# An Improved Estimation of Multiple-Point Fault Probabilities if the Faults Have Different Periodic Latencies

*by Frank Edler, Michael Soden and René Hankammer*
*Germany*

Fault tree analysis (FTA), reliability block diagrams (RBD) and event tree analysis (ETA) are established methods for assessing potential risks of hazardous events, in particular when resulting from coincidental events. Combining the Boolean algebra, probability theory and reliability data, they allow quantitative estimation of intrinsic risks from technical equipment like machinery control, aerospace systems or vehicle functions, among many others.

The quantitative reliability theory was mainly developed between the 1960s and the 1980s. At that time, simplifications and approximations for the mathematical formulae were needed to achieve calculation results within acceptable time, regarding restricted computer resources.

Our investigation revealed that some of these simplifications and approximations, often assumed as precise calculations in secondary literature, can lead to wrong results in quantitative risk assessment. When faults are combined, and individual latency periods exist, the currently established approximations may lead to results which are too optimistic in comparison with a precise probabilistic approach.

This publication proposes a new approximation for the computation of the related probabilities. The approach provides an upper-bound estimation. Using the developed formulae, the under-estimation of multiple-event probabilities can be avoided.

In addition, certain vagueness and over-simplification in the probabilistic treatment of events with latency periods can be eliminated. Examples of related shortcomings in the literature can be found, down to the early roots of reliability theory.

## 1. Introduction

### 1.1. Elementary Definitions and Terms

The theory for the determination of random fault probabilities distinguishes between following functions:

1. The **unreliability *P(T)*** — also found represented as *F(T)* — is a measure of the probability that a fault occurs during a given time span *T*, often called mission time (also system lifetime), during which the system is operating
2. The **unavailability *Q(t)*** is a measure of the probability that a fault (or combination of faults) is present at a given point in time *t*

NOTE: It is worthwhile to mention that certain secondary literature does not clearly distinguish between these functions, despite their different meanings and their time dependencies [Refs. 1 and 2].

### 1.2. Basic concepts for the Probabilistic Approach with Regard to System Safety and Reliability

One can find two elementary types of models for systems reliability and safety:

#### *1.2.1. Complete Separation of Control System and Supervising (Safety) System*

Such a system (safety) architecture is often found in machinery control, where the equipment under control (EUC) and the safety related system (SRS) are implemented independently (see IEC 61508) [Ref. 3].

The appropriate metric for a probabilistic safety evaluation is the so-called average probability of dangerous failure on demand ($PFD_{avg}$) of the SRS, if safety requirements are exclusively allocated to the SRS, and interventions (fault reactions) of the safety functions of the SRS are needed only in the "low demand mode of operation" [Ref. 3].

In the following, we will use the average unavailability $Q_{avg}$ synonymously for the $PFD_{avg}$:

$$PFD_{avg} = Q_{avg} \tag{1}$$

#### *1.2.2. Embedded Supervising (Safety) Systems*

If a separation between the control system and the supervising (safety) system cannot be argued, the overall system needs to be evaluated with regard to fault occurrence probability *P*. An example is a brake control system for automotive applications where the core system performs both the control functions (e.g., for ESP interventions), the fault diagnosis and the failure reaction in the same control unit.

In this case, safety requirements are allocated to the overall system and the appropriate metric for a probabilistic safety evaluation is the so-called probability of dangerous failure per hour (*PFH*) [Ref. 3].

$$PFH = \frac{P_{sys}(T)}{T} \tag{2}$$

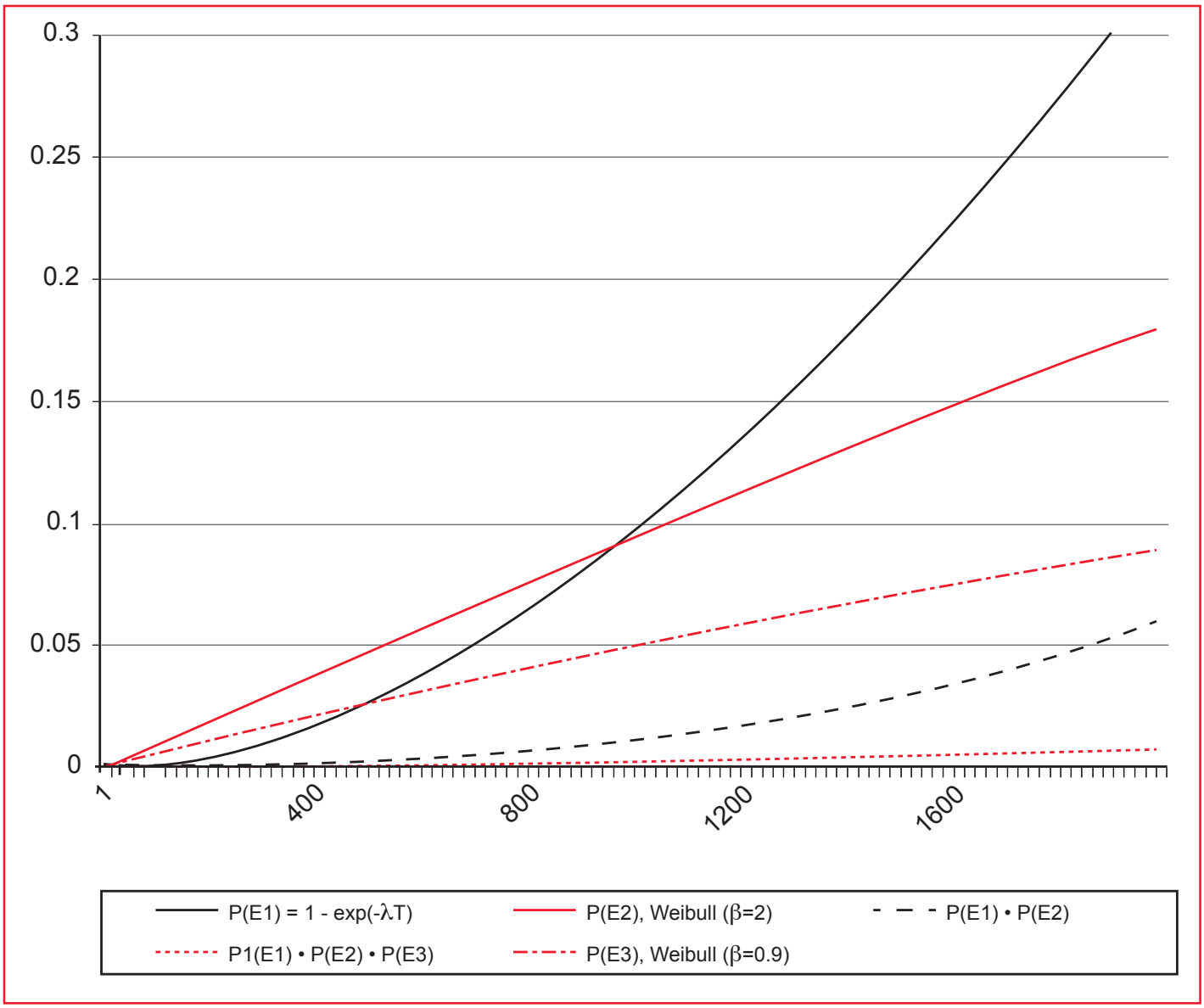


*Figure 1 — Examples for Fault Occurrence Probability Functions* P(t).

