Calculations for Functional Safety
Quantities, Formulas and Methods

Thomas Brunnengräber
tbrunnengraeber@thomas-brunnengraeber.de

29 November 2025

Contents

Foreword and Motivation

Whereas in the past, functional safety hardly played a role in many industries, and in the others was essentially ensured by detailed design rules, driven by (negative) experiences [1], today the trend is moving away from fixed design rules to quantitative requirements and evidence. This undoubtedly promotes innovation and competition, but it also carries the risk of unsafe systems entering the market.

The practice of the author as an assessor for functional safety shows again and again, that even experienced safety engineers find it difficult to perform correct calculations. This is often caused by a lack of understanding of the different variables, but just as often it is also due to a lack of knowledge about the calculation tools and methods used (especially FTA tools), coupled with an unjustifiably high level of trust in them.

This introduction is primarily intended for prospective and experienced safety engineers, but also to mathematicians or computer scientists, who are entrusted with the development of calculation tools. Reference is occasionally made to standards, however, knowledge of these standards is not presumed.

Preface

In the following, the term system is used, because this is common in this context. In fact, however, the term function would often be more correct, since a failure and thus all calculations generally refer to a function, which is to be executed by a technical system. The term system is meaningless without naming the considered (failure) function, because a system will usually execute several functions, which will have different failure behavior due to the generally different components involved, and whose different malfunctions will generally have different consequences. The (imprecise) term system is also used in the following, to avoid confusion with mathematical functions and thus make it easier to read.

In the field of reliability calculation usually the scientific notation of numerical values is used, for example 0.0123=1.23e-2=1.23E-2 or 1000=1E3=1.0E3 (whereas 1.0·10E3=10E3 is actually 1E4=10000 – and not 1000, as often assumed!).

Understanding sections 2 and 4 is a prerequisite for all other sections, they should therefore be read before taking a closer look at the examples given in sections 5 and 6. Those who are only interested in fault trees, can skip the sections on Markov modeling.

[1] a former colleague used to say: "safety was paid for in blood"

1 Introduction

For all types of technical systems, which can cause damage in case of malfunction safety must be demonstrated before they can be put into operation or placed on the market. Examples are machine tools, robots, road or rail vehicles, aircraft or power plants. For these systems, safety can be expressed in terms of hazard rates, failure rates, or generally occurrence rates for specific undesired events, which must be calculated by safety engineers.

In addition, there is another class of technical systems, for which safety must be demonstrated: Systems that are designed to protect against harm in the event of a hazard. Examples are fire detectors, emergency call systems, emergency relief valves or emergency pumps. These systems cannot cause any damage themselves, however, a malfunction in the event of a demand can increase the damage or make it possible in the first place. Safety of these systems is determined by their availability, which must meet a minimum level.

In this introduction, all quantities relevant for the description of safety are named and explained, and the mathematical relationships are explained. In particular, maintainable (or repairable) components and systems are considered intensively. Methods of calculation are also presented, especially fault tree analysis and Markov modeling. The mathematical background is also discussed, which, in the author's opinion, is essential for correct modeling.

2 Reliability and related variables

2.1 Reliability and unreliability

Reliability $R(t_1, t_2)$ is the probability, that a component/system/function does not fail in the time interval t_1 to t_2, regardless of whether it was working at time t_1.

Unreliability $F(t_1, t_2)$ is the probability, that a component/system/function fails in the time interval t_1 to t_2, regardless of whether it was working at time t_1. Consequently, it is the complementary probability (or converse probability) to the reliability:

$$F(t_1, t_2) = 1 - R(t_1, t_2) \quad \text{or} \quad R(t_1, t_2) = 1 - F(t_1, t_2) \tag{1}$$

For practically all questions one chooses $t_1 = 0$ and thus obtains the one-parameter functions $R(t_1 = 0, t_2 = t) = R(t)$ and $F(t_1 = 0, t_2 = t) = F(t)$. For the relationship between reliability and unreliability, the following applies accordingly:

$$F(t) = 1 - R(t) \quad \text{or} \quad R(t) = 1 - F(t) \tag{2}$$

$F(t)$ is sometimes also referred to as the probability of survival.

Note: Unreliability is often called probability of failure. However, unavailability is also often called probability of failure, although it is a completely different quantity. To avoid misunderstandings, the term "probability of failure" should not be used, therefore.

Note: Especially for vehicles, one sometimes relates reliability and also subsequent quantities to the distance s traveled. $F(t_1, t_2)$ then becomes $F(s_1, s_2)$ etc. In all formulas given, the time must then be replaced by the distance.

Example 2.1 *Let the probability p be asked, that a component with age t will fail within the next hour. It should not be assumed that it is still working at time t:*

$$p = F(t, t + 1\,\text{h}) = F(t + 1\,\text{h}) - F(t)$$

Example 2.2 *Let the probability p be asked, that a component with age t, which is still working at time t will fail within the next hour:*

$$p = \frac{F(t, t + 1\,\text{h})}{R(t)} = \frac{F(t + 1\,\text{h}) - F(t)}{R(t)} = \frac{R(t) - R(t + 1\,\text{h})}{R(t)}$$

Example 2.3 *It is known from many years of experience, that the reliability and unreliability follows the (cumulative) distribution functions shown in Figure 1.*

Question 1: What is the probability that the component will work for more than 40.000 hours?

Answer: $p = R(40\,000\,\text{h}) \approx 0.2$. Consequently, the component will work longer than 40000 hours with 20% probability.

Question 2: What is the probability, that the component will fail between 40000 and 50000 operating hours?

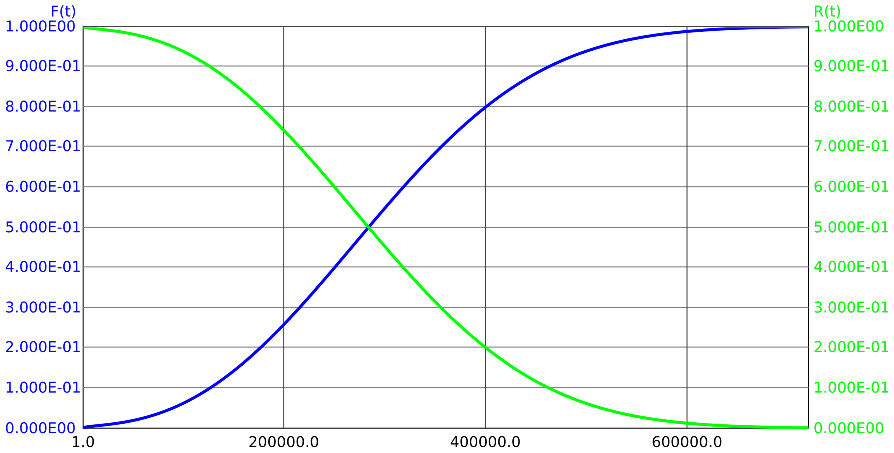


Figure 1: *Example reliability and unreliability function*

Answer: $p = F(50\,000\,\mathrm{h}) - F(40\,000\,\mathrm{h}) = R(40\,000\,\mathrm{h}) - R(50\,000\,\mathrm{h}) \approx 0.15$. *So the component will fail with 15% probability after 40000 to 50000 hours.*

Question 3: What is the probability that the component will fail between 40000 and 50000 hours of operation, if it was still working at 40000 hours?

Answer: $p = \dfrac{F(50\,000\,\mathrm{h}) - F(40\,000\,\mathrm{h})}{R(40\,000\,\mathrm{h})} \approx \dfrac{0.15}{0.2} = 0.75$.

2.2 Failure density and failure rate

The change in unreliability per time is the failure density. For any failure density function $f(t)$ holds:

$$F(t) = \int\limits_0^t f(\tau)\, d\tau \quad \text{or} \quad f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{3}$$

Unlike unreliability, failure density is not a probability. It can take any positive value and has a dimension (usually 1/time or 1/distance).

Since the unreliability for $t \to \infty$ approaches 1, the following must hold for any density function:

$$\int\limits_0^\infty f(\tau)\, d\tau = 1 \tag{4}$$

The failure rate $h(t)$ for arbitrary failure density functions is given as

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \tag{5}$$

With $f(t) = -\frac{dR(t)}{dt}$ we get:

$$h(t) = \frac{f(t)}{R(t)} = \frac{-dR(t)/dt}{R(t)} = -\frac{\dot{R}}{R} \tag{6}$$

$$R(t) = \mathrm{e}^{-\int\limits_0^t h(\tau)\,d\tau} \tag{7}$$

$$F(t) = 1 - \mathrm{e}^{-\int\limits_0^t h(\tau)\,d\tau} \tag{8}$$

A failure distribution is fully described by $f(t)$ or $F(t)$ or $R(t)$ or $h(t)$

Figure 2 shows an example failure distribution and the quantities describing it.

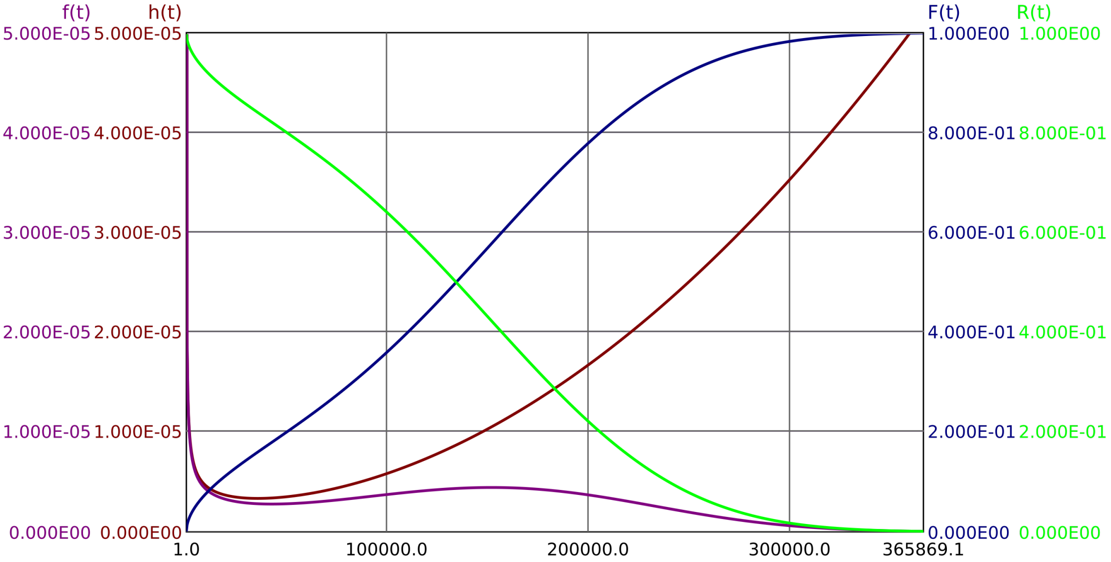


Figure 2: *distribution function where $h(t)$ resembles a bathtub*

Note: While the symbols $R(t)$, $F(t)$ and also $f(t)$ are largely uniformly used, no symbol has yet been established for the failure rate. Instead of $h(t)$ one also finds $\Lambda(t)$ or $\lambda(t)$.

The failure rate $h(t)$ indicates the probability of a failure per time interval, under the condition that the function has not failed at the beginning of the time interval:

$$h(t) = \frac{f(t)}{R(t)} = \frac{dF(t)/dt}{R(t)} = \frac{1}{R(t)} \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} \tag{9}$$

Here the time interval Δt must be sufficiently small! Therefore this equation must not be used to calculate an average failure rate over a longer period of time. The formulas required for this purpose are mentioned in section 3.

2.3 Bathtub curve

Each non-trivial component can fail in different ways. Each of these failure modes has its own failure distribution function. There are almost always failure modes with decreasing failure rate, these are usually due to production defects. For mechanical or even heavily loaded electronic components, there are also failure modes with increasing failure rate, these are in particular the failures due to wear or aging. The total failure rate is obtained by adding the individual failure rates of all n failure modes:

$$h(t) = \sum_{i=1}^{n} h_i(t) \tag{10}$$

As soon as there is at least one failure mode with falling failure rate and one with rising failure rate, the graph of the total failure rate $h(t)$ resembles a bathtub, see figure 2.

2.4 Mean Time to Failure (MTTF)

The Mean Time To Failure (MTTF) is the expected value of the time until failure. It is calculated for any failure distribution as follows:

$$\mathrm{MTTF} = \int\limits_{0}^{\infty} t \cdot f(t)\, dt \tag{11}$$

This value is referred to as natural MTTF in section 3, since it is the (arithmetic) mean value which is obtained experimentally, if the component is always operated until failure and then replaced. In practice, however, this is often not the case, so that other formulas apply, especially for the determination of mean failure rates, see section 3.

2.5 Distribution functions

In this section, some distribution functions are presented, which are relevant in practice or for subsequent considerations. Further distributions are described in Appendix C.

2.5.1 Exponential distribution

The exponential distribution is characterized by a constant failure rate $h(t) = const.$ The failure rate is therefore described by a single parameter, which is denoted by λ. The exponential distribution is the simplest and at the same time most important distribution function. It is true for memoryless components, i. e. when the age of the component has no significant influence on the failure rate (also called ergodic behavior). The time course of reliability $R(t)$, unreliability $F(t)$, failure rate $h(t)$ and failure density $f(t)$ is shown in Figure 3.

The exponential distribution is described by the following equations:

$$f(t) = \lambda \cdot \mathrm{e}^{-\lambda \cdot t} \tag{12}$$

$$F(t) = 1 - \mathrm{e}^{-\lambda \cdot t} \tag{13}$$

$$R(t) = \mathrm{e}^{-\lambda \cdot t} \tag{14}$$

The mean time to failure is:

$$\mathrm{MTTF} = \int_0^\infty t \cdot \lambda \cdot \mathrm{e}^{-\lambda \cdot t}\, dt = - \frac{(\lambda \cdot t + 1)\ \mathrm{e}^{-\lambda \cdot t}}{\lambda} \Big|_0^\infty = \frac{1}{\lambda} \tag{15}$$

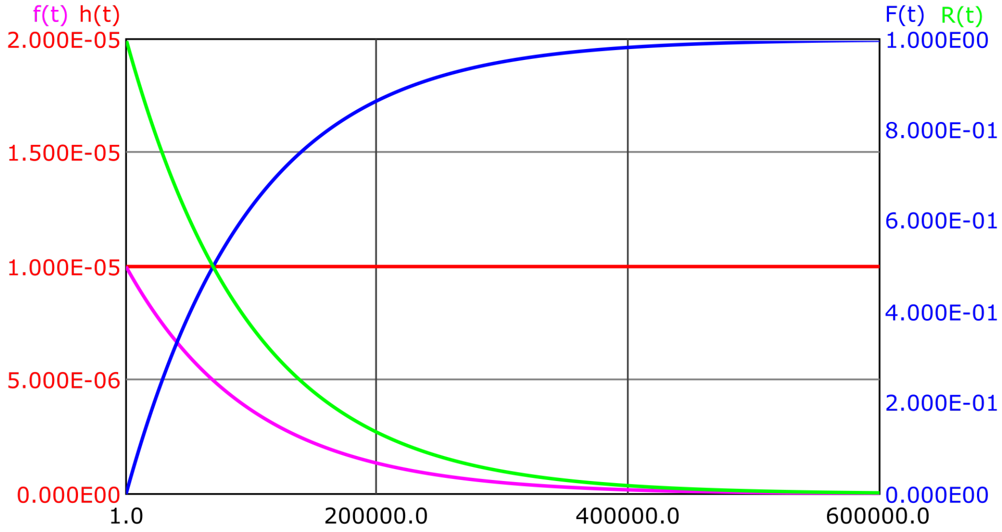


Figure 3: *Exponentional distribution with* $\lambda = 1.0\text{E}{-5}/\text{h}$

Example 2.4 *What is the probability* p*, that a component with age* t*, which is still working at time* t*, will fail within the next hour. Let it be known that the component can be described by a constant failure rate.*

$$\begin{aligned} p = \frac{F(t, t + 1\,\text{h})}{R(t)} &= \frac{F(t + 1\,\text{h}) - F(t)}{R(t)} = \frac{\text{e}^{-\lambda\cdot t} - \text{e}^{-\lambda\cdot(t+1\,\text{h})}}{\text{e}^{-\lambda\cdot t}} \\ &= \frac{\text{e}^{-\lambda\cdot t} - \text{e}^{-\lambda\cdot t}\cdot \text{e}^{-\lambda\cdot 1\,\text{h}}}{\text{e}^{-\lambda\cdot t}} = 1 - \text{e}^{-\lambda\cdot 1\,\text{h}} \end{aligned}$$

As expected, the age of the component t *does not appear in the result.*

Many elements can be described with sufficient accuracy by a constant failure rate. In particular, for elements of a system whose MTTF is much shorter than the overall system service life (and will therefore be replaced multiple times after failure, e. g. a conventional light bulb in a lamp), and which are not replaced preventively at certain pre-defined points in time, only a constant mean failure rate $h(t) = \overline{h} = \lambda$ can be specified within the scope of system calculations, since the actual failure rate function itself is random.

2.5.2 Weibull distribution

The Weibull distribution is a generalization of the exponential distribution. With an additional parameter $k > 0$ in the exponent, falling or rising default rates can be modeled. For $0 < k < 1$ a falling, for $k > 1$ an increasing failure rate results. For $k = 1$ the result is the exponential distribution.

$$h(t) = \lambda \cdot k \cdot (\lambda \cdot t)^{k-1} \tag{16}$$

$$f(t) = \lambda \cdot k \cdot (\lambda \cdot t)^{k-1}\text{e}^{-(\lambda\cdot t)^k} \tag{17}$$

$$F(t) = 1 - \text{e}^{-(\lambda\cdot t)^k} \tag{18}$$

$$\mathrm{MTTF} = \frac{1}{\lambda} \cdot \Gamma\left(1 + \frac{1}{k}\right) \tag{19}$$

Failure modes that are exclusively due to wear and tear, can usually be completely excluded for a certain time t_0. These failure modes can usually be well modeled with a Weibull distribution with $k > 1$ (increasing failure rate), which is additionally shifted to the right by $t_0 > 0$:

$$h(t) = \lambda \cdot k \cdot (\lambda \cdot (t - t_0))^{k-1} \quad \text{for } t > t_0 \tag{20}$$

Note: Especially in English-speaking countries, the Weibull distribution is often parameterized with $\mu = 1/\lambda$.

Figures 4 and 5 show a Weibull distribution with decreasing failure rate (k=0.5) and with increasing failure rate (k=3).

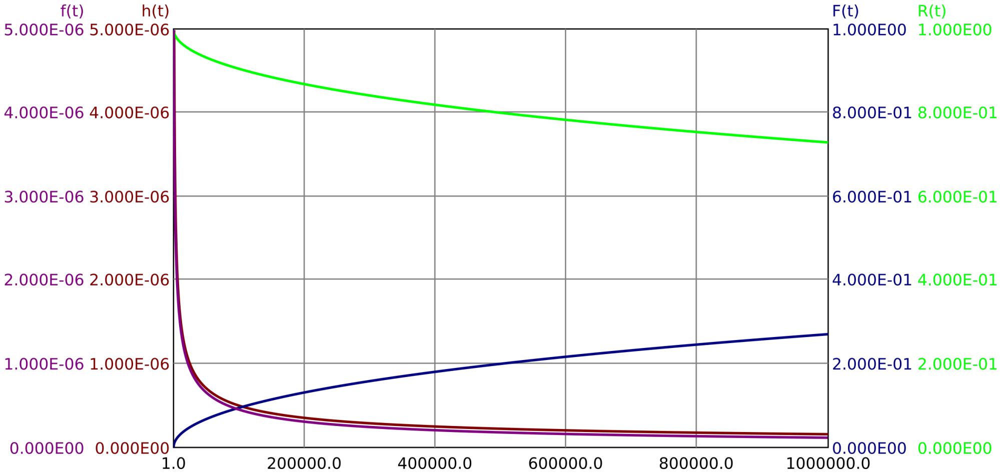


Figure 4: *Weibull distribution with* $\lambda = 1.0\mathrm{E}{-7}/\mathrm{h}$ *and* $k = 0.5$

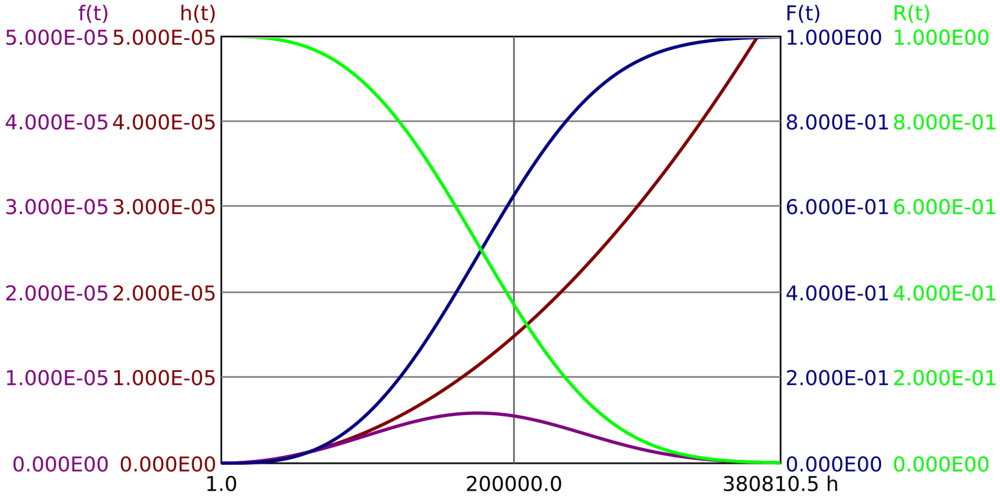


Figure 5: *Weibull distribution with* $\lambda = 5.0\mathrm{E}{-6}/\mathrm{h}$ *and* $k = 3.0$

2.5.3 Mortality

Human mortality is also a distribution function, although it does not directly follow a mathematical function. Figure 6 shows a cross-sectional view of the mortality of the mortality of the West German population in the years 1960-1962 is shown.

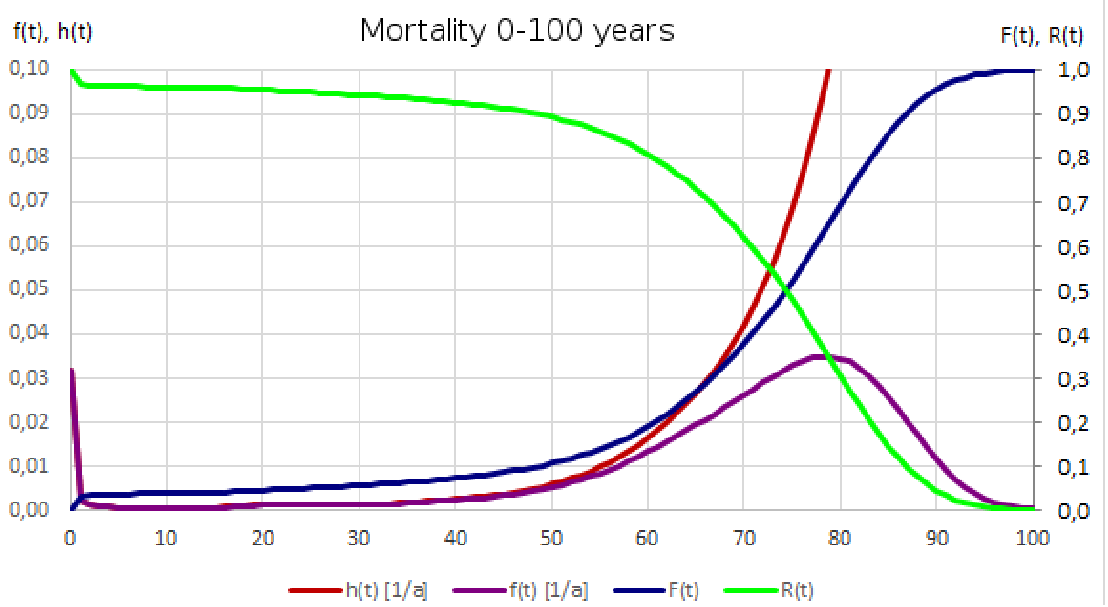


Figure 6: *Mortality 1962 (cross-sectional view)*

The cross-sectional analysis is based on the statistics of deaths during the period in question. It thus makes a statement in particular about the actual mean age at death of the people who died in this period. The mortality rate $h(t)$ thus indicates the probability here, that a person who had reached the age t dies within the time span Δt, divided by this time span Δt.

In contrast to the cross-sectional view, the so-called longitudinal view makes a statement about the mortality distribution of the people born in the respective period. Longitudinal statistical observations can therefore only be made for birth cohorts, of which no human being is still alive. For later cohorts, they represent forecasts in whole or in part. If the mortality distribution were independent of the year of birth, the cross-sectional and longitudinal distributions would be identical. For the longitudinal view, the quantities are immediately illustrative:

- Reliability (survival probability) $R(t)$ is the probability of reaching age t.
- The unreliability (failure probability) $F(t)$ is the probability of dying before reaching age t.
- The failure density $f(t)$ is the probability of dying at age between t and $t + \Delta t$, divided by the period Δt, with $\Delta t \to 0$.
- The failure rate $h(t)$ is the probability of dying at age between t and $t + \delta t$, given

the condition of having reached age t, divided by the period Δt, with $\Delta t \to 0$.

- The MTTF is the life expectancy of a newborn.

3 Mean failure rate and mean time to failure

For many components, the failure rate is highly time dependent. A mean failure rate is also often required for such components, among others for the following reasons:

- If system variables ($\overline{h_{\text{sys}}}$, $\overline{Q_{\text{sys}}}$) are to be calculated in a stationary way, only mean failure rates can be used due to the principle.
- If a component is likely to fail (and be replaced or repaired) multiple times during the system's operational lifetime, from the first failure on, the failure rate function itself is also a random variable, which becomes increasingly fuzzy as the number of failures (and thus replacements) increases. Even in the case of transient, i. e. continuously time-resolved, observations, no failure rate function can be given.
- If the component is to be replaced regularly as a preventive measure, so that it will most probably not fail, the question arises at what interval the component should be replaced, in order to keep the effective (residual) failure rate and thus the probability of failure as low as possible.

Therefore, in this section, the following tasks will be addressed:

1. What are the MTTF and mean failure rate for the case, that the component is operated until failure and then replaced? (Example: light bulb)
2. What are MTTF and effective mean failure rate for the case, that the component is regularly replaced as a preventive measure? (Example: timing belt of a car combustion engine)
3. If there are dangerous and non-dangerous failure modes of a component: How can the dangerous MTTF and dangerous mean failure rate be calculated for the above two cases?

It is often claimed, one should use the failure rate in the flat area of the "bathtub curve" for such questions. However, this is only correct if the component is really only operated in this range, i. e. early failures (especially production defects) can be absolutely excluded as well as failures due to aging and wear. These conditions are very often not met – and moreover, the bathtub curve often does not show a really flat area at all. Instead, so-called early failures overlap with late failures.

Note: Some readers may wonder, why the abbreviation MTTF is also used for the time between two failures, and not MTBF (Mean Time Between Failures). The answer is simple, that almost always when MTBF is mentioned, actually the MTTF is meant (or necessary in fact). In applications or calculations, where fault detection times or repair times are not insignificant, these must be explicitly mentioned anyway. Thus, there is no valid reason, neither in safety nor in reliability theory, to introduce or use a quantity "MTBF". [2]

[2] In fact, I am not sure, if I have ever seen a document in which the term MTBF has been used correctly – apart from theoretical textbooks

3.1 MTTF in long use without preventive replacement

First, the MTTF and the mean failure rate are to be calculated for a component, which has a significantly lower life expectancy than the nominal service life of the overall system. In this case, it can be assumed that the component will fail several times and will therefore have to be replaced several times.

For arbitrary failure distribution functions, the following holds:

$$\mathrm{MTTF} = \int_0^\infty t \cdot f(t)\, dt \tag{21}$$

If sufficient test or field data is available, then this integral can be easily calculated with a spreadsheet. If instead of $f(t)$ the data $F(t)$ or $R(t)$ are available, $f(t)$ can be easily obtained by numerical differentiation.

In general, the following applies to the failure density function

$$f(t) = h(t) \cdot R(t) = h(t) \cdot \mathrm{e}^{-\int_0^t h(\tau)\, d\tau} \tag{22}$$

and thus for the MTTF

$$\mathrm{MTTF} = \int_0^\infty t \cdot h(t) \cdot \mathrm{e}^{-\int_0^t h(\tau)\, d\tau}\; dt \tag{23}$$

Almost all components have multiple failure modes, which obey different failure distribution functions. Assuming that the failure distribution functions of the individual failure modes are known, how can the MTTF be calculated? For this, it must be assumed that the failure modes are independent of each other, i. e. they do not influence each other. In order for this prerequisite to be fulfilled it is necessary in particular that the component is replaced in the case of each failure. Then it holds for the total failure rate function $h(t)$ of the component, that it is given by the sum of the failure rate functions of the individual failure modes:

$$h(t) = \sum_{i=1}^{n} h_i(t) \tag{24}$$

If both all $h_i(t)$ and the respective associated reliability functions $R_i(t)$ are given by mathematical formulas, it is helpful to simplify the double integral:

$$\begin{aligned}\mathrm{MTTF} &= \int_0^\infty t \cdot h(t) \cdot \mathrm{e}^{-\int_0^t \sum_{i=1}^{n} h_i(\tau)\, d\tau}\; dt = \int_0^\infty t \cdot h(t) \cdot \mathrm{e}^{-\sum_{i=1}^{n} \int_0^t h_i(\tau)\, d\tau}\; dt \\ &= \int_0^\infty t \cdot h(t) \cdot \prod_{i=1}^{n} R_i(t)\; dt\end{aligned} \tag{25}$$

The MTTF determined in this way is called complete MTTF or natural MTTF, because it is the mean time to failure that results, if the component is used until failure and then replaced (as is the case in long-life systems such as machinery, aircraft, or rail vehicles).

The average failure rate of the component in the event, that the component is likely to fail (several times) and is then replaced each time, is the reciprocal of the complete MTTF:

$$\lambda = \frac{1}{\mathrm{MTTF}} \tag{26}$$

3.2 Preventive Exchange and Incomplete MTTF

In the case of preventive replacement after a time interval T, the incomplete MTTF(T) is required for the time interval 0 to T. The same applies if the natural MTTF of the component is much greater than the lifetime of the system in which it is used. From considerations which cannot be reproduced here, it follows:

$$\mathrm{MTTF}(T) = \frac{\int\limits_0^T t \cdot f(t)\, dt + T \cdot R(T)}{F(T)} \tag{27}$$

With $R(T) = 1 - F(T)$ and the already known formulas for the relationship between reliability and failure rate, one obtains a formula for calculating $\mathrm{MTTF}(T)$ for a given or experimentally determined failure rate function $h(t)$:

$$\begin{aligned}\mathrm{MTTF(T)} &= \frac{\int\limits_0^T t \cdot f(t)\, dt + T \cdot \big(1 - F(T)\big)}{F(T)} = \frac{\int\limits_0^T t \cdot f(t)\, dt + T}{F(T)} - T \\ &= \frac{\int\limits_0^T t \cdot h(t) \cdot \mathrm{e}^{-\int\limits_0^t h(\tau)\, d\tau}\, dt + T}{1 - \mathrm{e}^{-\int\limits_0^T h(t)\, dt}} - T\end{aligned} \tag{28}$$

For $T \to \infty$, the incomplete MTTF(T) transitions to the complete MTTF.

The reciprocal of the incomplete MTTF at time T is the effective failure rate λ_{eff}. It indicates in a very practical way how often the component would fail in spite of regular preventive replacements in case of a (very long) operating time of the entire system $T_{\text{Life,sys}}$:

$$\lambda_{\text{eff}}(T) = \frac{1}{\mathrm{MTTF}(T)} = \frac{N(T_{\text{Life,sys}})}{T_{\text{Life,sys}}} \tag{29}$$

Here $N(T_{\text{Life,sys}})$ means the countable failures of the component in the system. Therefore, MTTF(T) can also be called the effective MTTF for a given replacement interval T.

