of a fail-safe concept it is necessary to perform a failure mode analysis, at least where redundancy appears and for critical parts of the item considered.* Such an analysis is termed FMEA (Failure Modes and Effects Analysis) or alternatively FMECA (Failure Modes, Effects, and Criticality Analysis) if also the *failure severity* is of interest (*modes* should be preferred to *mode*). If failures and defects have to be considered, *Fault* is used instead of *Failure*. An FMEA/FMECA consists of the systematic analysis of failure (fault) *modes*, their *causes*, *effects*, and *criticality* [2.81, 2.83, 2.84, 2.87 - 2.93, 2.96 - 2.98], including *common-mode & common-cause* failures as well. All possible failure (fault) modes (for the item considered), their causes and consequences are systematically investigated, in one run or in several steps (design FMEA/FMECA, process FMEA/FMECA). For critical cases, possibilities to avoid the failure (fault) or to minimize (mitigate) its consequence must be analyzed and corresponding corrective (or preventive) actions *have to be realized.* The criticality describes the severity of the consequence of the failure (fault) and is designated by categories or levels which are function of the risk for damage or loss of performance. Considerations on failure modes for electronic components are in Tables 3.4 & A10.1 and Section 3.3.

The FMEA/FMECA is a *bottom-up* (inductive) procedure, performed preferably as a team work with designer and reliability engineers. The procedure is established in *international standards* [2.89]. It is easy to understand but can become time-consuming for complex equipment and systems. For this reason *it is recommended to concentrate efforts to critical parts*, in particular where redundancy appears. Table 2.5 shows the procedure for an FMEA/FMECA. Basic are steps 3 to 8. Table 2.6 gives an example of a detailed FMECA for the switch in Example 2.6, Point 7. Each row of Tab. 2.5 is a column in Tab. 2.6. Other worksheet forms are possible, see e.g. [2.83, 2.84, 2.89]. An FMEA/FMECA is *mandatory* for items with *fail-safe behavior* and where *redundancy* appears (to verify the effectiveness of the redundancy when failure occurs and to define the element *in series* on the reliability block diagram), as well as for failures which can cause a safety problem (liability claim). An FMEA/FMECA is also useful to support maintainability analyses.

For a visualization of the item's criticality, the FMECA is often completed by a *criticality grid* (*criticality matrix*), see e. g. [2.89]. In such a matrix, each failure mode give an entry (dot or other) with criticality category as ordinate and corresponding probability (frequency) of occurrence as abscissa (Fig. 2.13). Generally accepted classifications are *minor* (I), *major* (II), *critical* (III), and *catastrophic* (IV) for the criticality level and *very low*, *low*, *medium* and *high* for the probability of occurrence. In a criticality grid, the further an entry is far from the origin, the greater is the necessity for a corrective/preventive action.

Table 2.5 Basic procedure +) for performing an FMECA (according also to *IEC 60812* [2.89]) ++)

1. Sequential numbering of the step.
2. Designation of the element or part under consideration, short description of its function, and reference to the reliability block diagram, part list, etc. (3 steps in *IEC 60812*)
3. Assumption of a possible fault mode +++) (all possible fault modes have to be considered).
4. Identification of possible causes for the fault mode assumed in step 3 (a cause for a fault can also be a flaw in the design phase, production phase, transportation, installation or use).
5. Description of the symptoms which will characterize the fault mode assumed in step 3 and of its local effect (output/input relationships, possibilities for secondary failures or faults, etc.).
6. Identification of the consequences of the fault mode assumed in step 3 on the next higher integration levels (up to the system level) and on the mission to be performed.
7. Identification of fault detection provisions and of corrective actions which can mitigate the severity of the fault mode assumed in step 3, reduce the probability of occurrence, or initiate an alternate operational mode which allows continued operation when the fault occurs.
8. Identification of possibilities to avoid the fault+++) mode assumed in step 3, and *realization* of corresponding corrective (or preventive) actions.
9. Evaluation of the severity of the fault mode assumed in step 3 (FMECA only); e.g. I for minor, II for major, III for critical, IV for catastrophic (or alternatively, 1 for failure to complete a task, 2 for large economic loss, 3 for large material damage, 4 for loss of human life).
10. Estimation of the probability of occurrence (or failure rate) of the fault mode assumed in step 3 (FMECA only), with consideration of the cause of fault identified in step 4).
11. Formulation of pertinent remarks which complete the information in the previous columns and also of recommendations for corrective actions, which will reduce the consequences of the fault mode assumed in step 3.