This definition is provided by IEC 61508-1:2010, section 7.6.2.9, defining the *PFH* as "the average frequency of a dangerous failure of the safety function" [Ref. 3].

**Notes:** ISO 26262 defines a similar metric, called the "probabilistic metric for random hardware failures" (*PMHF*). Also, other industry sectors (aerospace, for instance) require equivalent probabilistic assessments [Ref. 4].

### 1.3. Time Dependency of Fault Probabilities

Per the definition, probabilities $P$ are values $0 \le P \le 1$. This is valid for every time interval within the mission time $T$. The probability of random fault occurrence $P(t)$ rises monotonically with increasing time $t$. For a given time interval $T$, this means that $P(T) \ge P(t)$ for every point in time $[0 \le t \le T]$. In the literature dealing with system reliability and system safety, this probability is also called the *unreliability* of a system.

It is worthwhile to mention that these statements are valid for every consideration of random faults, regardless of whether they are single faults or logical combinations of more than one fault.

If different faults are independent from each other, each of these faults has its individual occurrence probability function $P_i(t)$.

If we seek the system fault occurrence probability function $P_{sys}(t)$, we need to know which logical combinations of individual faults lead to the system fault under analysis.

To evaluate systems' reliability and safety, several analysis methods have been developed, providing models for multiple fault consideration based on Boolean algebra. Such Boolean analyses include Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and Reliability Block Diagrams (RBD).

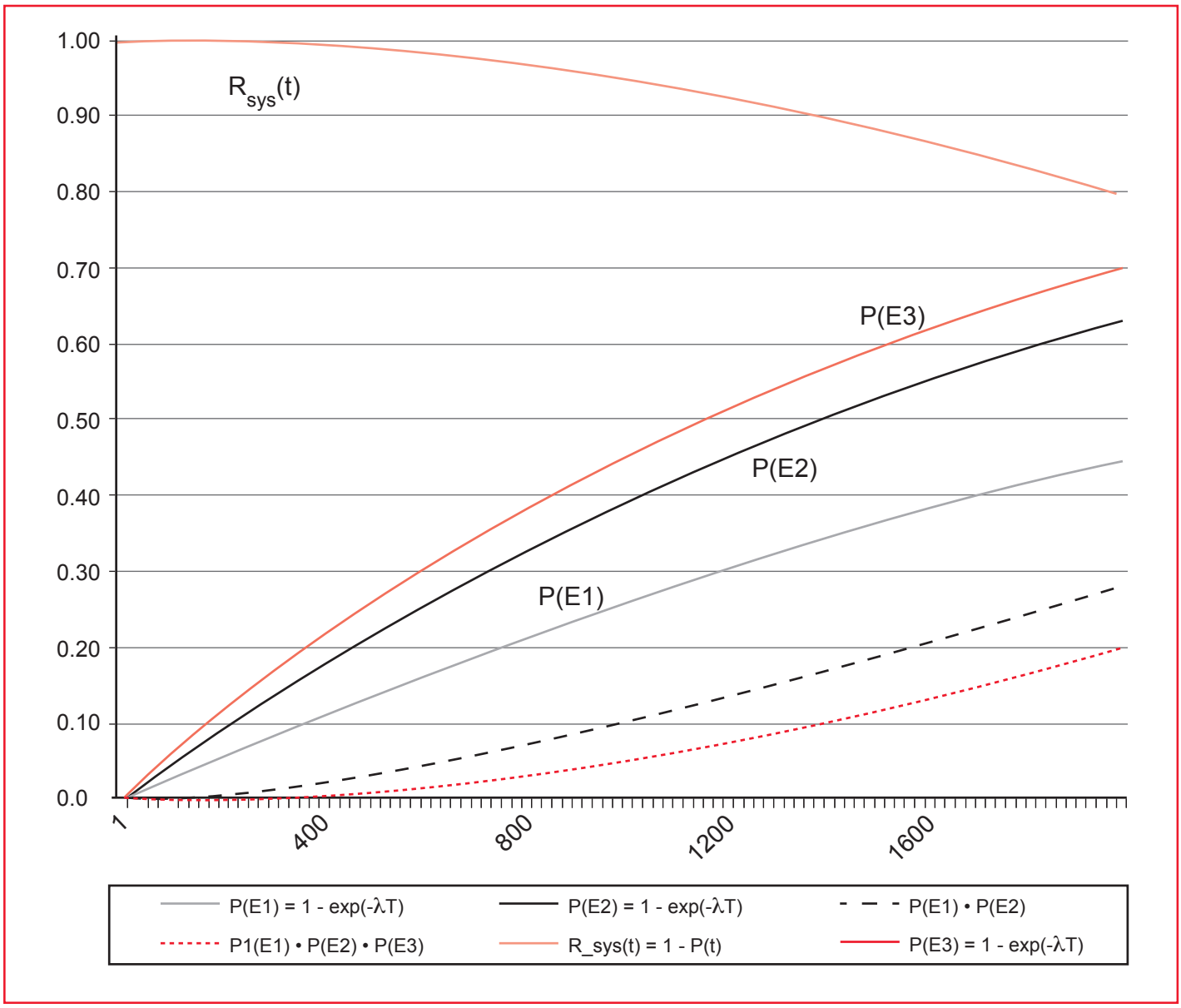


*Figure 2 — Time Dependency of the Occurrence Probability for an AND-Combination of Three Independent Faults Without Intermediate Repair or Inspection (Non-Repairable System).*

In particular, these Boolean analyses provide the possibility to evaluate redundant system architectures, where critical system faults may result from logical AND-combinations of individual faults.

If the following conditions are given:

1. the faults $F_1 \ldots F_N$ are mutual independent, and
2. for none of the potential faults $F_1 \ldots F_N$ tests or repair apply (i.e. *no individual latencies* have to be considered, which is treated in section 2) during the whole mission time $T$

the occurrence probability of the AND-combination of $N$ faults at any point in time $[0 \le t \le T]$ then is determined by the product:

$$P_{AND}(t) = \prod_{n=1}^{N} P_n(t) \qquad (3)$$

To determine the individual fault occurrence probability functions $P_n(t)$, specific reliability data in terms of failure models are needed.

Various failure models for this are described in the literature. Examples are constant failure rates and Weibull-distributed failure rates, among others.

Such failure models allow for the calculation of fault occurrence probability in function of time $P(t)$, based on one or few parameters that determine the shape of $P_n(t)$.

