Session Fifteen:

Protection Functions as Probabilistic Filters for Accidents

Andreas Belzner
Engine Functional Safety – Gas Turbine, Alstom

Abstract

A generalized model is developed for the “risk reduction” by a protection function. The relations between reliability parameters of the protection function, the demand rate and the resulting residual risk are given on a statistical basis. The three modes of operation, „low demand“, „high demand“ and „continuous demand“ are identified as special cases. It is shown, how “low demand” and “high demand” grade into each other.

The repeated testing of a protection function is decisive in this context. The distinction of “low demand” and “high demand” by only the average frequency of demand is not conclusive. This is shown by practical application examples. A simple guideline is derived for assigning a SIL to a high demand function.

1. Introduction

“Protection Functions” are instrumented control system functions for machinery or process installations, which are implemented for preventing specific accidents. Frequently, such functions induce an emergency shutdown of the controlled machinery. The over-speed protection function of a turbine is a typical example. The prevented accidents may affect assets only (equipment damages, production losses). They may endanger the health and safety of people, the environment or other values. Since the protection target is not relevant in the current context, the generic term “protection function” is used in this paper rather than “safety instrumented function”.

For such protection functions, two sets of requirements are typically specified:

- Functional Requirements:
- Safety Integrity Requirements

The first set of requirements defines the protective action: emergency shut-down or others, within a specific time and so on. The functional requirements include as well the conditions for triggering the action - process signals, threshold values, voting logic and so on. The second set of requirements describes the reliance, which can be put on the function: How certain can one be that the function will work as designed, when required?

In the context of IEC61508 and its derivatives, the Safety Integrity Level SIL is used as overall indicator for that reliance. As a requirement, the SIL is derived from risk analyses for the equipment to be protected. The preferred concept for these risk analyses can be expressed in a general scheme – see Figure 1. Accordingly, a protection function is specified as corrective measure for reducing the risk emission of a process or machinery to a tolerable level[1].

The scheme according to Figure 1 is increasingly read as “quantitative”. Risk levels are expressed as numerical figures. Thus, a “quantitative risk analysis” in the full sense of the term should establish a numerical relation between the following items:

- Risk of the process without protection functions - Unmitigated process risk
- Risk of the process with protection functions - Mitigated process risk or residual risk
- Risk mitigating effect of the protection function

In this paper, that relation is developed on a strictly probabilistic basis. The result is discussed with respect to definitions in IEC61508.

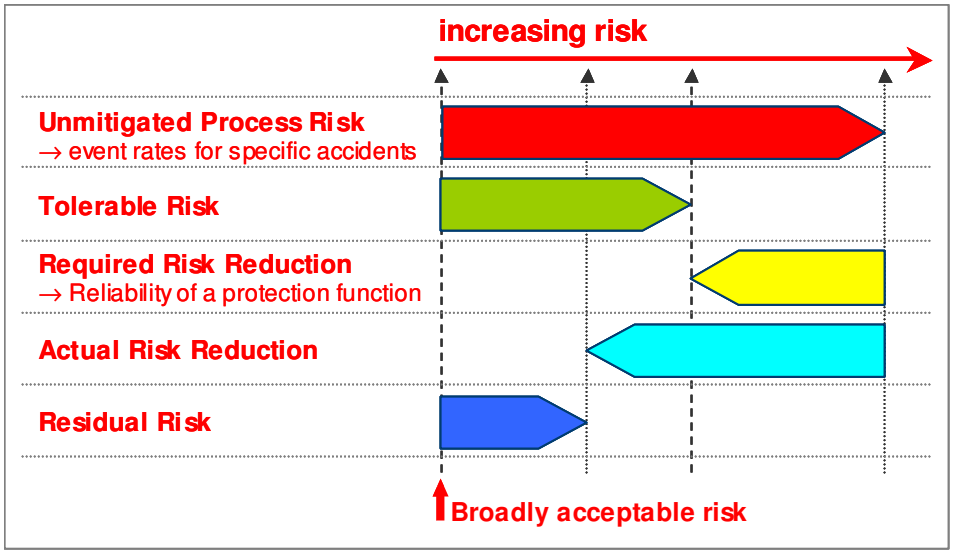

Figure 1 Quantitative Assignment of Risk Reduction Requirements to a Protection Function – General Concept

[1] IEC61508 /1/, part 5, 1998, Figure A.I - Risk reduction: general concepts; same Figure as IEC61511 /3/, part 3 2004, Figure 3; VDI/VDE2180 /5/, Blatt 1, 2007; Bild 4 – Risikoreduzierung durch PLT- und nicht-PLT-Schutzmaβnahmen; ISO 13849 /6/, part 1, 2007, Figure 2 — Overview of the risk reduction process for each hazardous situation

2. Key Terms

"Risk" is defined as "combination of the probability of occurrence of harm and the severity of that harm". For the harm, there is no generally applicable numerical measure. Thus, were risks are "quantified", this does typically apply in a strict sense to the "probability of occurrence" only. For that "probability", the "event rate" is used as measure.

An "event rate" has a meaning only, if it can be related to defined events. There must be clear criteria, which events are included and which not. In the context of "safety" and "protection", these criteria describe specific classes of accidents. This way, the "severity of harm" is defined for the quantitative assessment. As a boundary condition for a quantitative risk assessment, however, this is not sufficient in most cases. The following is typically defined:

- Which equipment unit or equipment scope is causing the accident?
- To which specific process hazard is the accident related?
- Who or what is suffering harm or damage?
- Which kind of harm or damage is suffered, on which level of severity?