Example 3.1 *The failure rate of the timing belt of an engine of a passenger car can be described by two superimposed Weibull distributions:*

$$\lambda_1 = 1\mathrm{E}{-9}/\mathrm{h}\,;\ k_1 = 0.3 \Rightarrow h_1(t) = 1\mathrm{E}{-9}/\mathrm{h} \cdot 0.3 \cdot (1\mathrm{E}{-9}/\mathrm{h} \cdot t)^{0.3-1}$$

$$\lambda_2 = 2\mathrm{E}{-4}/\mathrm{h}\,;\ k_2 = 4.0 \Rightarrow h_2(t) = 2\mathrm{E}{-4}/\mathrm{h} \cdot 4.0 \cdot (2\mathrm{E}{-4}/\mathrm{h} \cdot t)^{4.0-1}$$

Here $h_1(t)$ describes so-called early failures, such as those caused by defective components or faulty assembly, and $h_2(t)$ describes the wear-related failures of the belt.

For the failure rate of the timing belt, according to formula (24)*:*

$$h_{\text{ges}}(t) = h_1(t) + h_2(t)$$

Further let it be assumed that a passenger car should be able to operate economically for at least 5000 hours.

This failure rate function calculates the unreliability at the time $T = 5000\,\text{h}$ *to* $F(5000\,\text{h}) \approx 0.64$*. Thus, it would be expected in at least one out of every two vehicles, that the timing belt will break before reaching 5000 hours of operation. Since the rupture of an engine's timing belt usually results in a total loss of the engine and thus often a total economic loss of the vehicle, the question arises whether a preventive replacement after a certain time (or driving distance) is not sensible.*

In Figure 7, in addition to failure density $f(t)$*, failure rate* $h(t)$*, reliability* $R(t)$ *and unreliability* $F(t)$*, the effective* $\text{MTTF}(T)$ *and (dashed) the effective failure rate* $\lambda_{\text{eff}}(T)$ *are also shown as a function of time to preventive replacement* T*.*

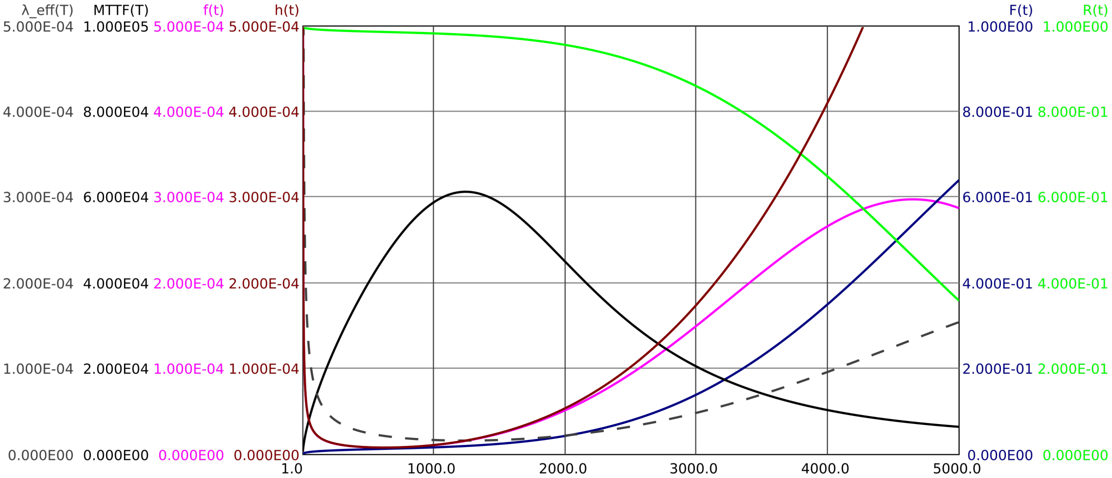


Figure 7: *Reliability of a timing belt*

It can be seen that for a replacement interval T *of about 1200 hours, the MTTF(T) reaches its maximum of about 61000 h. If the timing belt is changed after about 1200 hours, the effective failure rate is* $\lambda_{\text{eff}} \approx 1.6\text{E}{-}5/\text{h}$*. If the belt is changed more frequently, the effective (incomplete) MTTF(T) decreases, since early failures still have a relatively strong influence. If the belt is operated for a longer time, the effective MTTF(T) also decreases, as failures due to wear become more noticeable. Preventive replacement should therefore be prescribed after about 1200 hours (or a corresponding distance).*

The effective MTTF(T) of 61000 h at a replacement interval of 1200 h practically means, that only about one out of fifty (61000 h/1200 h≈50) belts will break in service. [3].

[3] The failure rate functions are, of course, imaginary and statistical uncertainties such as environmental conditions, road types, driving style, etc. are disregarded

3.3 Dangerous and non-dangerous failure modes, dangerous MTTF

As said already, most components can fail in different ways. In safety related applications, certain failure modes will be safety-critical, others will go to the safe side. For safety considerations, it is therefore often necessary to distinguish between dangerous (d) and safe (s) failure modes. The total failure rate at any time t is the sum of two partial failure rates for dangerous and non-dangerous failures:

$$h(t) = h_d(t) + h_s(t) \tag{30}$$

The density can be calculated using

$$\begin{aligned} f(t) &= h(t) \cdot R(t) = \big(h_d(t) + h_s(t)\big) \cdot R(t) \\ &= h_d(t) \cdot R(t) + h_s(t) \cdot R(t) \\ &= \varphi_d(t) + \varphi_s(t) \end{aligned} \tag{31}$$

into two partial failure densities φ_d and φ_s (φ_d and φ_s are not themselves densities, since their individual integrals are less than 1).

Accordingly, one can decompose the distribution function $F(t)$ into two subfunctions:

$$F(t) = \Phi_d(t) + \Phi_s(t) = \int\limits_0^t \varphi_d(\tau)\,d\tau + \int\limits_0^t \varphi_s(\tau)\,d\tau \tag{32}$$

From similar considerations as for the incomplete MTTF(T) one obtains for the effective dangerous $\mathrm{MTTF_d}(T)$:

$$\mathrm{MTTF_d}(T) = \frac{\int\limits_0^T t \cdot f(t)\,dt + T \cdot R(T)}{\Phi_d(T)} \tag{33}$$

Using the already known formulas for the relationship between reliability and failure rate, we obtain a formula for calculating $\mathrm{MTTF_d}(T)$ for given or experimentally determined failure rate functions $h(t)$ and $h_d(t)$:

$$\begin{aligned} \mathrm{MTTF_d}(T) &= \frac{\int\limits_0^T t \cdot f(t)\,dt + T \cdot R(T)}{\int\limits_0^T \varphi_d(t)\,dt} = \frac{\int\limits_0^T t \cdot h(t) \cdot R(t)\,dt + T \cdot R(T)}{\int\limits_0^T h_d(t) \cdot R(t)\,dt} \\ &= \frac{\int\limits_0^T t \cdot h(t) \cdot \mathrm{e}^{-\int_0^t h(\tau)\,d\tau}\,dt + T \cdot \mathrm{e}^{-\int_0^T h(t)\,dt}}{\int\limits_0^T h_d(t) \cdot \mathrm{e}^{-\int_0^t h(\tau)\,d\tau}\,dt} \end{aligned} \tag{34}$$

A simple formula comparison further yields the relationship:

$$\mathrm{MTTF_d}(T) = \mathrm{MTTF}(T)\frac{F(T)}{\Phi_d(T)} \tag{35}$$

Again, the effective mean dangerous failure rate λ_d can be calculated as the reciprocal:

$$\lambda_\mathrm{d}(T) = \frac{1}{\mathrm{MTTF}_\mathrm{d}(T)} \tag{36}$$

The following figure 8 shows the reliability parameters relevant for a component with three dangerous and three non-dangerous failure types (solid lines for dangerous failures, dashed lines for total failures):

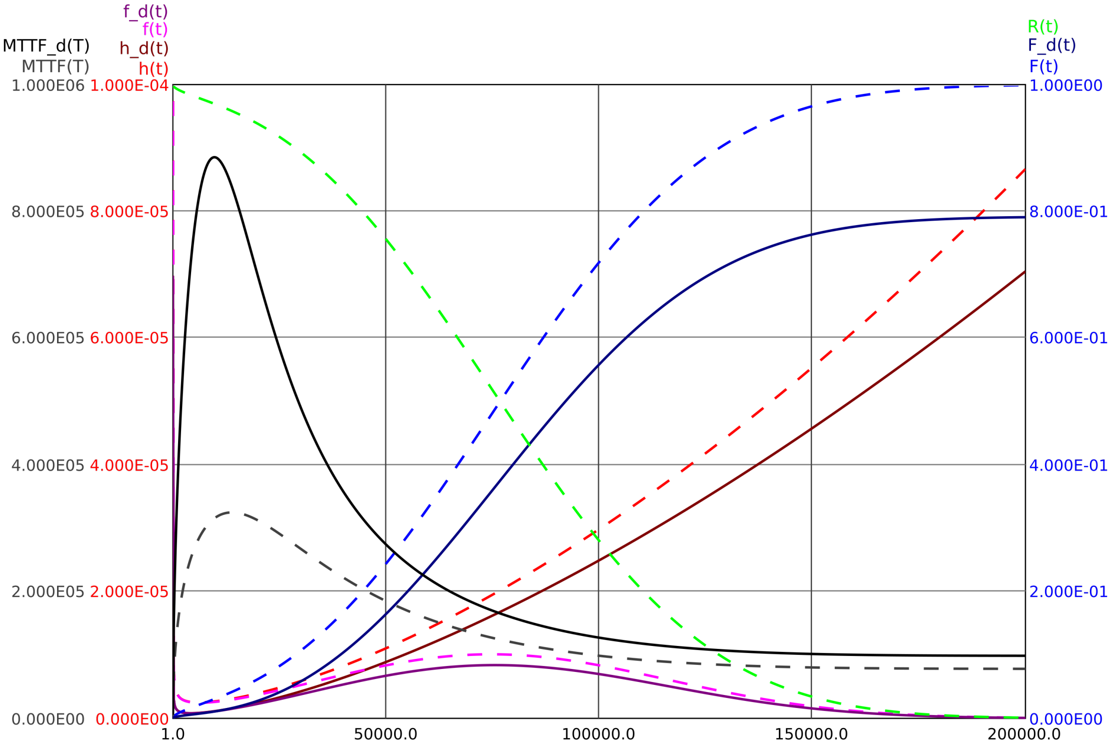


Figure 8: *Bathtub curve and quantities for dangerous and non-dangerous failures*

4 Recovery and availability

For components and systems, which are repaired or replaced in the event of a failure, further considerations and quantities are required.

4.1 Repairability

If it must be assumed, that during the specified period of use of the overall system, multiple failures of the function may occur, a system (or a function) is repairable. It does not matter whether the system is repaired in the literal sense, or single components or even the whole system is replaced by an equal or different one. Repairability is therefore not a matter of definition (like the definition of a smallest replaceable unit or of total loss), but results inevitably from the reliabilities of the components and the planned service lifetime. The much simpler modeling of a function as non-repairable may only be chosen if the unreliability of all components over the intended, specified service lifetime is small (approximately less than 0.1). This is practically never fulfilled in the case of long-lasting systems such as aircraft, locomotives, machinery or industrial plants, in the case of short-lived systems (such as passenger cars) only for some functions.

4.2 Diagnosis, test, recovery

According to [IEC 61508] and other standards, diagnostics are the measures, that detect a fault within the process fault tolerance time (PFTT, also called process safety time). This is the time that a physical process (e. g., a motor or valve in a machine) is allowed to be incorrectly controlled without resulting in an uncontrollable or dangerous state of the overall system.

Tests are the measures which reveal errors only after a more or less precisely defined fault detection time, for example, in the course of a restart (power-on-self test), a test routine to be performed regularly (test run) or during a maintenance measure (workshop inspection). The average time in which an existing fault is detected, is usually abbreviated to MTTD (Mean Time To Detect). If a test is performed at regular intervals T_{test}, then the MTTD $= T_{\text{test}}/2$.

In case of a detected defect, either the defective component is repaired or replaced, or a whole module is replaced or even the whole system (machine, vehicle,...) is taken out of operation and replaced by a new one. In any case, the function is restored, because this is usually still needed. With which measure the function is concretely restored, is irrelevant for the further considerations.

4.3 Availability and unavailability

Availability $A(t)$ is the probability, that a component/system/function works at time t.

Unavailability $Q(t)$ is the probability, that a component/system/function will not work at time t. Consequently, it is the complementary probability to availability:

$$A(t) = 1 - Q(t) \quad \text{or} \quad Q(t) = 1 - A(t) \tag{37}$$

Availability is the decisive variable for systems/functions, which are only required occasionally, in particular functions that are only required in exceptional or emergency cases (e. g. alarms or fire extinguishing devices). It is also an essential quantity for systems/functions which have redundancies, so-called multi-channel systems, more on this later.

For a component or system, which is never tested and therefore never repaired or replaced:

$$Q(t) = F(0, t) \tag{38}$$

Availability can be significantly increased by continuous diagnostics or regular tests and, if necessary, restoration. This is the reason why most emergency systems are tested regularly.

When a component is tested and repaired or replaced in case of a defect, $Q(t) = F(t)$ is valid only until the first test. In the case of regular tests at intervals of T_{test} the following equation is theoretically valid until the first restoration:

$$Q(t) = \frac{F(t - t \bmod T_{\text{test}}, t)}{R(0, t - t \bmod T_{\text{test}})} = \frac{F(t) - F(t - t \bmod T_{\text{test}})}{R(t - t \bmod T_{\text{test}})}$$

However, since it is not known when the first defect will occur and thus the first repair or replacement will be necessary, this formula is practically meaningless. For the same reason, a variable failure rate is also practically meaningless, because one can never say how long a component has been in use at time t, since one does not know when it was installed – it could already be a replacement. Consequently, a mean failure rate $\overline{h} = \lambda = 1/\text{MTTF}$ must always be determined and used according to section 3.

For components and systems, which are regularly (and completely) tested, the unavailability is a periodic sequence of initial pieces of the exponential distribution, therefore:

$$Q(t) = F(0, t \bmod T_{\text{test}}) = 1 - \mathrm{e}^{-\lambda(t \bmod T_{\text{test}})} \tag{39}$$

If the time t is small with respect to $\text{MTTF} = 1/\lambda$, then slightly conservatively

$$Q(t) \lessapprox \lambda \cdot (t \bmod T_{\text{test}}) \tag{40}$$

For an average failure rate $h(t) = \lambda = 1\text{E}{-5}/\text{h}$ and a test interval $T_{\text{test}} = 1000\,\text{h}$, unavailability $Q(t)$ and unreliability $F(t)$ are shown in Figure 9.

The unavailability decreases to zero with each test, then increases again. It is assumed that the regular test is complete, i. e. reveals all relevant faults of the component. If this is not the case this remaining part must be considered as a further unavailability with

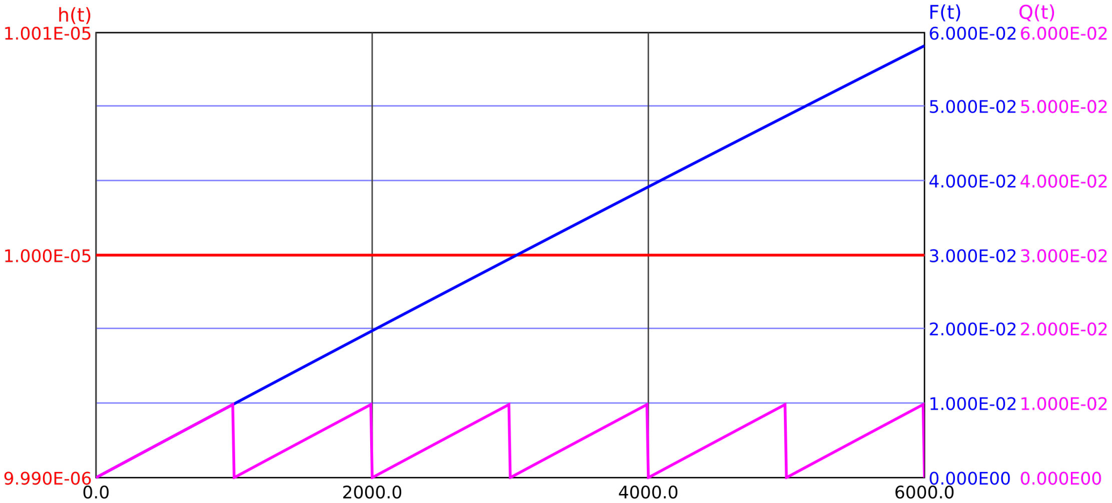


Figure 9: *Unreliability and unavailability with tests*

a correspondingly smaller failure rate, but longer test time (usually the system lifetime) must be added. Roughly speaking, one can simply add this second unavailability, in special software tools (FTA or Markov tools) an exact treatment is also possible.

Example 4.1 *A smoke detector has an average failure rate of* $\overline{h(t)} = \lambda = 1/100\,000\,\text{h} = 1\text{E}{-}5/\text{h}$. *It would be tested annually (every* $T = 8760\,\text{h}$*) and replaced if necessary. What is the probability that it will not work in the event of a fire?*

The mean unavailability over the test interval T_test *must be determined:*

$$\overline{Q(0..T)} = \frac{1}{T}\int_0^T 1 - \mathrm{e}^{-\lambda\cdot t}dt = \frac{1}{T}\left(t + \frac{1}{\lambda}\mathrm{e}^{-\lambda\cdot t}\right)\Bigg|_0^T = 1 + \frac{\mathrm{e}^{-\lambda\cdot T} - 1}{\lambda\cdot T} = 0.0426$$

When the unavailability is small (say $Q < 0.1$), the conservative approximation holds very well:

$$\overline{Q(0..T_\text{test})} \lessapprox 0.5\cdot\lambda\cdot T_\text{test} \tag{41}$$

In the previous example this would result in $\overline{Q(0..T_\text{test})} \approx 0.0438$ instead of 0.0426.

The unavailability is a probability, it can only take values from 0 to 1, but unlike unreliability, it is monotonically increasing only in the special case of a non-testable/non-repairable) system. After each test, however, unlike unreliability $F(t)$, the unavailability $Q(t)$ drops back to zero (or at least to a value close to zero in the case of a noncomplete test).

4.4 Time to repair, MRT

If only a partial function is affected by the defect, the continued operation of the surrounding larger system might be possible (if necessary with restrictions). In that case, the time required for repair and/or replacement (MRT, Mean Repair Time) must also be taken into account in the unavailability. Together with the time to detect the fault (MTTD), this results in the Mean Time To Restore (MTTR):

$$\text{MTTR} = \text{MTTD} + \text{MRT} \tag{42}$$

For the exact calculation of the mean unavailability, we can start from its definition:

$$\begin{aligned}\overline{Q} = \frac{T_\text{def}}{T_\text{overall}} &= \frac{T_\text{ud} + p_\text{def} \cdot \text{MRT}}{(1 - p_\text{def}) \cdot T_\text{test} + p_\text{def} \cdot (T_\text{test} + \text{MRT})} \\ &= \frac{T_\text{ud} + p_\text{def} \cdot \text{MRT}}{T_\text{test} + p_\text{def} \cdot \text{MRT}}\end{aligned} \tag{43}$$

where p_def denotes the probability, to find the function defective at the regular test time T_test.

$$p_\text{def} = F(T_\text{test}) = 1 - e^{-\lambda \cdot T_\text{test}}$$

and T_ud the mean time in each test interval, during which the function is undetectably unavailable due to the defect (i. e. the MTTD divided over all test intervals until failure)

$$\begin{aligned}T_\text{ud} &= \int_0^{T_\text{test}} f(t) \cdot (T_\text{test} - t)\, dt = \int_0^{T_\text{test}} \lambda \cdot e^{-\lambda \cdot T_\text{test}} \cdot (T_\text{test} - t)\, dt \\ &= \frac{e^{-\lambda \cdot T_\text{test}} - 1}{\lambda} + T_\text{test}\end{aligned}$$

By substituting in formula (43) we get for the mean unavailability

$$\begin{aligned}\overline{Q} &= \frac{\dfrac{e^{-\lambda \cdot T_\text{test}} - 1}{\lambda} + T_\text{test} + \text{MRT} \cdot (1 - e^{-\lambda \cdot T_\text{test}})}{T_\text{test} + \text{MRT} \cdot (1 - e^{-\lambda \cdot T_\text{test}})} \\ &= \frac{e^{-\lambda \cdot T_\text{test}} - 1}{\lambda \cdot T_\text{test} + \lambda \cdot \text{MRT} \cdot (1 - e^{-\lambda \cdot T_\text{test}})} + 1\end{aligned} \tag{44}$$

For negligible detection time $T_\text{test} \to 0$ (continuous diagnostics, small test intervals or fault revelation by immediately detectable malfunction) the mean (safety relevant) unavailability approaches

$$\overline{Q} = \frac{\lambda \cdot \text{MRT}}{\lambda \cdot \text{MRT} + 1} \tag{45}$$

as obtained by applying de l'Hospital's rule once to formula (44).

For negligible repair time MRT → 0 (e. g., out of service during repair), formula (44) simplifies directly to

$$\overline{Q} = \frac{e^{-\lambda \cdot T_\text{test}} - 1}{\lambda \cdot T_\text{test}} + 1 \tag{46}$$

If both test interval T_test and repair time MRT are small vs $MTTF$, holds with sufficient accuracy

$$\overline{Q} \lessapprox \lambda \cdot (0.5 \cdot T_\text{test} + \text{MRT}) \tag{47}$$

It is more difficult to derive an (exact) formula for the unavailability at a certain point in time, if the repair time is not negligible. A very good approximation is given by

$$Q(t) = 1 - \frac{e^{-\dfrac{\lambda \cdot (t \bmod T_{\text{test}})}{\lambda \cdot \text{MRT} + 1}}}{\lambda \cdot \text{MRT} + 1} \tag{48}$$

(without derivation). For repair time MRT → 0, formula (48) goes directly to formula (39):

$$Q(t) = 1 - \mathrm{e}^{-\lambda (t \bmod T_{\text{test}})}$$

For negligible detection time $T_{\text{test}} \to 0$ immediately results in

$$Q(t) = 1 - \frac{e^{-\dfrac{0}{\lambda \cdot \text{MRT} + 1}}}{\lambda \cdot \text{MRT} + 1} = 1 - \frac{1}{\lambda \cdot \text{MRT} + 1} = \frac{\lambda \cdot \text{MRT}}{\lambda \cdot \text{MRT} + 1} = \overline{Q}$$

thus formula (45).

4.5 Continuous diagnosis

In the case of continuous complete diagnosis (i. e. every error is detected immediately) the unavailability has nothing to do with the (un)reliability, so $Q(t) \neq F(t)$ is always valid. Unavailability then depends only on the (mean) failure rate $\overline{h} = \lambda$ and the time MRT needed for recovery:

$$Q(t) = \overline{Q} = \frac{\lambda \cdot \text{MRT}}{\lambda \cdot \text{MRT} + 1} = \text{const} \tag{49}$$

If the component is never tested and repaired or replaced if necessary, $Q(t) = F(t)$. This may be the case in (unmanned) space flight, but not in functional safety, because regular testing and repair or replacement are central measures of functional safety. Therefore, unreliability and unavailability must never be confused. Furthermore, unreliability and unavailability must never be added or multiplied or otherwise mathematically linked!

Example 4.2 *A component with the constant failure rate* $h(t) = \lambda = 1/10\,000\,\text{h} = 1\text{E}{-}4/\text{h}$ *is tested every 5000 hours and, if necessary, immediately repaired or replaced. What are the levels of unavailability and unreliability at times T=19999 and T=20001 hours?*

$$\begin{aligned}
Q(19999\,\text{h}) &= 1 - \mathrm{e}^{-\lambda \cdot (19999 - 15000\,\text{h})} \approx 0.3935 \\
Q(20001\,\text{h}) &= 1 - \mathrm{e}^{-\lambda \cdot (20001 - 20000\,\text{h})} \approx 0.0001 \\
F(19999\,\text{h}) &= 1 - \mathrm{e}^{-\lambda \cdot 19999\,\text{h}} \approx 0.8646 \\
F(20001\,\text{h}) &= 1 - \mathrm{e}^{-\lambda \cdot 20001\,\text{h}} \approx 0.8647
\end{aligned}$$

4.6 Operational and safety availability

Often, as a safety engineer, you hear the sentence: "The failure is not critical, it only effects availability." This phrase is based on a lack of understanding of reliability and availability. Both can be safety-related quantities, but do not have to be.

Example 4.3 *The availability of a smoke detector indicates, with which probability it will report a smoke development. This is obviously a safety-relevant quantity, in many applications minimum values are prescribed, therefore (or maximum values for the unavailability). The more often you test it, the greater the availability (the closer to 1). The greater the failure rate, the more often one has to test (and repair) to achieve the required availability. The reliability (or failure rate) alone does not allow any statement about the safety here, since it is irrelevant for safety, how often the smoke detector breaks down – as long as the failure is detected and repaired quickly. Rather, reliability is an operationally relevant variable here: The worse the reliability (i. e., the greater the failure rate) of the smoke detector, the more frequently it has to be tested and replaced, in order to achieve the availability specified for safety reasons.*

4.7 Failure rate during tests

Due to the tests and repair, if necessary, the density function $f(t)$ loses its meaning. It is replaced by a new quantity, usually called "failure frequency". In [NUREG] the formula sign $w(t)$ is used for it, however, no harmonized formula symbol has yet been established for this quantity. In Figure 10 all three quantities $h(t)$, $w(t)$ and $f(t)$ are shown for a function with constant failure rate $h(t) = \lambda = 1\text{E}{-}5/\text{h}$, which is tested every 30000 hours, are shown.

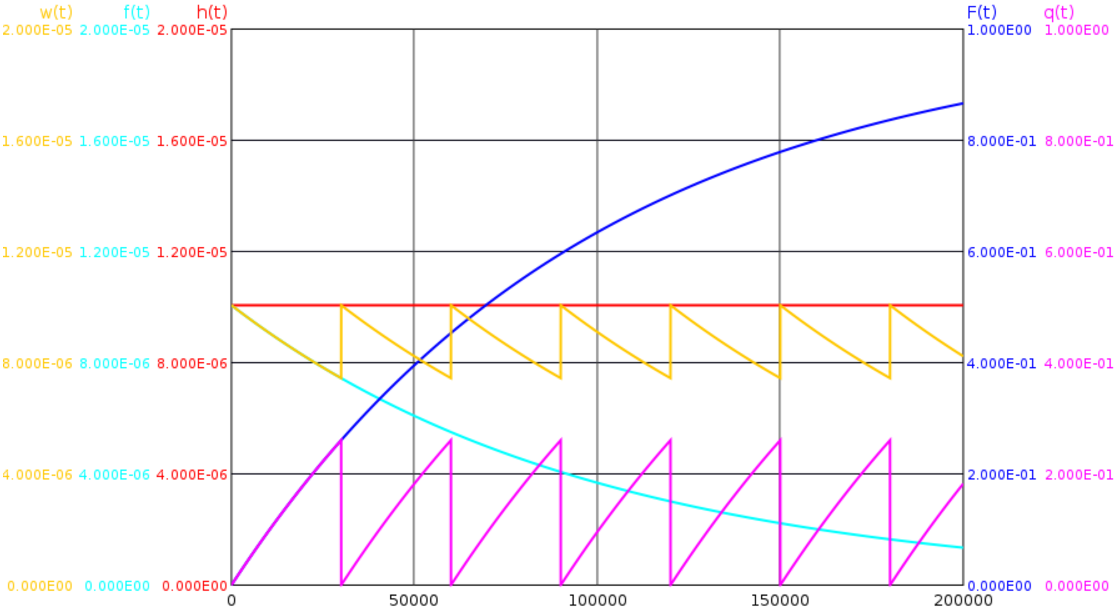


Figure 10: *Quantities in case of regular tests*

In contrast to the density $f(t)$ $w(t)$ never becomes zero, because due to the repair the system is always in a state (again), in which it can fail (again). Immediately after (complete) tests, i. e. when the unavailability returns to zero, the failure frequency increases again to the failure rate $h(t)$. The integral of the failure frequency $w(t)$ over time can thus become arbitrarily large. Only up to the first failure or the first test $w(t)$ and $f(t)$ are identical.

The failure rate, i. e. the frequency of transition to the failure state under the condition, that the system is capable of failure at time t, is now calculated as

$$h(t) = \frac{w(t)}{A(t)} = \frac{w(t)}{1 - Q(t)} \tag{50}$$

where $A(t)$ denotes availability or $Q(t)$ denotes unavailability at time t.

5 Unavailability of complex functions

Unavailability is the essential parameter for safety functions, which are only rarely required. Examples of simple components that perform such safety functions are circuit breakers (should trip in case of overcurrent), pressure relief valves (should open in case of overpressure) or ceiling sprinklers (should release water in case of excessive temperature). Their functional architecture is shown in figure 11.

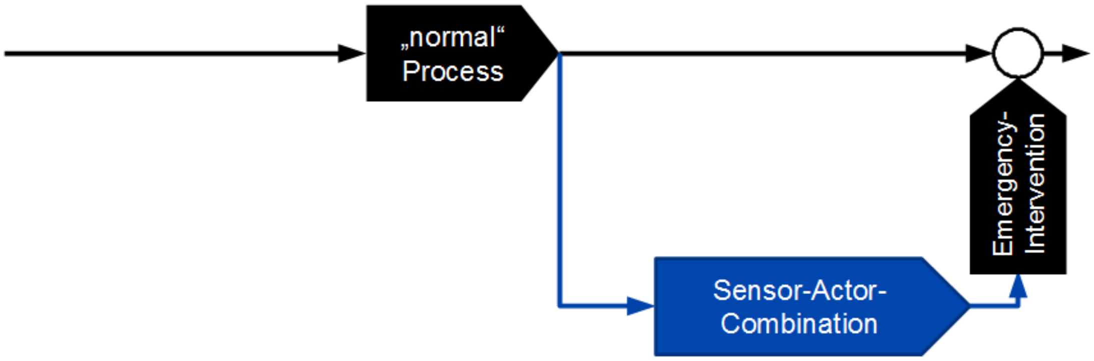


Figure 11: *Simple safety system for low demand mode*

Of course, there are also more complex systems that perform infrequently needed safety functions, nowadays mostly computer-controlled. Examples are monitoring and emergency systems in the chemical industry or in power plants, fire detection and fire fighting systems, smoke extraction systems, evacuation systems, etc. Their architecture is exemplified in Figure 12. The term "process " is very broad in this context, it can be simply the normal operation of a building, apparatus or machine.

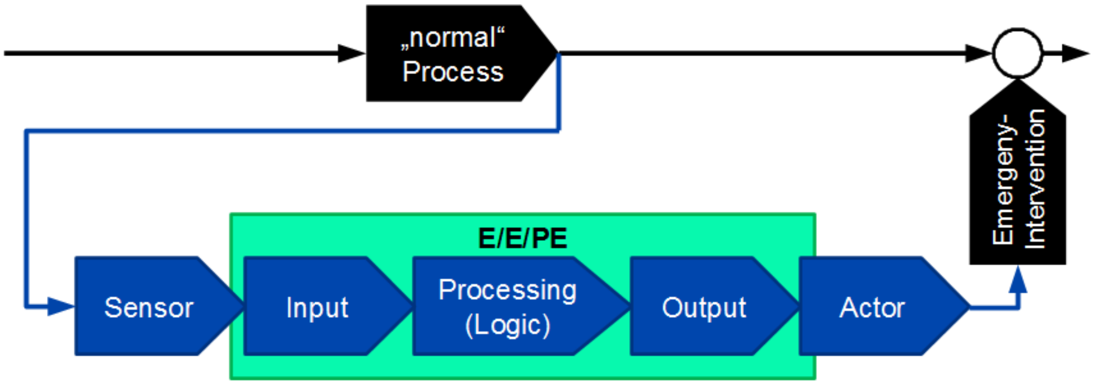


Figure 12: *Complex safety system for low demand mode*

Normally, the existence of the safety function(s) is not noticed. Only in the case of a request (if this ever occurs) does it become apparent, whether the safety function is actually available [4]. A safety-critical fault (i. e. one that prevents the safety function

[4] Under certain circumstances, it also only becomes apparent then, whether the safety function is correctly designed, e. g. the actuators are correctly dimensioned, but this is not the subject of functional safety

in the case of a request) can only be detected if the component or the system is tested regularly [5] or if it does not function when required.