As we see, the occurrence probability $P(t)$ for multiple combinations of individual faults is generally a complex function.

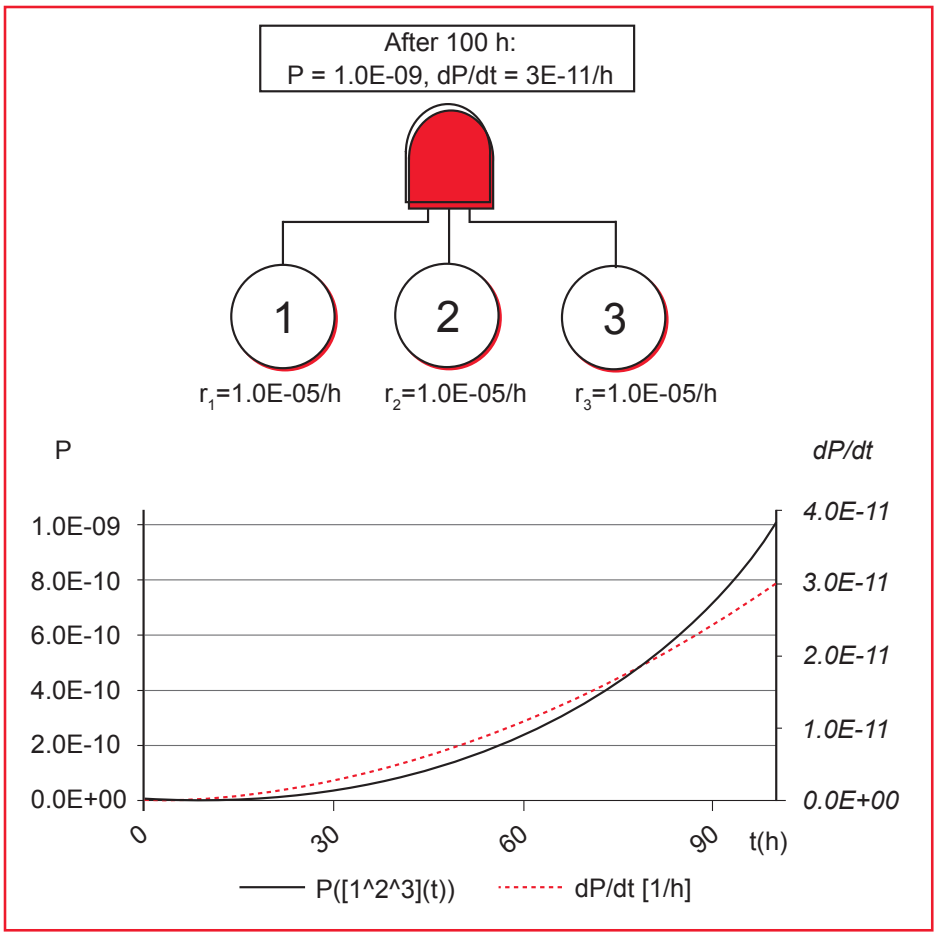


*Figure 3 — Time Dependency of the Fault Occurrence Probability* P(t) *in for Three Faults with Constant Failure rates. (Note: It is worthwhile to mention that both the fault occurrence probability* P(t)*, and its first derivate* dP/dt*, also known as failure density [Ref. 5] or failure frequency [Ref.3], are approximately polynomial functions of* t.*)*

Even if all failure rates $r_n$ are assumed as constant and $r_nT<<1$ and thus (quasi-linear functions in time),

$$1 - e^{-r_n*t} \approx r_n*t \qquad (4)$$

the probability of AND-combinations if two or more faults is non-linear.

In conclusion, no time-independent failure rate can be derived for AND-combinations of faults. The average of the so-called PFH for such AND-combinations then is determined by the occurrence probability $P_{AND}(T)$ over mission time divided by the mission time $T$.

$$PFH = \prod_{n=1}^{N} \frac{P_n(T)}{T} \qquad (5)$$

**Note:** It is worthwhile to mention that both the fault occurrence probability $P(t)$, and its first derivate $dP/dt$, also known as failure density [Ref. 5] or failure frequency [Ref. 3], are approximate polynomial functions of $t$.

## 2. Impact of Latencies on Reliability and Safety Metrics

The previous section considered combinations of faults, without taking into account any possibility of removing faults after their initial occurrence within the mission time. This is also called a non-repairable system in the literature [Ref. 6].

But if there are certain points in time within the mission time where the absence of fault occurrence can be approved, this changes the probability of the presence of related faults after these points in time. Every point in time $t_i$ where the absence of a certain fault can be ensured "sets a new game" for the random fault occurrence until $t_{i+1}$, the next of such points in time.

The next focus is the unavailability $Q(t)$ describing the probability of fault presence in a function of time. In the following, we will use the expression latency for the time interval $[t_i, t_{i+1}]$ between two "reset points" of the unavailability $Q(t)$.

**Note:** It is worthwhile to mention that it doesn't make a difference if the approval of the fault-free state is achieved by human inspection, intrinsic fault diagnostics or removal of the fault by repair. The probability of fault presence (unavailability) at the related point of time is zero in any of these cases. However, certain literature calls systems with such characteristics "repairable systems" [Ref. 6].

The consideration of latencies bears some fundamental challenges for the probabilistic approach to determine reliability and safety metrics.

The probability of multiple-point fault occurrence cannot be treated in the same manner as the non-repairable system described in section 1.3 because this probability is not determined by the unreliability functions $P(t)$ but by the unavailability functions $Q(t)$ of each related fault.

If the individual unavailability functions $Q_n(t)$ are known, the overall unavailability function $Q(t)$ of the multiple fault combination is determined by

$$Q(t) = \prod_{n=1}^{N} Q_n(t) \qquad (6)$$

In case of latencies, the individual unavailability functions $Q_n(t)$ are non-monotonic functions such that their product $Q(t)$ may become complex. In particular, if the latency intervals of the individual faults are different, $Q(t)$ can exhibit a quasi-erratic behavior because each "reset point" of each unavailability function $Q_n(t)$ leads to a discontinuity in $Q(t)$.