+) Steps are columns in Tab. 2.6. ++) FMEA by omitting steps 9 & 10. +++) *Fault* includes *failure & defect.*

The procedure for the FMEA/FMECA has been developed for *hardware*, but can also be used for *software* as well [2.87, 2.88, 5.95, 5.99]. For mechanical items, the FMEA/FMECA is an essential tool in reliability analysis (Section 2.5).

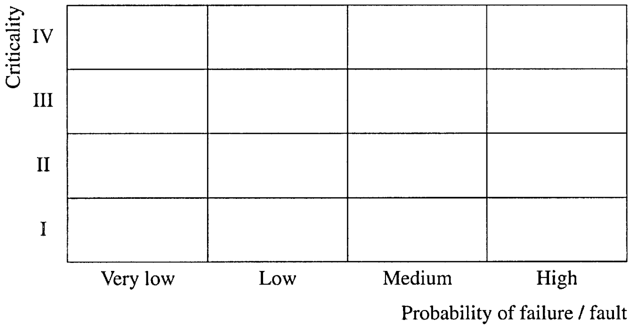


Figure 2.13 Example of criticality grid for an FMECA (according to *IEC 60812* [2.89])

Table 2.6 Example of a detailed FMECA for elements E_1 – E_7 in Point 7 of Example 2.6 (p. 51)

FAILURE (FAULT) MODES AND EFFECTS ANALYSIS / FAILURE (FAULT) MODES, EFFECTS, AND CRITICALITY ANALYSIS

Equipment: *control cabinet XYZ*
Item: *LED display circuit*
Prepared by: *A. Birolini* **Date:** rev. *Sept. 13, 2000*

FMEA / FMECA

Mission / required function: *fault signaling*
State: *operating phase* **Page:** *1&2*