The unavailability is practically always a time-dependent function $Q(t)$. If there are no events with constant unavailability, the unavailability of a system Q_{sys} at time $t = 0$ is zero. Only if there are events with constant unavailability, Q_{sys} will be greater than zero already at $t = 0$. In any system there will be components, which have at least one failure mode which is not immediately apparent. The unavailability will therefore increase monotonically until the next test, and decrease to a smaller value (in the case of complete tests, to the value at $t = 0$) immediately after a test. If there are failures that are never detected, the unavailability will increase, at least on average, until the end of the system's operation.

Since it is never known at which point in time the safety function will be required, only the average value of the unavailability over the lifetime of the process or the safety system is of interest:

$$\overline{Q} = \frac{1}{T_{\text{Life}}} \int\limits_{0}^{T_{\text{Life}}} Q(t)dt \tag{51}$$

In [IEC 61508], this mean $\overline{Q}$ is referred to as Probability of Failure on Demand (PFD for short).

5.1 Calculation with fault trees

Frequently, the safety system is modeled with the help of fault trees. These are very suitable for modeling such systems, and the unavailability of the system $\overline{Q_{\text{sys}}}$ can be be computed very easily and mathematically accurately (assuming, of course, that the unavailabilities of the components are known).

Although ultimately only the mean value of the unavailability is of interest, nevertheless, according to formula (51), the time-dependent function must be calculated at a sufficient number of grid points and integrated over them.

The base events of a fault tree model the components with their failure modes and, if applicable, the measures for restoration. The standard model for a basic event is the so-called "restorable event", also referred to as a testable or repairable event, see appendix A.1. This model describes a (constant) failure rate and a (mean) detection time, as well as repair time, if applicable. If the failure is not detected by diagnostics or testing, i. e. remains in the system until the end of the operating time, the event shall be detected with the model "non-repairable event" according to Annex A.2 shall be described. In this case, non-constant failure rates are also possible. Sometimes the unavailability in case of the request also depends neither on a time since a last test nor on the age of the system, or the event does not describe a failure at all but rather the probability of the presence of an external boundary condition or the probability of an operator error. Then the unavailability is a constant (Appendix A.3).

[5] for certain components a visual inspection may be sufficient

As logical connections almost exclusively AND and OR are used, therefore only these shall be considered here. [6]

Even if today the calculation is performed based on Binary Decision Diagrams (Binary Decision Diagrams, BDD for short), the calculation shall be explained here with the help of Minimal Cut-Sets (MCS).

A minimum cut is a combination of basic events, which is necessary and sufficient for the occurrence of the top event (for example, the failure of a safety function). For so-called coherent fault trees – which are fault trees that do not contain negating gates such as NOT, XOR, NAND, etc. – there is exactly one set of minimal cuts. For incoherent fault trees, we speak of prime implicants instead of minimal cuts, and there are in general several possible sets of prime implicants. Since negating gates rarely needed, they are not mentioned in the following.

5.1.1 Unavailability of an AND operation

An AND operation of two or more basic events leads to a minimum cut with just these basic events. An AND-connection of branches of a tree usually leads to longer minimal cuts as well, the exact number and length depends on the structure of the linked branches.

The probability that a minimum cut is satisfied at a time t, i. e., the unavailability resulting from a minimum cut, is

$$Q_{\mathrm{MCS}}(t) = \prod_{j=1}^{m} Q_j(t) \tag{52}$$

Where m is the number of basic events in that minimal cut. The number m is called the order of the minimal cut.

Example 5.1 *There are two fire detectors in a room. Each has a failure rate of* $\lambda = 1\mathrm{E}{-5}/\mathrm{h}$. *The two fire detectors are tested simultaneously approximately every* 10 000 h *and replaced immediately in case a failure is detected in the test. What is the probability that none of them will report the fire in the event of a fire?*

Figure 13 shows the corresponding fault tree. It consists of two base events of type "repairable event", which are linked by an AND gate.

There is only one minimal cut, namely {BM.1 & BM.2}. Since it contains two elements (literals), it is a minimal cut of second order. Consequently, using formulas (52) *for the unavailability of the minimal cut and* (39) *for the unavailabilities of the fire detectors, the following applies*

$$Q_{\mathrm{sys}}(t) = Q_{\mathrm{BM.1}}(t) \cdot Q_{\mathrm{BM.2}}(t) = Q^2_{\mathrm{BM}}(t) = \left(1 - \mathrm{e}^{-\lambda(t \bmod T_{\mathrm{test}})}\right)^2 = 1 - 2\mathrm{e}^{-\lambda(t \bmod T_{\mathrm{test}})} + \mathrm{e}^{-2\lambda(t \bmod T_{\mathrm{test}})}$$

With the above quantities, a periodicity with a period of 10 000 h *is obtained, the exact progression is shown in figure 14.*

[6] So-called majority deciders (M-out-N) are nothing else than an abbreviation for an OR gate over several AND gates, so these are included. See section 6.1.6.

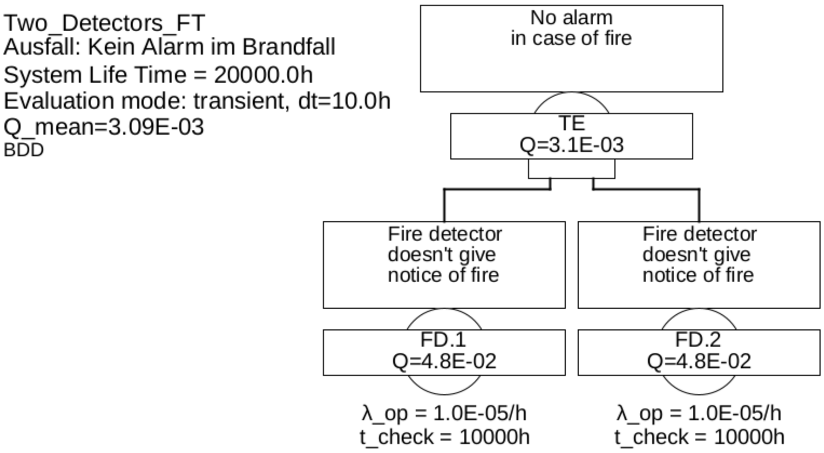

Two_Detectors_FT
Ausfall: Kein Alarm im Brandfall
System Life Time = 20000.0h
Evaluation mode: transient, dt=10.0h
Q_mean=3.09E-03
BDD
No alarm in case of fire
TE
Q=3.1E-03
Fire detector doesn't give notice of fire
Fire detector doesn't give notice of fire
FD.1
Q=4.8E-02
FD.2
Q=4.8E-02
λ_op = 1.0E-05/h
t_check = 10000h
λ_op = 1.0E-05/h
t_check = 10000h

Figure 13: *Redundant fire detectors*

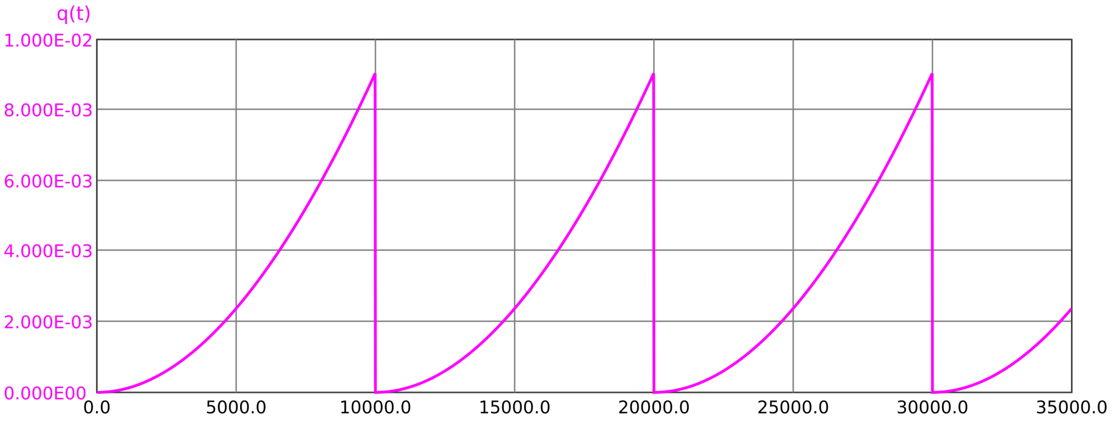


Figure 14: *Time course of the unavailability of two similarly redundant components that are regularly tested at the same times (detail)*

Due to the periodicity it is sufficient to calculate the average value over one period:

$$\overline{Q} = \frac{1}{T_{\text{Life}}} \int_{0}^{T_{\text{Life}}} Q(t)\,dt = \frac{1}{10\,000\,\text{h}} \int_{0\,\text{h}}^{10\,000\,\text{h}} 1 - 2\mathrm{e}^{-\lambda t} + \mathrm{e}^{-2\lambda t}\,dt$$

$$= \frac{1}{10\,000\,\text{h}} \left[t + \frac{2\mathrm{e}^{-\lambda t}}{\lambda} - \frac{\mathrm{e}^{-2\lambda t}}{2\lambda} \right]_{0\,\text{h}}^{10\,000\,\text{h}} = 0.003\,094\,59\ldots \approx 3.1\text{E}{-3}$$

The system usage time (lifetime) does not matter because of the periodic tests.

The reader may determine by his own calculation, that using the simplified formula $Q_{\text{BM}}(t) \lessapprox \lambda \cdot t$ *instead of the exact formula used here* $Q_{\text{BM}}(t) = 1 - \exp(-\lambda t)$ *practically the same result is calculated.*

5.1.2 Unavailability of an OR operation

An OR-operation of two or more basic events leads to a corresponding number of minimal cuts. An OR-operation of branches of a tree usually also leads to several minimal cuts, the exact number depends on the structure of the linked branches.

The total unavailability of the system is approximately the sum of the unavailabilities of the n minimal cuts:

$$Q_{\mathrm{sys}}(t) \lessapprox \sum_{i=1}^{n_{\mathrm{MCS}}} Q_{\mathrm{MCS},i}(t) = \sum_{i=1}^{n_{\mathrm{MCS}}} \left(\prod_{j=1}^{m_{\mathrm{Lit},i}} Q_j(t) \right) \tag{53}$$

This formula is an approximation that only holds, when the individual unavailabilities are very small.

A better approximation, which can be calculated almost as easily, is the Esary-Proschan formula:

$$Q_{\mathrm{sys}}(t) \lessapprox 1 - \prod_{i=1}^{n_{\mathrm{MCS}}} \left(1 - Q_{\mathrm{MCS},i}(t)\right) \tag{54}$$

This approximation can be used well in practice, since it is always conservative (i. e. $Q_{\mathrm{sys}}(t)$ never estimates too small), tends towards the exact result for small unavailabilities, and does not become larger than one for large unavailabilities. [7]

The exact result is obtained by disjoint decomposition of the minimum cuts. A method for disjoint decomposition is described in [EN 61025]. However, this is only suitable for very small fault trees [8].

Binary decision diagrams (BDDs) can be created with little effort even for very large fault trees, without having to determine minimum cuts at all. Moreover, they already imply disjunction in the calculation. Therefore, they allow an exact calculation of the unavailability with much less effort than the approximation via minimal cuts. Finally, BDDs are by far the fastest method for determining the minimum cuts. Modern FTA tools therefore use BDDs for all operations.

Example 5.2 *In principle, an automatic fire extinguishing system consists of a fire detector (FD), a control unit (CTRL) and an fire extinguishing unit (FE). A fire is extinguished only if these three units function in the event of a fire.*

This is modeled by the fault tree shown in Figure 15. Mathematically, one could place all three basic events directly under the upper OR gate, but this would violate the FTA rule "top-down design". This rule states that a fault tree shall always be developed from the top event down, and is one of the most important rules of all. And if you think about why the extinguishing system does not extinguish, it can only be because it itself is not working or that it is not activated. The control system and fire detectors only come into play when it comes to the question of why the extinguishing system is not activated, i. e. one level lower.

[7] one can also estimate a lower bound via minimal paths, but this differs so much from the actual value in practical tasks that it is meaningless

[8] and for these the overlap of the minimum cuts is small anyway for correctly designed systems, a disjoint decomposition is unnecessary

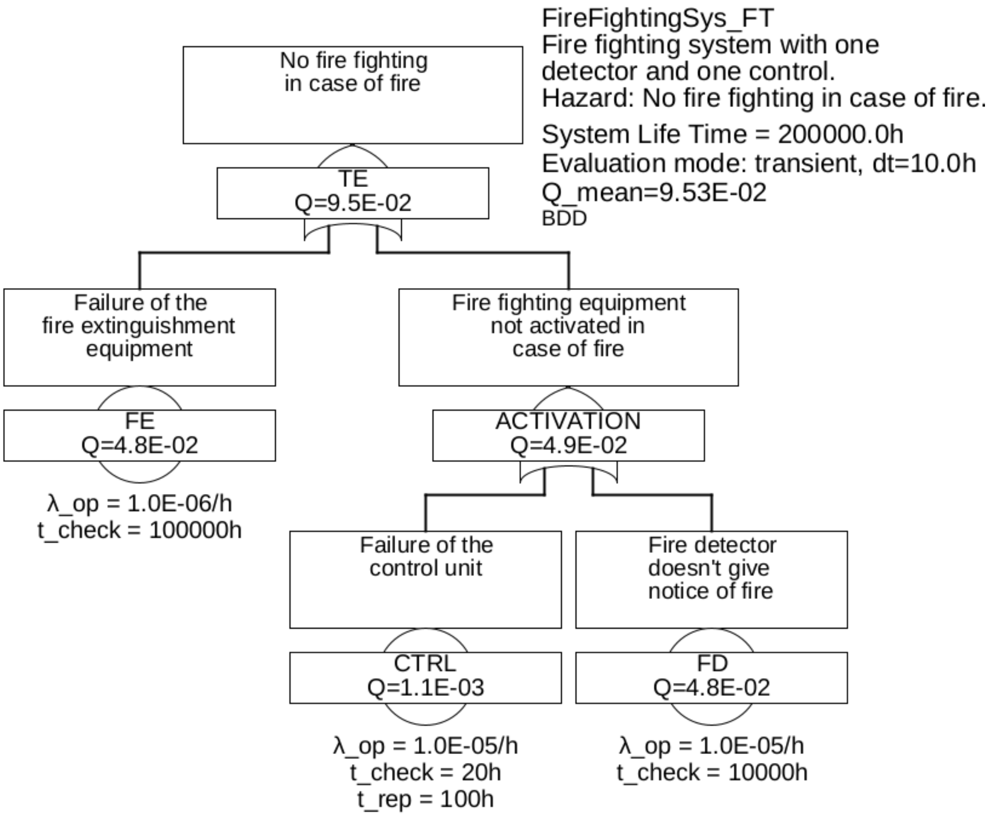

FireFightingSys_FT
Fire fighting system with one detector and one control.
Hazard: No fire fighting in case of fire.
System Life Time = 200000.0h
Evaluation mode: transient, dt=10.0h
Q_mean=9.53E-02
BDD
No fire fighting in case of fire
TE
Q=9.5E-02
Failure of the fire extinguishment equipment
FE
Q=4.8E-02
λ_op = 1.0E-06/h
t_check = 100000h
Fire fighting equipment not activated in case of fire
ACTIVATION
Q=4.9E-02
Failure of the control unit
CTRL
Q=1.1E-03
λ_op = 1.0E-05/h
t_check = 20h
t_rep = 100h
Fire detector doesn't give notice of fire
FD
Q=4.8E-02
λ_op = 1.0E-05/h
t_check = 10000h

Figure 15: *Brandlöschanlage*

There are three minimal cuts, namely {FE}, {CTRL} and {FD}. All three are first order. If one uses the approximate formula (53) *for the system nonavailability, one obtains*

$$Q_{\text{sys}}(t) \lessapprox Q_{\text{FE}}(t) + Q_{\text{CTRL}}(t) + Q_{\text{FD}}(t)$$

and thus for the mean value

$$\overline{Q_{\text{sys}}} \lessapprox \overline{Q_{\text{FE}}} + \overline{Q_{\text{CTRL}}} + \overline{Q_{\text{FD}}}$$

Using the values mentioned in figure 15 and the approximation formulas (41) *and* (47)*, we finally obtain*

$$\begin{aligned}\overline{Q_{\text{sys}}} &\approx 0.5\lambda_{\text{FE}}T_{\text{Test,FE}} + \lambda_{\text{CTRL}}(0.5\,T_{\text{Test,CTRL}} + T_{\text{MRT,CTRL}}) + 0.5\lambda_{\text{FD}}T_{\text{Test,FD}} \\ &= 0.05 + 0.0011 + 0.05 = 0.1011\end{aligned}$$

This approximate calculation differs from the exact value (not derived here) $Q = 0.0953...$ *by only 5% — an accuracy absolutely sufficient for practice.*

If one uses the estimation according to Esary-Proschan (54)*, one obtains*

$$Q_{\text{sys}}(t) \lessapprox 1 - [(1 - Q_{\text{FE}}(t)) \cdot (1 - Q_{\text{CTRL}}(t)) \cdot (1 - Q_{\text{FD}}(t))]$$

Using the same approximations as before for the individual unavailabilities, we obtain for the mean system unavailability

$$\begin{aligned}\overline{Q_{\text{sys}}} &\lessapprox 1 - \big[(1 - 0.5\lambda_{\text{FE}}T_{\text{Test,FE}}) \\ &\qquad \cdot (1 - \lambda_{\text{CTRL}}(0.5\,T_{\text{Test,CTRL}} + T_{\text{MRT,CTRL}})) \cdot (1 - 0.5\lambda_{\text{FD}}T_{\text{Test,FD}})\big] \\ &= 1 - [(1 - 0.05) \cdot (1 - 0.0011) \cdot (1 - 0.05)] = 0.098\,49...\end{aligned}$$

This approximation differs from the exact value $Q = 0.0953...$ *by only 3%.*

5.1.3 Unavailability of combinations of AND and OR gates

For such simple systems as in the previous examples, one will hardly use fault tree. Practically, fault trees always consist of a plurality of AND and OR gates, which often link a multitude of basic events.

Example 5.3 *Finally, the two previous examples are to be combined. Let the two smoke detectors be redundant again, i. e. mounted next to each other and interconnected in such a way, that one of them is sufficient to report a fire.*

The fault tree is shown in Figure 16.

The three minimum cuts are: {FE}, {CTRL}, {FD.1 & FD.2}

According to approximate formula (53)*, system unavailability is approximately:*

$$Q_{\text{sys}}(t) \lessapprox \sum_{j=1}^{n} Q_{\text{MCS},i}(t) = Q_{\text{FE}}(t) + Q_{\text{CTRL}}(t) + Q_{\text{FD.1}}(t) \cdot Q_{\text{FD.2}}(t)$$

For the interested reader who is familiar with BDDs, the BDD should still be given for the sake of completeness.

If you select the variable order Extinguishing device (FE), Control (CTRL), Fire detector.1 (FD.1), Fire detector.2 (FD.2), the binary decision diagram BDD shown in Figure 17 is obtained.

An exact formula for system unavailability can be derived directly from the BDD:

$$Q_{\text{sys}}(t) = Q_{\text{FE}}(t) + (1 - Q_{\text{FE}}(t)) \cdot [Q_{\text{CTRL}}(t) + (1 - Q_{\text{CTRL}}(t)) \cdot (Q_{\text{FD.1}}(t) \cdot Q_{\text{FD.2}}(t))]$$

In this formula, all events are automatically disjoint. It should be noted that other formulas result with other variable orders, these are however all mathematically equivalent.

If we compare the exact formula with the approximation formula in the last example, we see immediately, that for all fault trees which do not contain negating gates the approximate formula (53) always gives a too large result. For small fault trees, the difference is negligible for all correctly designed systems [9], however, for large fault trees with many thousands of minimum cuts, even then the error can become very large.

[9] correct design means that the test intervals are appropriate to the failure rates, so that all unavailabilities are very small at all times

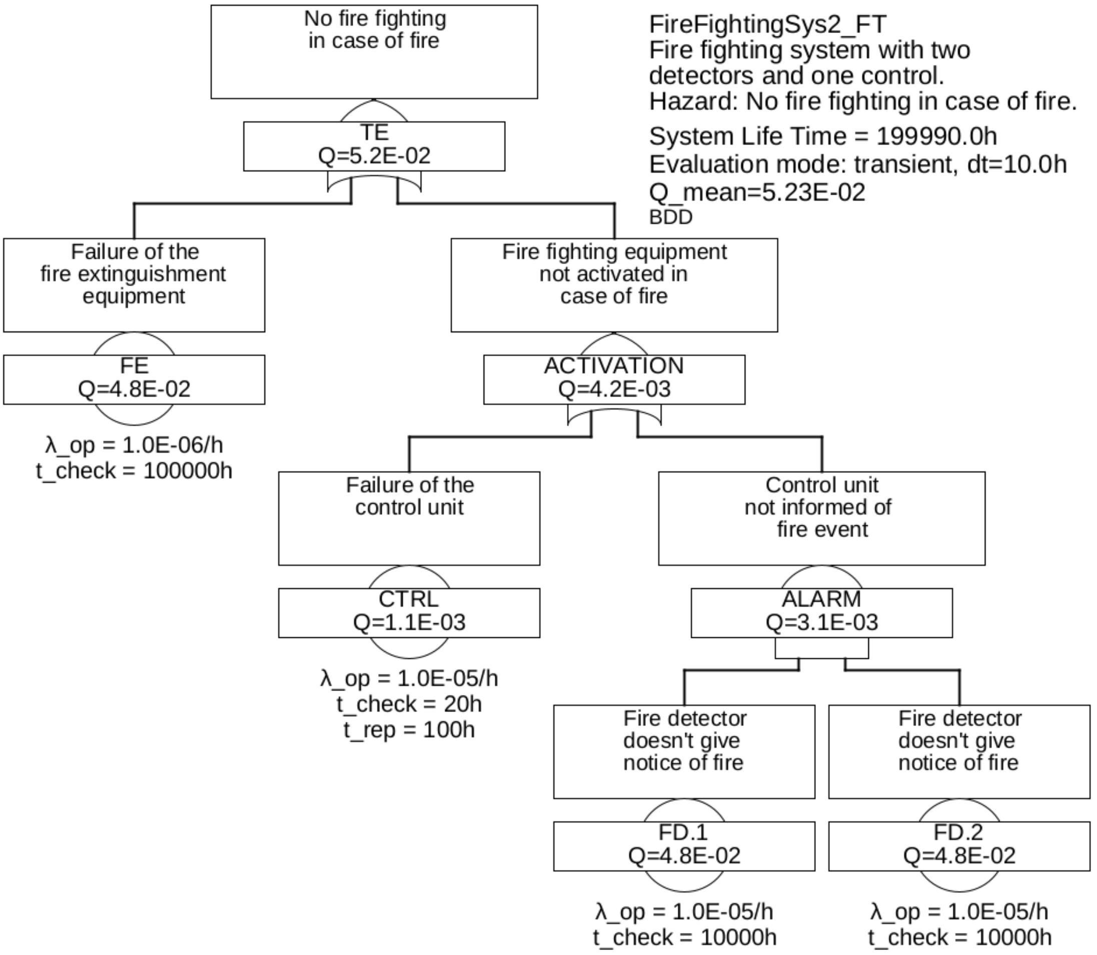

No fire fighting in case of fire
TE
Q=5.2E-02
FireFightingSys2_FT
Fire fighting system with two detectors and one control.
Hazard: No fire fighting in case of fire.
System Life Time = 199990.0h
Evaluation mode: transient, dt=10.0h
Q_mean=5.23E-02
BDD
Failure of the fire extinguishment equipment
FE
Q=4.8E-02
λ_op = 1.0E-06/h
t_check = 100000h
Fire fighting equipment not activated in case of fire
ACTIVATION
Q=4.2E-03
Failure of the control unit
CTRL
Q=1.1E-03
λ_op = 1.0E-05/h
t_check = 20h
t_rep = 100h
Control unit not informed of fire event
ALARM
Q=3.1E-03
Fire detector doesn't give notice of fire
FD.1
Q=4.8E-02
λ_op = 1.0E-05/h
t_check = 10000h
Fire detector doesn't give notice of fire
FD.2
Q=4.8E-02
λ_op = 1.0E-05/h
t_check = 10000h

Figure 16: *Fire extinguishing system with redundant sensors*

Therefore, large fault trees can practically only be calculated with BDDs, especially since already the determination of minimum cuts is practically only possible with the help of BDDs for large fault trees (even better with ternary decision diagrams).

5.1.4 Transient and steady-state computation, computing with averages

In general, to determine the average unavailability of a system, the integral must be calculated according to formula (51), as shown in example 5.1. Practically this means that the fault tree must be calculated for many time points, which can take some time for large fault trees even with modern computers. Here, of course, a possibly existing periodicity can be exploited, as also happened in example 5.1. If there is no periodicity (for example because there is at least one event without regular tests), then there will be no quasi-stationary state [10] set. In this case, the calculation must always be performed according to formula (51), i. e. numerical integration over the lifetime. Since this calculation considers also transient, i. e. non-periodic processes correctly, it is called transient

[10] quasi-stationary means, that the unavailability may fluctuate around a mean value, but the mean value does not change with time

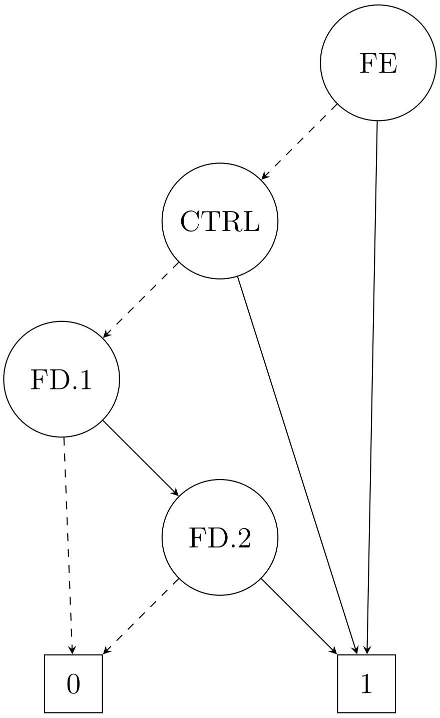


Figure 17: *BDD for the fire extinguishing system with redundant fire detectors*

calculation, in [ASTRA TM] simply time-dependent calculation.

To reduce the computation time, one can come up with the idea, to calculate the fault tree only once with the mean values of the unavailabilities of the basic events. This calculation assumes a steady-state quasi-stationary condition, and is therefore also called stationary calculation.

However, the calculation with mean values is not correct even in the steady state, because this would swap integral and product in the order, which is mathematically wrong:

$$\overline{Q_{\text{MCS}}} = \frac{1}{T_{\text{Life}}} \int_0^{T_{\text{Life}}} Q(t)\,dt = \frac{1}{T_{\text{Life}}} \int_0^{T_{\text{Life}}} \prod_{i=1}^{n} Q_i(t)\,dt \quad \neq \quad \prod_{i=1}^{n} \frac{1}{T_{\text{Life}}} \int_0^{T_{\text{Life}}} Q_i(t)\,dt = \prod_{i=1}^{n} \overline{Q_i}$$

The size of the error that occurs when calculating with mean values, depends on many parameters. In the case of two similar AND-linked events as in example 5.1, which are tested at the same time, the calculated result is about 1/3 too small:

$$\overline{Q_{\text{FD.1}}} \cdot \overline{Q_{\text{FD.2}}} \approx 4.8\text{E}{-2} \cdot 4.8\text{E}{-2} \approx 2.3\text{E}{-3}... \neq 3.1\text{E}{-3}$$

The error 1/3 comes from the integration of the quadratic term, which is responsible for the parabolic sections clearly visible in figure 14. Formula-wise this becomes particularly clear, if one uses the approximate formula $Q(t) \lessapprox \lambda \cdot t$:

$$\overline{Q_{\text{correkt}}} = \frac{1}{T} \int_0^{T} Q_1(t) \cdot Q_2(t)\,dt \approx \frac{1}{T} \int_0^{T} \lambda t \cdot \lambda t\,dt = \frac{\lambda^2}{3T} T^3 = \frac{\lambda^2 T^2}{3}$$

$$\overline{Q_{\text{wrong}}} = \frac{1}{T}\int\limits_0^T Q_1(t)\,dt \cdot \frac{1}{T}\int\limits_0^T Q_2(t)\,dt \approx \left(\frac{1}{T}\int\limits_0^T \lambda t\,dt\right)^2 = \left(\frac{\lambda}{2T}T^2\right)^2 = \frac{\lambda^2 T^2}{4}$$

For higher powers, i. e. higher order minimum cuts, the relative error becomes even larger, however, their absolute contribution is usually only small. A calculation with mean values can therefore be used in practice for rough calculations, but the final calculation should always be done according to formula (51), which makes a numerical integration necessary.

It should be noted, that a stationary calculation can also be performed with maximum values instead of mean values. In this case, the calculated unavailability is always (quite) conservative.

5.2 Calculation with Markov Models

System unavailability can also be calculated using Markov models. Markov models represent the states in which a system can be, as well as the transitions between the states. In classical Markov models, transitions are described by means of transition rates. Transitions away from the original state, in particular failures, are usually abbreviated as λ. Transitions toward the original state, i. e., measures of restoration, are usually abbreviated as μ. Thus, a Markov model is mathematically described by a linear differential equation system:

$$\dot{\vec{p}}(t) = A(t)\,\vec{p}(t) \tag{55}$$

Here $A(t)$ is the (generally time-dependent) transition matrix and $\vec{p}$ is the vector of the residence probabilities of the system states.

Since the system is in exactly one state at any time, the sum of all state probabilities must always be one:

$$\|\vec{p}(t)\| = \sum_{i=1}^{n} p_i(t) = 1 \tag{56}$$

The sum of the residence probabilities in the states $p_j(t) \in p(\vec{t})$, in which the safety function is not given, indicates the system unavailability:

$$Q(t) = \sum_{j=1}^{m} p_j(t) \tag{57}$$

The mean unavailability is again given by formula (51).

The restoration rate μ is almost always defined in the literature as the reciprocal of the mean recovery time: [11]

$$\mu \overset{\text{def}}{=} 1/\text{MTTR} \tag{58}$$

For errors that are detected by regular tests, this results in the following for the restoration rate

$$\mu = 1/\text{MTTR} = \frac{1}{0.5 \cdot T_{\text{test}}} = 2/T_{\text{test}} \tag{59}$$

[11] That this is in fact a definition and not a factually justifiable formula, becomes visible in example 5.4 with example 5.5

Example 5.4 *Figure 18 shows the Markov model for fire detection using redunant fire detectors, as considered in Example 5.1.*

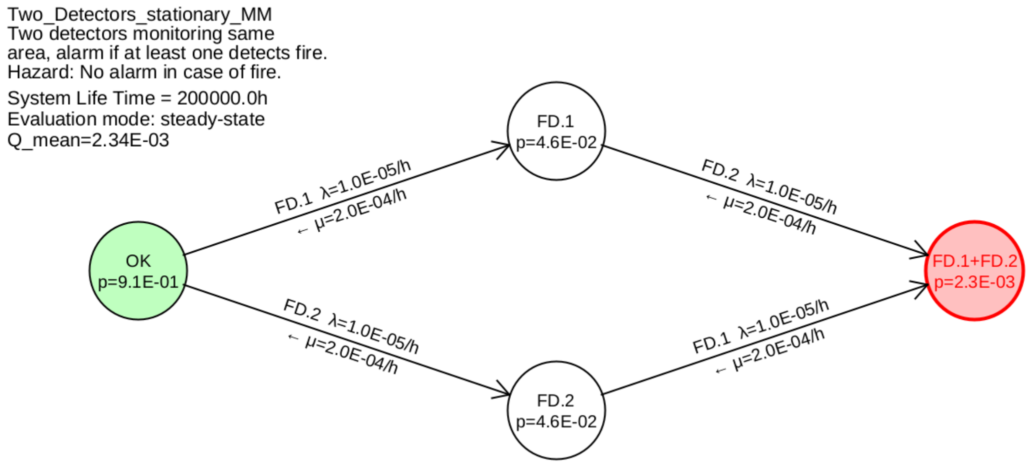

Two_Detectors_stationary_MM
Two detectors monitoring same area, alarm if at least one detects fire.
Hazard: No alarm in case of fire.
System Life Time = 200000.0h
Evaluation mode: steady-state
Q_mean=2.34E-03
OK
p=9.1E-01
FD.1
p=4.6E-02
FD.2
p=4.6E-02
FD.1+FD.2
p=2.3E-03
FD.1 λ=1.0E-05/h
← μ=2.0E-04/h
FD.2 λ=1.0E-05/h
← μ=2.0E-04/h
FD.2 λ=1.0E-05/h
← μ=2.0E-04/h
FD.1 λ=1.0E-05/h
← μ=2.0E-04/h

Figure 18: *Redudant fire detector, stationary calculation*

The failure rates λ for the fire detectors are indicated above the transition arrows in each case, the recovery rates μ below each and indicated with a small arrow for the opposite direction. [12].