The correct determination of safety metrics like $PFD_{avg}$ (mean unavailability) would require an integration over the mission time $T$, followed by averaging:

$$PFD_{avg} = Q_{avg}[0 \ldots T] = \frac{1}{T}\int_0^T Q(t) \qquad (7)$$

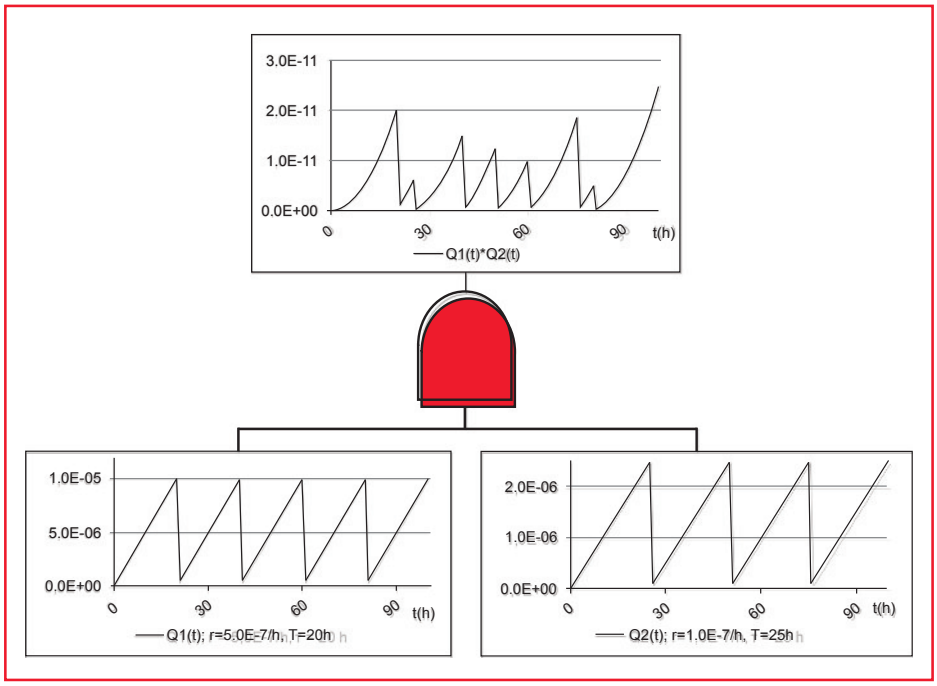


*Figure 4 — Illustration of an Unavailability Function Q(t) as a Product of Two Independent Unavailability Values with Different Timing Characteristics.*

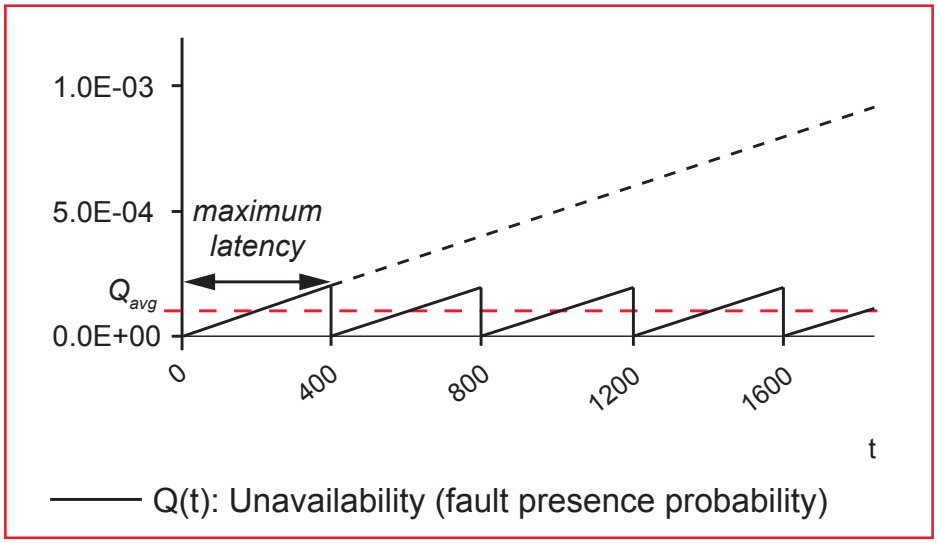


*Figure 5 — Saw-tooth Function of the Unavailability Q(t) with Periodic Inspection Intervals.*

As we will show in section 4, the determination of the PFH is even more complex in this case.

### 2.1. Overview on Models and Mathematical Approaches for Latencies

As we see in the example in the previous section, the consideration of time-dependent effects generally complicates the probabilistic assessment of systems' reliability and safety, as seen in IEC 61508-6 [Ref. 3].

The fundamental issue is that, in addition to the pure Boolean logic, some deterministic timing behavior also needs to be modeled. In reality, the behavior of redundant systems after occurrence of faults will be even more complex. Fault detection (either implemented by internal functionality or by external supervision) will lead to state transitions from the fault-free state to certain fault reaction states (e.g., functional degradation, repair modes, etc.).

Generally, no probabilistic model is yet established that covers all aspects and possible effects of such time-dependent state transitions.

An approach for modeling the time dependency is the Markov model, in which not only fault occurrence probabilities (represented by failure rates) but also the fault removal actions by repair are treated as random events in time (represented by repair rates). Despite this, the Markov model provides closed mathematical solutions because it can be transformed into linear differential equations. The underlying assumption that fault detection and repair themselves are random events can lead to a probabilistic assessment of critical fault coincidence being non-conservative (i.e., too optimistic) in certain cases [Ref. 7 and 8].

Other time-dependent effects result if not only the Boolean AND-combination of faults is relevant, but also the sequence of their occur-

rence. For instance, the unavailability of an emergency release valve is only critical if it occurs *before* a dangerous overpressure is present. The mathematical treatment of such event sequences leads to complex models like dynamic FTA or Petri nets which are described in the literature but are not broadly applied in the industry [Ref. 6].

### 2.2. Models for Periodic Inspection and Repair

Let us consider a system element with certain random failure modes that are relevant for the reliability or safety of a redundant system. In a periodic sequence of time intervals $\tau$, this element is inspected whether the fault is present or not.

If the fault is not present, we know now that the maximum time for random fault occurrence is $\tau$ (until the next inspection). If the fault is present at the point of time of inspection, a time to repair may be needed to achieve the fault-free state again.

If we know the unreliability function *P(t)*, we can determine the probability of the fault occurrence for each inspection interval.

In case of a constant failure rate *r* (and only in case of constant failure rates), the probability of fault occurrence within every inspection interval is given by

$$Q(\tau) = 1 - e^{1-r*\tau} \approx r * \tau \;\; if \;\; r * \tau \;\; << \;\; 1 \qquad (8)$$

The unavailability *Q(t)* (i.e., the probability of fault presence) rises from zero to its maximum value between the start and end of any consecutive inspection interval. It is worthwhile to repeat that the unreliability *P(t)* (i.e., the fault occurrence probability) is a monotonically increasing function and is not affected by periodic inspection.

The next illustration shows that the mean unavailability for a fault with constant failure rate is derived as

$$Q_{avg} \approx \frac{1}{2} r * \tau \qquad (9)$$

If a repair can be made during the operation of the system, the Mean Time To Repair (MTTR) needs to be considered along with the unavailability. In the literature, we find the following formula for this case:

$$Q_{avg} = 1 - e^{1-r*\tau} + r * MTTR \qquad (10)$$

## 3. Gaps and Vagueness in the Current Literature

As only in redundant systems the periodic inspection and repair mitigate the risk of critical events, the above considerations for the probability of fault presence (unavailability) *Q(t)* of single faults need to be set into the context of multiple faults.