The term "reference event" is used in this study for that definition and for the described accidents. See Reference /7/ for further guidance on the concept of the "reference event". The risk terms in Figure 1 can be rephrased, accordingly:

- Unmitigated process risk → "**Unmitigated accident rate**": expected event rate for the reference event to occur, assuming that the protection function under assessment is not installed.
- Residual risk → "**Mitigated accident rate**": expected event rate for the reference event, assuming that the protection function under assessment is installed

In the following, the term "demand rate" is also used instead of "unmitigated accident rate", for shortness and simplicity. In the frame of a quantitative risk analysis, which refers to a specific accident scenario, it is only that accident or reference event, which puts a "relevant" demand on the protection function[2].

For the protection function, it is assumed in this study, that it is capable of preventing the reference event completely, whenever it would otherwise occur. Thus, reference events can occur only due to failures of the protection function. The protection function acts as a "probabilistic filter" for accidents – see Figure 2.

[2] Consequently, in the given context the term "demand" does not apply to any actual triggering of the protection function in its use life. It does also not apply to each case, where the function could have prevented some harm or damage. It applies to those events only, where the harm or damage to be prevented is included in the definition of the reference event.

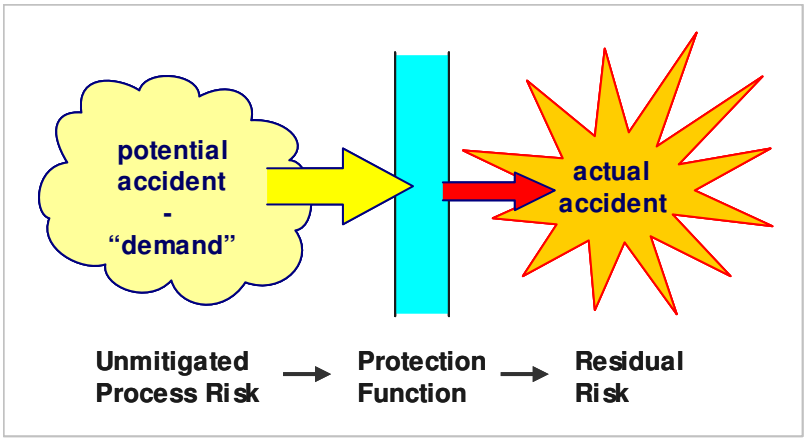

Figure 2 Protection Function as "Probabilistic Filter" for Accidents

The "mesh size" of that filter is given by the propensity of a protection function to fail. In probabilistic terms, this is the "unreliability". The two basic probabilistic parameters for the unreliability a protection function are the following. See Table 1 for the parameter notion, which is used in this study.

F_R Failure rate: Applies to the overall loss of the safety function, which can be detected by a functional test of the function as a whole[3].

T_R Test rate: Rate of functional tests of the function, which reveal the overall loss of the safety function and lead to restoration of the intended safety state.

According to IEC 61508, the test rate T_R would be read as inverse of the regular proof test interval TI. In the current context an additional diagnostic mechanism is introduced. A protection function may be triggered by minor process deviations, leading to some undesired consequences in case the function has failed, however without causing the "reference event". This may happen a couple of times between "relevant" demands and can be claimed as a risk reduction measure. More specifically: this is a measure for reducing the risk of meeting the protection function failed in a situation, which will lead to the "reference event"[4]. It is assumed in the following, it that this "testing by minor process demands" is included in the parameter T_R. See in section 6 for examples and further discussion.

The notion in Table 1 is used rather than the established notion of IEC 61508, in order to differentiate clearly between quantities without or "before" protection

[3] This rate F_R can be identified in first instance with the PFH-value according to the IEC standards /1/, /2/, /3/, /4/ or with the "average probability of dangerous failure per hour", which is used in ISO13849 /6/ (part 1, Table 3).

[4] In ISO 13848 /6/, the term "Fault detection by the process" is used for this type of functional test (ISO13849-1, Annex E, Table E.1)

("unmitigated" U) and those with or "after" protection ("mitigated "M). Rates, times and probability densities are indicated by the subscripts R, T, and PD.

Table 1 – Formula Symbols and Definitions

No.	Symbol	Dimension and Definition		Equation
1	U_R	rate	Unmitigated accident rate used synonymously with "demand rate"	-
2	U_T	time	Mean time between accidents - unmitigated	$U_T = 1 / U_R$
3	M_R	rate	Mitigated accident rate	-
4	M_T	time	Mean time between accidents - mitigated	$M_T = 1 / M_R$
5	RRF	ratio	Risk Reduction Factor I	$RRF = U_R / M_R$
6	F_R	rate	Rate of "dangerous" failures of the protection function – see text section 2	-
7	F_T	time	Mean time between "dangerous" failures of the protection function (MTBF).	$F_R = 1 / F_R$
8	T_R	rate	Test rate, covering proof test and tests by "minor process demands" – see text section 2	-
9	T_T	time	Test interval, i.e. mean time between tests, including "minor process demands"	$U_T = 1 / U_R$
10	TI	time	Proof test interval according to IEC 61508	-
11	DC	ratio	Diagnostic coverage: fraction of a failure rate, which is covered by a diagnostic test	-
12	F_{RD}	rate	Detected failure rate with respect to a specific diagnostic test	$F_{RD} = F_R$ x DC
13	F_{RU}	rate	Not detected part of the failure rate with respect to a specific diagnostic test	$F_{RU} = F_R$ x (1- DC)
14	D_R	rate	Diagnostic test rate used synonymously with "demand rate"	-
15	D_T	time	Mean time between diagnostic tests	$D_T = 1 / D_R$
16	PFD(t)	prob.	Probability of failing on demand of the protection function, as function of time	-
17	PFD_{avg}	prob.	Probability of failing on demand - as average over time	-
18	$U_{PD}(t)$	$time^{-1}$	Probability density function for the occurrence of the next "demand"	equation (A3)
19	$M_{PD}(t)$	$time^{-1}$	Probability density function for the occurrence of an accident	equation (A7)

3. Mitigated Accident Rates – Example Calculations

For numerical calculations in this study a simple model function is used. This is a single channel function, with a single test interval and a test coverage of 100%. The reliability parameters are assigned the following values.