With the state vector

$$\vec{p} = \begin{pmatrix} \text{OK} \\ \text{FD.1} \\ \text{FD.2} \\ \text{FD.1} + \text{FD.2} \end{pmatrix}$$

applies to the linear differential equation system

$$\begin{pmatrix} -2\lambda & \mu & \mu & 0 \\ \lambda & -\mu-\lambda & 0 & \mu \\ \lambda & 0 & -\mu-\lambda & \mu \\ 0 & \lambda & \lambda & -2\mu \end{pmatrix} \vec{p}(t) = \dot{\vec{p}}(t) \tag{60}$$

5.2.1 Stationary calculation

If every failure is detectable, there will also be a transition out of each state. Consequently, the states will be in equilibrium after an arbitrarily long time, so the time derivative of the state vector will become zero. If all detection and repair times are relatively short in relation to the lifetime of the system, the equilibrium will be practically taken after relatively short time.

[12] Often separate lines are shown for restoration, but the representation with only one line seems clearer

The residence probabilities in this stationary system state can be easily calculated, by setting $\dot{\vec{p}}(t) = 0$ and then replacing any equation by the sum of the state probabilities, which must always be one.

Since the steady state lasts forever, the transient has no significant effect on the integral in formula (51), so the mean value of the unavailability is approximately equal to the unavailability in the steady state:

$$\overline{Q_{\text{sys}}} \approx Q_{\text{stat}} \tag{61}$$

Example 5.5 *Replacing the fourth row in equation system* (60) *with the sum row, then the stationary solution is described by the following linear equation system:*

$$\begin{pmatrix} -2\lambda & \mu & \mu & 0 \\ \lambda & -\mu-\lambda & 0 & \mu \\ \lambda & 0 & -\mu-\lambda & \mu \\ 1 & 1 & 1 & 1 \end{pmatrix} \vec{p_{\text{stat}}} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

For the state vector in the steady state we get

$$\vec{p_{\text{stat}}} = \begin{pmatrix} \text{OK} \\ \\ \text{FD.1} \\ \\ \text{FD.2} \\ \\ \text{FD.1} + \text{FD.2} \end{pmatrix} = \begin{pmatrix} \dfrac{\mu^2}{\mu^2 + 2\lambda\mu + \lambda^2} \\ \dfrac{\lambda\mu}{\mu^2 + 2\lambda\mu + \lambda^2} \\ \dfrac{\lambda\mu}{\mu^2 + 2\lambda\mu + \lambda^2} \\ \dfrac{\lambda^2}{\mu^2 + 2\lambda\mu + \lambda^2} \end{pmatrix}$$

The unavailability is the residence probability of the state FD.1+FD.2, also $\overline{Q_{\text{stat}}} = \dfrac{\lambda^2}{\mu^2 + 2\lambda\mu + \lambda^2}$.

With the numerical values used for example 5.1 $\lambda = 1.0\text{E}{-5}/\text{h}$ *and* $T_{\text{test}} = 10\,000\,\text{h}$ *we get* $\mu = 2/(10\,000\,\text{h}) = 2.0\text{E}{-4}/\text{h}$ *and thus*

$$\overline{Q_{\text{stat}}} = \frac{(1.0\text{E}{-5}/\text{h})^2}{(2.0\text{E}{-4}/\text{h})^2 + 2 \cdot 1.0\text{E}{-5}/\text{h} \cdot 2.0\text{E}{-4}/\text{h} + (1.0\text{E}{-5}/\text{h})^2} \approx 0.0023$$

The mean unavailability in example 5.1 was exactly calculated to be $\overline{Q_{\text{sys}}} = 0.003\,094...$, *so the result obtained via the stationary evaluation of the Markov model is clearly too optimistic. On the one hand, this is due to the fact that formula* (58) *is only valid for continuous maintenance and repair, and formula* (59) *is always somewhat optimistic, but also because of the structure of the Markov model, which obviously does not reflect reality correctly — see the next example.*

5.2.2 Transient calculation

In many practical applications, the steady state is not even approached, because the operating time is too short. If there are failures that cannot be detected or repaired, there are even absorbing states, so the steady state is given by the accumulation of the probability of residence in one or more failure states, so that $Q(t \to \infty) = 1$ holds [13]. In this case, the stationary solution of the differential equation system is of no interest. Instead, the mean unavailability must be calculated by formula (51) during the transition from the original state to the end of the system's operating time. This requires numerical integration of the differential equation system.

Numerical integration opens up possibilities for modeling that go beyond classical Markov models. In particular, it is possible to use time-varying transition rates and even to consider transitions at specific points in time. The latter in turn enables the realistic consideration of regular tests.

Example 5.6 *Figure 19 shows a Markov model for the redundant fire detectors, in which it is taken into account that the tests, and thus the recovery, are not continuous, but occur at specific points in time. Furthermore, it is considered, that in case of defect of both fire detectors (state "FD.1+FD.2") both defects are detected at the same time and also the repair takes place at the same time, thus the system is restored to its original state.*

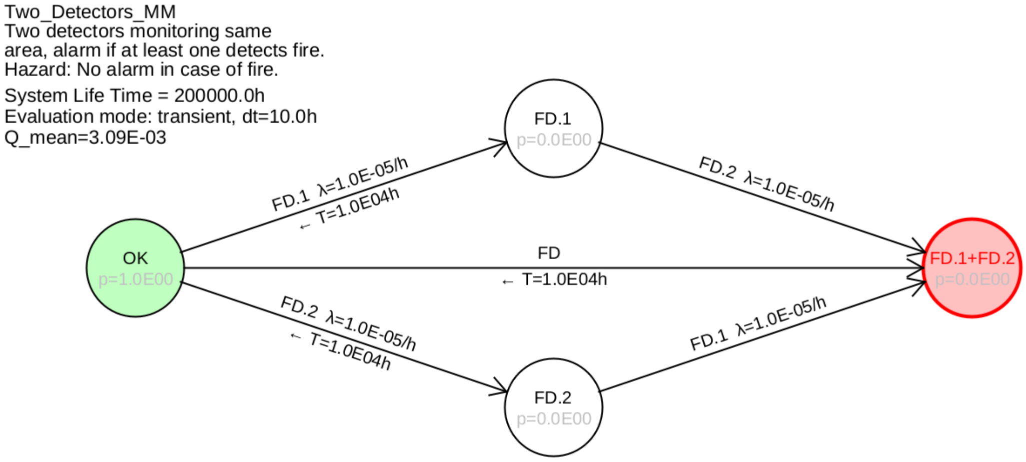


Figure 19: *Redundant fire detectors with restoration at discrete times*

Note: No failure rate is given at the transition arrow from "OK" to "FD.1+FD.2", therefore this is zero. Only the regular recovery every 10000 h is relevant here, this is under the transition arrow and is indicated with a small arrow to the left. Conversely, under the transition arrows "FD.1" and "FD.2" to "FD.1+FD.2" no restoration is stated, so this is zero.

[13] absorbing states are always failure states, otherwise the model is incorrect

The result of this modeling and calculation with an integration step size of 10 hours is $Q = 3.09\text{E}{-}3$ *and now practically agrees with the exact value.*

Classical Markov models with constant transition rates are only conditionally suitable for the calculation of unavailability, the results are usually too optimistic. Extended Markov models with discrete-time transitions allow realistic modeling and calculation and are therefore much more suitable.

It must be mentioned that the calculation of discrete-time transitions requires a sufficiently small integration step size. For small test intervals or even continuous diagnosis, constant transition rates must be used.

Example 5.7 *Figure 20 shows the Markov model for the fire extinguishing system with redundant fire detectors introduced in Example 5.3. The recovery of the control CTRL is treated as a continuous transition, since the integration step size of 10 h is only slightly smaller than the test interval (20 h). The result is consistent with that of the fault tree.*

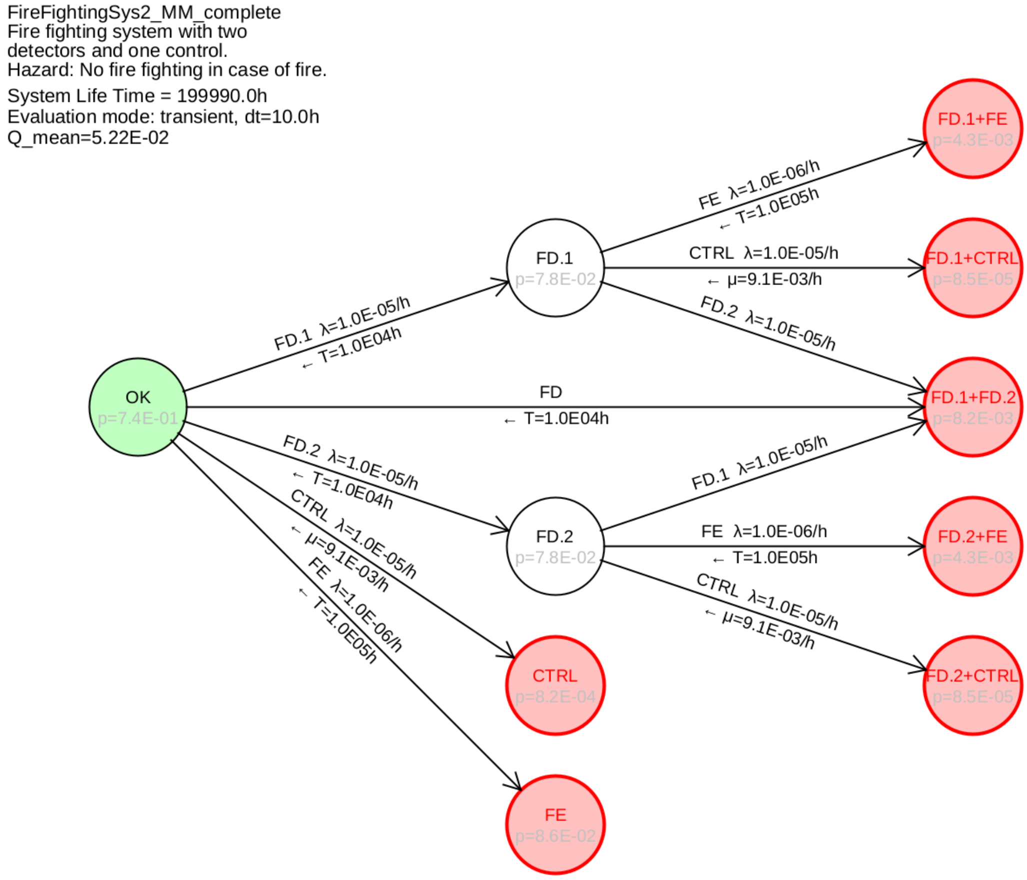


Figure 20: *Fire fighting system. State probabilities are shown for T=199990 h, i. e. just before the next test would occur. Thus, they present the maximum unavailabilities.*

6 Failure rate of complex functions

The failure rate is the essential quantity for safety functions, that are required continuously or at least frequently (quasi-continuously). Examples of systems that implement continuously required safety functions, are aircraft engines (shall always provide the required thrust and, most importantly, shall not falsely stall), position control systems (shall always ensure the specified position), drive controls (shall always provide required torques, speeds or positions, or shall not start untimely), railroad signaling systems (shall never indicate a too permissive signal term or give a too permissive drive command) but also airbag controls (shall never falsely trigger the airbag), ABS controls (shall never reduce brake pressure too much), Train door controls (shall never open the door at the wrong time). As soon as the safety function fails there is an immediate dangerous situation. The word "immediate" does not mean, that damage must necessarily occur, but only, that under normal external conditions, damage is not improbable. [14].

Examples of systems that implement quasi-continuously required safety functions, include aircraft landing gears (only need to function during landing, but landing is inevitable), brakes of all vehicles (need to function only when brakes are requested, but the request is almost certain to come – only in exceptional cases coasting to standstill will be possible).

The principle structure of such safety functions is shown in Figure 21.

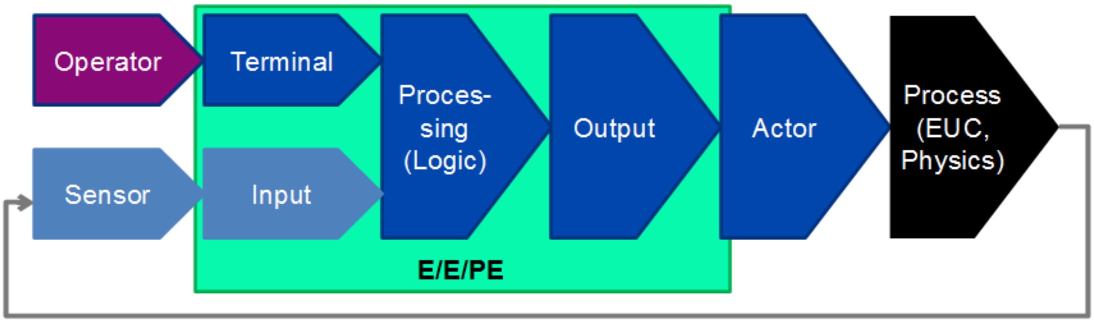


Figure 21: *Typical architecture of safety functions with continuous demand*

Characteristically, a failure of the safety function directly affects the behavior of the physical process (which is given, for example, by the equations of motion of the vehicle, the aircraft, of the machine or the reaction dynamics of the chemicals and apparatuses) and thus leads to the hazard – regardless of whether the damage occurs immediately or after a foreseeable time.

For continuous safety functions, the concept of process fault tolerance time (PFTT, also called process safety time) is existential: This is the time for which the safety function may be violated, without this resulting in a hazard. In the case of a highly dynamic drive control system or the attitude control system of a fighter jet, this is a maximum of

[14] In contrast to safety functions with rare requests, which are only needed at all in the case of an uncommon external condition (request)

a few milliseconds, in the case of a brake, it may be a few seconds, in the case of the fuel supply of a large power plant, perhaps a few minutes. Any diagnostic measures that may be in place must detect the fault within this time and initiate an adequate response, for example, initiate a safety shutdown or isolate the defective control or actor and activate a redundant control path. A mere error message to the operator is usually not sufficient for continuous or quasi-continuous safety functions, since the operator usually cannot restore the function before the damage occurs.

The failure rate one will experience for a system that is operated over a lifetime T is given by the number of failures that can be seen during the lifetime T divided by this time, see formula (62) which is identic to formula (28):

$$\overline{h_{\text{sys}}}(T) = \frac{N_{\text{sys}}(T)}{T} = \frac{1}{\text{MTTF}(T)} \tag{62}$$

The mean time between two failures MTTF [15] can be determined by equation (28), given the failure density function $f(t)$:

$$\text{MTTF}(T) = \frac{\int\limits_0^T t \cdot f(t)\, dt + T}{F(T)} - T \tag{63}$$

The failure density function $f(t)$ can be calculated for any particular instance of time t by fault trees or transient evaluation of Markov models.

In [IEC 61508] this mean value $\overline{h}$ is called Probability of Failure per Hour (PFH for short). [16]. This formula is valid for arbitrary failure rate or failure density function, no matter whether the system will probably never fail or probably fail several times during lifetime, and no matter whether the system or parts of it are periodically inspected and repaired.

At the top level, $\overline{h_{\text{sys}}}$ represents the hazard rate, often abbreviated as HR (for hazard rate) (cf. [EN 50126]). If the system under consideration is only a sub-function of a safety function, $\overline{h_{\text{sys}}}$ is accordingly called Functional Failure Rate (FFR).

$\overline{h_{\text{sys}}}$ is the relevant measure of safety for all safety functions, the failure of which can lead to damage without further conditions (i. e., safety functions with continuous or at least frequent demand).

Remark: Many controllers perform both continuous safety functions and rarely required ones. In this case, the control system must take into account both the unavailability in

[15] One might expect to read the term MTBF here. That would in fact be more correct liguistically, but unfortunately the term MTBF is defined with a different meaning in literature and cannot be used here, therefore. On the other hand, the thoughts and formulas stated in section 3 are valid as well for systems consisting of many components and tests and repairs, thus there is no reason to use a different term here.

[16] Note: Some formulas in the informative Appendix B in [IEC 61508-6] are inconsistent with this, however, the meaning of PFH as a synonymous term to $\overline{h}$ as defined here is obvious from the rest of the standard and is the only reasonable definition

the request case $\overline{Q}$ as well as the frequency of a wrong command to the actuators $\overline{h}$ must be determined. [17].

6.1 Calculation with fault trees

The calculation of the failure rate $\overline{h}$ is much more difficult than the calculation of the unavailability $\overline{Q}$, both in terms of establishing a correct fault tree and in terms of the actual mathematical calculation. Nevertheless, for most safety functions, fault tree analysis is a suitable method for determining the failure rate, and often the only practicable method of modeling. Unfortunately, however, there is no standardization for this [18] although the essential mathematical principles are already mentioned in [NUREG]. Therefore, it is essential that the analyst familiarizes himself intensively with the properties and peculiarities of the tool used, and, in case of doubt, to convince himself of the correct function of the tool by means of simple tests. The following examples can be the basis of such tests.

6.1.1 System without redundancies

In the simplest case, the safety function is realized by a number n of components, which are all mandatory for the safety function. If one component fails, the safety function fails. The fault tree consists only of OR gates.

Example 6.1 *The fault tree shown in Figure 22 describes such a system, which consists of the components sensors, control and actuators. Here it is assumed that the system must run continuously, there is no possibility of an emergency shutdown in case of detected errors. This is often the case, for example, an aircraft cannot simply be brought to a safe state if the speed sensor system is detected as faulty, because this is absolutely necessary for the flight to continue until landing.*

If one of these n components fails in a dangerous way [19], the safety function is no longer guaranteed. The minimal cuts are obvious: {SENS}, {CTRL}, {ACTOR}.

For the total failure rate, the formula already known from section 3 applies

$$h(t) = \sum_{i=1}^{n} h_i(t) \tag{64}$$

Since every fault leads directly to failure, neither system lifetime nor fault detection or repair times play a role, but only the failure rates of the components.

If we assume constant failure rates for all components, the above formula also gives the average failure rate, with the values given in the fault tree thus $h(t) = \mathrm{const} = \overline{h} =$

[17] In general, two different fault trees or Markov models are necessary for this, since in particular the diagnosis concerning $\overline{Q}$ differs from that for $\overline{h}$, and therefore different basic events (based on a different FMEDA) are needed, and often also different gates

[18] [EN 61025] does not specify how fault trees can be used to calculate failure rates – neither in terms of modeling nor in terms of calculation.

[19] see later examples for dangerous and non-dangerous failures

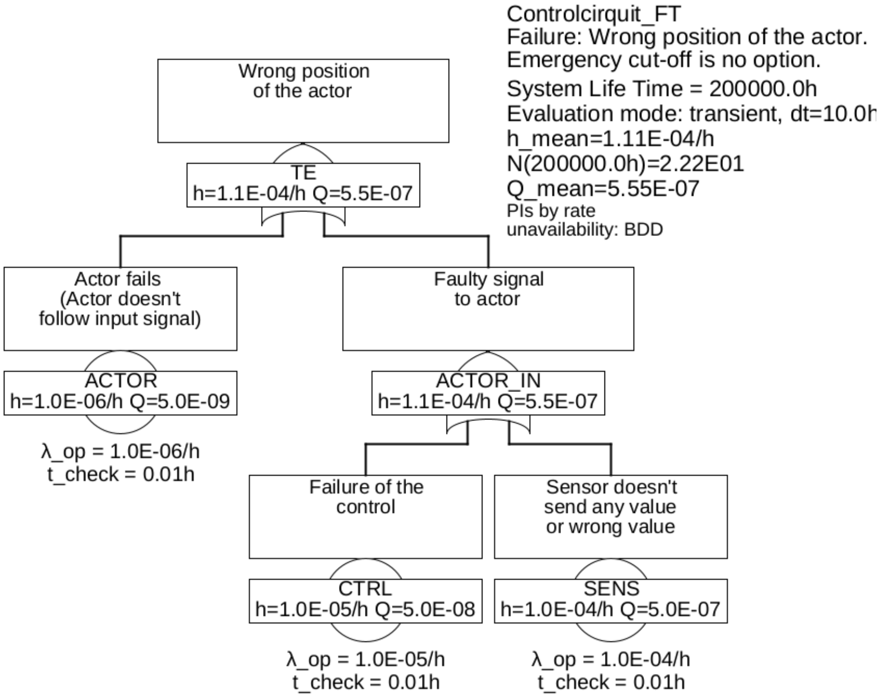


Figure 22: *Fault tree of a simple safety function with continuous demand*

$1.0\text{E}{-}6/\text{h} + 1.0\text{E}{-}5/\text{h} + 1.0\text{E}{-}4/\text{h} = 1.11\text{E}{-}4/\text{h}.$

This example was undoubtedly trivial, and hardly anyone would think of to construct a fault tree (or a Markov model) for such a system.

6.1.2 System with redundancies

Fault trees only become really interesting and almost indispensable as a model for systems with redundancies (multi-channel). In the case of redundancies, not every single failure leads to the failure of the safety function, the fault tree will therefore contain at least one AND gate and there will be at least one minimum cut, which contains more than one basic event, i. e. has an order greater than one.

Example 6.2 *In example 6.1 the sensor system is obviously a weak point. Therefore, two sensors will now be used in a redundant arrangement, i. e. in such a way that both sensors measure the same physical quantity. As already in example 6.1 let it be assumed, that the system must be running, there is no possibility of an emergency shutdown in case of detected errors.*

If a sensor delivers no values at all or obviously wrong values, the measured value of the other sensor can now be used. However, if it is not clear which of the two sensors is defective, the controller still cannot calculate a correct signal for the actor. The same also applies in the case that one sensor is known to be defective, and now the second one fails before the first one has been repaired.

The sensors must therefore now be distinguished with regard to their failure modes: There are defects of the sensors which can be detected by the control system (SENS_ DET, such as wire breakage), and those which cannot be detected by the controller (SENS_ UNDET). The corresponding fault tree is shown in figure 23.

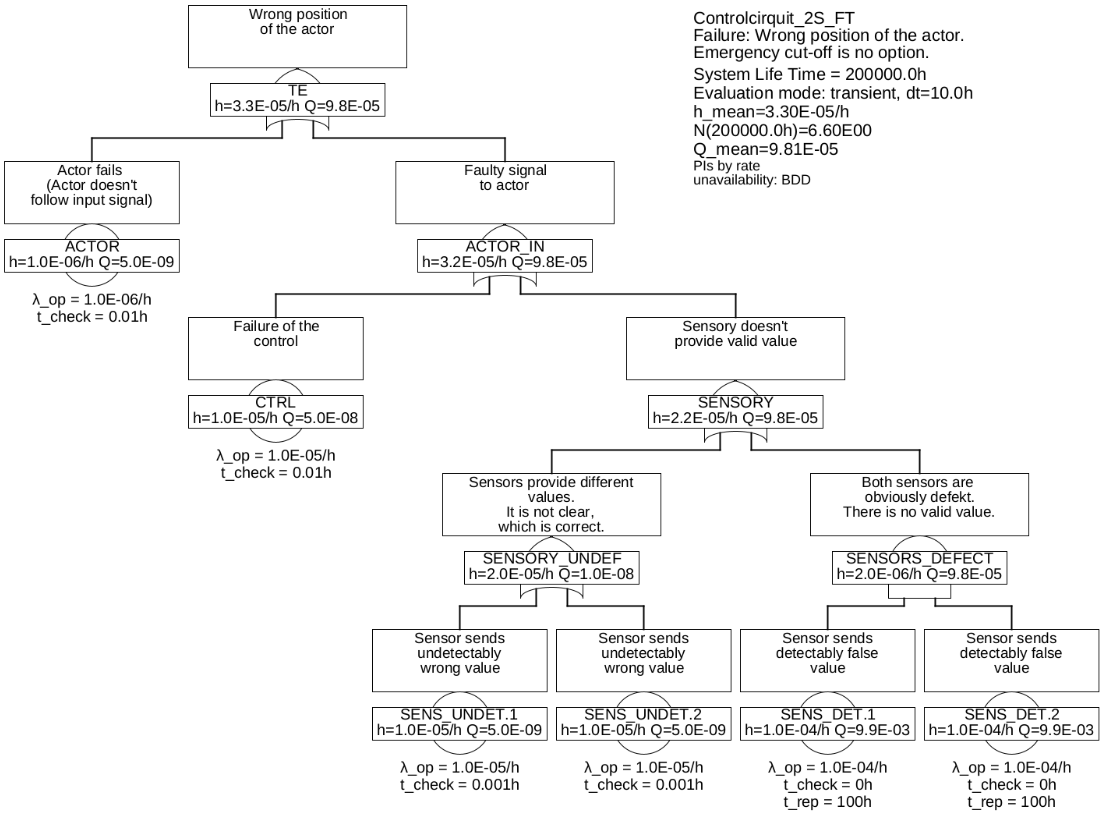


Figure 23: *Fault tree of a safety function with continuous demand and redundant sensors*

The minimum cuts are:

- *{AKTOR}*
- *{CTRL}*
- *{SENS_ UNDET.1}*
- *{SENS_ UNDET.2}*
- *{SENS_ DET.1& SENS_ DET.2}*

The question now is how to calculate the occurrence rate $h_{\text{MCS}}(t)$ of the minimal cut {SENS_ DET.1 & SENS_ DET.2}. The statement of this minimum cut is the following:

1. *Sensor 1 is known to be defective (i. e. not available, $Q_{\text{SENS\_DET.1}}$), and now sensor 2 also fails (with failure rate $\lambda_{\text{SENS\_DET.2}}$)*
   OR

2. Sensor 2 is known to have failed (so not available, $Q_{\text{SENS\_DET.2}}$), and now sensor 1 also fails (with failure rate $\lambda_{\text{SENS\_DET.1}}$).

Therefore, the minimum cut can be calculated by [20]

$$h_{\text{MCS}}(t) \lessapprox \lambda_{\text{SENS\_DET.1}} \cdot Q_{\text{SENS\_DET.2}}(t) + \lambda_{\text{SENS\_DET.2}} \cdot Q_{\text{SENS\_DET.1}}(t)$$

For the events SENS_DET.x the unavailability is needed as well. According to formula (48)*, this generally depends on the time to detection and the repair time. Since in these events only the failures are considered, which are immediately detectable, the detection time is modeled to zero. The repair time is the time for which the other sensor must hold out, either until a safe condition is reached (e. g. the aircraft has landed) or until a repair has been made while the aircraft is in operation. It is assumed here to be 100 h.*

With formula (47) *applies*

$$\overline{Q} \approx \lambda \cdot \text{MRT} = 1\text{E}{-4}/\text{h} \cdot 100\,\text{h} = 0.01$$

and thus for the minimum cut

$$h_{\text{MCS}}(t) = \overline{h_{\text{MCS}}} = 1\text{E}{-4}/\text{h} \cdot 0.01 + 1\text{E}{-4}/\text{h} \cdot 0.01 = 2\text{E}{-6}/\text{h}$$

Since the failure rates of the other minimum cuts are also constant, the total failure rate of the system is therefore

$$h_{\text{sys}} = 1\text{E}{-6}/\text{h} + 1\text{E}{-5}/\text{h} + 2 \cdot 1\text{E}{-5}/\text{h} + 2\text{E}{-6}/\text{h} = 3.3\text{E}{-5}/\text{h}$$

The formula used in the example for the occurrence rate of a minimum cut can be extended to minimum cuts of any order $m = n_{\text{Lit}}$:

$$\begin{aligned} h_{\text{MCS}}(t) \lessapprox\; & h_1(t) \cdot Q_2(t) \cdot Q_3(t) \cdot \ldots \cdot Q_m(t) \\ & + h_2(t) \cdot Q_1(t) \cdot Q_3(t) \cdot \ldots \cdot Q_m(t) \\ & + \ldots \\ & + h_m(t) \cdot Q_1(t) \cdot Q_2(t) \cdot \ldots \cdot Q_{m-1}(t) \\ & = \sum_{j=1}^{m} \left(h_j(t) \cdot \prod_{k=1,k\neq j}^{m} Q_k(t) \right) \end{aligned} \tag{65}$$

Formula (65) is correct only for $Q_i \to 0$. The exact formula for two events with arbitrarily large unavailabilities is derived in Example 6.7. However, the error only becomes significant for large unavailabilities, so for correctly designed systems (i. e., when the detection and repair times are much smaller than the MTTF). Moreover, the formula is always conservative, so that even for incorrectly designed systems the failure rate is not estimated too small.

[20] for exactness, see comment on formula (65)

For the system failure rate (or more generally: the occurrence rate of the top event), the following applies

$$\begin{aligned} h_{\text{sys}}(t) &\lessapprox h_{\text{MCS1}}(t) + h_{\text{MCS2}}(t) + \ldots + h_{\text{MCSn}}(t) \\ &= \sum_{i=1}^{n_{\text{MCS}}} \left(\sum_{j=1}^{n_{\text{Lit,MCS}_\text{i}}} \left(h_j(t) \cdot \prod_{k=1, k \neq j}^{n_{\text{Lit,MCS}_\text{i}}} q_{i,k}(t) \right) \right) \end{aligned} \tag{66}$$

This formula is valid exactly only, if all minimum cuts consist of only one event. Otherwise it can be that the minimum cuts overlap each other, so that the result is somewhat too large. This can be taken into account by disjunction of the minimum cuts as in the calculation of the system unavailability. However, this operation is very time-consuming and reaches the performance limits of modern PCs for large fault trees even when BDDs are used.

6.1.3 Single Channel Fail-Safe

In the last example, it was assumed that the process cannot simply be switched off and brought into a safe state, if an fault is detected. For many processes, this is quite possible, for example, a train can still be brought to a safe stop if the speed measurement fails. It is not even necessary to know exactly which component has failed, but it is also possible to request the safe state in case of inconsistencies of any kind. This will be illustrated in the next example.

Occasionally one speaks of a fail-safe architecture, if the control system is able to to bring the process into a safe state in case of detected failures. However, the term is extremely fuzzy, because there's no definition which failure modes or what proportion of dangerous failure modes must be detected, in order for a system to be called "fail-safe". [21].

Example 6.3 *In this example it is assumed that the control system controls the actor in such a way, that the process goes to a safe state (for example, switching off the power supply or applying the brakes).*

In this case, the detectable failures of the sensors SENS_ DET are no longer dangerous and can therefore be ignored. And also the situation that a sensor delivers wrong values, but it is not clear which one, is not critical, because in case of a discrepancy, the control system will also control the actuator in such a way that the process reaches a safe state.

The only dangerous case regarding the sensors is the case, that both sensors deliver unrecognizable wrong values at the same time, i. e. the failures SENS_ UNDET.1 and SENS_ UNDET.2 are present at the same time, and the wrong values are so similar, that they are not recognizable as faulty by the control. So the two failures would not only have to be similar in detail, but also happen so fast one after the other, that this would not be visible to the control system, i. e. typically within the process fault tolerance time (PFTT). One may be tempted to assume that such a case will practically never occur.