(1) *No.*	*(2)* *Element, Function, Position*	*(3)* *Assumed fault mode*	*(4)* *Possible causes*	*(5)* *Symptoms, local effects*	*(6)* *Effect on mission*	*(7)* *Fault detection possibilities*	*(8)* *Possibilities to avoid the fault mode in (3)*	*(9)* *Se-verity*	*(10)* *Probability of occurrence*	*(11)* *Remarks and suggestions*
1.	TR_1, NPN Si transistor in plastic - package (E_4)	Short BCE, CE	Bad solder joint	Redundancy failed; $U_{CE} = 0$; no consequence to other elements	practically no consequence	$U_{CE}=0$, $U_{RC}>0$	——	1	$p = 10^{-5}$	a) λ for $\theta_A = 50°C$ and G_B b) it is possible to notify the failure of TR_1 (Level detector)
			Inherent failure						$\lambda = 1.8 \ 10^{-9} \ h^{-1}$	
		Short BC	Bad solder joint	LED lights dimly; disappears by bridging CE; no consequence to other elements	Partial failure	$U_{BC}=0$, $U_{RC}>0$	Use a transistor of better quality; impr. handling, assembly, and soldering proc.	2	$p = 10^{-5}$	
			Inherent failure						$\lambda = 0.3 \ 10^{-9} \ h^{-1}$	
		Short BE	Bad solder joint	Circuit faulty; disappears by bridging CE; no consequence to other elements	Complete (possibly partial) failure	$U_{BE}=0$, $U_{RB1}>0$		3	$p = 10^{-5}$	
			Inherent failure						$\lambda = 0.3 \ 10^{-9} \ h^{-1}$	
		Open	Wrong connection, cold solder joint			$U_C=V_{CC}$, $U_B=U_1$		3	$p = 10^{-4}$	
			Inherent failure						$\lambda = 0.6 \ 10^{-9} \ h^{-1}$	
		Intermit-tent failure	Damage, cold solder joint	Circuit works intermittently; no consequence to other elements	Partial to complete failure	——	Improve handling, assembly & soldering procedures	2 to 3	$p = 10^{-4}$	
		Drift	Damage	The circuit works correctly even with large parameter deviations; no consequence to other elements	Practically no consequence	——	Improve handling	1 to 2	$p = 10^{-4}$	
			Wearout				——		$\lambda = 0.1 \ 10^{-9} \ h^{-1}$	
2.	LED (E_1)	Open	Wrong connection, damage, cold solder joint	LED does not light; no consequence to other elements	Complete failure	$U_{RB1}>0$, $U_{LED} \approx V_{CC}$	Improve handling, assembly & soldering procedures	3	$p = 10^{-3}$	a) λ for $\theta_A = 30°C$ and G_B b) be careful when forming the leads c) Observe the max. soldering time; distance between package and board > 2 mm d) pay attention to the cleaning medium e) hermet. package
			Inherent failure				Reduce θ_A		$\lambda = 0.8 \ 10^{-9} \ h^{-1}$	
		Short	Bad solder joint	LED does not light; no consequence to other elements	Complete failure	$U_{LED}=0$, $U_{RC}>0$	Improve soldering procedure	3	$p = 10^{-5}$	
			Inherent failure				Reduce θ_A		$\lambda = 0.3 \ 10^{-9} \ h^{-1}$	
		Intermit-tent failure	Damage, cold solder joint	LED lights intermittently; no consequence to other elements	Partial to complete failure	——	Improve handling, assembly & soldering procedures	2 to 3	$p = 10^{-4}$	
		Drift	Damage	LED lights dimly; no consequence to other elements	Partial failure	——	Improve handling	2	$p = 10^{-4}$	
			Wearout				Reduce θ_A		$\lambda = 0.2 \ 10^{-9} \ h^{-1}$	
			Corrosion				Prot. against humid.		$\lambda \approx 0$	

Table 2.6 (cont.)

3.	R_C,Film resistor to limit the collector current (E_2)	Open	Damage, cold solder joint	Circuit faulty, works again by bridging R_C with an equivalent resistor; no consequence to other elements	Complete failure	$U_{B1} > 0$, $U_{RC} \approx V_{CC}$	Improve handling, assembly & soldering procedures	3	$p = 10^{-4}$	a) λ for $\theta_A = 50°C$ and G_B b) a short on R_C can produce a short on V_{CC}
			Inherent failure				Use composition resistors(if possible)		$\lambda = 0.3\ 10^{-9}\ h^{-1}$	
		Short	Inherent failure	Circuit faulty; LED lights very brightly; secondary failure of LED and/or TR_1 and/or TR_2	Complete failure	$U_{RC}=0$, $U_{LED} \approx V_{CC}$	Put 2 resistors in series (R_{B1} / 2)	3	$\lambda \approx 0$	
		Intermittent failure	Damage, cold solder joint	Circuit works intermittently; no consequence to other elements	Partial to complete failure	——	Improve handling, assembly & soldering procedures	2 to 3	$p = 10^{-4}$	
		Drift	Damage	The circuit works correctly even with large parameter deviations; no consequence to other elements	Practically no consequence	——	Improve handling	1	$p = 10^{-6}$	
			Wearout				——		$\lambda \approx 0$	
4.	R_{B1},Film resistor to limit the base current (E_3)	Open	Damage, cold solder joint	Circuit faulty, works again by bridging R_{B1} with an equivalent resistor; no consequence to other elements	Complete failure	$U_C=V_{CC}$, $U_{RB2} > 0$	Improve handling, assembly & soldering procedures	3	$p = 10^{-4}$	a) λ for $\theta_A = 50°C$ and G_B b) a short on R_{B1} can produce a failure of TR_1
			Inherent failure				Use composition resistor (if possible)		$\lambda = 0.3\ 10^{-9}\ h^{-1}$	
		Short	Inherent failure	Partial failure; TR_1 can fail because of a too high base current	Partial failure	$U_{RB1}=0$, $U_{RC} > 0$	Put 2 resistors in series (R_{B1} / 2)	2	$\lambda \approx 0$	
		Intermittent failure	Damage, cold solder joint	Circuit works intermittently; no consequence to other elements	Partial to complete failure	——	Improve handling, assembly & soldering procedures	2 to 3	$p = 10^{-4}$	
		Drift	Damage	The circuit works correctly even with large parameter deviations; no consequence to other elements	Practically no consequence	——	Improve handling	1	$p = 10^{-6}$	
			Wearout				——		$\lambda \approx 0$	
5.	R_{B2} (E_6)	see Point 4								
6.	TR_2 (E_7)	see Point 1								
7.	PCB and solder joints (E_5)	see Points 1 to 4								