The question is how to determine the probabilistic metrics $PFD_{avg}$ and *PFH* for combinations of faults with latencies?

### 3.1. Influence of the Inspection Intervals on the Probability of Multiple-Point Faults

The result of our literature investigation was that this topic seems merely treated in a self-consistent probabilistic framework.

Our first observation is that most of the literature is focused on the determination of the unavailability Q. But the unavailability is only suitable for reliability and safety evaluation in cases where control and supervising systems can be regarded as independent, and only the supervising system shall be assessed (as we explained in the introduction, see section 1.2.1).

The question of how to obtain a suitable estimation of the average failure rate (PFH), needed for assessing embedded supervising/safety systems (see section 1.2.2), is not addressed at all in most of the investigated literature.

Our second observation is that the influence of latencies on the probabilities of multiple faults does not seem to be clearly addressed, which may lead to incorrect probabilistic assessment results.

Besides the already cited literature, our investigation included the following sources:

- International standards addressing and describing the probabilistic assessment of (multiple) fault occurrence probabilities [Refs. 3 and 4]
- International and national standards addressing and describing the probabilistic assessment via fault tree analysis [Refs 1 and 8]
- Books dealing with general approaches on the assessment of systems' reliability and safety [Refs. 5, 6, 7, 10 and 11]
- Guidelines on the application of probabilistic assessment of systems' reliability and safety in the context of different industry sectors [Refs. 1, 2 and 12]
- Articles in different journals on systems' reliability and safety, which deal in particular with the effects of periodic inspection, maintenance and repair of redundant systems [Refs. 8, 13 and 15]

It is worthwhile to mention that international standards that require probabilistic risk assessment, like IEC 61508 [Ref. 3] or ISO 26262 [Ref. 4], do not provide precise requirements on how to accomplish it in a correct mathematical framework.

As we will outline, such a correct mathematical framework seems not yet fully established and differ-

ent approaches are published. This makes it difficult for analysts and assessors to obtain certainty that safety and reliability analyses provide correct or at least sufficiently conservative results.

### 3.2. Treatment of Unique Inspection Intervals

In the case that different faults have all the same latencies $\tau<T$ and the same periodic inspection points in time (i.e., unique inspection intervals between $t$=0, $\tau$, 2$\tau$, …), one can consider the first time interval $\tau$ as time basis for the determination of the probability that all relevant faults occur within [0…$\tau$]:

$$P(\tau) = \prod_{n=1}^{N} P_n(\tau) \qquad (11)$$

For this first inspection interval, and only for this, the unavailability Q and the unreliability $P$ are identical:

$$Q(t) = P(t) \quad for \quad t = [0 \ldots \tau] \qquad (12)$$

In the case of constant failure rates $r_1 \ldots r_N$, the probability of fault occurrence within this inspection interval (and consecutive ones) is given by

$$Q_{avg}(\tau) = \prod_{n=1}^{N} 1 - e^{1-r_n * \tau} \approx \prod_{n=1}^{N} r_n * \tau = \tau^N * \prod_{n=1}^{N} r_n$$
$$if \quad r_n * \tau << 1 \quad for\ all\ n \qquad (13)$$

For the above approximation, the mean unavailability is then calculated as

$$Q_{avg}[0 \ldots \tau] = \int_0^{\tau} \frac{Q(t)}{\tau}$$
$$= \frac{1}{N+1} * \tau^{N+1} * \prod_{n=1}^{N} \frac{r_n}{\tau} = \frac{1}{N+1} * \tau^N * \prod_{n=1}^{N} r_n \qquad (14)$$

Let us consider the possibly that the system lifetime is not an integer multiple of $\tau$. T then decomposes into $M$-1 complete inspection intervals and a $M^{th}$ residual time interval $0 < \tau_{res} <= \tau$.

In the $M^{th}$ time interval, the mean unavailability may be equal or less (but not greater) than for complete inspection intervals of duration $\tau$.

Hence, the above approximation provides an upper bound estimation of the mean unavailability over the whole system lifetime $T$, regardless of whether $T$ is an integer multiple of $\tau$ or not. Such we can derive:

$$PFD_{avg} \le Q_{avg}(\tau) \le \frac{1}{N+1} * \tau^N * \prod_{n=1}^{N} r_n \qquad (15)$$

Surprisingly, certain literature provide a different formula for the determination of $Q_{avg}$ by multiplying the means of each unavailability $Q_{n\_avg}$, being approximately

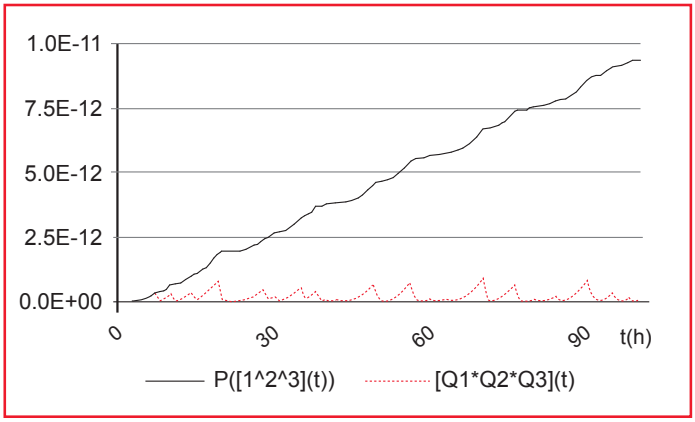


*Figure 6 — Unreliabilty P and Unavailability Q for a Triple Fault Where Each Fault has Individual Latency $\tau_i$ and Failure Rate $r_i$. (Note: Parameters in this example are $r_1$ = 1E-05/h, $r_2$ = 1E-05/h, $r_3$ = 1E-05/h, $\tau_1$ = 10 h, $\tau_2$ = 7 h, $\tau_3$ = 19 h)*

1/2 * $r_n$ * $\tau$ (see above, or Ref. 14). But this mathematical operation provides lower values than the mean of the product as previously described.

This approach has already been criticized [Ref. 3].

An upper bound for the average failure rate PFH in every inspection interval is easily derived:

$$PFH = \frac{Q_{avg}(\tau)}{\tau} \le \frac{1}{N+1} * \tau^{N-1} * \prod_{n=1}^{N} r_n \qquad (16)$$

### 3.3. Treatment of Dissimilar Inspection Intervals

If we now consider that different inspection intervals $\tau_n$ may exist for different faults $F_n$, the previous considerations will not apply any longer because there is no unique periodic time base for the calculation of $P$ and Q.

Figure 6 illustrates the complexity of the unavailability and unreliability in function of time for an example of three different inspection intervals.