F_R Failure rate: $5 \cdot 10^{-6}$/h, equal to 0.0438 / year[5]

T_R Test Rate: 0.333 per year – corresponding to a test interval of 3 years

This defines a function in the range of SIL1. See Figure 3 for the graph of PFD(t) for the model function.

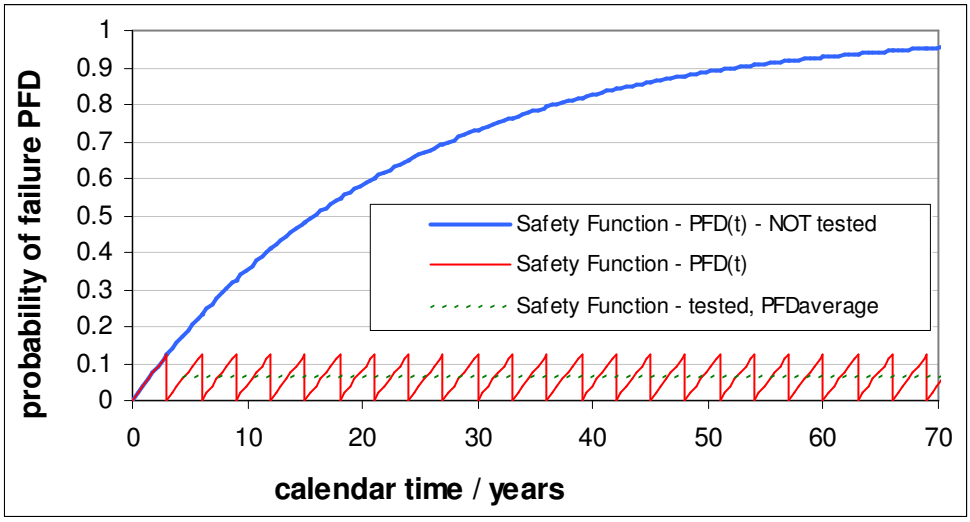

Figure 3 Probability of Failing on Demand PFD(t) of a Simple Protection Function – numerical parameters as given above

Assume, that a function with the given architecture and reliability parameters is used for preventing accidents in a storage area for hazardous liquids, which occur as a consequence of the overflow of tanks during filling. The function could comprise a level supervision, which is closing a valve in the filling line. Assume that only trained personnel is filling the tanks, according to clear procedures. Under these conditions, the process risk analysis may yield an expectancy of once every 10 years for the reference event (example **A**). This may be an accident with injury to a limited number of persons due to the overflow of a single tank during filling.

A protection function with the given architecture and reliability parameters could also be used an internal combustion engine, as a protection layer against overstressing and loss of mechanical integrity in the loaded parts of the engine. Assuming, that the reference event is expected only as consequence of hidden

[5] In the notion of IEC 61508, this would be λ_D.

component flaws in conjunction with the failure of an automatic control system to react properly, the expected mean time between events could be significantly higher than 10 years. Say 150 years for the sake of an example (example **B**).

According to IEC 61508, both cases would be qualified as “low demand cases”. Hence, an “average probability of failing on demand” PFD_{avg} can be attributed to the function. The relation between mitigated and unmitigated accident rates and the reliability parameters of the function reads as follows:

(1) $$M_R = U_R \cdot PFD_{avg}$$

(2) $$PFD_{avg} = F_T / 2 \cdot F_R = F_R / (2 \cdot T_R)$$

(3) $$\rightarrow \quad M_R = U_R \cdot F_R / (2 \cdot T_R)$$

See Figure 4 for a graph of the relation $M_R = f(U_R)$ under these boundary conditions. The protection function is working as a risk reducer. It reduces the rate of accidents by a fixed factor. Hence, a “risk reduction factor” RRF can be ascribed to the protection function as a characteristic parameter of the function:

(4) $$RRF = 1 / PFD_{avg} \quad \leftrightarrow \quad RRF = 2 \cdot T_R / F_R$$

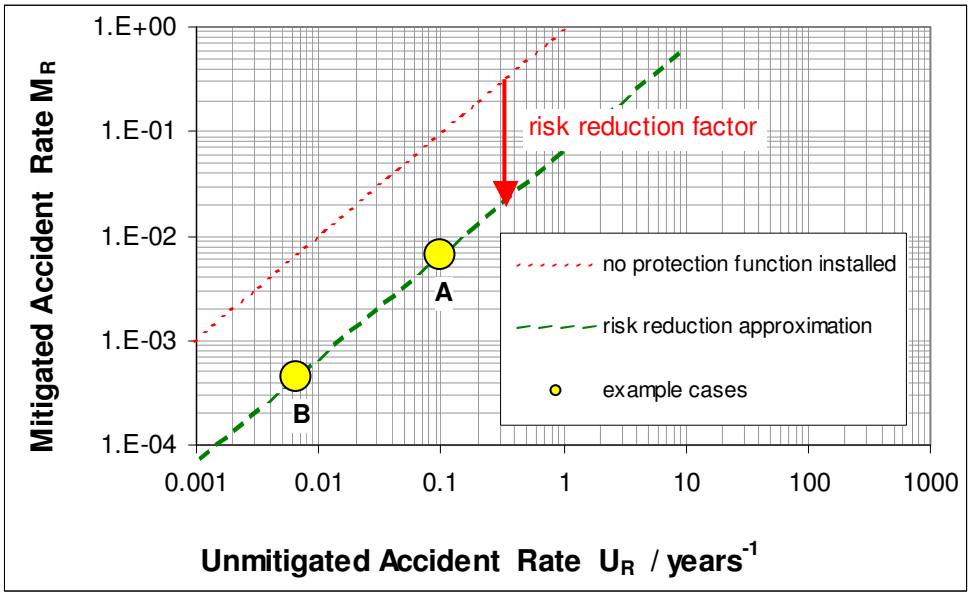

Figure 4 Protection Function as Risk Reduction Factor

Example calculation for "low" demand rates - examples **A** and **B** in the text

With the parameter values given above, the following results are obtained:

PFD_{avg}: 0.0657

RRF: 15.2

Example **A**: unmitigated accident rate U_R: 0.1 / y $\rightarrow M_R = 2.61$ / y

Example **B**: unmitigated accident rate U_R: $6.65 \cdot 10^{-3}$ / y $\rightarrow M_R = 4.38 \cdot 10^{-4}$ / y

Unfortunately, the simple relations above are not applicable over the entire range of potential demand rates. Assume, that a function of the given architecture and reliability parameters is used in a production facility for preventing harmful contact between moving machinery and service personnel. This could be a manufacturing cell with a robot, where the robot needs to be stopped as soon as a person is entering the dangerous area. This could also be a CNC engine, which needs to be stopped as soon as the cover of the cubicle is opened.

If these installations were not protected, accidents would be expected at a generally higher rate, than given in examples **A** and **B** above. Still, even for a specified reference event these numbers could vary in a wide range depending on the actual conditions. For the sake of the argument, assume:

Example **C**: one accident in average every 20 weeks $\rightarrow U_R = 2.61$ per year

Example **D**: one accident in average each second day $\rightarrow U_R = 183$ per year

In these cases, the expected average time between accidents with protection function is determined by the mean time between failures of the protection function itself. With a failure rate F_R of 0.0438 per year ($5 \cdot 10^{-6}$/h) for the example function, the mean time between failures of the protection function is 22.83 years. This time needs to elapse in average with the protected equipment, before it is able to cause the reference event, i.e. the accident under investigation. As soon as the protection function has failed, it takes a bit more time until the conditions for the reference event are given. This “bit more time”, however, does not contribute significantly to the mean time between events. For the two examples above this results in:

Example **C**: 22.83 years plus 20 weeks = 23.21 years $\rightarrow M_R = 0.0431$ per year

Example **D**: 22.83 years plus 2 days = 22.84 years $\rightarrow M_R = 0.0438$ per year

The average rate of accidents **with** protection function cannot be higher than the failure rate F_R of the protection function itself. Thus, the failure rate F_R provides an upper boundary for the mitigated accident rate M_R – see Figure 5. If the rate of accidents “before” the protection function is sufficiently high, the protection function changes its operation mode from reducing the risk to limiting the risk. In the area indicated by the examples in Figure 5, the protection function is working in a “risk-limiting mode”, rather than in a “risk reduction mode”.

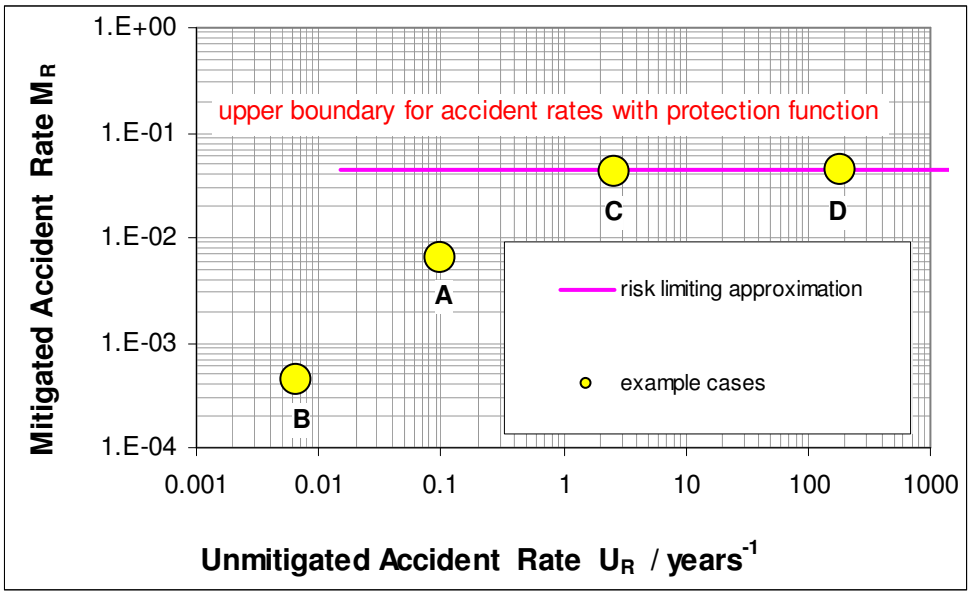

Figure 5 Protection Function as Risk Limiter

4. Risk Reduction Mode versus Risk Limiting Mode

According to the above, there are two operation regimes for a protection function, depending on the unmitigated accident rate ("demand rate"):