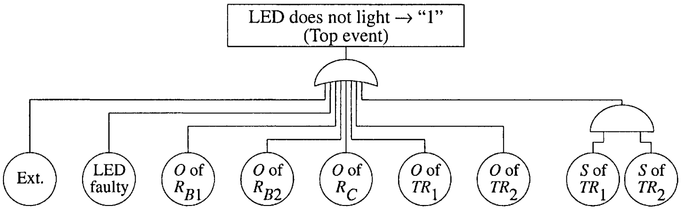


Figure 2.14 Example of *fault tree* (FT) for the electronic switch given in Example 2.6, Point 7, p.51 (O = open, S = short, Ext. are possible external causes, such as power out, manufacturing error, etc.); as in use for FTA, "0" holds for operating and "1" for failure (Section 6.9.2)

A further possibility to investigate failure-causes-to-effects relationships is the *Fault Tree Analysis* (FTA) [A2.5 (IEC 61025)]. The FTA is a *top-down* (deductive) procedure in which the undesired event, for example a critical failure at system level, is represented (for coherent systems) essentially by AND and OR combinations of causes at lower levels. It is a current rule in FTA [A2.5 (IEC 61025)] to use "0" for operating and "1" for failure (the top event "1" being in general a failure). Some examples for *fault trees* (FT) are in Figs. 2.14, 6.40, 6.41. In a fault tree, a *cut set* is a set of basic events whose occurrence (of all) causes the *top event* to occur. *Minimal cut sets*, defined as per Eq. (2.43) can be identified. Algorithms have been developed to obtain from a *fault tree* the *minimal cut sets* (and *minimal path sets*) belonging to the system considered, see e.g. [2.33]. From a complete and correct fault tree it is possible to compute the reliability for the nonrepairable case and the point availability for the repairable case, when *active redundancy* and *totally independent elements* can be assumed (Eqs. (2.45) & (2.48), Section 6.9.1). To consider some dependencies, *dynamic gates* have been introduced (Section 6.9.2). For computation purposes, *binary decision diagrams* have been developed (Sections 6.9.3).

Compared to FMEA/FMECA, FTA can take *external influences* (human and/or environmental) better into account, and handle situations where *more than one primary fault* (multiple faults) has to occur in order to cause the undesired event at system level. However, it does not necessarily go through all possible *fault modes*. Combination of FMEA/FMECA and FTA can provide better assurance for completeness of analysis. However, for consistency checks, FMEA/FMECA and FTA should be performed separately and independently. FMEA/ FMECA and FTA can also be combined with *Event Tree Analysis* (Section 6.9.4), leading to *causes-to-effects charts* and showing relationship between causes and their single or *multiple consequences* as well as efficacy of mitigating factors.