[21] A complete detection and handling of all critical faults is commonly considered impossible

In fact, this case is unlikely to occur due to independent random events, but experience shows that you should always assume the existence simultaneous failures of redundant components due to external circumstances that have not been taken into account. Flight AF447 or the Fukushima disaster are well-known examples of this. In order to model reality as correctly as possible, one should assume a factor for the proportion of common failures due to external circumstances that are not known or not explicitly taken into account. In [IEC 61508] this is called Common-Cause-Factor and is denoted by β. In addition, a guideline is given in [IEC 61508] which can be helpful in estimating this factor. Figure 24 shows the fault tree created in this way. Here $\beta = 2\%$ is assumed between the events SENS_ UNDET.1 and SENS_ UNDET.2 and therefore they are renamed SENS_ UNDET_ CC.

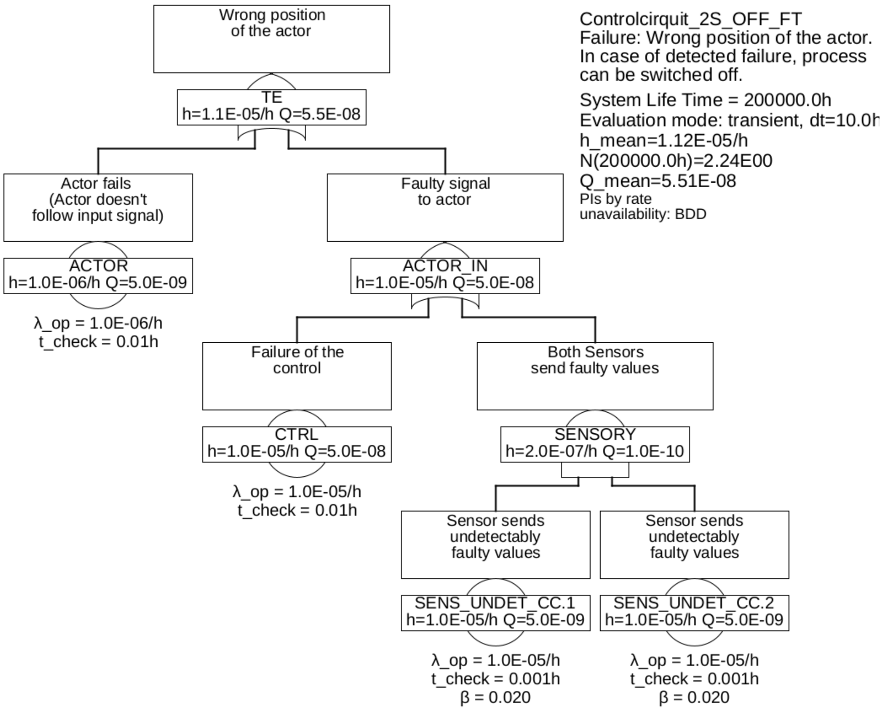


Figure 24: *Fault tree of a safety function with continuous demand, redundant sensors and easily accessible safe state*

The minimum cuts and their partial entry rates are listed in table 1.

Table 1: *Minimum cuts for example 6.3*

Minimum cuts	Occurrence rate $\overline{h}$
CTRL	1.0E-05/h
AKTOR	1.0E-06/h
SENS_UNDET_CC.COM	2.0E-07/h
SENS_UNDET_CC.1 & SENS_UNDET_CC.2	9.604E-14/h

In this table, SENS_ UNDET_ CC.COM denotes the common cause event, that both sen-

sors fail simultaneously in an undetectable manner (due to an external event acting simultaneously). Its occurrence rate is $\beta \cdot \lambda_{\mathrm{SENS\_UNDET\_CC}} = 0.02 \cdot 1.0\mathrm{E}{-5}/\mathrm{h} = 2.0\mathrm{E}{-7}/\mathrm{h}$.

The failure rate of the sensor system (gate "SENSORY") thus changes from 2.2E−5/h *to* 2.0E−7/h.

In general: In modeling, failures, which go directly to the safe side or in case whose occurrence some measure will be taken, that is always available and most likely to bring the process in a safe state, can be omitted. However, it is essential to check whether these measures are actually available and suitable, to achieve a safe state (of the process!) in all cases. In order to be able to carry out this check, it is imperative that all assumed measures and safe states are mentioned and, especially in the case of generic components, are included in the documentation of the product intended for the customer.

For events below AND gates, proper modeling of unavailability is required. This is based on fault detection and recovery times. In addition, it may be necessary to consider simultaneous failures of redundant components, either by common cause factors β or by an explicit basic event.

For correct modeling of diagnostics and inspection, you need knowledge of the physical or technical process in which the safety function is embedded. If this knowledge is not available (e. g. in case of generic safety systems), all assumptions must be documented as conditions regarding the validity of the fault tree and, if necessary, passed on to customers.

6.1.4 Modeling regular tests and diagnosis

In example 6.3 it was assumed, that the process can easily be brought into a safe state. The safety is largely determined by the failure rate of the control system. It is now obvious to add a diagnostic unit which monitors the activity of the control system. If the diagnostic unit detects a fault, the process (e. g. the machine or the process plant), is ordered to a safe state (standstill, idle) via an additional, simple binary emergency actuator (e. g., a relay or a shut-off valve). The basic architecture of such controls or regulators is shown in Figure 25. It is often referred to as single-channel with diagnostics, in short 1oo1D (for 1-out-of-1).

The systematic quality of the diagnostic unit, i. e. the proportion of failures detectable in time by the diagnosis in the total (dangerous) failure modes of the diagnosed component, is called the Diagnostic Coverage (DC). Assuming the diagnostic unit monitors the supply voltages, the processor clock and the regular execution of the critical software tasks (watchdog function), but not the logic of the computing units, the memories, or the input/output units (A/D and D/A converters etc.) of the controller, according to tables in relevant standards, you might get a diagnostic coverage of 70%.

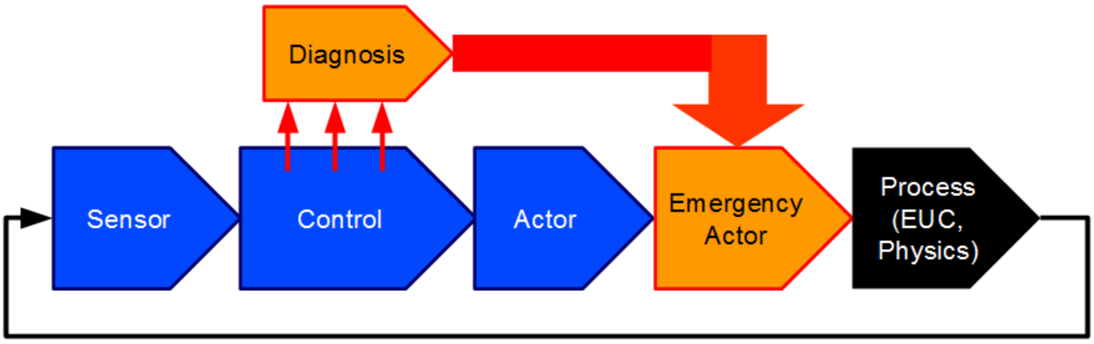


Figure 25: *Control loop with diagnostics and emergency actor for shutdown*

There are now at least three ways to model the diagnosis:

1. One decreases the failure rate of the diagnosed component (here CTRL) according to the diagnostic coverage. So the diagnosis does not appear explicitly in the fault tree. The advantage is obviously a simple fault tree. The disadvantage is that the diagnosis is not explicitly mentioned as a safety-relevant component, so it is implicitly assumed that the diagnostics will always work. In fact, however, also the diagnostics and especially the shutdown path is subject to random failures and must therefore be tested regularly in most applications.

2. One divides the failures modes of the diagnosed component according to the diagnostic coverage to two basic events, one for the failures not detectable by the diagnosis (CNTRL_UNDET), one for the detectable ones (CTRL_DET).

   The failure of the diagnostics itself is also modeled as a basic event (DIAG) with a specific failure rate and test interval. The event for the detectable failures is connected to the diagnostics using an AND gate, cf. Figure 26 left.

3. As before, but the basic event of the diagnostic failure is defined as a condition (DIAG_COND), and connected by means of INHIBIT gate to the failure to be diagnosed CTRL_DET), cf. figure 26 on the right.

The difference between variants 2 and 3 is the following: With the AND gate, formula (65) applies. Thus, when linking CTRL_DET and DIAG, the result is

$$h_{\text{AND}} = h_{\text{CTRL\_DET}} \cdot Q_{\text{DIAG}} + h_{\text{DIAG}} \cdot Q_{\text{CTRL\_DET}}$$

But this does not reflect the reality, because the failure rate of the diagnosis h_{DIAG} has no influence on the occurrence rate of the system failure, but only its unavailability Q_{DIAG}. Thus, as long as Q_{DIAG} is constant, the failure rate of the link should also remain the same. This is achieved by marking an event as a condition, and using INHIBIT to link to the "normal" parts of the fault tree described by occurrence rates h and unavailabilities Q. Thus, the occurrence rate of the condition is ignored (as if it were zero), and thus the second summand in previous formula becomes zero – exactly what is desired here:

$$h_{\text{INHIBIT}} = h_{\text{CTRL\_DET}} \cdot Q_{\text{DIAG}} + 0 \cdot Q_{\text{CTRL\_DET}}$$

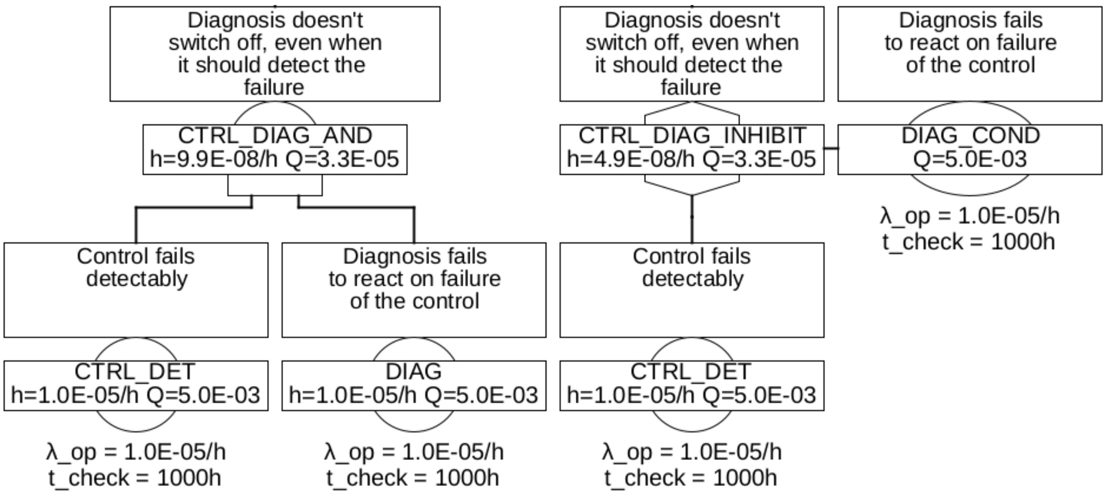


Figure 26: *And gate and inhibit gate with condition*

Annotation: The distinction between AND and INHIBIT may be handled with different strictness in different tools, since there is no standardization for this use case either.

Remark: Often, a conditional event is also used to describe the probability, that certain boundary conditions exist. In this case, this probability is entered directly as a constant, see appendix A.3.

Remark: Conditions can be linked together (e. g. by means of AND or OR gates), before they are connected as a total condition to an INHIBIT gate.

Example 6.4 *The figures 27 and 28 represent the fault tree for an architecture, in which the control system is diagnosed and, in the event of a detectable failure, the process is shut down.*

The fault tree was split into two partial fault trees to save space. The partial tree for the gate "EM_ OFF" was connected to the parent fault tree by means of a transfer gate connected to the parent fault tree. The transfer gate itself has no effect on the calculation, it is only a reference to a branch elsewhere.

It is assumed that the shut-down via the emergency actuator also takes place, if the controller detects that the main actuator is defective. In many applications, it can be easily recognized in time, that the controlled variable increasingly deviates from the set-point, or the control system reads back the manipulated variable (e. g. position of the actor) via an additional input or sensor. The controller can report an actuator fault to the diagnostics simply by putting itself into a failure state that can be clearly recognized by the diagnostics (e. g. no longer resets a watchdog or stops bus communication).

The minimum cuts are listed in table 2.

As soon as there are minimal cuts with more than one event, the unavailability of the events contained therein is relevant, and thus the fault detection and repair times are essential. Therefore, these must be correctly selected and justified, as shown in table 3.

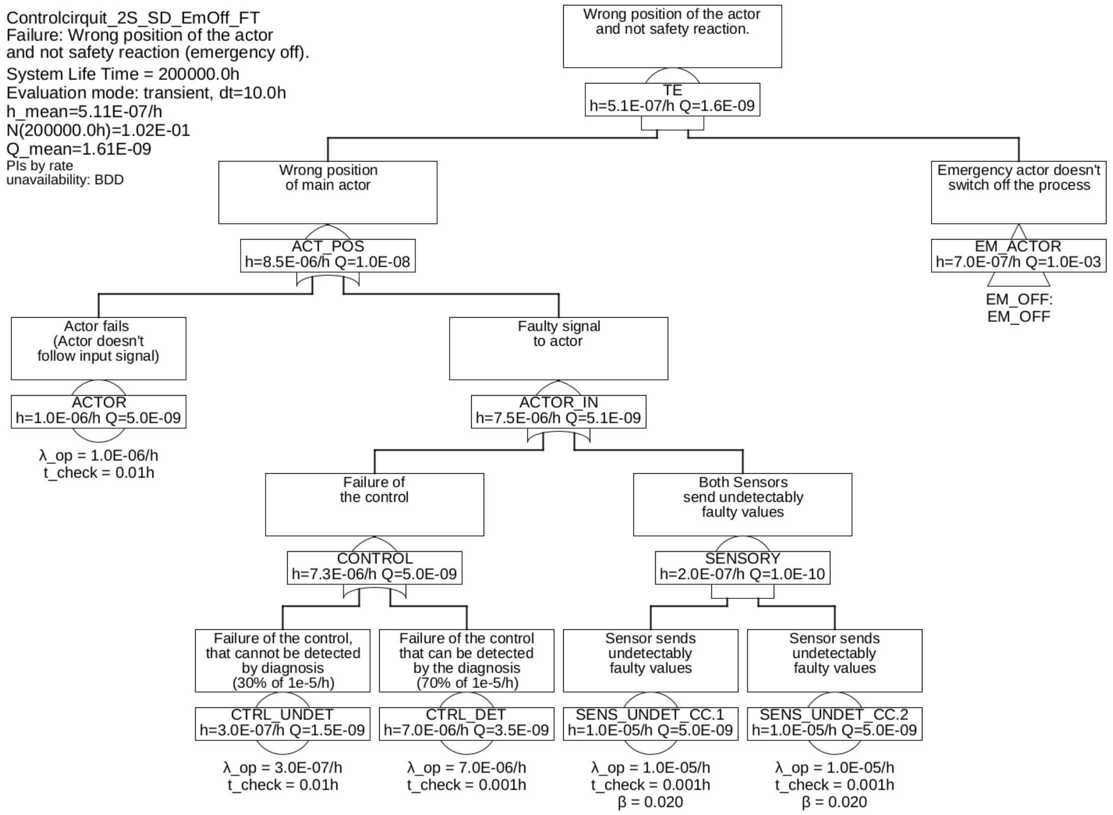


Figure 27: *Control loop with diagnostics and emergency shutdown*

Table 2: *Minimum cuts for example 6.4*

Minimum cuts	**Occurrence rate $\overline{h}$**
CTRL_UNDET	3.0E-07/h
SENS_UNDET_CC.COM	2.0E-07/h
CTRL_DET & EM_ACTOR	6.988E-09/h
CTRL_DET & DIAG	3.495E-09/h
ACTOR & EM_ACTOR	9.983E-10/h
SENS_UNDET_CC.1 & SENS_UNDET_CC.2	9.604E-14/h

The process fault tolerance time was assumed to be 0.01 h.

The occurrence rate of dangerous failures of the system is now only 5.1E-7/h and is largely determined by the undetected errors of the control system. Further improvements could be achieved by using special safety processors (for example dual-core processors in lock-step mode) and special memory (ECC).

6.1.5 Two-Channel Fail-Safe

The system considered in Example 6.4 is sometimes referred to as a fail-safe single-channel system with diagnostics (1oo1D).

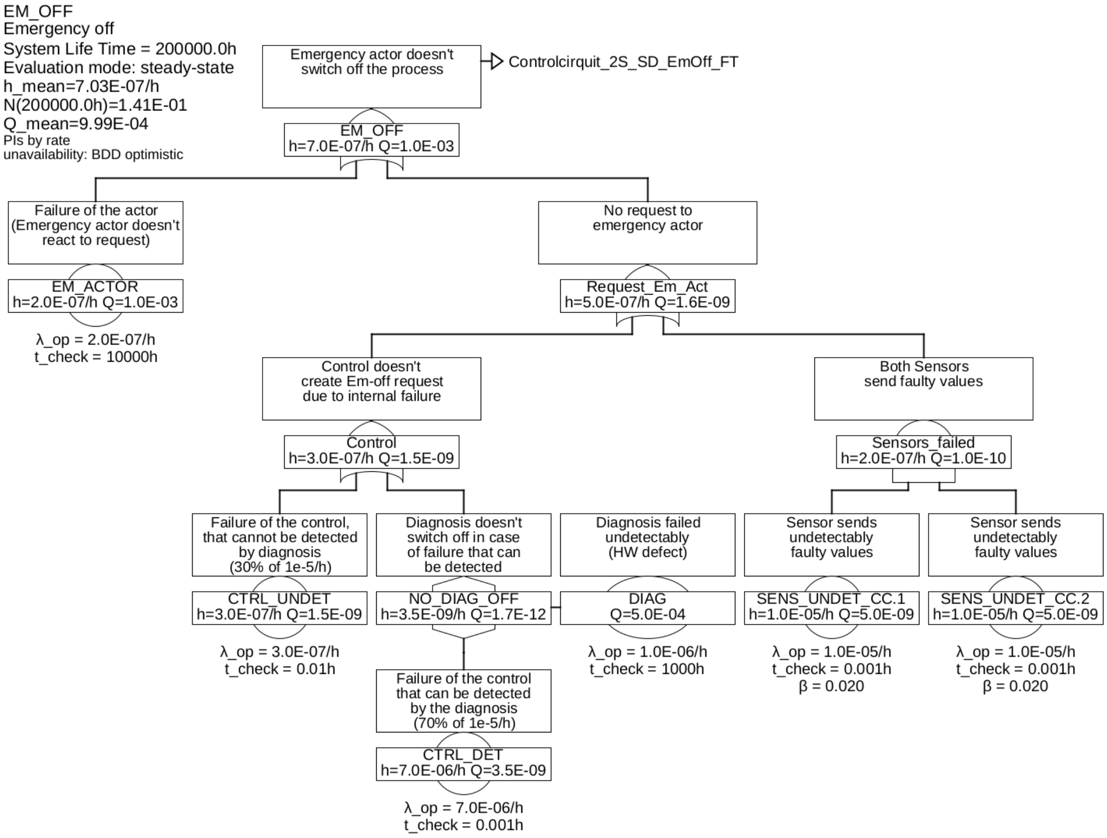

EM_OFF
Emergency off
System Life Time = 200000.0h
Evaluation mode: steady-state
h_mean=7.03E-07/h
N(200000.0h)=1.41E-01
Q_mean=9.99E-04
PIs by rate
unavailability: BDD optimistic
Emergency actor doesn't switch off the process
Controlcirquit_2S_SD_EmOff_FT
EM_OFF
h=7.0E-07/h Q=1.0E-03
Failure of the actor (Emergency actor doesn't react to request)
EM_ACTOR
h=2.0E-07/h Q=1.0E-03
λ_op = 2.0E-07/h
t_check = 10000h
No request to emergency actor
Request_Em_Act
h=5.0E-07/h Q=1.6E-09
Control doesn't create Em-off request due to internal failure
Control
h=3.0E-07/h Q=1.5E-09
Both Sensors send faulty values
Sensors_failed
h=2.0E-07/h Q=1.0E-10
Failure of the control, that cannot be detected by diagnosis (30% of 1e-5/h)
CTRL_UNDET
h=3.0E-07/h Q=1.5E-09
λ_op = 3.0E-07/h
t_check = 0.01h
Diagnosis doesn't switch off in case of failure that can be detected
NO_DIAG_OFF
h=3.5E-09/h Q=1.7E-12
Failure of the control that can be detected by the diagnosis (70% of 1e-5/h)
CTRL_DET
h=7.0E-06/h Q=3.5E-09
λ_op = 7.0E-06/h
t_check = 0.001h
Diagnosis failed undetectably (HW defect)
DIAG
Q=5.0E-04
λ_op = 1.0E-06/h
t_check = 1000h
Sensor sends undetectably faulty values
SENS_UNDET_CC.1
h=1.0E-05/h Q=5.0E-09
λ_op = 1.0E-05/h
t_check = 0.001h
β = 0.020
Sensor sends undetectably faulty values
SENS_UNDET_CC.2
h=1.0E-05/h Q=5.0E-09
λ_op = 1.0E-05/h
t_check = 0.001h
β = 0.020

Figure 28: *Control loop with diagnostics and emergency shutdown, sub-tree for emergency shutdown*

Table 3: *basic events for example 6.4*

Event	**Fault detection means**	**Fault detection time**
CTRL_UNDET	system failure, single fault	irrelevant
CTRL_DET	diagnosis	0.001 h
EM_ACTOR	annual test	approx. 10000 h
DIAG	switch-on self-test after monthly maintenance/cleaning	approx. 1000 h
ACTOR	control (unexpected process behavior)	0.01 h
SENS_UNDET_CC	a) difference of sensors	immediately (0.001 h)
SENS_UNDET_CC	b) Simultaneous failure of both sensors: considered via common cause β, single failure	irrelevant

Controllers for high safety requirements are often built up from two individual controllers of the same type, each of which is provided with its own diagnostics. If each of the controls is capable of putting the process to a safe state in the event of a detected fault, this is sometimes referred to as a two-channel fail-safe system, or 1-out-of-2 system with diagnostics, or 1oo2D for short. However, one should use these designations with caution, as they are not harmonized and are used differently and even contradictory in the literature. [22].

Example 6.5 *The fault tree of a two-channel control system, consisting of the sensors already known from the previous examples, which is used jointly by two controllers, each with its own diagnostics and actuator, is shown in figure 29 with the underlying tree shown in Figure 30. Since the channels have the same structure, only the partial fault tree of the first channel is shown.*

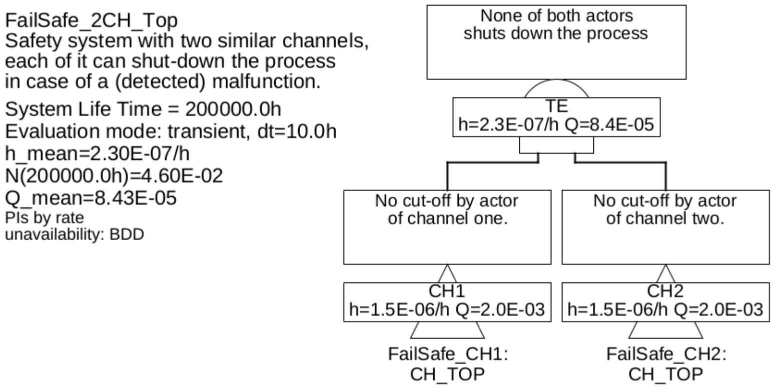

FailSafe_2CH_Top
Safety system with two similar channels,
each of it can shut-down the process
in case of a (detected) malfunction.
System Life Time = 200000.0h
Evaluation mode: transient, dt=10.0h
h_mean=2.30E-07/h
N(200000.0h)=4.60E-02
Q_mean=8.43E-05
PIs by rate
unavailability: BDD
None of both actors shuts down the process
TE
h=2.3E-07/h Q=8.4E-05
No cut-off by actor of channel one.
No cut-off by actor of channel two.
CH1
h=1.5E-06/h Q=2.0E-03
CH2
h=1.5E-06/h Q=2.0E-03
FailSafe_CH1: CH_TOP
FailSafe_CH2: CH_TOP

Figure 29: *Top tree of a homogeneous-redundant control system with safety shutdown in case of detected fault*

Each controller can set the process to a safe state via its actuator if faults in the sensory are detected, the diagnostic unit of this channel uses the same actuator for this purpose in case it detects a fault of the controller. At least for undetectable failures of sensors and electronics, as well as failures of actuators, failures due to common causes cannot be excluded. Therefore, not only (as before) the undetectable failures of sensors, but also the undetectable failures of the controllers and the failures of the actuators are provided with common cause factors.

[22] In [IEC 61508] this architecture is referred to as 1oo2 instead of 1oo2D, since according to this standard a diagnosis must always be present. In part 6 of the standard, 1oo2D is used to refer to a type of fail-operational architecture, which is very unusual and therefore often misunderstood, especially since the accompanying text does not clearly explain this

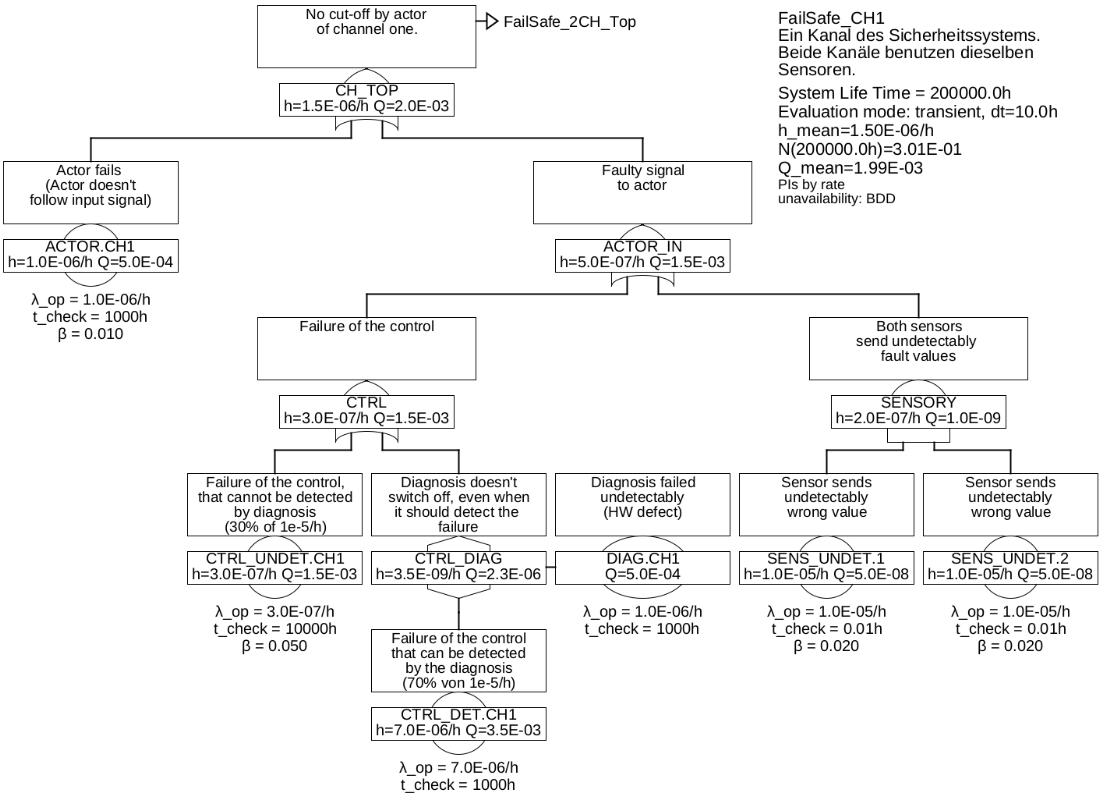


Figure 30: *One channel of a homogeneous redundant control system with safety shutdown in case of detected fault*

The minimum cuts listed in table 4 can be determined for the system. From table 4 it is clear, that the common cause failures are the major events. This is not unique to

Table 4: *Minimum cuts for example 6.5*

Minimum cuts	**Occurrence rate $\overline{h}$**
SENS_UNDET.COM	2.0E-07/h
CTRL_UNDET.COM	1.5E-08/h
ACTOR.COM	1.0E-08/h
ACTOR.CH1 & CTRL_UNDET.CH2	1.548E-09/h
ACTOR.CH2 & CTRL_UNDET.CH1	1.548E-09/h
ACTOR.CH1 & ACTOR.CH2	9.699E-10/h
CTRL_UNDET.CH1 & CTRL_UNDET.CH2	8.106E-10/h
CTRL_UNDET.CH1 & CTRL_DET.CH2 & DIAG.CH2	5.745E-12/h
CTRL_DET.CH1 & DIAG.CH1 & CTRL_UNDET.CH2	5.745E-12/h
ACTOR.CH1 & CTRL_DET.CH2 & DIAG.CH2	4.542E-12/h
ACTOR.CH2 & CTRL_DET.CH1 & DIAG.CH1	4.542E-12/h
SENS_UNDET.1 & SENS_UNDET.2	9.604E-13/h
CTRL_DET.CH1 & DIAG.CH1 & CTRL_DET.CH2 & DIAG.CH2	2.393E-14/h

this example, but corresponds to practical experience. For this reason, a common cause analysis must always be performed for multichannel systems, and a variety of measures must be taken to keep the rate of common cause failures (mathematically described by the β factor) as low as possible.

The progression of the failure rate over time is shown in Figure 31. At first glance, it may seem surprising that the failure rate of the system is not constant, although the failure rates of all components are constant. This is due to the time-varying unavailability of each channel, which is included in the failure rate according to formula (65)*. Due to the high common cause fractions (see minimum cuts in Table 4), which are directly – without multiplication with an unavailability – included in the system failure rate, the time dependence is, however, only small (note the scale for $h(t)$ in Figure 31).*

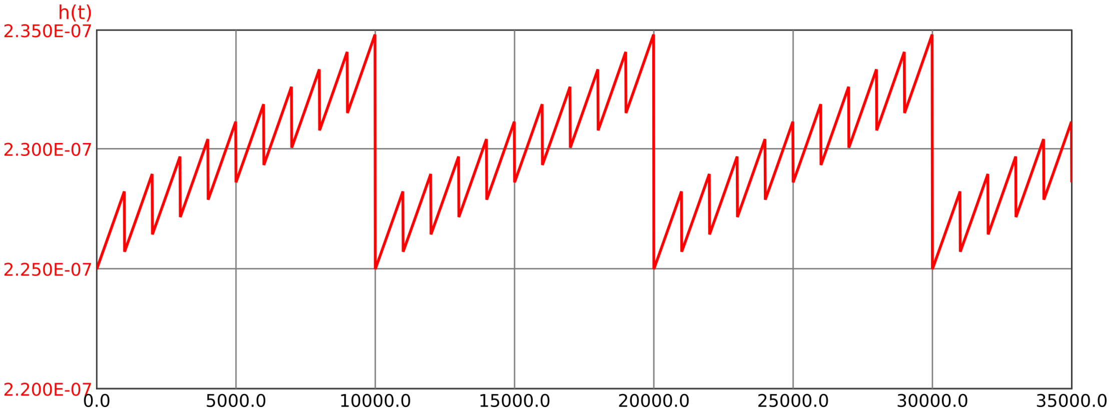


Figure 31: *Course of failure rate over time of a homogeneous-redundant system with regular tests*

6.1.6 Fail operational systems

As mentioned in the introductory example 6.1, there are a large number of processes that cannot simply be brought into a safe state.

If the safety requirements are not very high a two-channel architecture is often sufficient, whereby, in the event of a detected fault, each channel can switch itself off or declare itself defective to a selection circuit. A good self-diagnosis of each channel is essential for this, because only if it is clear which channel is defective, it is possible to switch over to the intact channel. The switchover itself must be performed by a selection circuit.