The "reset points" where $Q(t)$ falls to zero because one of the individual saw-tooth curves of $Q_n(t)$ is zero exhibit a quasi-erratic timing. This is especially true if the $\tau_n$ do not have a least-common multiple less than half of the system lifetime. In this case, it is not possible to find a periodicity in the plot.

The plot of the unreliability $P$, being the "memory" of fault probability that is accumulated from each intersection after Q is reset to zero, also exhibits an irregular aspect.

The illustrations above were derived by chart calculations. The determination of $P$ and $PFH$ required complex counter and memory functions and treat integer values only for the points $t$ in time and the inspection intervals $\tau_n$. To treat floating point values for these parameters, even a numerical integration would be required for the computation of $P(t)$.

Although we investigated various dedicated literature, we didn't find concrete proposals for how to cope with the estimation of $Q_{avg}$ and *PFH* in the case of dissimilar inspection intervals.

The only approach we found is offered by some software tools (e.g., for quantitative fault tree analysis) that estimate the unavailability **Q** of the multiple faults by the product of the maximum unavailability $Q_n$ within the individual $\tau_n$:

$$Q_{max} = \prod_{n=1}^{N} r_n * \tau_n \qquad (17)$$

For a conservative estimation of $Q_{avg}$ and *PFH* in this case we didn't find accountable information.

### 3.4. Interpretation of Our Literature Investigation

The most important result of our research into various publications is that most of the investigated literature treats the probability of a fault's occurrence (unreliability) over system lifetime *P(T)* with much less intensity as the probability of a fault's presence (unavailability) at representative points of time *Q(t)*. Despite the fact that the determination of an average unreliability (*PFH*) is declared as necessary for the evaluation of certain system architectures (see section 1.2.2) and is addressed by several international standards for functional safety like IEC 61508 [Ref. 3]and ISO 26262 [Ref. 4] (among others), we found little information in the literature on how to determine this metric.

The second point we found remarkable is that for the influence of latencies, in particular the treatment of regular inspection for fault detection and repair, only certain literature provides the correct formulae for the unavailability Q with regard to multiple-point faults. Other sources provide formulae that are questionable, as described earlier.

The third result is that we could not find a generalized treatment of dissimilar latencies in the literature.

In conclusion, there is a need for an improved calculation basis for the estimation of multiple-point fault probabilities and the influence of these probabilities on the commonly addressed metrics $PFD_{avg}$ and *PFH*.

## 4. Proposed Probabilistic Approach for the Treatment of Dissimilar Latencies

To cope with the problem of dissimilar latencies, we developed a purely probabilistic approach.

### 4.1. Determination of an Appropriate Time Base for Dissimilar Latency Periods

Let us consider the case of three faults, each with individual failure rate and individual inspection interval, as illustrated in Figure 6.

In this example the inspection intervals ($\tau_1$, $\tau_2$, $\tau_3$) are chosen such that no periodicity is reached within the exemplary system lifetime ($T$=100$h$) because the least common multiple is greater than $T$.

The example is chosen such that none of the $\tau_n$ is an integer multiple of another. Hence the points in time $t_i$, where at least one individual unavailability $Q_n(t)$ is reset to zero, make up a series that appears erratic within the system lifetime, despite being determined by three periodic functions.

At any of these "reset points" $t_i$ the probability of triple fault coincidence is zero because the certainty of the absence of at least one of the contributing faults, i.e., $Q_n(t_i)=0$, results in the product of the unavailability values $Q(t_i)=Q_1(t_i)*Q_2(t_i)*Q_3(t_i)$ being zero, as well.

Due to the dissimilar inspection intervals $\tau_n$, the time intervals between two reset points $[t_i \ldots t_{i+1}]$ vary considerably as we see in the illustration.

However, it is obvious that such intervals can be shorter, but never longer than the smallest value of the inspection intervals.

Hence, we can derive a characteristic value that we will call the *maximum fault accumulation time (MFAT)* for $N$ independent faults with individual inspection intervals:

$$MFAT = \min(\tau_1 \ldots \tau_N) \qquad (18)$$

This time base can now be used similarly for probability estimations, similarly as it is the case for unique inspection intervals $\tau$ as described in section 3.2.

### 4.2. Upper Bound Probability Calculations

Seeking the probability of coincidence that all three faults in the above example occur in any intersection interval, we see that at the reset points $t_i$, being the integer multiple of one of the inspection intervals, the probability of presence of other faults may (in the worst case) achieve the maximum value that is given by the product of the failure rate $r_n$ and the inspection interval $\tau_n$ of the related fault (i.e., the maxima of the saw-tooth functions):

$$Q_n(\tau_n) = 1 - e^{1-r_n*\tau_n} \leq r_n * \tau_n \qquad (19)$$

For each time interval of the length *MFAT* as defined above, the upper bound for the probability of coincidence is hence given by the upper bound product of unavailability values $Q_n$.

$$Q(MFAT) \leq \prod_{n=1}^{N} r_n * \tau_n \qquad (20)$$

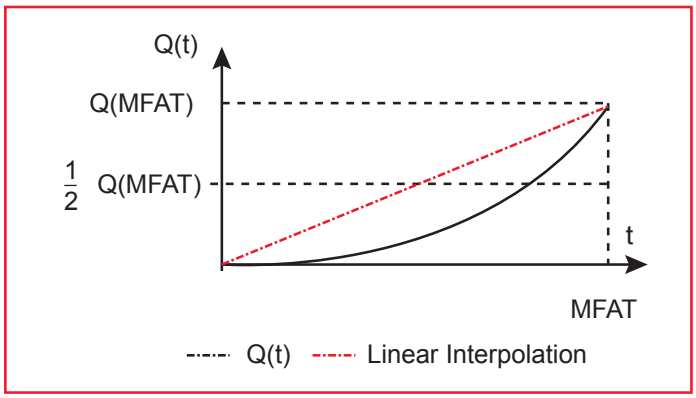


*Figure 7 — Linear Interpolation of the Polynomial Unavailability Function Q(t), Providing an Upper Bound.*

#### 4.2.1. Upper Bound of the Average PFD

An upper bound for the mean unavailability can be obtained quickly, considering that if the products of failure rates and inspection intervals are small numbers ($r_n * \tau_n << 1$), the function $Q(t)$ within the *MFAT* interval is a convex polynomial function always remaining below the linear interpolation between the beginning and the end of the *MFAT* interval.

Hence, using the linear interpolation as an upper bound for the estimation of $Q_{avg}$ we obtain:

$$Q_{avg} \leq \frac{1}{2} * \prod_{n=1}^{N} r_n * \tau_n = \frac{1}{2} * Q(MFAT) \qquad (21)$$

We will call this — fairly pessimistic — estimation of $Q_{avg}$ in the following "linear probabilistic estimation."