Further methods / tools which can support *causes-to-effects analyses* are *sneak analysis* (circuit, path, timing), *worst-case analysis, drift analysis*, *stress-strength analysis*, *Ishikawa diagrams*, *Kepner-Tregoe method*, *Shewhart cycles* (Plan-Analyze-Check-Do), and *Pareto diagrams*, see e.g. [1.22, 2.13, A2.5 (IEC 60300-3-1)].

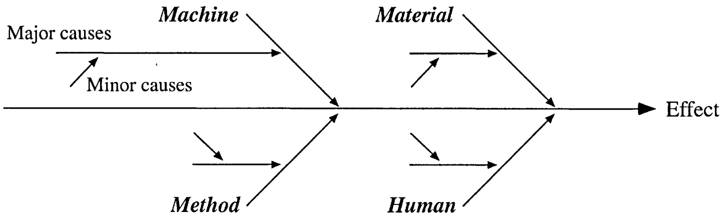


Figure 2.15 Typical structure of a cause and effect (Ishikawa or fishbone) diagram (causes can often be grouped into *Machine*, *Material*, *Method*, and *Human (Man)*, into *failure mechanisms*, or into a combination of all them, as appropriate)

Table 2.7 gives a comparison of important tools used for *causes-to-effects analyses*. Figure 2.15 shows the basic structure of an Ishikawa (fishbone) diagram. The Ishikawa diagram is a graphical visualization of the relationships between *causes and effect*, grouping the causes into *machine*, *material*, *method*, and *human* (*man*), into *failure mechanisms*, or into a combination of all them, as appropriate.

Performing an FMEA /FMECA, FTA, or any other similar investigation presupposes a *detailed* technical knowledge and *thorough understanding* of the item and the technologies considered. This is necessary to *identify all relevant* potential flaws (during design, development, manufacture, operation), their causes, and the more appropriate *corrective or preventive actions*.

2.7 Reliability Aspects in Design Reviews

Design reviews are important to point out, discuss, and eliminate *design weaknesses*. Their objective is also to *decide about continuation or stopping* of the project on the basis of objective considerations (*feasibility checks* in Fig. 1.6 and in Tables A3.3 and 5.3). The most important design reviews are described in Table A3.3 for hardware an in Table 5.5 for software. To be effective, design reviews must be supported by *project specific checklists*. Table 2.8 gives an example of catalog of questions which can be used to generate project specific checklists for reliability aspects in design reviews (see Table 4.3 for maintainability and Appendix A4 for other aspects). As shown in Table 2.8, checking the reliability aspects during a design review is more than just verifying the value of the predicted reliability or the source used for failure rate calculation. The purpose of a design review is in particular to discuss selection and use of components and materials, adherence to given *design guidelines*, presence of *potential reliability weaknesses*, and results of *analysis and tests*. Tables 2.8 and 2.9 can be used to support this aim.

Table 2.7 Important tools for causes-to-effects-analysis (see also [A2.5 (IEC 60300-3-1)] and Sections 6.92 - 6.9.4)