For higher safety requirements, the diagnostic coverage of the channel-internal diagnostics of the individual channels is often not sufficient, so there is too high a rate of contradictory output from the individual channels, without a channel indicating that it is defective. In this case, the selection circuit would have a 50% chance, of selecting the correct one. The probability of turning off the correct channel, can be improved considerably, by comparing the outputs of three channels. Provided that systematic errors and failures due to common cause are sufficiently rare, usually at least two channels will determine the correct output quantity. The selection circuit is therefore constructed in such a way that it uses the results of the two channels whose results are identical or at least closest to each other. Such an architecture is called a 2-out-of-3 architecture (2oo3, or 2oo3D if each channel has its own diagnostics). [23].

Regardless of the number of channels, the selection circuit must have a minimum failure rate, in order not to limit the overall safety by its own failures. Sometimes the selection is also made by the mechanics, for example, in which each of three channels drives one actuator, which can be mechanically overridden by two others. With appropriate "intelligence" of the selection circuitry, a 2oo3 system can still operate correctly even with two failed channels, if the failures are detected by the channel diagnostics and reported to the selection logic.

Example 6.6 *This example reuses the components of example 6.1. However, now three sensors and three controllers (computers) are used, in such a way that each of the controllers gets the values of all three sensors. Thus, if one sensor fails, all three controllers can continue to operate, in contrast to an architecture where each controller would only have access to one sensor. In addition, each controller can detect sensor faults. The signals for the single actuator calculated by the three controllers are compared by a selection logic and selected according to majority decision (2-of-3).*

The fault tree is shown in Figure 32, with the sub-trees in 33 and 34.

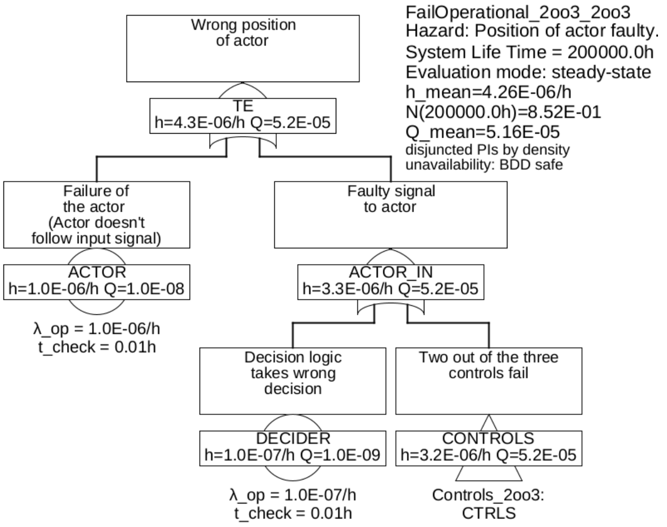


Figure 32: *Homogeneous-redundant control system with 3 channels without safety shutdown*

The "CTRLS" gate in Figure 33 and "SENSORY" in Figure 34 are combination gates, they are explained below.

In addition to the failure rates of all components, the unavailabilities of the controls and

[23] In contrast to 1oo2, 2oo2, 1oo3, 3oo3, confusion is not possible with 2oo3, because each view gives the same result

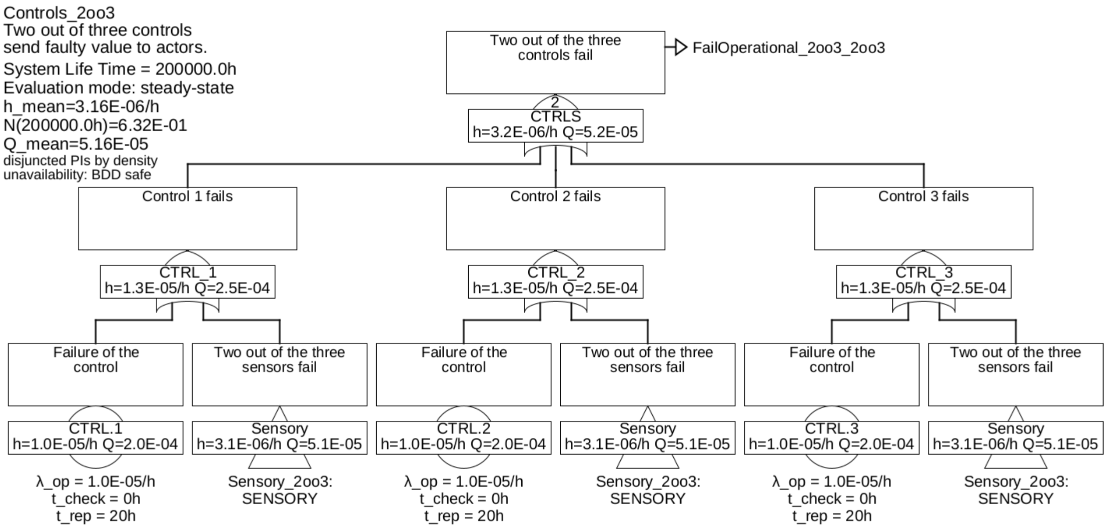


Figure 33: *Redundant controls (2oo3) using the same sensors*

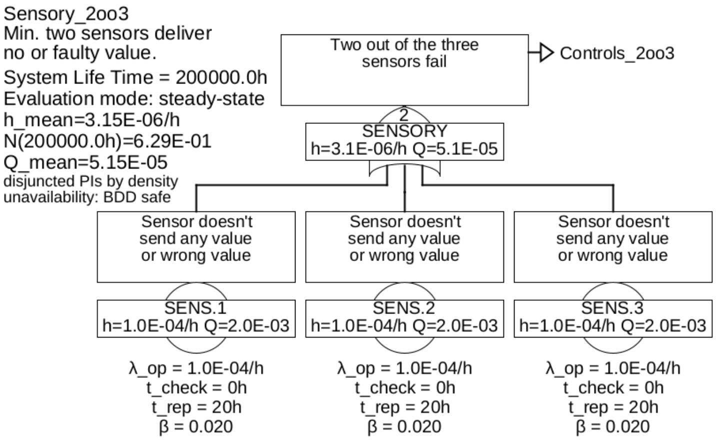


Figure 34: *Redundant sensors (2oo3) shared by all controls*

the sensors are relevant. Here it was assumed that all failures of the controls as well as all independent failures of the sensors reveal themselves immediately by discrepancies in the selection unit, so the detection time t_{test} is zero. The time to repair, i. e., the time that the remaining channels must endure, was assumed to be 20 h (think for example of a long distance airplane, which can only be repaired after landing, or a ship, where the repair of an aggregate is done at sea, but takes a while).

The minimum cuts are listed in table 5.

The total failure rate has decreased from 1.11E-4/h to 4.26E-6/h compared to example 6.1, and is now mainly determined by sensor failures due to common cause (β was assumed to be 2%).

Table 5: *Minimum cuts for example 6.6*

Minimum cuts	**Occurrence rate $\overline{h}$**
SENS.COM	2.0E-06/h
ACTOR	1.0E-06/h
SENS.1 & SENS.2	3.842E-07/h
SENS.1 & SENS.3	3.842E-07/h
SENS.2 & SENS.3	3.842E-07/h
DECIDER	1.0E-07/h
CTRL.1 & CTRL.2	4.0E-09/h
CTRL.1 & CTRL.3	4.0E-09/h
CTRL.2 & CTRL.3	4.0E-09/h

In the previous example, so-called COMBINATION-Gates, also called voting gates, were used for the gates "control" and "sensory". They are just an abbreviation for the corresponding combination of AND and OR gates. The number in the gate (often abbreviated m, so here $m = 2$) indicates, how many of the n inputs must fail at least (i. e. must be fulfilled), so that the event described by the gate occurs. Thus $m = 1$ means a pure OR gate, $m = n$ means a pure AND gate, $1 < m < n$ means a combination of an OR with several AND gates, as shown in Figure 35 as an example for a 2-of-3 gate.

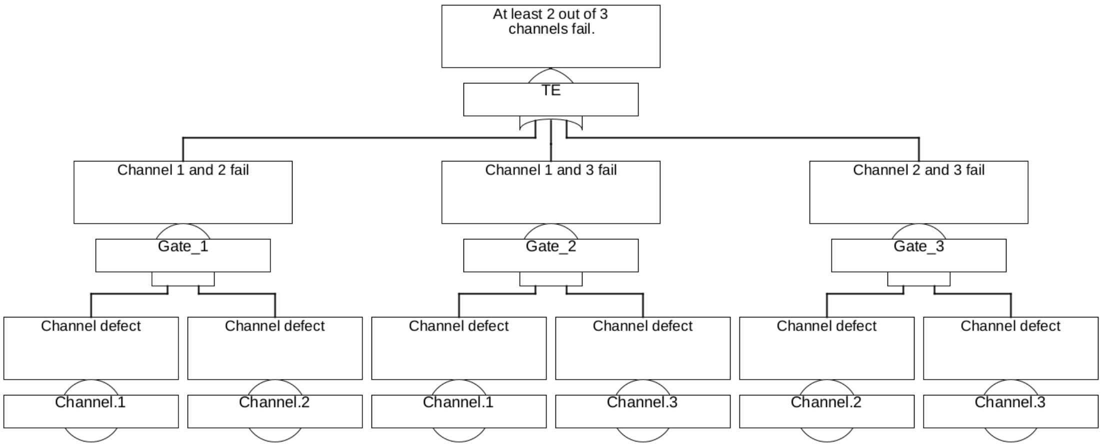


Figure 35: *Equivalent of a 2-out-of-3 gate with discrete OR and AND gates*

For calculation, the combination gates are converted into the corresponding combination of AND and OR gates. Therefore, there are no special formulas or calculation methods for these gates.

6.1.7 Transient and steady-state calculation

Like the mean system unavailability (see section 5.1.4), the mean system failure rate can also be determined using either a steady-state calculation or a transient calculation.

The only difference is, that the mathematical error described in section 5.1.4 when using mean values only occurs for third order minimal cuts (i. e. minimal cuts with three or more basic events) in calculation of the failure rate, and not already for second-order minimum cuts as in the case of unavailability. This is due to the fact that according to formula (65) for a minimal cut of second order no multiplication of unavailabilities occurs yet. So if it is clear that the system is (apart from a negligible transient phase compared to the operating time) will be in a quasi-stationary state, the system failure rate can usually be calculated in good approximation with mean values.

6.2 Calculation with Markov models

Regarding the modeling there are no differences to chapter 5.2.

As for the calculation of the unavailability, first either the steady state must be calculated, or the linear differential equation system must be integrated over the lifetime.

The occurrence frequency $w_i(t)$ of a state i is the sum of the m transition rates $h_{i,j}$, which lead to this state, each multiplied by the residence probability in the original state of the respective edge $p_{\text{Origin}_{i,j}}$:

$$w_i(t) = \sum_{j=1}^{m} h_{\text{in}_{i,j}}(t) \cdot p_{\text{Origin}_{i,j}}(t) \tag{67}$$

The system failure frequency is the sum of the state occurrence frequencies for all n failure states

$$w_{\text{sys}}(t) = \sum_{i=1}^{n} w_i(t) = \sum_{i=1}^{n} \sum_{j=1}^{m} h_{\text{in}_{i,j}}(t) \cdot p_{\text{Origin}_{i,j}}(t) \tag{68}$$

The failure frequency $w(t)$ is identical to the searched failure rate $h(t)$ only, if the residence probability in all failure states is zero, since in practice in the case of a (quasi-)continuously required safety function a system failure is detected practically immediately (namely by the occurrence of an accident), which leads to the immediate termination of operation. Operation is resumed only after the system has been repaired or replaced by another or new one, the time until then must not be taken into account for the calculation of the failure rate (otherwise it would become too optimistic, as can be easily demonstrated with extreme examples).

Thus, if one wishes to use a Markov model to calculate the failure rate $h_{\text{sys}}(t)$ or $\overline{h_{\text{sys}}}$, one either has to calculate a transition from all failure states with a very high rate μ back to a non-failure state (usually back to the initial state), or one has to divide the failure frequency $w(t)$ by the probability , of not being in a failure state:

$$h_{\text{sys}}(t) = \frac{w_{\text{sys}}(t)}{1 - \sum\limits_{i=1}^{n} p_i(t)} \tag{69}$$

If the probabilities of the failure states are zero, we get $h(t) = w(t)$. Formula (69) can and should always be used to be on the safe side, even if – as mentioned before – transitions with large recovery rate μ have already been inserted in the model.

Example 6.7 *The above formulas will now be applied to a simple Markov model. For this purpose, a simple diversitary two-channel system is assumed, consisting of the differently constructed (diversitary) channels A and B. Channels A and B therefore have different failure rates λ_{A} and λ_{B}. Both channels A and B are tested regularly, but at different intervals T_{A} and T_{B}. This results in different $\mu_A = 2/T_{\mathrm{A}}$ and $\mu_B = 2/T_{\mathrm{B}}$.*

If both channels fail, the continuously required safety function fails, thus terminates its operation due to an accident. Repairing or replacing the system after an accident leads back to the original OK state. The probability of staying in the A&B state during operation is zero, which is due to a very large μ_{rep} compared to the failure rates.

The associated Markov model is shown in Figure 36.

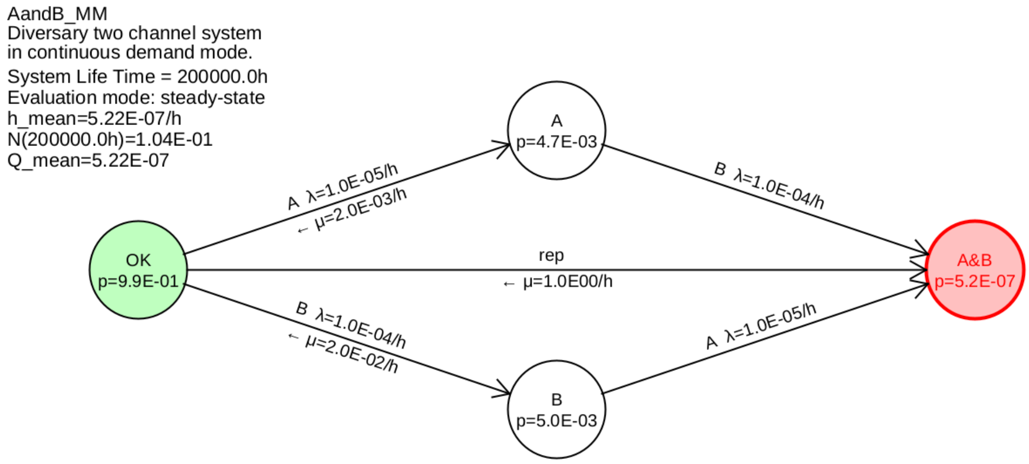


Figure 36: *Diversity-redundant system for continuous demand*

The transition matrix is:

$$T = \begin{pmatrix} -\lambda_A - \lambda_B & \mu_A & \mu_B & \mu_{\mathrm{rep}} \\ \lambda_A & -\mu_A - \lambda_B & 0 & 0 \\ \lambda_B & 0 & -\mu_B - \lambda_A & 0 \\ 0 & \lambda_B & \lambda_A & -\mu_{\mathrm{rep}} \end{pmatrix}$$

For the stationary calculation one of the lines is set to 1 (here the last one was taken):

$$\begin{pmatrix} -\lambda_B - \lambda_A & \mu_A & \mu_B & \mu_{\mathrm{rep}} \\ \lambda_A & -\mu_A - \lambda_B & 0 & 0 \\ \lambda_B & 0 & -\mu_B - \lambda_A & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \vec{p}(t) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

According to formulas (68) *and* (69)*, the system failure occurrence rate results in*

$$h_{\mathrm{sys}} = \frac{p_{\mathrm{A}} \cdot \lambda_{\mathrm{B}} + p_{\mathrm{B}} \cdot \lambda_{\mathrm{A}}}{1 - p_{\mathrm{A\&B}}}$$

The state probabilities required in this formula p_{A}, p_{B} *and* $p_{\mathrm{A\&B}}$ *are obtained by solving the system of equations. Thus* h_{sys} *is given by*

$$\begin{aligned} h_{\mathrm{sys}} &= \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}^2 + \lambda_{\mathrm{A}}^2\lambda_{\mathrm{B}} + \lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\mu_{\mathrm{A}} + \lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\mu_{\mathrm{B}}}{\lambda_{\mathrm{A}}^2 + \lambda_{\mathrm{B}}^2 + \lambda_{\mathrm{A}}\lambda_{\mathrm{B}} + (\lambda_{\mathrm{a}} + \lambda_{\mathrm{B}})\,\mu_{\mathrm{A}} + (\lambda_{\mathrm{A}} + \lambda_{\mathrm{B}})\,\mu_{\mathrm{B}} + \mu_{\mathrm{A}}\mu_{\mathrm{B}}} \\ &= \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\,(\lambda_{\mathrm{A}} + \lambda_{\mathrm{B}} + \mu_{\mathrm{A}} + \mu_{\mathrm{B}})}{\lambda_{\mathrm{A}}\,(\lambda_{\mathrm{A}} + \mu_{\mathrm{A}} + \mu_{\mathrm{B}}) + \lambda_{\mathrm{B}}\,(\lambda_{\mathrm{B}} + \mu_{\mathrm{A}} + \mu_{\mathrm{B}}) + \lambda_{\mathrm{A}}\lambda_{\mathrm{B}} + \mu_{\mathrm{A}}\mu_{\mathrm{B}}} \end{aligned}$$

It should be noted, that the rate μ_{rep} *does not appear in the result, since it is truncated by formula* (69). *This corresponds exactly to the expectation, that the numerical value of this rate must be irrelevant. This formula is now valid for any test interval, in contrast to formula* (65), *which is only valid for sufficiently small test intervals (otherwise formula* (65) *becomes somewhat too large).*

For suitable test intervals $T_{\mathrm{test,A}} \ll 1/\lambda_{\mathrm{A}}$ *and* $T_{\mathrm{Test,B}} \ll 1/\lambda_{\mathrm{B}}$, λ_{A} *is negligible vs.* μ_{A} *and* λ_{B} *is negligible vs.* μ_{B}, *and even more so is* $\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}$ *negligible vs.* $\mu_{\mathrm{A}}\mu_{\mathrm{B}}$. *Thus, we get the conservative approximation:*

$$\begin{aligned} h_{\mathrm{sys}} &\lessapprox \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\,(\mu_{\mathrm{A}} + \mu_{\mathrm{B}})}{\lambda_{\mathrm{A}}\,(\mu_{\mathrm{A}} + \mu_{\mathrm{B}}) + \lambda_{\mathrm{B}}\,(\mu_{\mathrm{A}} + \mu_{\mathrm{B}}) + \mu_{\mathrm{A}}\mu_{\mathrm{B}}} \\ &= \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\left(\frac{1}{\mu_{\mathrm{A}}} + \frac{1}{\mu_{\mathrm{B}}}\right)}{\lambda_{\mathrm{A}}\left(\frac{1}{\mu_{\mathrm{A}}} + \frac{1}{\mu_{\mathrm{B}}}\right) + \lambda_{\mathrm{B}}\left(\frac{1}{\mu_{\mathrm{A}}} + \frac{1}{\mu_{\mathrm{B}}}\right) + 1} \end{aligned}$$

Under the same condition (suitable test intervals) is also valid $\lambda_{\mathrm{A}}/\mu_{\mathrm{A}} \ll 1$ *and* $\lambda_{\mathrm{B}}/\mu_{\mathrm{B}} \ll 1$ *and consequently the approximation:*

$$h_{\mathrm{sys}} \lessapprox \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\left(\frac{1}{\mu_{\mathrm{A}}} + \frac{1}{\mu_{\mathrm{B}}}\right)}{\frac{\lambda_{\mathrm{A}}}{\mu_{\mathrm{B}}} + \frac{\lambda_{\mathrm{B}}}{\mu_{\mathrm{A}}} + 1}$$

Replacing now the repair rates by the test intervals by $\mu_{\mathrm{i}} \approx 2/T_{\mathrm{test,i}}$, *one obtains*

$$h_{\mathrm{sys}} \approx \frac{\lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\,(T_{\mathrm{Test,A}} + T_{\mathrm{Test,B}})}{\lambda_{\mathrm{A}}T_{\mathrm{Test,B}} + \lambda_{\mathrm{B}}T_{\mathrm{Test,A}} + 2}$$

Under the additional condition, that the test intervals would also be sufficiently short for the failure rate of the other channel, i. e. $\lambda_{\mathrm{A}}T_{\mathrm{test,B}} \ll 1$ *and* $\lambda_{\mathrm{B}}T_{\mathrm{test,A}} \ll 1$ *the products in the denominator can be neglected:*

$$h_{\mathrm{sys}} \approx \lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\frac{T_{\mathrm{Test,A}} + T_{\mathrm{Test,B}}}{2}$$

This is the formula (65) *already known for the calculation of the failure rate of a minimal cut, applied to the single minimal cut of this Markov model {A&B}:*

$$h_{\mathrm{sys}} = h_{\mathrm{MCS}} \lessapprox \lambda_{\mathrm{A}}Q_{\mathrm{B}} + \lambda_{\mathrm{B}}Q_{\mathrm{A}} \lessapprox \lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\frac{T_{\mathrm{Test,B}}}{2} + \lambda_{\mathrm{B}}\lambda_{\mathrm{A}}\frac{T_{\mathrm{Test,A}}}{2} = \lambda_{\mathrm{A}}\lambda_{\mathrm{B}}\frac{T_{\mathrm{Test,A}} + T_{\mathrm{Test,B}}}{2}$$

6.3 Expected value of failures

For repairable or replaceable systems, in addition to the failure rate, the expected value of failures $N(T)$ over the lifetime T is also of interest:

$$N_{\text{sys}}(T) = \overline{h_{\text{sys}}}(T) \cdot T = \text{PFH} \cdot T \tag{70}$$

7 Unreliability of complex functions

Unreliability is the essential variable for safety functions, which are supposed to function over a certain period of time, and which cannot be maintained and repaired during this time, or only to a limited extent.

Only a few systems and their safety functions fall into this category, manned space missions, for example. What is asked here is not the frequency of failures, i. e., accidents per hour or accidents per kilometer, but the probability that the mission will be successful, i. e. that all space travelers will return to earth in good health (hence the occasionally used term "mission time" instead of system lifetime). The mission is fixed, a simple reaching of a safe state is not possible (although there may be abort scenarios for certain emergencies). Failures due to wear and tear during the mission can be neglected usually. All components are intensively checked before each mission so that they are like new. After launch, most safety-related components cannot be repaired. This does not mean that there can be no diagnostics, however, this only serves to to shut down a component to prevent further damage (if this is possible) or to switch over to a replacement component (if available).

Since few safety engineers ever have to calculate the unreliability of such systems, this chapter is kept quite short.

Of course, unreliability is not only relevant in the context of safety (rather rare there, as mentioned). Also the question "How likely is, that a new car has to go to the workshop unscheduled within the first 5 years?" is also a question about unreliability. However, it can be answered easily without fault trees or Markov models, since there are usually no redundancies, and therefore the formulas (24) and (8) can be applied directly, i. e.

$$F(T) = 1 - \mathrm{e}^{-\int\limits_0^T \sum\limits_{i=1}^n h_i(t)\,dt} = 1 - \mathrm{e}^{-\sum\limits_{i=1}^n \int\limits_0^T h_i(t)\,dt} = 1 - \prod_{i=1}^n \mathrm{e}^{-\int\limits_0^T h_i(t)\,dt} \tag{71}$$

This formula can be easily calculated using a spreadsheet even in the case of complicated time-dependent failure rates $h_i(t)$.

7.1 Calculation with fault trees

Fault trees can be well used to calculate the unreliability of complex systems. There are two ways of calculation:

1. Directly via the unreliabilities $F(T)$ of the basic events, using the same mathematical methods as for unavailability shown in section 5. Thus, when calculating over minimum cuts, the unreliability of each minimum cut is first calculated according to

$$F_{\mathrm{MCS}}(T) = \prod_{i=1}^m F_i(T) \tag{72}$$

and then the system unreliability using Esary-Proschan's formula:

$$F_{\text{sys}}(T) \lessapprox 1 - \prod_{j=1}^{n} (1 - F_{\text{MCS},i}(T)) \tag{73}$$

Even faster and more accurate is the use of BDDs.

This method is very fast, but it only works, if there are no links to unavailabilities or other probabilities which are not unreliabilities (such as the probability that an external boundary condition is satisfied). In particular, the fault tree must not contain any conditions or INHIBIT gates. As soon as a base event describes an unavailability or other condition, this method will give too optimistic results [24].

2. Via the calculation of the failure rate $h(t)$ (transient calculation necessary!) shown in the previous section 6 and applying the formula (8).

$$F_{\text{sys}}(T) = 1 - \mathrm{e}^{-\int_0^T h_{\text{sys}}(t)\,dt}$$

The method is much slower, because the calculation of the failure rate $h(t)$ is already more complex, and this must also be done for many points in time. However, it delivers correct results even if the failure tree contains basic events, which describe unavailabilities or other conditions. Although this should be the exception in case of safety functions, for which the unreliability is really relevant, but may occasionally occur.

Example 7.1 *For the fault tree shown in Figure 37, the unreliability at time point* $T = 200\,000\,\text{h}$ *is to be calculated using both methods presented. The unreliability of the basic events A and B is described here by Weibull distributions, where for A there is an increasing failure rate (Weibull exponent > 1) and for B a decreasing failure rate (Weibull exponent < 1).*

Method 1:

The unreliability of the basic event A results in:

$$F_{\text{A}}(T) = 1 - \mathrm{e}^{-(\lambda \cdot T)^k} = 1 - \mathrm{e}^{-(6.0\text{E}-6/\text{h} \cdot 200\,000\,\text{h})^{4.0}} \approx 0.874$$

For basic event B results to

$$F_{\text{B}}(T) = 1 - \mathrm{e}^{-(4.0\text{E}-6/\text{h} \cdot 200\,000\,\text{h})^{0.4}} \approx 0.599$$

and for basic event C it is

$$F_{\text{C}}(T) = 1 - \mathrm{e}^{-1.0\text{E}-5/\text{h} \cdot 200\,000\,\text{h}} \approx 0.865$$

The minimum cuts are {A} and {B&C}, for the system unreliability, according to formula (73) *we get*

$$F_{\text{sys}}(T) \lessapprox 1 - (1 - F_{\text{A}}(T)) \cdot (1 - F_{\text{B}}(T) \cdot F_{\text{C}}(T)) \approx 1 - (1 - 0.874) \cdot (1 - 0.599 \cdot 0.865) = 0.939$$

[24] A good tool will warn the user accordingly or automatically switch to another algorithm

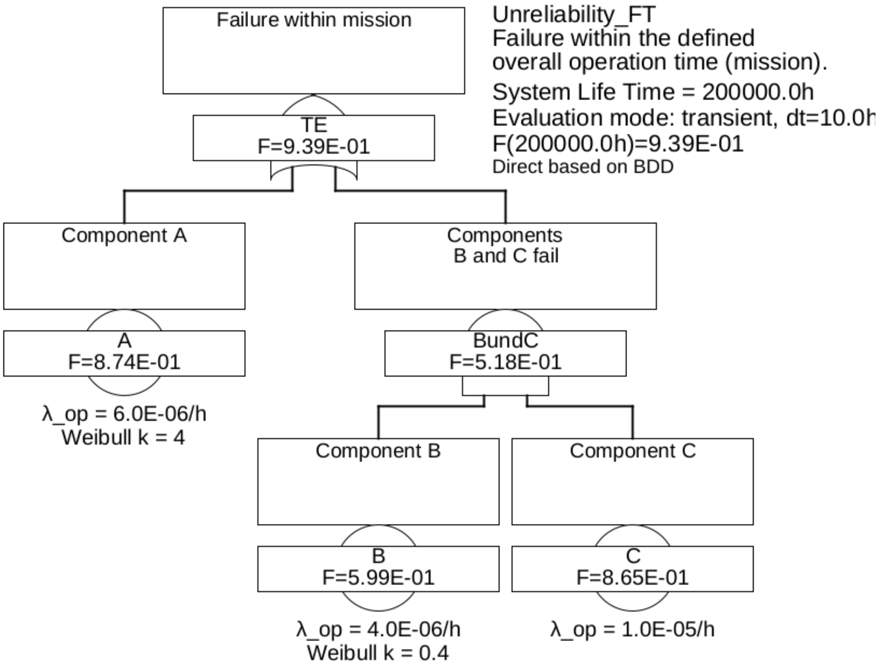


Figure 37: *Calculation of unreliability using fault tree*

Modern tools will use BDDs, so the system unreliability results in

$$F_{\text{sys}}(T) = F_{\text{A}}(T)+(1-F_{\text{A}}(T))\cdot(F_{\text{B}}(T)\cdot F_{\text{C}}(T)) \approx 0.874+(1-0.874)\cdot(0.599\cdot 0.865) = 0.939$$

The variable order A, B, C was chosen, any other order gives the same result.

Method 2:

The failure rates of the basic events A and B are given by Formula (16), the unavailabilities $Q(t)$ by formula (18). The system failure rate $h(t)$ can now be calculated with Formula (65). The unreliability is thus calculated to be $F_{\text{sys}}(T) \approx 0.964$. This is somewhat too large, since the unavailabilities here are very large (so the system is practically unusable). If one applies instead the formula (78) from appendix B.1, the correct result is $F_{\text{sys}}(T) \approx 0.939$. The time course of failure density $f(t)$, failure rate $h(t)$ and unreliability $F(t)$ is shown in Figure 38.

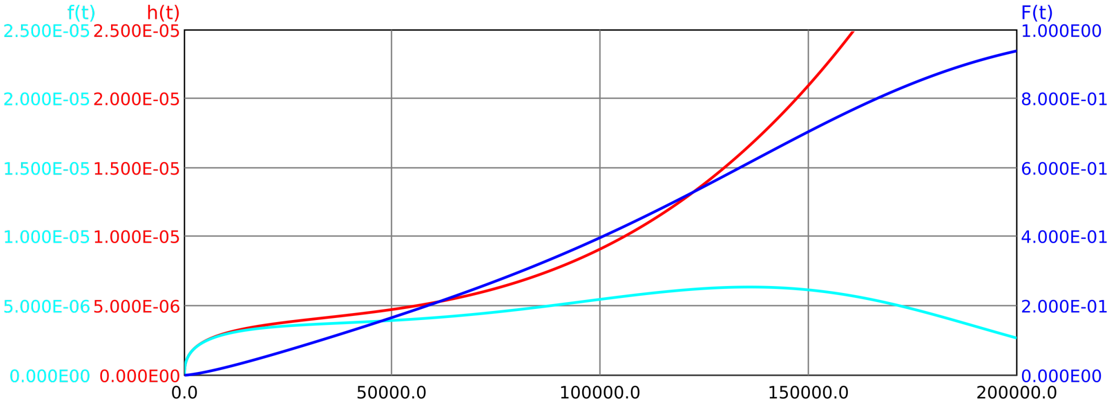


Figure 38: *Time history of failure rate, failure density and unreliability for example 7.1*

7.2 Calculation with Markov Models

The system unreliability can also be calculated using Markov models. The calculation must now basically be done by integration of the differential equation system (transient calculation), since a steady state will never be reached. The system unreliability at a certain point in time is given by the sum of the residence probabilities in the failure states at this point in time.

If, as in example 7.1, failure distributions with non-constant failure rates are used, the transition rates are time dependent. This makes the integration considerably more complex, since now the Jacobian matrix required for the integration of stiff differential equation systems must be inverted at least once at each time step.

Example 7.2 *Figure 39 shows the Markov model, which shows the structure of the fault tree from example 7.1. illustrates.*

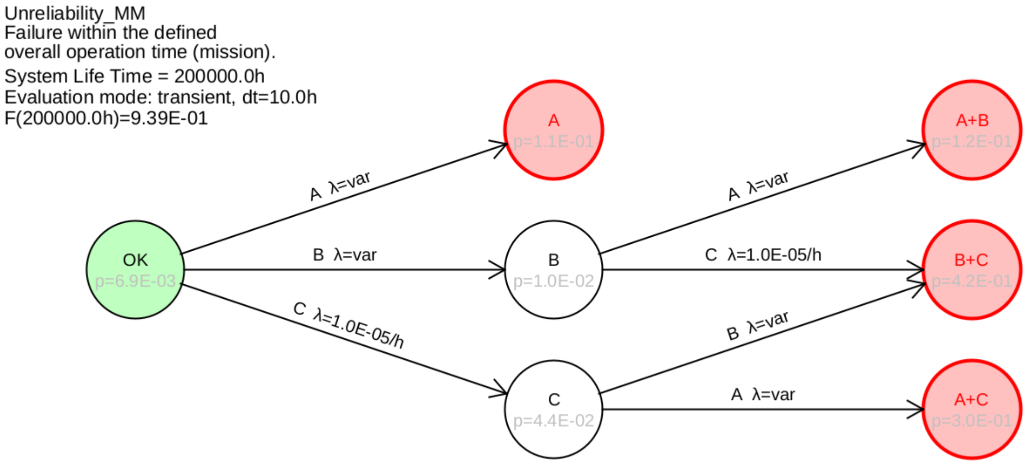


Figure 39: *Markov model with calculation of unreliability*

The results are practically identical to those calculated in example 7.1 with fault trees.