The following — less pessimistic — estimation of $Q_{avg}$ is a little more complex:

Without further assumption, we only know that within a *MFAT* interval, the individual unavailability values remain below their upper bound values, which are defined by:

$$Q_n(t) \leq r_n * \tau_n \quad for\ all\ t = [0 \ldots MFAT] \qquad (22)$$

The worst case occurs if the end of all inspection intervals $\tau_n$ coincide in one point in time. Per definition, this is the end of a *MFAT* interval, being the end of the shortest inspection interval.

As such, every individual unavailability $Q_n$ rises within the *MFAT* interval from an initial value which has the upper bound

$$Q_n(t = 0) \leq r_n * (\tau_n - MFAT) \quad for\ all\ \ Q_n \qquad (23)$$

Hence, we obtain an upper bound for the overall unavailability Q in function of time within every *MFAT* interval:

$$Q(t) \leq \prod_{n=1}^{N} (r_n * (\tau_n - MFAT + t)) \ for\ t = [0 \ldots MFAT] \qquad (24)$$

We obtain the estimate for the mean overall unavailability $Q_{avg}$ with:

$$Q_{avg}[0 \ldots MFAT] = \frac{1}{MFAT} * \int_0^{MFAT} Q(t) \leq \frac{1}{MFAT} * \int_0^{MFAT} \prod_{n=1}^{N} (r_n * (\tau_n - MFAT + t)) \qquad (25)$$

As $Q(t)$ is estimated by the product of $N$ linear functions in time (i.e., a polynomial function), this integral provides a closed mathematical solution.

We will call this less pessimistic (but still upper-bound) estimation of $Q_{avg}$ in the following "polynomial probabilistic estimation."

#### 4.2.2. Example

We illustrate this for a triple fault:

Without loss of generality, we may assume that $\tau_1$ represents the minimum of the three individual $\tau_n$ (i.e. $\tau_1 = MFAT$).

If the other faults have longer latencies, i.e., $\tau_2 > MFAT$ and $\tau_2 > MFAT$, they bring the maximum initial

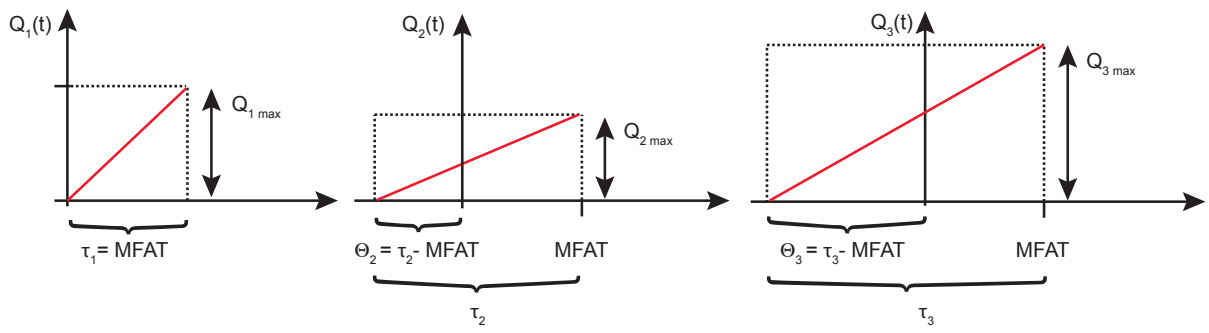


*Figure 8 — Worst-case Approach for the Unavailability Values $Q_i(t)$ for Latencies $\tau_i \geq$ MFAT.*

unavailability values into the *MFAT* defined by the differences $\Theta_n$ between the $\tau_n$ and *MFAT*

$$\Theta_2 = \tau_2 - MFAT;\ \Theta_3 = \tau_3 - MFAT \quad (26)$$

$$Q_2(t{=}0) \le r_2 * \Theta_2;\ Q_3(t{=}0) \le r_3 * \Theta_3;\ whereas\ Q_1(t{=}0) = 0 \quad (27)$$

Hence, the individual unavailabilities within the *MFAT* interval cannot exceed the following upper bounds:

$$Q_1(t) \le r_1 * t;\ Q_2(t) \le r_2 * (t + \Theta_2);\ Q_3(t) \le r_3 * (t + \Theta_3) \quad (28)$$

If we now apply the above integral for $Q_{avg}$, we obtain the polynomial function of t developing the integral over the product of the $Q_n$

$$\begin{aligned} Q_{avg} \le & \frac{1}{MFAT} * \int_0^{MFAT} r_1 * t * r_2 * (t+\Theta_2);\ Q_3(t) * r_3 * (t+\Theta_3) \\ = & r_1 * r_2 * r_3 * \left(\frac{1}{4} MFAT^3 + \frac{1}{3} * MFAT^2 * (\Theta_2+\Theta_3)\right. \\ & \left. + \frac{1}{2} MFAT * \Theta_2 * \Theta_3\right) \end{aligned} \quad (29)$$

Obviously, the polynomial for an AND-combination of faults with more than three different latencies will become more complex due to the increasing number of cross-terms of the $\theta_n$ but it can be equivalently calculated for any higher polynomial order.

## 5. Conclusions

### 5.1. Summary

According to our literature investigation, this paper presents a new probabilistic treatment of dissimilar fault latencies for the case that the latencies result from periodic inspection and repair.

In comparison to other approaches, such as Markov models, the proposed treatment of latencies in the assessment of multiple-point fault probabilities is based purely on probabilistic considerations in the context of deterministic timing behavior, without further implicit assumptions.

### 5.2. Benefit of the Results

In comparison to previously published approaches, the newly developed formulae provide credible upper-bound estimations for the mean probability of fault presence (also called mean unavailability or $PFD_{avg}$) and the mean failure frequency (also called *PFH*) of multiple-point faults.

For each multiple fault combination, these metrics can be calculated based on the individual failure rates (*r*) and latency parameters ($\tau$). In a complex system, where generally many of such fault combinations need to be assessed (e.g., represented by the cut sets of a fault tree), each combination may require an individual calculation.

Despite the probabilistic background for their derivation being complex, the presented formulae are sufficiently simple for the integration into software tools for reliability and safety assessment. In comparison, a precise mathematical solution appears numerically difficult to implement for assessing complex repairable systems.

It is worthwhile to mention that using the applied worst-case approach for estimating the fault coincidence probabilities, even latencies that are longer than the mission time of a system, can be modelled. If, for instance, certain elements of a system are operating before mission start, the impact of potential fault accumulation in the pre-operation time spans can be assessed with the presented formulae as well. Such systems can be found in the automotive context, when some elements of a system are operated outside the key cycles and others only during the key cycles.

### 5.3. Limits and Potential Shortcomings of the Model

One point that remains open after the above considerations is the impact of variances in the inspection intervals, which we treated as strictly periodic in our approach. It would be worthwhile to investigate this in detail because even a Gaussian statistical variance on the average latency would certainly lead to a shift of the *PFH* and $PFD_{avg}$. The reason is that the occurrence probability of multiple-point faults is determined by a polynomial, hence a convex function in time. Thus, the longer variations would contribute with a higher weight in the average than the shorter variations. Hence, a shift of the *PFH* and $PFD_{avg}$ to bigger values could be expected. On the other hand, a purely random timing of inspection intervals, which is a premise of the Markovian approach, leads to smaller values in the estimation of $PFD_{avg}$, as we mentioned earlier. It would be worthwhile to investigate the impact of these concurring effects in detail. But this remains a topic for future work.