Tool	Description	Application	Effort
FMEA / FMECA (Fault Modes Effects Analysis / Fault Modes, Effects and Criticality Analysis) +)	Systematic *bottom-up* investigation of the effects (consequences) at system (item) level of the *fault modes* of all parts of the system considered, as well as of manufacturing flaws and (as far as possible) of user's errors / mistakes +)	Development phase (design FMEA/FMECA) and production phase (process FMEA / FMECA); mandatory for all interfaces, in particular where *redundancy* appears and for *safety* relevant parts	Very large if performed for all elements (0.1 MM for a PCB)
FTA (Fault Tree Analysis)	Quasi-systematic *top-down* investigation of the effects (consequences) of faults (failures and defects) as well as of external influences on the reliability and / or safety of the system (item) considered; the top event (e. g. a specific catastrophic failure) is the result of AND & OR combinations of elementary events	Similar to FMEA / FMECA; however, combination of more than one fault (or elementary event) can be better considered as by an FMEA / FMECA; also is the influence of *external events* (natural catastrophe, sabotage etc.) easier to be considered	Large to very large, if many top events are considered
Ishikawa Diagram (Fishbone Diagram)	Graphical representation of the causes-to-effects relationships; the causes are often grouped in four classes: machine, material, method / process, and human (man) dependent	Ideal for team-work discussions, in particular for the investigation of design, development, or production weaknesses	Small to large
Kepner-Tregoe Method	Structured problem detection, analysis, and solution by complex situations; the main steps of the method deal with a careful problem analysis, decision making, and solution weighting	Generally applicable, in particular by complex situations and in interdisciplinary work-groups	Largely dependent on the specific situation
Pareto Diagram	Graphical presentation of the frequency (histogram) and (cumulative) distribution of the problem causes, grouped in application specific classes	Supports the objective decision making in selecting the causes of a fault and thus in defining the appropriate corrective action (*Pareto rule*: 80% of the problems are generated by 20% of the possible causes)	Small
Correlation Diagram	Graphical representation of (two) quantities with possible functional (deterministic or stochastic) relation on an appropriate x/y-Cartesian coordinate system	Assessment of a relationship between two quantities	Small

+) *Faults* include *failures* and *defects*, allowing *errors* as possible causes as well; MM stays for man month

Table 2.8 Example of a catalog of questions for the *preparation of project specific* checklists for the evaluation of reliability aspects in preliminary design reviews (Appendices A3 and A4) of complex equipment and systems with high reliability requirements

1. Is it a new development, redesign, or change / modification?
2. Is there test or field data available from similar items? What were the problems?
3. Has a list of preferred components been prepared and consequently used?
4. Is the selection/qualification of nonstandard components and material specified? How?
5. Have the interactions among elements been minimized? Can interface problems be expected?
6. Have all the specification requirements of the item been fulfilled? Can individual requirements be reduced?
7. Has the mission profile been defined? How has it been considered in the analysis?
8. Has a reliability block diagram been prepared?
9. Have the environmental conditions for the item been clearly defined? How are the operating conditions for each element?
10. Have derating rules been appropriately applied?
11. Has the junction temperature of all semiconductor devices been kept lower than 100°C?
12. Have drift, worst-case, and sneak path analyses been performed? What are the results?
13. Has the influence of on-off switching and of external interference (EMC) been considered?
14. Is it necessary to improve the reliability by introducing redundancy?
15. Has an FMEA / FMECA been performed, at least for the parts where redundancy appears? How? Are single-point failures present? Can nothing be done against them? Are there safety problems? Can liability problems be expected?
16. Does the predicted reliability of each element correspond to its allocated value? With which π-factors it has been calculated?
17. Has the predicted reliability of the whole item been calculated? Does this value correspond to the target given in the item's specifications?
18. Are there elements with a limited useful life?
19. Are there components which require screening? Assemblies which require environmental stress screening (ESS)?
20. Can design or construction be further simplified?
21. Is failure detection, localization, and removal easy?

22 Are hidden failures possible?

23. Have reliability tests been planned? What does this test program include?
24. Have the aspects of manufacturability, testability, and reproducibility been considered?
25. Have the supply problems (second source, long-term deliveries, obsolescence) been solved?

Table 2.9 Example of form sheets for detecting and investigating potential *reliability weaknesses* at assembly and equipment level

a) Assembly design

Position	Component	Failure rate λ		Deviation from reliability design guidelines	Component selection and qualification	Problems during design, develop., manufact., test, use	El. test and screening
		Parameters	λ (FITs)				

b) Assembly manufacturing

Item	Layout	Placing	Soldering	Cleaning	El. tests	Screening	Fault (defect, failure) analysis	Corrective actions	Transportation and storage

c) Prototype qualification tests

Item	Electrical tests	Environmental tests	Reliability tests	Fault (defect, failure) analysis	Corrective actions

d) Equipment or system level

Assembling	Test	Screening (ESS)	Fault (defect, failure) analysis	Corrective actions	Transportation and storage	Operation (field data)