A Models for basic events

The basic events of fault trees or the edges (transitions) of Markov models either model events or conditions (states). Different models are required for this, depending on whether we are dealing with one-time or multiple random events, regular events, or conditions (states). The most important ones are mentioned below, but there are also others. The exact definition of each model might differ between different tools, since there is no harmonization or at least de-facto standard available.

A.1 Model restorable

With this model, also called "Dormant Failure Model" or "Repairable" or "Testable" [25], for example, the following failure scenarios can be modeled:

- failures that lead directly to system failure (and thus are detected immediately).
- failures that lead to system failure only in the presence or subsequent occurrence of other events, but which can be detected by regular tests.

This model is the standard model, it can be used to represent almost all failures of technical components such as electrics/electronics, hydraulics, pneumatics etc., from a simple wire up to complete control systems.

If neither detection time nor repair time are negligible, the unavailability $Q(t)$ is very well approximated by the formula (48) mentioned in chapter 4:

$$Q(t) = 1 - \frac{e^{-\dfrac{\lambda \cdot (t \bmod T_{\text{test}})}{\lambda \cdot \text{MRT} + 1}}}{\lambda \cdot \text{MRT} + 1}$$

with the test interval T_{test} and the mean repair time per failure MRT (including time to replace).

The mean unavailability $\overline{Q}$ is given by the formula (44) derived in chapter 4.

$$\overline{Q} = \frac{e^{-\lambda \cdot T_{\text{test}}} - 1}{\lambda \cdot T_{\text{test}} + \lambda \cdot \text{MRT} \cdot (1 - e^{-\lambda \cdot T_{\text{test}}})} + 1$$

as well as by formula (45) in case of negligible detection time $T_{\text{test}} \rightarrow 0$

$$\overline{Q} = \frac{\lambda \cdot \text{MRT}}{\lambda \cdot \text{MRT} + 1}$$

or formula (46) in case of negligible repair time MRT → 0:

$$\overline{Q} = \frac{e^{-\lambda \cdot T_{\text{test}}} - 1}{\lambda \cdot T_{\text{test}}} + 1$$

[25] Some tools provide separate model for Testable and Repairable. The clear separation simplifies understanding, however, sometimes both a failure detection time greater than zero and a repair time greater than zero are needed

The model can often also be used if there is no defined test or inspection interval, but a failure reveals itself during operation in a non-critical situation. If there are no tests and a failure only reveals itself, if another event occurs, the test interval must be set to the nominal operation time, or the model "non-restorable" must be used.

If the failure rate is not constant, a mean failure rate must be calculated using formula (26) in conjunction with (25):

$$\lambda_{\text{eff}} = \frac{1}{\text{MTTF}} = \frac{1}{\int\limits_0^\infty t \cdot f(t)\,dt} = \frac{1}{\int\limits_0^\infty t \cdot h(t) \cdot \mathrm{e}^{-\int\limits_0^t \sum\limits_{i=1}^n h_i(\tau)\,d\tau}\,dt} \tag{74}$$

The model can also be used as a description of conditions.

A.2 Model non-restorable

This model can be used to model the following failure scenarios, for example:

- Failures that lead directly to system failure,
- failures that only lead to system failure, if other events have already occurred or are still occurring, and which are recognized also only then.

Only with this event model it makes sense to consider time-variant failure rates (e. g. Weibull distributions) for a transient calculation.

The unreliability is calculated according to the known formula (8) to be

$$F(T) = 1 - \mathrm{e}^{-\int\limits_0^T h(t)\,dt} \tag{75}$$

The average failure rate with respect to $F(T)$ is thus given by

$$\begin{aligned} F(T) &= 1 - \mathrm{e}^{-\int\limits_0^T h(t)\,dt} = 1 - \mathrm{e}^{-\overline{h(T)}\cdot T} \\ \Rightarrow \overline{h(T)} &= \frac{1}{T}\int\limits_0^T h(t)\,dt \end{aligned} \tag{76}$$

Thus, if an unreliability $F(T)$ is to be calculated for a non-repairable element with a principally time-dependent failure rate, either the unreliability must be calculated via integration using formula (75), or a constant failure rate must be used, which was calculated according to formula (76). It is not allowed to use the mean effective failure rate calculated according to formula (29). λ_{eff} must be used!

The average unavailability over the planned operating time $\overline{Q(T)}$ is given by

$$\overline{Q(T)} = \frac{\int\limits_0^T F(t)\,dt}{T} \tag{77}$$

The maximum unavailability is given at the end of the planned deployment time.

The model may obviously only be used if it is certain that the component is not defective at time $t = 0$. It is therefore forbidden to assume any short (planned) operating times, such as a single flight or a single car trip, since before these it is not ensured that all components are as new (in contrast to a space mission).

The model can also be used as a description of conditions.

A.3 Model constant

In particular, for constant unavailabilities $Q = \text{const}$, but also for the (constant) probability that an external boundary condition is satisfied, the model "constant" is used.

The model is used almost only as a description of conditions.

A.4 General recommendations on basic models

It is useful to combine multiple failure modes into one basic event. It is important that all failure modes to be modeled by this one basic event, do not differ with respect to the modeling of the restoration, i. e., in particular, have the same fault detection time and, if applicable, repair time.

In the case of complex components (such as an electronic board or an entire control system), it is neither necessary nor useful, to record each of the tens of thousands of failure modes individually as a basic event. Typically, the number of failure modes observable at the interfaces is quite manageable anyway (typical: binary signal high instead of low or vice versa, analog signal too high/too low, bus communication failed/life sign invalid, bus variable unrecognizably wrong).

Thus, as a rule, it makes sense to describe a complex assembly by two to four basic events:

1. one basic event for failures that are detected immediately,
2. one basic event for failures that are detected during daily tests,
3. one basic event for failures detected during regular inspections,
4. one basic event for failures that are never detected or detected only when requested.

All possible failures are typically assigned to one of these categories in an FMEA. The failure rate for each of these maximum four basic events is the sum of the individual failure rates of all failure modes, which have been assigned to the respective category in the FMEA.

B Supplements for system failure rate calculation with fault trees

B.1 Improvement for very high unavailability

Formula (66) from section 6 provides somewhat overly conservative results for large unavailabilities. Since large unavailabilities are always a sign of improperly designed systems, this is not relevant in practice. Nevertheless, one more formula should be mentioned here which provides less conservative results.

If instead of the failure rates one uses the failure frequencies $w(t)$ which are conditional with respect to the recovery, then one can first calculate the system failure frequency $w_{\text{sys}}(t)$ using the following formula:

$$\begin{aligned} h_{\text{sys}}(t) &= \sum_{i=1}^{n_{\text{MCS}}} \frac{w_{\text{MCS}_\text{i}}(t)}{1 - Q_{\text{MCS}_\text{i}}(t)} \\ &= \sum_{i=1}^{n_{\text{MCS}}} \frac{\sum_{j=1}^{n_{\text{Lit},\text{MCS}_\text{i}}} \left(w_j(t) \cdot \prod_{k=1,k\neq j}^{n_{\text{Lit},\text{MCS}_\text{i}}} q_{i,k}(t) \right)}{1 - \prod_{k=1}^{n_{\text{Lit},\text{MCS}_\text{i}}} q_{i,k}(t)} \end{aligned} \tag{78}$$

C Other distribution functions

C.1 Normal distribution

The normal distribution (Gaussian distribution) has the density function

$$f(t) = \frac{1}{\sqrt{2\pi\sigma^2}}\,\mathrm{e}^{-\dfrac{(t-\mu)^2}{2\sigma^2}} \tag{79}$$

with the mean $\mu = \text{MTTF}$ and the standard deviation σ. It should be noted, that the function already starts at $t = -\infty$ and that this proportion cannot be set to 0.

Consequently, the distribution function is given by

$$F(t) = \int_{-\infty}^{x} f(t)dt = \frac{1}{\sqrt{2\pi\sigma^2}}\int_{-\infty}^{x}\mathrm{e}^{-\dfrac{(t-\mu)^2}{2\sigma^2}}dt = 0.5\left(1 + \operatorname{erf}\left(\frac{t-\mu}{\sqrt{2\sigma^2}}\right)\right) \tag{80}$$

where erf(x) is the so-called error function. There is no closed representation for this integral, it must therefore always be determined numerically. Accordingly, there is also no closed representation for the failure rate $h(t)$.

The figure 40 shows a normal distribution with mean $\mu = 1\text{E}6\,\text{h}$ and standard deviation $\sigma = 1\text{E}5\,\text{h}$.

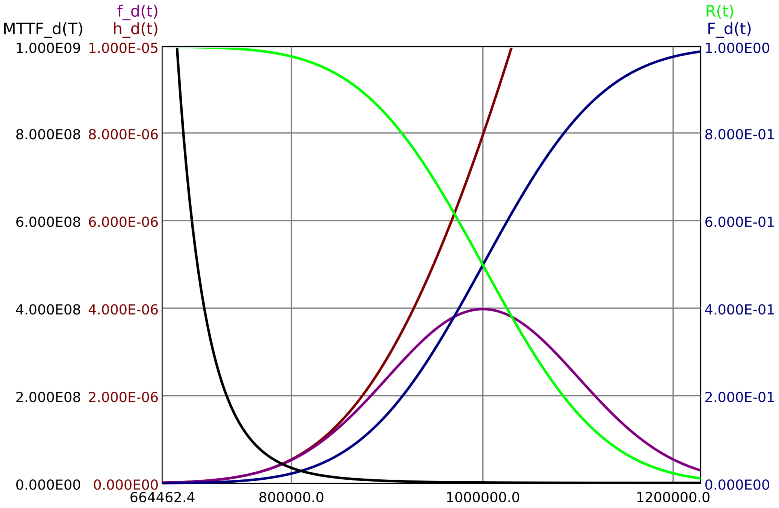


Figure 40: *Normal distribution with mean* $\mu = 1\text{E}6\,\text{h}$ *and standard deviation* $\sigma = 1\text{E}5\,\text{h}$

C.2 Uniform distribution

The uniform distribution is characterized by a constant outage density $f(t) = \text{const}$ within an interval $t_1 \ldots t_2$. Outside this interval it is 0. It is therefore also called a rectangular distribution. It does not occur in nature and technology, but it is suitable for thought experiments or for plausibility checks of formulas.

$$f(t) = \frac{1}{t_2 - t_1} \quad \text{for } t_1 \le t < t_2 \quad \text{, else } 0 \tag{81}$$

$$F(t) = \begin{cases} 0 & \text{for } t < t_1 \\ \dfrac{t - t_1}{t_2 - t_1} & \text{for } t_1 \le t < t_2 \\ 1 & \text{for } t \ge t_2 \end{cases} \tag{82}$$

$$R(t) = \begin{cases} 1 & \text{for } t < t_1 \\ \dfrac{t_2 - t}{t_2 - t_1} & \text{for } t_1 \le t < t_2 \\ 0 & \text{for } t \ge t_2 \end{cases} \tag{83}$$

$$h(t) = \frac{\frac{1}{t_2 - t_1}}{\frac{t_2 - t}{t_2 - t_1}} = \frac{1}{t_2 - t_1} \cdot \frac{t_2 - t_1}{t_2 - t} = \frac{1}{t_2 - t} \quad \text{for } t_1 \le t < t_2 \quad \text{, else } 0 \tag{84}$$

$$\text{MTTF} = \int_{t_1}^{t_2} t \cdot \frac{1}{t_2 - t_1}\, dt = \frac{1}{t_2 - t_1} \left[\frac{t^2}{2} \right]_{t_1}^{t_2} = \frac{1}{t_2 - t_1} \frac{t_2^2 - t_1^2}{2} = \frac{t_1 + t_2}{2} \tag{85}$$

A uniform distribution is shown in Figure 41. It can be seen that the failure rate $h(t)$ approaches infinity for $t \to t_2$, i. e., has a pole at t_2.

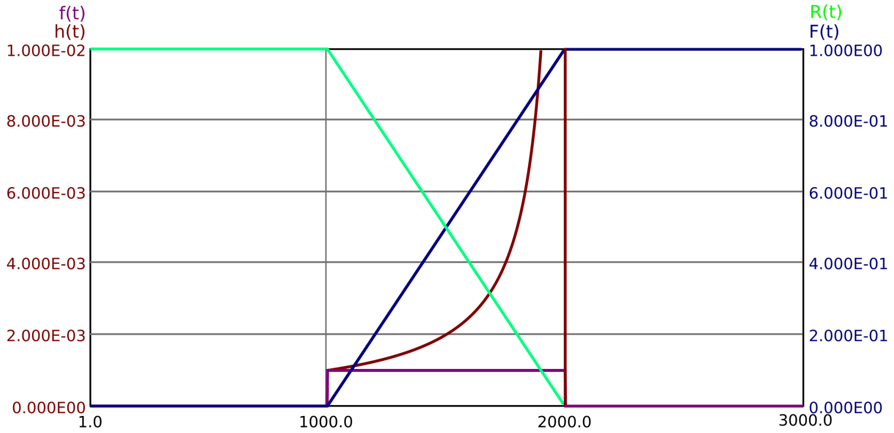


Figure 41: *Uniform distribution between t_1 and t_2*

C.3 Dirac distribution

The Dirac distribution is the mathematical description of determinism: Only at time T does the density $f(t)$ take a value other than 0. Thus, the density must have the property of a Dirac shock of height 1 at time T:

$$f(t) = \delta(t - T) \tag{86}$$

Here $\delta(t)$ is the Dirac function with the property $\int_{-\infty}^{+\infty} \delta(t)\,dt = 1$. So at time T the unreliability jumps from 0 to 1:

$$F(t) = \int\limits_0^\infty f(t)\,dt = \int\limits_0^\infty \delta(t-T)\,dt = \sigma(t-T) \tag{87}$$

Here $\sigma(t-T)$ denotes the unit jump function at time T. For the reliability, the immediate result is:

$$R(t) = 1 - \sigma(t-T) \tag{88}$$

The MTTF is obviously T, which also results computationally:

$$\mathrm{MTTF} = \int\limits_0^\infty t \cdot \delta(t-T)\,dt = T \tag{89}$$

The delta distribution is a special case of numerous distributions, for example the uniform distribution (namely for $t_1 \to t_2$) or the normal distribution (for scatter $\sigma \to 0$).

D Importances

Importances indicate the influence of each basic event on a system parameter. In the literature a whole series of importances can be found, which are often defined differently and almost always without naming the system parameter for which they were defined. Thus, also regarding the importances, it is often only spoken of "failure probabilities".

Importances for the system failure rate h_{sys} (called PFH in [IEC 61508]) are practically searched in vain in the literature. This is understandable in so far, as importances are almost always defined in connection with fault trees, and the computation of the system failure rate with fault trees is also treated only rarely (e. g. in [NUREG]). Some importances can be applied directly to the failure rate, some analogously, and some importances cannot be meaningfully defined for the failure rate at all.

Although importances are mostly defined for use with fault trees, some of them can also be applied to other models such as Markov models.

D.1 General Notes

In the sections 5 to 7 it was shown that often a transient (time-dependent) calculation is necessary to get correct values. With importances one can often do without this, because on the one hand many importances are already relative quantities by definition, inaccuracies in numerator and denominator cancel each other out, and on the other hand the purpose of importances is only that, to prioritize basic events or minimum cuts, for which it also depends only on ratios or orders of magnitude and not on certain numerical values.

To keep the formulas short and memorable, the dependence on the system lifetime T or the averaging will not be mentioned in the following: Instead of $F(T)$, F is written for short, instead of $\overline{Q}(T)$ is written Q for short, and instead of $\overline{h}(T)$ is written h for short.

D.2 Partial Derivative (PD) and Birnbaum Importance (BI)

Immediately obvious as a measure of the importance of individual basic events is the partial derivative (partial derivative, PD) of the system value Q, F or h.

The partial derivatives of system unavailability Q and system reliability F are also called Birnbaum importance. [26].

D.2.1 Partial derivative for system unavailability

The derivative of system unavailability Q_{sys} according to the unavailability of each basic event Q_x is given by:

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,x}} = \frac{\partial Q_{\text{sys}}}{\partial Q_x} = \frac{Q_{\text{sys}}(\mathbf{Q} + \partial Q_x) - Q_{\text{sys}}(\mathbf{Q})}{\partial Q_x} \tag{90}$$

[26] There is no known source, that refers to a partial derivative of the system failure rate as "Birnbaum importance"

Where $\mathbf{Q}$ denotes the vector of (mean values of) unavailabilities of all basic events.

Using the approximation formula (53) for the system non-availability for fault trees, the partial derivative is calculated to be

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,x}} \approx \frac{\partial \sum_{i=1}^{n_{\mathrm{MCS}}} \left(\prod_{j=1}^{m_{\mathrm{Lit},i}} Q_j(t) \right)}{\partial Q_x} = \sum_{i=1}^{n_{\mathrm{MCS}}} \begin{cases} 0 & \text{if basic event } x \notin \mathrm{MCS}_i \\ \prod_{j=1, j\neq x}^{m_{\mathrm{Lit},i}} Q_j & \text{if basic event } x \in \mathrm{MCS}_i \end{cases} \tag{91}$$

Using BDDs, the partial derivative $\frac{\partial Q_{\mathrm{sys}}}{\partial Q_x}$ can be easily determined exactly. Moving each basic event in turn to the top of the BDD, as shown in Figure 42, this results in

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,x}} = \frac{\partial\big((1 - Q_x) \cdot \mathrm{BDD}_0 + Q_x \cdot \mathrm{BDD}_1\big)}{\partial Q_x} = \mathrm{BDD}_1 - \mathrm{BDD}_0 \tag{92}$$

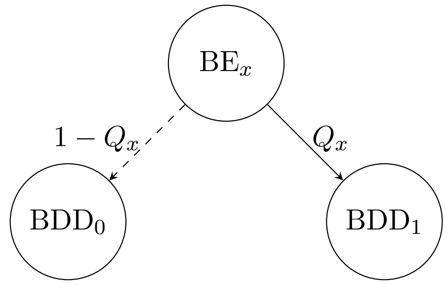


Figure 42: *For calculating the partial derivative with BDDs*

Where BDD_0 is the low branch for basic event x i.e. the system unavailability in the case, that basic event x has not failed, and BDD_1 the high branch i.e. the system unavailability in the case, that basic event x has failed. Thus one can also write

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,x}} = \mathrm{BDD}_{x,1} - \mathrm{BDD}_{x,0} = Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(Q_x := 0) \tag{93}$$

Where $Q_{\mathrm{sys}}(Q_x := 1)$ means the system unavailability, which results if one sets the unavailability of basic event x to 1, and leaving the unavailability of all other basic events at their original values.

Since $\mathrm{BDD}_{x,0}$ gives the probability, with which the system is not available, even if component x is OK, and $\mathrm{BDD}_{x,1}$ is the probability, that the system is then unavailable, if component x also fails, the difference is the probability that the system is in a state in which component x is critical, i.e., the failure of component x would lead to system failure.

D.2.2 Partial derivative for system unreliability

The partial derivative for system unreliability can also be specified:

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{F,x}} = \frac{\partial F_{\mathrm{sys}}}{\partial F_x} = \frac{F_{\mathrm{sys}}(\mathbf{F} + \partial F_x) - F_{\mathrm{sys}}(\mathbf{F})}{\partial F_x} \tag{94}$$

Here $\mathbf{F}$ denotes the vector of unreliabilities of all basic events at a given time (usually at the system end-of-life).

Example D.1 *Let the fault tree of a system be BE1 AND BE2. Thus holds:*

$$F_{\text{sys}}(T) = F_{\text{BE1}}(T) \cdot F_{\text{BE2}}(T)$$

The derivative to $F_{\text{BE1}}(T)$ is $F_{\text{BE2}}(T)$ and vice versa.

As explained in section 7, a fault tree for calculating system unreliability can also contain conditions, i. e. basic events, which are described by their unavailability Q. For these basic events, one can substitute the partial derivative $\mathrm{I}^{\mathrm{PD}}_{\mathrm{F,x}} = \frac{partial F_{\text{sys}}}{\partial Q_x}$, however, the above formulas do not apply or apply only approximately.

D.2.3 Partial derivative for system failure rate

For the system failure rate h a partial derivation only according to the occurrence rate h_x of a basic event $\frac{\partial h_{\text{sys}}}{\partial h_x}$ makes little sense, since the system failure rate h according to formula (66) also depends on the unavailability of each basic event:

$$h_{\text{sys}}(t) \lessapprox \sum_{i=1}^{n_{\text{MCS}}} \left(\sum_{j=1}^{n_{\text{Lit,MCS}_\text{i}}} \left(h_j(t) \cdot \prod_{k=1,k\neq j}^{n_{\text{Lit,MCS}_\text{i}}} q_{i,k}(t) \right)\right) \tag{95}$$

Of course, one could use two derivatives $\mathrm{I}^{\mathrm{PD}}_{\mathrm{h_h,x}} = \frac{\partial h_{\text{sys}}}{\partial h_x}$ and $\mathrm{I}^{\mathrm{PD}}_{\mathrm{h_Q,x}} = \frac{\partial h_{\text{sys}}}{\partial Q_x}$. However, Q_x again depends on the failure rate of the same for most basic events:

$$h_{\text{sys}} = \text{fkt}(h_x, Q_x = \text{fkt}(h_x)) \tag{96}$$

For regularly tested and repaired components, for example, the mean unavailability is $\overline{Q} \approx \lambda \cdot (T_{\text{test}}/2 + \text{MRT}) = h \cdot (T_{\text{test}}/2 + \text{MRT})$.

Therefore it makes more sense to define the importance $\mathrm{I}^{\mathrm{PD}}_{\mathrm{h,x}}$ as the derivative with respect to the (mean) failure rate of the basic event λ_i:

$$\mathrm{I}^{\mathrm{PD}}_{\mathrm{h,x}} = \frac{\partial h_{\text{sys}}}{\partial \lambda_x} = \frac{h_{\text{sys}}(\boldsymbol{\lambda} + \partial\lambda_x) - h_{\text{sys}}(\boldsymbol{\lambda})}{\partial \lambda_x} \approx \frac{\partial \left(\sum_{i=1}^{n_{\text{MCS}}} h_{\text{MCS,i}} \right)}{\partial \lambda_x} = \sum_{i=1}^{n_{\text{MCS}}} \frac{\partial h_{\text{MCS,i}}}{\partial \lambda_x} \tag{97}$$

Using formula (65) for the failure rate $h_{\text{MCS,i}}$ of each minimal cut

$$\begin{aligned} h_{\text{MCS}} \lessapprox\ & h_1 \cdot Q_2 \cdot Q_3 \cdot \ldots \cdot Q_m \\ & + h_2 \cdot Q_1 \cdot Q_3 \cdot \ldots \cdot Q_m \\ & + \ldots \\ & + h_m \cdot Q_1 \cdot Q_2 \cdot \ldots \cdot Q_{m-1} \end{aligned} \tag{98}$$

results in

$$
\begin{aligned}
\frac{\partial h_{\mathrm{MCS,i}}}{\partial \lambda_x} \approx & \frac{\partial(h_1 \cdot Q_2 \cdot Q_3 \cdot \ldots \cdot Q_m)}{\partial \lambda_x} \\
& + \frac{\partial(h_2 \cdot Q_1 \cdot Q_3 \cdot \ldots \cdot Q_m)}{\partial \lambda_x} \\
& + \ldots \\
& + \frac{\partial(h_m \cdot Q_1 \cdot Q_2 \cdot \ldots \cdot Q_{m-1}}{\partial \lambda_x} \\
& = \sum_{j=1}^{m} \frac{\partial \left(h_j \cdot \prod\limits_{k=1,k\neq j}^{m} Q_k \right)}{\partial \lambda_x}
\end{aligned}
\tag{99}
$$

If basic event x is not included in MCS$_i$, this derivative is zero. Otherwise, the summand with $j = x$ is equal to $\prod\limits_{k=1,k\neq j}^{m} Q_k$ (where the unavailabilities of this product are all independent of base event x), and all summands with $j \neq x$ are equal to $h_j \frac{\partial Q_x}{\partial \lambda_x} \prod\limits_{k=1,k\neq j,k\neq x}^{m} Q_k$.

Thus applies

$$
\mathrm{I}_{\mathrm{h,x}}^{\mathrm{PD}} \approx \sum_{i=1}^{n_{\mathrm{MCS}}} \begin{cases} 0 & \text{if BE } x \notin \mathrm{MCS_i} \\ \prod\limits_{k=1,k\neq x}^{m_{\mathrm{Lit},i}} Q_k + \frac{\partial Q_x}{\partial \lambda_x} \cdot \sum\limits_{j=1,j\neq x}^{m_{\mathrm{Lit},i}} \left(h_j \cdot \prod\limits_{k=1,k\neq j,k\neq x}^{m_{\mathrm{Lit},i}} Q_k \right) & \text{wenn BE } x \in \mathrm{MCS_i} \end{cases}
\tag{100}
$$

Example D.2 *Let a system consist of two different components with constant failure rates λ_1 and λ_2, which are regularly tested at different intervals $T_{\mathrm{Test,i}}$ and repaired immediately if necessary. The system then fails dangerously, if one of the components has failed and in this state the second component still fails. The fault tree is thus BE1 AND BE2. So there is only one minimum cut, namely {BE1, BE2}. Thus holds:*

$$
\overline{h_{\mathrm{sys}}} \lessapprox \lambda_1 \cdot \overline{Q_2} + \lambda_2 \cdot \overline{Q_1}
$$

For the mean unavailability of each component applies $\overline{Q_x} \approx \lambda_x \cdot T_{\mathrm{test},x}/2$ and thus for its derivative with respect to λ_x: $\frac{\partial Q_x}{\partial \lambda_x} \approx T_{\mathrm{test},x}/2$.

Thus applies

$$
\mathrm{I}_{\mathrm{h,1}}^{\mathrm{PD}} \approx \overline{Q_2} + \lambda_2 \cdot \frac{T_{\mathrm{Test,1}}}{2} = \lambda_2 \cdot \frac{T_{\mathrm{Test,2}}}{2} + \lambda_2 \cdot \frac{T_{\mathrm{Test,1}}}{2} = \lambda_2 \frac{T_{\mathrm{Test,1}} + T_{\mathrm{Test,2}}}{2}
$$

and

$$
\mathrm{I}_{\mathrm{h,2}}^{\mathrm{PD}} \approx \lambda_1 \cdot \frac{T_{\mathrm{Test,2}}}{2} + \overline{Q_1} = \lambda_1 \cdot \frac{T_{\mathrm{Test,2}}}{2} + \lambda_1 \cdot \frac{T_{\mathrm{Test,1}}}{2} = \lambda_1 \frac{T_{\mathrm{Test,1}} + T_{\mathrm{Test,2}}}{2}
$$

D.2.4 Calculation for Markov models

Due to the above mentioned property, that the partial derivatives of unavailability or unreliability are equal to probability, that the system is in a state from which it enters a failure state when event x occurs, the partial derivative with respect to Q_x or F_x is equal to the sum of the (average) residence probabilities of all m_x states, from which an edge of the base event x leads to a failure state:

$$\mathrm{I}^{\mathrm{B}}_{\mathrm{Q,x}} = \sum_{j=1}^{m_x} \overline{p_j} \tag{101}$$

D.3 Risk-Reduction (RR)

The risk reduction potential (RR) indicates how much $\overline{Q}$, $F(T)$ or $\overline{h}$ would be reduced, if basic event BE_x would never occur, i. e. component x could not fail (at least not with this failure mode).

$$I^{\mathrm{RR}}_{Q,x} = Q_{\mathrm{sys}}(\mathbf{Q}) - Q_{\mathrm{sys}}(Q_x := 0) \tag{102}$$

$$I^{\mathrm{RR}}_{F,x} = F_{\mathrm{sys}}(\mathbf{F}) - F_{\mathrm{sys}}(F_x := 0) \tag{103}$$

The improvement potential can also be directly applied to the system failure rate, because due to the definition it is irrelevant by which quantity the quality of a basic event is defined – or by which combination of quantities. However, one must then sensibly set $h_x = 0$ and $Q_x = 0$ at the same time:

$$I^{\mathrm{RR}}_{h,x} = h_{\mathrm{sys}}(\mathbf{h}, \mathbf{Q}) - h_{\mathrm{sys}}(h_x := 0, Q_x := 0) \tag{104}$$

D.4 Risk-Reduction-Worth (RRW)

The Risk-Reduction-Worth (RRW) indicates, how much $\overline{Q}$, $F(T)$ or $\overline{h}$ would be relatively reduced, if component x did not fail:

$$I^{\mathrm{RRW}}_{Q,x} = \frac{Q_{\mathrm{sys}}(\mathbf{Q}) - Q_{\mathrm{sys}}(Q_x := 0)}{Q_{\mathrm{sys}}(Q_x := 0)} = \frac{Q_{\mathrm{sys}}(\mathbf{Q})}{Q_{\mathrm{sys}}(Q_x := 0)} - 1 \tag{105}$$

$$I^{\mathrm{RRW}}_{F,x} = \frac{F_{\mathrm{sys}}(\mathbf{F}) - F_{\mathrm{sys}}(F_x := 0)}{F_{\mathrm{sys}}(F_x := 0)} = \frac{F_{\mathrm{sys}}(\mathbf{F})}{F_{\mathrm{sys}}(F_x := 0)} - 1 \tag{106}$$

$$I^{\mathrm{RRW}}_{h,x} = \frac{h_{\mathrm{sys}}(\mathbf{h}, \mathbf{Q}) - h_{\mathrm{sys}}(h_x := 0, Q_x := 0)}{h_{\mathrm{sys}}(h_x := 0, Q_x := 0)} = \frac{h_{\mathrm{sys}}(\mathbf{h}, \mathbf{Q})}{h_{\mathrm{sys}}(h_x := 0, Q_x := 0)} - 1 \tag{107}$$

The Risk-Reduction-Worth can obviously assume arbitrarily large values. The larger, the more effective is the improvement of component x. A value of ≈ 0 on the other hand means, that component x has practically no influence. Attention: The summand -1 is often omitted.

D.5 Fussell-Vesely-Importance (FV)

Dividing the risk reduction potential by the original system size, we get the Fussell-Vesely importance:

$$I^{\mathrm{FV}}_{Q,x} = \frac{I^{\mathrm{RR}}_{Q,x}}{Q_{\mathrm{sys}}(\mathbf{Q})} = \frac{Q_{\mathrm{sys}}(\mathbf{Q}) - Q_{\mathrm{sys}}(Q_x := 0)}{Q_{\mathrm{sys}}(\mathbf{Q})} \tag{108}$$

$$I^{\mathrm{FV}}_{F,x} = \frac{I^{\mathrm{RR}}_{F,x}}{F_{\mathrm{sys}}(\mathbf{F})} = \frac{F_{\mathrm{sys}}(\mathbf{F}) - F_{\mathrm{sys}}(F_x := 0)}{F_{\mathrm{sys}}(\mathbf{F})} \tag{109}$$

$$I^{\mathrm{FV}}_{h,x} = \frac{I^{\mathrm{RR}}_{h,x}}{h_{\mathrm{sys}}(\mathbf{h},\mathbf{Q})} = \frac{h_{\mathrm{sys}}(\mathbf{h},\mathbf{Q}) - h_{\mathrm{sys}}(h_x := 0, Q_x := 0)}{h_{\mathrm{sys}}(\mathbf{h},\mathbf{Q})} \tag{110}$$

The Fussell-Vesely importance can be calculated very easily based on minimum cuts: $Q_{\mathrm{sys}}(Q_x := 0)$ is the fraction of system unavailability, which is supplied by the minimal cuts, containing base event x *not*. Consequently, $Q_{\mathrm{sys}}(\mathbf{Q}) - Q_{\mathrm{sys}}(Q_x := 0)$ is the fraction of system unavailability, which is supplied by the minimum cuts, which contain base event x. Thus, approximately (for small Q_{MCS}):

$$I^{\mathrm{FV}}_{Q,x} \approx \frac{\sum_{i=1}^{n_{\mathrm{MCS}}} \begin{cases} 0 & \text{if } \mathrm{BE}_x \notin \mathrm{MCS}_i \\ Q_{\mathrm{MCS},i} & \text{if } \mathrm{BE}_x \in \mathrm{MCS}_i \end{cases}}{Q_{\mathrm{sys}}(\mathbf{Q})} \tag{111}$$

The same holds for $I^{\mathrm{FV}}_{F,x}$ and $I^{\mathrm{FV}}_{h,x}$. The Fussell-Vesely importance is thus the probability, that at least one minimal cut, containing component x, has led to the system failure when the system failed.