- Risk **reduction** mode at low rates
- Risk **limiting** mode at high rates

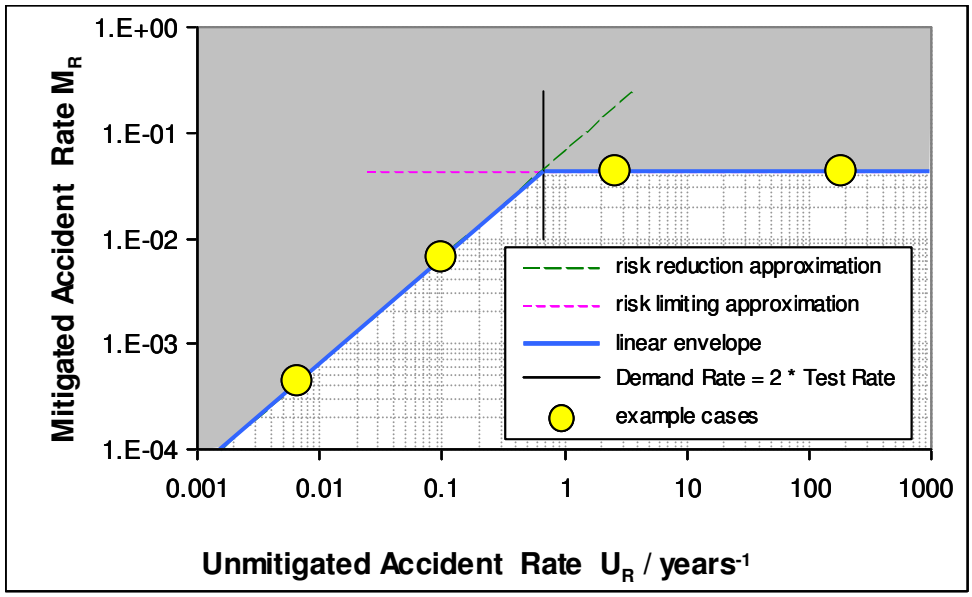

Figure 6 Protection Function as Probabilistic Filter - Linear Envelope for the Overall "Filter Function"

As shown in Figure 6, the relation $M_R = f(U_R)$ can be expressed with two linear approximations over the entire range of demand rates.

For the "Risk reduction mode" the linear approximation is given with equation (1): $M_R = U_R \cdot PFD_{avg}$

For the protection function according to Figure 3 this takes the following form of equation (3): $M_R = U_R \cdot F_R / (2 \cdot T_R)$

For the "Risk limiting mode" the linear approximation is:

(5) $M_R = F_R$

Equations (3) and (5) can be combined: to a single expression:

(6) $M_R = Minimum\left[U_R \cdot F_R / (2 \cdot T_R); F_R\right]$

The transition from "low" into "high" unmitigated accident rates is defined by the intersection of the two linear approximations. The intersection point is given by: Equations (3) and (5) give:

(7) $U_R = F_R / PFD_{avg}$ general case

(8) $U_R = 2 \cdot T_R$ protection function with a single test interval

In a statistical model system, not to speak of the reality, the mitigated accident rate would not abruptly change the slope at a specific point. Rather, the function $M_R = f(U_R)$ will change gradually from one regime into the other, following a hyperbolic function graph. The generalized function should be identified in order to confirm, that the equations above represent indeed two special cases of a single problem. The generalized function is also needed for assessing the approximation error of the linear equations.

Indeed, a generalized relation $M_R = f(U_R, F_R, T_R)$ can be derived from statistical considerations. See the Annex – "Generalized Approach – Derivation and Formulas". The equations in the Annex may be too complicated for practical applications. Still, they confirm that the "linear approximations" according to equation (6) are reasonably close to the statistically expected result – see the Figures A3, A4 in the Annex and Figure 7. The transition range between "risk reduction mode" and "risk limiting mode" is quite narrow range in terms of demand rate: approximately 0.3 to 1.5 per year in this specific case, corresponding to a range from 1 to 4.5 in units of the test rate T_R.

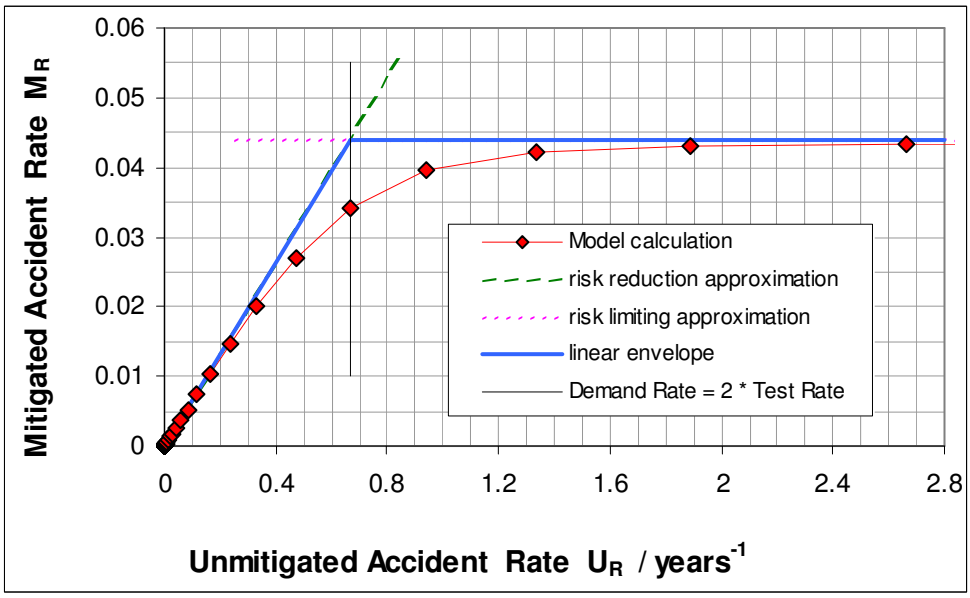

Figure 7 Protection Function as Probabilistic Filter - Model Calculation and Linear Envelope