Another open point is that we assumed the periodic inspection and repair as perfect, resulting in resetting the individual probabilities of fault presence to zero after the inspection interval. In the case of imperfect inspection and repair, e.g., due to diagnostic gaps or human errors during repair, a residual fault probability would result after each inspection interval. This is outlined in IEC 61508-6 [Ref. 3], illustrating the impact on the evolution of the *PFD* and $PFD_{avg}$ after several inspection

*Table 1 — Terms, Acronyms and Definitions.*

| Acronym or Term | Definition | Equivalent of Synonymous Expressions |
|---|---|---|
| ETA | Event Tree Analysis | |
| EUC | Equipment Under Control | |
| FTA | Fault Tree Analysis | |
| *MFAT* | Maximum Fault Accumulation Time | |
| *MTTR* | Mean Time To Repair | |
| *P(t)* | Unreliability | Probability of fault occurrence |
| *PFD* | Probability of dangerous Failure on Demand | *Q(t)* |
| $PFD_{avg}$ | Average Probability of dangerous Failure on Demand | $Q_{avg}$ |
| *PFH* | Probability of dangerous Failure per Hour | Average failure frequency |
| *Q(t)* | Unavailability | Probability of fault presence |
| $Q_{avg}$ | Average Unavailability | |
| *r* | Failure Rate | |
| RBD | Reliability Block Diagram | |
| SRS | Safety-Related System | |
| T | Mission time | System lifetime |
| $\tau$ | Inspection interval | Latency |
| $\Theta$ | Difference between $\tau$'s and the *MFAT* | |

intervals. This resulting complication of the probabilistic assessment of multiple-point faults with latencies can be avoided if a "failure split" is applied between the detected fraction of a fault occurrence and the undetected one. Such an approach is outlined in ISO 26262-10 [Ref. 4], but it results in an increasing number of single events that need to be considered in the assessment of systems' reliability and safety. As a result, the required number of base events in a fault tree would considerably increase.

Further, the treatment of potential common cause failures (CCF) that may lead to quasi-instantaneous occurrence of multiple-point faults is out of the scope of this publication. The assessment of CCFs for different faults with individual failure rates also seems to be a topic that is rarely addressed in the literature. Further investigations would be required to treat this in more detail.

Finally, this publication deals exclusively with the constant failure rate model. Other models include time-dependent failure rates (e.g., the Weibull distribution). If failure rates are time dependent, much more effort is needed to determine the multiple fault probabilities because the polynomial approach that we derived above cannot be applied. Also, this topic seems not yet to be investigated in detail according to our research, and because the main focus of previous publications is on the constant failure rate models, we consider this topic less relevant than those we mentioned earlier.

### 5.4. Outlook

A target for future work will be to integrate the presented estimations for multi-point faults efficiently with state-of-the-art algorithms for quantitative fault tree evaluation. One example is the Binary Decision Diagrams (BDD) approach, which is used in many tool implementations for computation of the top event probability [Ref. 16]. Since each combination of (repairable) events requires a determination of a potentially different *MFAT*, the impact on the complexity of the evaluation needs to be investigated (i.e., the algorithm for the probability cannot be simply linearized to the size of the BDD through caching).

Moreover, the effect of cutoffs — as a technique to reduce the complexity by bounding the cut-sets to a certain number of events [Ref. 10] — require further considerations with respect to the presented approach. Because all fault latencies in a multi-event cut-set need to be taken into account to determine the *MFAT*, further theoretical work on cut-off strategies (and/or heuristics in building BDDs) is required.

## 6. Appendix: Terms, Acronyms and Definitions

See Table 1.

## 7. Acknowledgements

We would like to express our great appreciation to Doug Barnes (kVA, USA) for his valuable and constructive suggestions that have helped to improve the quality of the manuscript.

Special thanks also to Mario Winkler (ikv++ technologies ag, Berlin). His simple question, *"How to treat dissimilar latencies in quantitative fault tree analysis?"* was the starting point of our research, which turned out to be much more complex than expected.

## References

1. IEC 61025: *Fault Tree Analysis (FTA)*, second edition, International Electrotechnical Commission, 2006.
2. Stamatelatos, M., W.E. Vesely et al. *Fault Tree Handbook with Aerospace Applications*. NASA, Version 1.1, Washington, D.C., 2002.
3. IEC 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (Parts 1-7)*, Second Edition, International Electrotechnical Commission, 2010.
4. ISO 26262: *Road vehicles – Functional safety*, First edition, International Organization for Standardization, 2011.
5. Kumamoto, H., E. J. Henley. *Probabilistic Risk Assessment and Management for Engineers and Scientists*, John Wiley & Sons, Second Edition, 2000.
6. Birolini, A. *Reliability Engineering: Theory and Practice. 6th* edition, Springer-Verlag, 2010.
7. Smith, D.J. *Reliability, Maintainability and Risk. 8th edition*, Elsevier, 2011.
8. Gulland, W.G. *Repairable Redundant Systems and the Markov Fallacy*. Whitepaper, see http://4-sightconsulting.co.uk/Current_Papers/Markov_Fallacy/Markov_Paper.pdf, July 10, 2004.
9. DIN 25424-2 - *Handrechenverfahren zur Auswertung eines Fehlerbaumes, Fault Tree Analysis; Manual Calculation Procedures for the Evaluation of a Fault Tree*, April 1990.
10. Dutuit, Y., and A. Rauzy. "Approximate Estimation of System Reliability via Fault Trees," *Reliability Engineering and System Safety*, Vol. 87, Issue 2, pp 163-172, 2005.
11. Ericson, Clifton A. "Chapter 11 Fault Tree Analyses," *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, 2005.
12. U.S. Department of Defense: *Military Handbook – Electronic Reliability Design Handbook*. MIL-HDBK-338B, October 10, 1998.
13. Bukowski, J.V. "Modeling and Analyzing the Effects of Periodic Inspection on the Performance of Safety-Critical Systems," *IEEE Transactions on Reliability*, Vol. 50, No. 3, 2001.
14. Vesely, W.E. et al. *Fault Tree Handbook*, U.S. Nuclear Regulatory Commission (NUREG) 0492, Washington D.C., 1981.
15. Vaurio, J.K. "Unavailability Analysis of Periodically Tested Standby Components," *IEEE Transaction on Reliability*, Vol. 44, No. 3, 1995.
16. Rauzy, A. "Binary Decision Diagrams for Reliability Studies," *Handbook of Performability Engineering*, pp 381-396, 2008.