Alternatively, you can use the formula of Esary-Proschan (54)

$$Q_{\mathrm{sys}}(t) \lessapprox 1 - \prod_{i=1}^{n_{\mathrm{MCS}}} (1 - Q_{\mathrm{MCS},i}(t)) \tag{112}$$

then you get

$$I^{\mathrm{FV}}_{Q,x} \approx \frac{1 - \prod_{i=1}^{n_{\mathrm{MCS}}} \begin{cases} 1 & \text{if } \mathrm{BE}_x \notin \mathrm{MCS}_i \\ 1 - Q_{\mathrm{MCS},i} & \text{if } \mathrm{BE}_x \in \mathrm{MCS}_i \end{cases}}{Q_{\mathrm{sys}}(\mathbf{Q})} \tag{113}$$

D.6 Risk Achievement (RA)

For unavailability and unreliability, risk achievement (RA) is defined as follows:

$$I^{\mathrm{RA}}_{Q,x} = Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(\mathbf{Q}) \tag{114}$$

$$I^{\mathrm{RA}}_{F,x} = F_{\mathrm{sys}}(F_x := 1) - F_{\mathrm{sys}}(\mathbf{F}) \tag{115}$$

With the previously introduced definition of partial derivative (Birnbaum importance) and risk-reduction potential, the following applies immediately:

$$\begin{aligned} I^{\mathrm{RA}}_{Q,x} + I^{\mathrm{RR}}_{Q,x} &= (Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(\mathbf{Q})) + (Q_{\mathrm{sys}}(\mathbf{Q}) - Q_{\mathrm{sys}}(Q_x := 0)) \\ &= Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(Q_x := 0) \\ &= I^{\mathrm{PD}}_{Q,x} \end{aligned} \tag{116}$$

No RA can be specified for the system failure rate h, since the failure rate of a component (or in general: the occurrence rate of an event) is not dimensionless and therefore does not know an upper bound $h_{\max}$, and therefore there is no upper bound $h_{\mathrm{sys}}(h_{\max,x})$.

D.7 Risk-Achievement-Worth (RAW)

If one puts the RA in relation to the original system size, we get the factor by which the risk would increase, if the component x had always failed (Risk-Achievement-Worth, RAW):

$$I^{\mathrm{RAW}}_{Q,x} = \frac{Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(\mathbf{Q})}{Q_{\mathrm{sys}}(\mathbf{Q})} = \frac{Q_{\mathrm{sys}}(Q_x := 1)}{Q_{\mathrm{sys}}(\mathbf{Q})} - 1 \tag{117}$$

$$I^{\mathrm{RAW}}_{F,x} = \frac{F_{\mathrm{sys}}(F_x := 1) - F_{\mathrm{sys}}(\mathbf{F})}{F_{\mathrm{sys}}(\mathbf{F})} = \frac{F_{\mathrm{sys}}(F_x := 1)}{F_{\mathrm{sys}}(\mathbf{F})} - 1 \tag{118}$$

Attention: The summand -1 is often omitted.

As for the RA, the RAW is not applicable for failure rates, since in general no limit value exists.

D.8 Criticality Importance (CRI)

Criticality Importance (CRI) is defined as the ratio of the relative change in system size to the relative change in component size:

$$I^{\mathrm{CRI}}_{Q,x} = \frac{\frac{\partial Q_{\mathrm{sys}}}{Q_{\mathrm{sys}}}}{\frac{\partial Q_x}{Q_x}} = \frac{Q_{\mathrm{sys}}(\mathbf{Q} + \partial Q_x) - Q_{\mathrm{sys}}(\mathbf{Q})}{Q_{\mathrm{sys}}(\mathbf{Q})} \cdot \frac{Q_x}{\partial Q_x} = I^{\mathrm{PD}}_{Q,x} \cdot \frac{Q_x}{Q_{\mathrm{sys}}(\mathbf{Q})} \tag{119}$$

$$I^{\mathrm{CRI}}_{F,x} = \frac{\frac{\partial F_{\mathrm{sys}}}{F_{\mathrm{sys}}}}{\frac{\partial F_x}{F_x}} = \frac{F_{\mathrm{sys}}(\mathbf{F} + \partial F_x) - F_{\mathrm{sys}}(\mathbf{F})}{F_{\mathrm{sys}}(\mathbf{F})} \cdot \frac{F_x}{\partial F_x} = I^{\mathrm{PD}}_{F,x} \cdot \frac{F_x}{F_{\mathrm{sys}}(\mathbf{F})} \tag{120}$$

It can be extended to the failure rate, by describing the component quantities h_x and Q_x as a function of the failure rate of the component, as in the case of the partial derivative:

$$I^{\mathrm{CRI}}_{h,x} = \frac{\frac{\partial h_{\mathrm{sys}}}{h_{\mathrm{sys}}}}{\frac{\partial \lambda_x}{\lambda_x}} = \frac{h_{\mathrm{sys}}(\boldsymbol{\lambda} + \partial \lambda_x) - h_{\mathrm{sys}}(\boldsymbol{\lambda})}{h_{\mathrm{sys}}(\boldsymbol{\lambda})} \cdot \frac{\lambda_x}{\partial \lambda_x} = I^{\mathrm{PD}}_{h,x} \cdot \frac{\lambda_x}{h_{\mathrm{sys}}(\boldsymbol{\lambda})} \tag{121}$$

It is the probability that component x led to the failure, when the system failed. It thus gives an indication where to look for the failure first, when the system has failed. Or put another way: The greater the criticality importance, the stronger the effect of a relative improvement of the component. It is therefore sometimes called Upgrading Importance.

D.9 Importances for generic basic events

It is also interesting to ask, how much the system property Q_{sys}, F_{sys} or h_{sys} changes, if one changes a component which is used multiple times. Thus, it is not the importance of a single event that is considered, but the importance of all events which refer to the same generic basic event (GBE), including possibly existing common cause factors β. This is included in the following section for Example 3.

In particular, the importances I^{PD} and I^{CRI} are important with respect to generic basic events, because they indicate how much the system size changes in absolute and relative terms, respectively, if the base size changes – for instance because it is not known exactly.

For fault trees, the partial derivative after the generic basic event xgen for system unavailability is calculated using the approximate formula (53) to be

$$\mathrm{I}^{\text{PD}}_{\text{Q,xgen}} \approx \frac{\partial \sum\limits_{i=1}^{n_{\text{MCS}}} \left(\prod\limits_{j=1}^{m_{\text{Lit},i}} Q_j(t) \right)}{\partial Q_{\text{xgen}}} = \sum_{i=1}^{n_{\text{MCS}}} \begin{cases} 0 & \text{if GBE } x \notin \text{MCS}_i \\ a Q_{\text{xgen}}^{a-1} \prod\limits_{j=1, j\neq \text{xgen}}^{m_{\text{Lit},i}} Q_j & \text{wenn GBE } x \in \text{MCS}_i \end{cases} \tag{122}$$

where a means the number of basic events in the minimum cut i, which refer to the same generic basic event xgen. The expression $j \neq$ xgen means, that all basic events, which refer to the generic basic event xgen, are to be ignored, regardless of their index in the minimal cut.

The partial derivative for the system failure rate is calculated based on minimum cuts to be

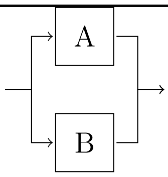
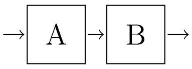
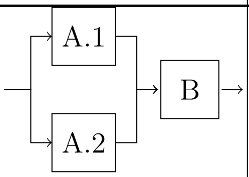
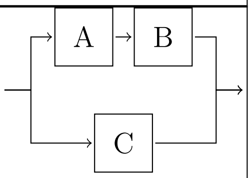
$$\mathrm{I}^{\text{PD}}_{\text{h,xgen}} \approx \sum_{i=1}^{n_{\text{MCS}}} \begin{cases} 0 & \text{if GBE } x \notin \text{MCS}_{\text{i}} \\ a^2 \lambda_{\text{xgen}}^{a-1} \left(\dfrac{\partial Q_{\text{xgen}}}{\partial \lambda_{\text{xgen}}} \right)^{a-1} \cdot \prod\limits_{j=1, j\neq \text{xgen}}^{m_{\text{Lit},i}} Q_j & \\ + a \lambda_{\text{xgen}}^{a-1} \left(\dfrac{\partial Q_{\text{xgen}}}{\partial \lambda_{\text{xgen}}} \right)^{a} \cdot \sum\limits_{j=1, j\neq \text{xgen}}^{m_{\text{Lit},i}} \left(h_j \cdot \prod\limits_{k=1, k\neq j, k\neq x}^{m_{\text{Lit},i}} Q_k \right) & \text{if GBE } x \in \text{MCS}_{\text{i}} \end{cases} \tag{123}$$

D.10 Example importances for system unavailability

For some simple architectures, the importances with respect to Q_{sys} are mentioned in the following table. In Example 3, two similar events A.1 and A.2 are ANDed. Thus, the importances introduced in section D.9 with respect to the underlying generic basic event (A) are also of interest here. These are denoted here by $I_{\text{Q,genA}}$, whereas $I_{\text{Q,A}}$ denotes the importance of the single event A.1 or A.2, respectively. A common-cause factor between A.1 and A.2 was not assumed ($\beta_A = 0$).

Note: The mean values $\overline{Q_x}$ were always used in the calculations, i. e. $\overline{Q_{\text{A.1}}} \cdot \overline{Q_{\text{A.2}}}$ instead of $1/T \cdot \int_0^T Q_{\text{A.1}}(t) \cdot Q_{\text{A.2}}(t)\ dt$. In addition, the approximation formula (41) was used for the unavailabilities of the single events.

Table 6: *Importances for Q_{sys} for simple architectures.*

Value	Example 1	Example 2	Example 3	Example 4
Block diagram				
Minimal-cut sets	{A & B}	{A}, {B}	{A.1 & A.2}, {B}	{A & C}, {B & C}
λ_A	1E−4/h	1E−4/h	1E−4/h	1E−4/h
$T_{\text{test,A}}$	1000 h	1000 h	1000 h	1000 h
λ_B	1E−3/h	1E−3/h	1E−6/h	1E−5/h
$T_{\text{test,B}}$	10 h	10 h	10 h	
λ_C			1E−3/h	
$T_{\text{test,C}}$			50 h	
$\overline{Q_A}$	0.050 000	0.050 000	0.050 000	
$\overline{Q_B}$	0.005 000	0.005 000	0.000 005	0.000 050
$\overline{Q_C}$			0.025 000	
Q_{sys}	$Q_A \cdot Q_B$	$Q_A + (1 - Q_A) \cdot Q_B$	$Q_B + (1 - Q_B) \cdot Q_{A.1} \cdot Q_{A.2}$	$Q_C \cdot (Q_A + (1 - Q_A) \cdot Q_B)$
$\overline{Q_{\text{sys}}}$	0.000 250 00	0.054 750 00	0.002 504 99	0.001 251 19
$Q_{\text{sys}}(Q_{\text{A}} := 0)$	0.000 000 00	0.005 000 00	0.000 005 00	0.000 001 25
$Q_{\text{sys}}(Q_{\text{A}} := 1)$	0.005 000 00	1.000 000 00	0.050 004 75	0.025 000 00
$Q_{\text{sys}}(Q_{\text{B}} := 0)$	0.000 000	0.050 000	0.002 500 00	0.001 250 00
$Q_{\text{sys}}(Q_{\text{B}} := 1)$	0.050 000	1.000 000	1.000 000	0.025 000 00
$Q_{\text{sys}}(Q_{\text{C}} := 0)$			0.000 000 00	
$Q_{\text{sys}}(Q_{\text{C}} := 1)$			0.050 047 50	
$Q_{\text{sys}}(Q_{\text{genA}} := 0)$	0.000 000	0.005 000 00	0.000 005 00	0.000 001 25
$Q_{\text{sys}}(Q_{\text{genA}} := 1)$	0.005 000 00	1.000 000 00	1.000 000 00	0.025 000 00
I^{PD} via derivation:				
$\text{I}^{\text{PD}}_{\text{Q,A}}$	0.005 000 00	0.995 000 00	0.050 000	0.024 998 75
$\text{I}^{\text{PD}}_{\text{Q,B}}$	0.050 000	0.950 000	0.997 500 00	0.023 750 00
$\text{I}^{\text{PD}}_{\text{Q,C}}$			0.050 047 50	
$\text{I}^{\text{PD}}_{\text{Q,genA}}$	0.005 000 00	0.995 000 00	0.099 999 50	0.024 998 75

continued on next page

Value	Example 1	Example 2	Example 3	Example 4
I^{PD} over $Q_{\mathrm{sys}}(Q_x := 1) - Q_{\mathrm{sys}}(Q_x := 0)$				
$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,A}}$	0.005 000 00	0.995 000 00	0.049 999 75	0.024 998 75
$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,B}}$	0.050 000	0.950 000	0.997 500 00	0.023 750 00
$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,C}}$			0.050 047 50	
$\mathrm{I}^{\mathrm{PD}}_{\mathrm{Q,genA}}$	0.005 000 00	0.995 000 00	0.999 995 00 (f)	0.024 998 75
$\mathrm{I}^{\mathrm{RR}} = Q_{\mathrm{sys}} - Q_{\mathrm{sys}}(Q_x := 0)$				
$\mathrm{I}^{\mathrm{RR}}_{\mathrm{Q,A}}$	0.000 250 00	0.049 750 00	0.002 499 99	0.001 249 94
$\mathrm{I}^{\mathrm{RR}}_{\mathrm{Q,B}}$	0.000 250 00	0.004 750 00	0.000 004 99	0.000 001 19
$\mathrm{I}^{\mathrm{RR}}_{\mathrm{Q,C}}$			0.001 251 19	
$\mathrm{I}^{\mathrm{RR}}_{\mathrm{Q,genA}}$	0.000 250 00	0.049 750 00	0.002 499 99	0.001 249 94
$\mathrm{I}^{\mathrm{RRW}} = Q_{\mathrm{sys}}/Q_{\mathrm{sys}}(Q_x := 0) - 1$				
$\mathrm{I}^{\mathrm{RRW}}_{\mathrm{Q,A}}$	∞	9.950 000	499.997 500 00	999.950 000
$\mathrm{I}^{\mathrm{RRW}}_{\mathrm{Q,B}}$	∞	0.095 000 00	0.001 995 00	0.000 950 00
$\mathrm{I}^{\mathrm{RRW}}_{\mathrm{Q,C}}$			∞	
$\mathrm{I}^{\mathrm{RRW}}_{\mathrm{Q,genA}}$	∞	9.950 000 00	499.997 500 00	999.950 000 00
I^{FV} via $\mathrm{I}_{\mathrm{RR}}/Q_{\mathrm{sys}}$:				
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,A}}$	1.000 000 00	0.908 675 80	0.998 003 98	0.999 000 95
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,B}}$	1.000 000 00	0.086 757 99	0.001 991 03	0.000 949 10
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,genA}}$	1.000 000 00	0.908 675 80	0.998 003 98	0.999 000 95
I^{FV} over $1 - Q_{\mathrm{sys}}(x := 0)/Q_{\mathrm{sys}}$:				
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,A}}$	1.000 000 00	0.908 675 80	0.998 003 98	0.999 000 95
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,B}}$	1.000 000 00	0.086 757 99	0.001 991 03	0.000 949 10
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,genA}}$	1.000 000 00	0.908 675 80	0.998 003 98	0.999 000 95
I^{FV} over minimal cuts:				
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,A}}$	1.000 000 00	0.913 242 01	0.998 008 97	0.999 050 90
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,B}}$	1.000 000 00	0.091 324 20	0.001 996 02	0.000 999 05
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{Q,genA}}$	1.000 000 00	0.913 242 01	0.998 008 97	0.999 050 90
$\mathrm{I}^{\mathrm{RA}} = Q_{\mathrm{sys}}(x := 1) - Q_{\mathrm{sys}}$:				
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,A}}$	0.004 750 00	0.945 250 00	0.047 499 76	0.023 748 81
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,B}}$	0.049 750 00	0.945 250 00	0.997 495 01	0.023 748 81
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,C}}$			0.048 796 31	
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,genA}}$	0.004 750 00	0.945 250 00	0.997 495 01 (f)	0.023 748 81
$\mathrm{I}^{\mathrm{RA}} = \mathrm{I}^{\mathrm{PD}} - \mathrm{I}^{\mathrm{RR}}$:				
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,A}}$	0.004 750 00	0.945 250 00	0.047 500 01	0.023 748 81
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,B}}$	0.049 750 00	0.945 250 00	0.997 495 01	0.023 748 81
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,C}}$			0.048 796 31	
$\mathrm{I}^{\mathrm{RA}}_{\mathrm{Q,genA}}$	0.004 750 00	0.945 250 00	0.097 499 51	0.023 748 81

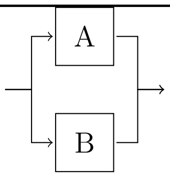
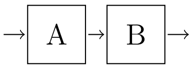
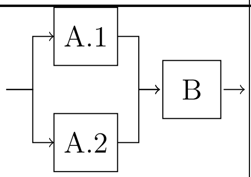
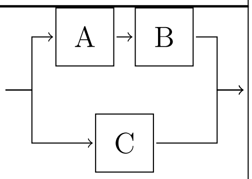
continued on next page

Value	Example 1	Example 2	Example 3	Example 4
$\mathrm{I}^{\mathrm{RAW}} = Q_{\mathrm{sys}}(x := 1)/Q_{\mathrm{sys}} - 1$:				
$\mathrm{I}^{\mathrm{RAW}}_{\mathrm{Q,A}}$	19.000 000 00	17.264 840 18	18.962 075 66	18.981 018 03
$\mathrm{I}^{\mathrm{RAW}}_{\mathrm{Q,B}}$	199.000 000 00	17.264 840 18	398.203 588 84	18.981 018 03
$\mathrm{I}^{\mathrm{RAW}}_{\mathrm{Q,C}}$			39.000 000 00	
$\mathrm{I}^{\mathrm{RAW}}_{\mathrm{Q,genA}}$	19.000 000 00	17.264 840 18	398.203 588 84	18.981 018 03
$\mathrm{I}^{\mathrm{CRI}} = \mathrm{I}^{\mathrm{PD}} \cdot Q_x/Q_{\mathrm{sys}}$:				
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{Q,A}}$	1.000 000 00	0.908 675 80	0.998 008 97	0.999 000 95
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{Q,B}}$	1.000 000 00	0.086 757 99	0.001 991 03	0.000 949 10
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{Q,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{Q,genA}}$	1.000 000 00	0.908 675 80	1.996 007 96	0.999 000 95

D.11 Example importances for system failure rate

For some simple architectures, the importances with respect to h_{sys} are mentioned in the following table. In Example 3, two similar events A.1 and A.2 are ANDed. Thus, the importances introduced in section D.9 with respect to the underlying generic base event are also of interest here. These are denoted here by $I_{\mathrm{h,genA}}$, whereas $I_{\mathrm{h,A}}$ denotes the importance of the single event A.1 or A.2, respectively.

Table 7: *Importances for h_{sys} for simple architectures*

Value	Example 1	Example 2	Example 3	Example 4
Block diagram				
minimal-cuts	{A & B}	{A}, {B}	{A.1 & A.2}, {B}	{A & C}, {B & C}
λ_A	1E−4/h	1E−4/h	1E−4/h	1E−4/h
$T_{\mathrm{test,A}}$	1000 h	1000 h	1000 h	1000 h
λ_B	1E−3/h	1E−3/h	1E−6/h	1E−5/h
$T_{\mathrm{test,B}}$	10 h	10 h	10 h	
λ_C			1E−3/h	
$T_{\mathrm{test,C}}$			50 h	
$\overline{Q_A}$	0.050 000	0.050 000	0.050 000	
$\overline{Q_B}$	0.005 000	0.005 000	0.000 005	0.000 050
$\overline{Q_C}$			0.025 000	
h_{sys}	$h_A \cdot Q_B + h_B \cdot Q_A$	$h_A + h_B$	$h_{A.1} \cdot Q_{A.2} + h_{A.2} \cdot Q_{A.1} + h_B$	$h_A \cdot Q_C + h_C \cdot Q_A + h_B \cdot Q_C + h_C \cdot Q_B$

continued on next page

Value	**Example 1**	**Example 2**	**Example 3**	**Example 4**
h_{sys}	$h_A \cdot h_B \cdot (T_A + T_B)/2$	$h_A + h_B$	$h_A \cdot h_A \cdot T_A + h_B$	$h_A \cdot h_C \cdot (T_A + T_C)/2 + h_B \cdot h_C \cdot (T_B + T_C)/2$
h_{sys}	5.0500E−5/h	1.1000E−3/h	1.1000E−5/h	5.2800E−5/h
$h_{\text{sys}}(A{:=}0)$	0.000 000 00/h	0.001 000 00/h	0.000 001 00/h	0.000 000 30/h
$h_{\text{sys}}(B{:=}0)$	0.000 000/h	0.000 100 00/h	0.000 010 00/h	0.000 052 50/h
$h_{\text{sys}}(C{:=}0)$			0.000 000 00/h	
$h_{\text{sys}}(\text{genA}{:=}0)$	0.000 000 00/h	0.001 000 00/h	0.000 001 00/h	0.000 000 30/h
I^{PD} via derivative:				
$\partial h_{\text{sys}}/\partial\lambda_A$	$h_B \cdot (T_A + T_B)/2$	1	$h_A \cdot T_A$	$h_C \cdot (T_A + T_C)/2$
$\partial h_{\text{sys}}/\partial\lambda_B$	$h_A \cdot (T_A + T_B)/2$	1	1	$h_C \cdot (T_B + T_C)/2$
$\partial h_{\text{sys}}/\partial\lambda_C$			$h_A \cdot (T_A + T_C)/2 + h_B \cdot (T_B + T_C)/2$	
$\partial h_{\text{sys}}/\partial\lambda_{\text{genA}}$	$h_B \cdot (T_A + T_B)/2$	1	$2h_A \cdot T_A$	$h_C \cdot (T_A + T_C)/2$
$\text{I}^{\text{PD}}_{\text{h,A}}$	0.505 000 00	1.000 000 00	0.100 000 00	0.525 000 00
$\text{I}^{\text{PD}}_{\text{h,B}}$	0.050 500 00	1.000 000	1.000 000	0.030 000
$\text{I}^{\text{PD}}_{\text{h,C}}$			0.052 800 00	
$\text{I}^{\text{PD}}_{\text{h,genA}}$	0.505 000 00	1.000 000	0.200 000 00	0.525 000 00
$\text{I}^{\text{RR}} = h_{\text{sys}} - h_{\text{sys}}(x := 0)$:				
$\text{I}^{\text{RR}}_{\text{h,A}}$	0.000 050 50/h	0.000 100 00/h	0.000 010 00/h	0.000 052 50/h
$\text{I}^{\text{RR}}_{\text{h,B}}$	0.000 050 50/h	0.001 000 00/h	0.000 001 00/h	0.000 000 30/h
$\text{I}^{\text{RR}}_{\text{h,C}}$			0.000 052 80/h	
$\text{I}^{\text{RR}}_{\text{h,genA}}$	0.000 050 50/h	0.000 100 00/h	0.000 010 00/h	0.000 052 50/h
$\text{I}^{\text{RRW}} = h_{\text{sys}}/h_{\text{sys}}(x := 0) - 1$:				
$\text{I}^{\text{RRW}}_{\text{h,A}}$	∞	0.100 000 00	10.000 000 00	175.000 000 00
$\text{I}^{\text{RRW}}_{\text{h,B}}$	∞	10.000 000 00	0.100 000 00	0.005 714 29
$\text{I}^{\text{RRW}}_{\text{h,C}}$			∞	
$\text{I}^{\text{RRW}}_{\text{h,genA}}$	∞	0.100 000 00	10.000 000 00	175.000 000 00
I^{FV} via $\text{I}^{\text{RR}}/h_{\text{sys}}$:				
$\text{I}^{\text{FV}}_{\text{h,A}}$	1.000 000 00	0.090 909 09	0.909 090 91	0.994 318 18
$\text{I}^{\text{FV}}_{\text{h,B}}$	1.000 000 00	0.909 090 91	0.090 909 09	0.005 681 82
$\text{I}^{\text{FV}}_{\text{h,C}}$			1.000 000 00	
$\text{I}^{\text{FV}}_{\text{h,genA}}$	1.000 000 00	0.090 909 09	0.909 090 91	0.994 318 18
I^{FV} over $1 - h_{\text{sys}}(x := 0)/h_{\text{sys}}$:				
$\text{I}^{\text{FV}}_{\text{h,A}}$	1.000 000 00	0.090 909 09	0.909 090 91	0.994 318 18
$\text{I}^{\text{FV}}_{\text{h,B}}$	1.000 000 00	0.909 090 91	0.090 909 09	0.005 681 82
$\text{I}^{\text{FV}}_{\text{h,C}}$			1.000 000 00	

continued on next page

Value	Example 1	Example 2	Example 3	Example 4
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{h,genA}}$	1.000 000 00	0.090 909 09	0.909 090 91	0.994 318 18
I^{FV} via minimal cuts:				
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{h,A}}$	1.000 000	0.090 909 09	0.909 090 91	0.994 318 18
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{h,B}}$	1.000 000 00	0.909 090 91	0.090 909 09	0.005 681 82
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{h,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{FV}}_{\mathrm{h,genA}}$	1.000 000 00	0.090 909 09	0.909 090 91	0.994 318 18
$\mathrm{I}^{\mathrm{CRI}} = \mathrm{I}^{\mathrm{PD}} \cdot h_x / h_{\mathrm{sys}}$:				
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{h,A}}$	1.000 000	0.090 909 09	0.909 090 91	0.994 318 18
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{h,B}}$	1.000 000 00	0.909 090 91	0.090 909 09	0.005 681 82
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{h,C}}$			1.000 000 00	
$\mathrm{I}^{\mathrm{CRI}}_{\mathrm{h,genA}}$	1.000 000 00	0.090 909 09	1.818 182	0.994 318 18

E Glossary and list of abbreviations

Table 8: *Terms and abbreviations*

Term	**Meaning**
$\lessapprox$	About the same, but certainly smaller. Means here: The formula is slightly conservative, but for correctly designed systems (unavailabilities only slightly larger than zero) practically well usable.
Failure density	$f(t)$, derivative of →unreliability.
Failure rate	→occurrence rate.
Basic event	An event of a →element.
Condition	Condition Event. A basic event described only by a probability (typ. unavailability), not by an occurrence rate.
β	The common cause factor relating to the occurrence rate or unavailability of multiple events that are not completely independent.
Occurrence rate	The rate of occurrence of an event conditioned with respect to availability or reliability. When it refers to an event describing a failure, also called failure rate.
Element	Any →component, human behavior, or environmental condition, that affects the behavior of the system.
Event	A situation or state that an element or system can enter.
EUC	Equipment under Control, term from [IEC 61508], here always denoted by "process".
$f(t)$	→failure density
$F(t)$	→unreliability
Failure rate	→Occurrence rate
FT	Fault Tree, Fault Tree
FTA	Fault tree analysis
h	→occurrence rate
HR	Hazard Rate, actual or calculated (i. e., estimated) occurrence rate of a hazard.
Edge	The representation of a basic event in a Markov model.
Component	A technical unit that can usually fail with different failure modes.
MRT	Mean repair time, mean time between detection of a failure and repair, if the process (in [IEC 61508]: the "EUC") is still operated in case of a detected failure.
MTTD	Mean time to detect, mean time to detect failure.
MTTF	Mean time to failure and also mean time of fault free operation between two failures.

continued on next page

Table 8: *Terms and abbreviations*

Term	**Meaning**
MTTR	Mean time to restoration. Recovery time. Includes the →MTTD and the →MRT.
Unavailability	probability $Q(t)$ that a →element will not work, if it is requested at time t.
PFD	Probability of Failure on Demand, denoting the mean →unavailability $\overline{Q}$ in [IEC 61508].
PFH	Probability of Failure per Hour, designation of the mean conditional failure frequency (failure rate) → *overlineh* of a system in [IEC 61508].
PFTT	Process Fault Tolerance Time, also Process Safety Time, time a process can be operated with incorrect manipulated variables without entering an unsafe status.
PI	Prime Implicant, Prime Implicant. Equivalent of a minimum cut in the case of incoherent fault trees. In the case of coherent fault trees, prime implicants are identical to minimal cuts.
Q	→unavailability
Sub-tree	A partial fault tree referenced by transfer gate as → branch in a higher fault tree.
System lifetime	The planned deployment time of the system under consideration. Needed when the quantity of interest is not constant and not periodic, i. e., in particular to determine → unreliability, or when basic events of the model "non-restorable" are included in the fault tree or Markov model.
THR	Tolerable Hazard Rate, target for safety functions with continuous or frequent demand.
TPFD	Tolerable Probability of Failure on Demand, acceptable unavailability, target value for safety functions with rare (low) demand.
TPFH	Tolerable Probability of Failure per Hour, acceptable failure rate, target for safety functions with continuous or frequent demand. Mathematically and at the top level also logically identical to →THR.
Unreliability	probability $F(t_1, t_2)$ that a →element fails during the time period $t_1 \ldots t_2$.

continued on next page

Table 8: *Terms and abbreviations*

Term	**Meaning**
$w(t)$	occurrence frequency in the case of testable and/or repairable events. Unlike $h(t)$, $w(t)$ is conditional only with respect to the last test or replacement, not with respect to the availability of the system. Thus, $w(t)$ is often referred to as unconditional occurrence frequency. Unlike $f(t)$, $w(t)$ is conditional with respect to the last test or swap, so its integral over time can become larger than 1.
Branch	The part of a fault tree, which is below a certain gate including the gate itself. Special case: a base event is also a branch.

F Bibliography

References

[EN 50126] *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, CENELEC (2017).

[EN 50129] *Railway Applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*, CENELEC (2017).

[EN 61025] *Fault tree analysis (FTA)*, IEC (2006).

[EN 61165] *Application of Markov techniques*, IEC (2006)

[IEC 61508] *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC (2010).

[IEC 61508-6] *Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*, IEC (2010)

[ISO 13849] *Safety of machinery – Safety-related parts of control systems*, ISO (2015)

[ISO 26262] *Road vehicles – Functional safety*, ISO (2011)

[NUREG] *The Fault Tree Handbook*, NUREG-0492, US Nuclear Regulatory Commission (1981).

[U. Weber] *Theory and Execution of Fault Tree Analyses for Railway Applications*, TÜV SÜD Rail GmbH (2010)

[ASTRA TM] *ASTRA 3.x: Theoretical Manual*, Sergio Contini and Vaidas Matuzas, EUR 25052 EN 2011

[PSA IMP] *An overview of PSA importance measures*, M. van der Borst, H. Schoonakker, Reliability Engineering and System Safety 72 (2001) 241-245.

G History of changes

Table 9: *History of changes*

Date	**Change**
29.11.2025	Formula (62) replaced by formula (28)