Results of the model calculation according to equation (A10) in the Annex for the protection function in Figure 3

Figure 7a – top: logarithmic scales

Figure 7b – bottom: linear scales

The transition from “risk reduction mode” to “risk limiting mode” is related to the repeated functional testing, which keeps the unreliability of the protection function at a certain level. If the period of interest is sufficiently long, this level of unreliability can be described with an average. In this case, PFD_{avg} is characteristic for the unreliability of the protection function. The “period of interest” is the average expected time U_T between relevant demands to the function.

Conversely, if the average expected time between demands is short in relation to the test period T_T, the unreliability of the protection function does not attain a stable level in the period of interest. Instead, PFD(t) is constantly rising. In this case, it is rather the slope of PFD(t), i.e. the function failure rate F_R, which characterizes it.

The two modes of operation of a protection function can be differentiated from each other by the following criteria. Note, that there is a transition range, where neither of the two cases is unambiguously given.

Risk Reduction Mode

- Failures of the protection function are revealed with the highest probability by the next test.
- The test rate T_R is higher, than the demand rate U_R. Conversely, the mean time between tests is shorter than the mean time between demands: $T_T < U_T$. The function PFD(t) is represented by its average value over time: PFD_{avg}.
- There is no single “decisive time” or “decisive rate” in the overall system. The mitigated failure rate M_R depends likewise on the unmitigated accident rate U_R, the failure rate F_R and the test rate T_R of the protection function.
- The design of the protection system may admit compromises between failure rate, testing demands and a robust design. Failure rate by itself is not paramount for applications.
- A scheme for regular testing of the overall system and its components is essential. The protection function may have to stay ready for use, “ever vigilant”, for extended periods without process demand. Apart from the numerical effect of test rates in reliability calculations, the regular testing is an essential precondition for any reliance to be put on a system under these conditions.

Risk Limiting Mode

- The function is tested by the real application at a higher rate, than could be attained with tests: $U_T < T_T$. Therefore, failures of the protection function are revealed with the highest probability by the next accident.
- The mitigated accident rate or “residual risk” M_R is directly given by the failure rate F_R of the protection function. The “demand rate” U_R has no significant influence on the mitigated accident rate.

- A low failure rate of the protection function is critical for the application. Consequently, diagnostic measures will be a critical feature for functions in “risk limiting mode”. They are necessary for attaining low failure rates F_R.

5. Relation to the IEC Safety Standards

The operation modes of a protection “risk reduction mode” and “risk limiting mode” according to the above are related to the “low demand mode” and “high demand mode” according to IEC 61508 and IEC 61511. The relevant definitions in IEC 61508 are:

IEC 61508-4 (2010), clause 3.5.16, mode of operation:

way in which a safety function operates, which may be either

- low demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- high demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- continuous mode: where the safety function retains the EUC in a safe state as part of normal operation

IEC 61508-4 (2010), clause 3.5.17: target failure measure

target probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either

- the average probability of a dangerous failure of the safety function on demand, (for a low demand mode of operation);
- the average frequency of a dangerous failure [h-1] (for a high demand mode of operation or a continuous mode of operation)

With respect to the demand regime and target failure measure there is a clear correspondence:

- Risk reduction mode $\leftrightarrow$ low demand mode
  $\rightarrow$ Target failure measure PFD_{avg}
- Risk limiting mode $\leftrightarrow$ high demand mode and continuous mode
  $\rightarrow$ Target failure measure: Failure rate PFH or, in the current notion, F_R

There are differences in the definitions, however:

- The definition of “demand” in the frame of a given quantitative risk analysis is concretely defined in this study. See the definition of the “reference event” in section 2. In IEC 81508 it remains unclear, what is actually counted as a “demand” to a protection function and, thus, contributes to a “demand rate”.

- The “continuous mode” is not differentiated from the “high demand mode” from the viewpoint of this study. The current approach looks at the statistical effects of a protection function in a given application only. With respect to technical realization and functionality, typical protection functions in “continuous mode” may be different from typical protection functions in “demand mode”. With respect to the statistical behavior this distinction makes no sense. The “continuous mode” is just the boundary case of the “risk limiting mode” at infinitely high demand rates.
- This study defines the transition between the “demand modes” by the rate of demand rate to test rate, with the transition area according to equations (7) and (8). “One year” is not a relevant criterion, in this context[6].
- For the “risk limiting” mode of operation, this study directly identifies the “mitigated accident rate” with the failure rate of the protection function: $M_R = F_R$. For the “high demand case”, IEC 61508 is not so strict. The “residual hazard rate” is related to the “dangerous failure rate of the E/E/PE safety-related system”, however, with allowance for additional effects by “other risk reduction measures”[7]. There is not necessarily a contradiction: “high demand mode” according to IEC 61508 and “risk limiting mode” according to this study are not the same. It remains to be discussed how “other risk reduction measures” would be represented in the frame of the current approach – see in the following section 6.

For specifying reliability parameters sufficiently stringent, the proper choice of the demand mode is not critical, anyway. This is obvious from Figures 6 and 7. Both of the two linear approximations represent absolute upper boundaries for mitigated accident rates M_R. In the transition area both approximations are conservative. Therefore, with respect to safety applications each approach is “valid” in the entire range of demand rates U_R, as long as it consequently followed.

It is not necessarily prudent, to specify a protection function in “risk reduction mode” according to “risk limiting” criteria and vice versa. However, it cannot be considered “unsafe”, in first instance. If the requirements to a protection function become unreasonably stringent in a given risk analysis, this may be an indication that the inappropriate approximation was used. If the procedures and templates in a company are set up according to a specific demand mode, there is no need to change only because the demand rate resulting from a risk analysis passes a certain limit.

[6] In the first edition of IEC 61508 /1/, “frequency of demands . . . greater than twice the proofcheck frequency” was still used as a second criterion for assigning the “high demand mode” (part 4, clause 3.5.12). According to this study, “twice the test rate” is the **only** decisive criterion where equation (7) applies.

[7] IEC 61508 /2/, part 5, clause A.5.2 and part 4, clause 3.4.2

6. Other Risk Reduction Measures

According to IEC 61508, an "other risk reduction measure" is a "measure to reduce or mitigate risk that is separate and distinct from, and does not use [the protection function under discussion][8]. The question remains from text section 5 above, whether such measures can be claimed for reducing the requirement to the failure rate F_R of a protection function. Four different "other risk reduction measures" are discussed, in this respect:

- Active "unintelligent process devices" such as pressure relief valves
- Passive measures such as protective housings or walls, reducing the "severity of harm" should a failure of process or engine occur
- Functional tests by "minor process demands" – see section 2
- Reduction of the exposure parameter of occupancy factor of people, for reference events involving harm to people

The first two of the above measures are already accounted for in the determination of the unmitigated accident rate, according to the approach of this study. They are already implemented in a given design of process, engine or plant, when the safety integrity requirements to an additional instrumented protection function are determined. Where such measures are implemented and need to fail in order to admit the reference event, the assessment will assign the "risk reduction mode" in most realistic cases[9]. Hence, such measures will actually be effective for reducing the "mitigated accident rate M_R.

The assessment will also assign the "risk reduction mode", when the third of the above measures is accounted for - functional tests by "minor process demands". The expected rate is generally higher for less severe accidents than for grave or even catastrophic events. Consequently, if the reference event defines a grave event as "relevant accident", the failure of the protection function is revealed with the highest probability by a "minor process demand", if at all such minor process demands can be claimed as "functional test"– see the second paragraph below.

The same protection function in the same application may be assigned the "risk limiting mode" in a given assessment, if the reference event defines a less severe accident as "relevant"[10]. The requirement to the failure rate F_R could be

[8] IEC 61508 /2/, part 4, clause 3.4.2

[9] If, for example a pressure relief valve with a test regime according to good engineering practice is installed for preventing fatal accidents, any additional protection function will most likely operate in the risk reduction mode. The demand rate with respect to a fatal accident will hardly exceed the test rate of the pressure relief valve.

[10] Take as an example the probabilistic determination of the safety integrity requirement to a process temperature supervision function of an internal combustion engine with fuel flow limitation. This assessment could yield the expected rates of light engine damages every few months and of heavy engine damages affecting structural parts of the engine once in 15 to 20 years. With a proof test period of 3 years, the operation modes result as given above.

even more stringent, in this case. It is a general perception at least in the power generation industry, that the operational / commercial demands to protection functions are actually more stringent, than the safety related demands. The safety related demands are usually related to heavy and, consequently, seldom incidents.

It is subject of a separate discussion, under which conditions a testing by "minor process demands" may be accounted for in a proper risk assessment and/or SIL assignment. In any case, a failure of the protection function to react properly on these "minor" demands must have a sufficiently high chance to be detected and to be repaired, before further consequential damage ensues.

Finally, with respect to number four in the list of "other risk reduction measures" above: Reducing the exposure of people to a given process hazard is helpful in the "risk reduction mode", and has usually no effect in the "risk limiting mode".

Take the example of a manufacturing cell with a robot, where the robot needs to be stopped as soon as a person is entering the dangerous area, with the numerical examples **C** and **D** in section 3. In this case, it was shown that the rate of accidents is reduced by less than 2%, if the exposure rate is reduced by a factor of 70 (from once in 20 weeks to once in 2 days).

In risk graphs or in other risk assessment methods, which specify risk reduction factors $RRF_{required}$ by estimating demand rates, frequently an "occupancy parameter" or "exposure parameter" is used. For assigning safety integrity requirements to protection functions in the "risk-limiting mode", this is not compatible with statistical considerations in most cases. See Reference /8/ for a further discussion.

In summary, "other risk reduction measures" reduce mitigated accident rates M_R and, consequently, alleviate the requirement to the failure rate F_R of a protection function only as far, as they move the protection function under assessment in the "risk reduction mode". They may do so by either reducing the demand rate U_R sufficiently in relation to a given test rate T_R, or by increasing the test rate sufficiently in relation to a given demand rate.

7. Diagnostics

Assume, that the example function in Figure 3 is upgraded by introducing a diagnostic measure. This is a check on a specific functionality within the function. Diagnostic checks are typically executed more frequently than proof tests, i.e. with higher rates. On the other hand, diagnostic tests cover the entire required functionality only partially, i.e. the "diagnostic coverage" is less than 100%.

For example, if the unreliability of a function is ascribed to a shut-off valve in a process media line to a significant degree, the situation can be improved by regular testing of that valve – e.g. by a partial stroke test. In this case, the requirement can be understood from the IEC safety standards, that the diagnostic test rate should exceed the "demand rate" by a factor of 100 in order to be assumed as effective[11].

Assume that the partial stroke test in the example above covers 55% of the total function failure rate and that this test can be executed once each 48 hours. Consequently, the diagnostic coverage of 55% could be claimed only, if the demand is expected at a rate of less than once every 200 days, i.e. less than 1.8 per year. Thus, for a demand of, say once every 100 days the test would have to be disregarded for the validation of the function against a specific "target failure measure".

The effect of the stroke test on the mitigated accident rate can be quantified according to the approach of this study. To this end, the failure rate of the function is split in the "detected part" F_{RD} and the undetected part" F_{RU} as usual. In the current notion:

(9) $$\rightarrow \quad F_R = F_{RD} + F_{RU} = F_R \cdot DC + F_R \cdot (1 - DC)$$

The decomposition of the protection function unreliability in two additive parts can be carried through the entire derivation in the Annex. Accordingly, this is also valid for the linear approximations according to equation (6)[12]:

(10) $$M_R = Minimum\left[U_{RD} \cdot F_{RD} / (2 \cdot D_R);\, F_{RD}\right] + Minimum\left[U_{RU} \cdot F_{RU} / (2 \cdot T_R);\, F_{RU}\right]$$

In other words: The "detected" part of the protection function appears in this treatment as a separate protection function, which contributes to the overall effect of risk reduction/limitation according to its own share F_{RD} of the overall failure rate F_R and according to its own test rate D_R.

[11] IEC 61508-2 (2010), clause 7.4.4.1.4: When estimating the safe failure fraction of an element, . . . credit shall only be taken for the diagnostics if . . .the ratio of the diagnostic test rate to the demand rate equals or exceeds 100. See also IEC 62061 /4/, clause 6.3.2 and ISO 13849 /6/, part 1, clause 4.5.4

[12] In the notion of IEC 61508, λ_{DD} and λ_{DU} would be used instead of F_{RD} and F_{RU}, respectively.

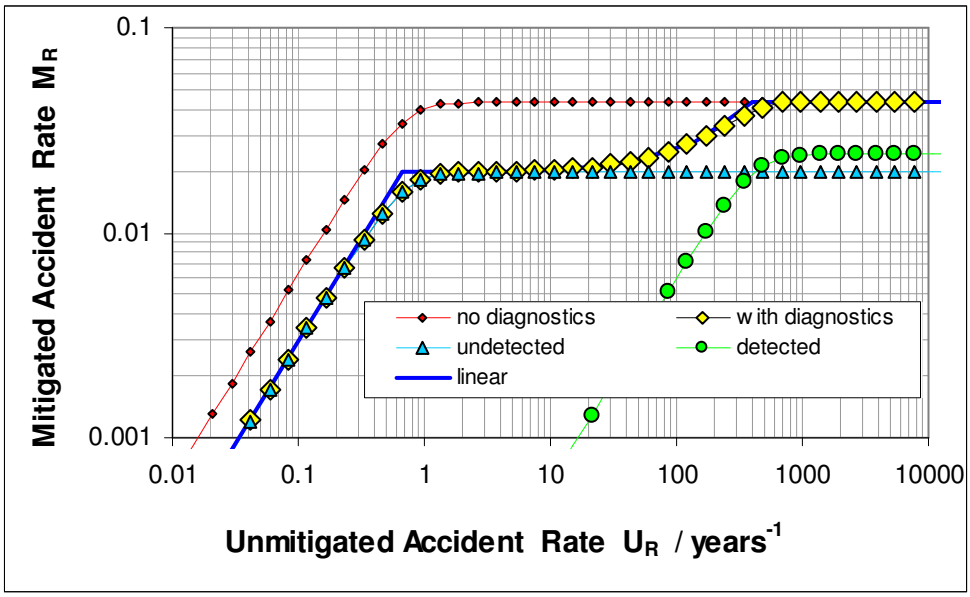

Figure 8 Single Channel Protection Function with Diagnostics,

Model calculation and linear envelope; basis function according to Figure 3, with DC 55% and diagnostic interval of 0.005 a (ca. 2 days, Diagnostic test rate D_R: 200/year)

In Figure 8 the relation $M_R = f(U_R)$ is shown for the numerical example above ($F_R = 10^{-6}$ / h, T_R = 1/3a, DC = 55%, D_R = 1/48 $h^{-1} \approx 0.05\ a^{-1}$). The decomposition in "detected" and "undetected" part and the linear approximation of the overall relation according to equation (9) are shown as well.

The graph illustrates how the effect of the diagnostic test disappears gradually, when the demand rate approaches and exceeds the diagnostic rate. The diagnostic test becomes ineffective as the "detected part" of the overall function switches from "risk reduction mode" to "risk limiting mode".

Figure 8 confirms again, that the "linear approximation" according to equation (10) is reasonably close to the results of the model calculation. In Figure 9 the linear approximation is used for calculating the "relative efficiency" of the diagnostic test. This is the actual contribution to the risk mitigation (in terms of avoided M_R) at a given demand rate, in relation to the maximum possible risk reduction by the diagnostic test (55% in the given case). The diagnostic test starts to become effective at a demand rate of **twice** the diagnostic test rate It has attained 95% of relative efficiency, when the demand rate is one order of magnitude below diagnostic test rate. Thus, for a demand of once every 100 days according to the example above, the test may be regarded as "effective" to nearly full extent.

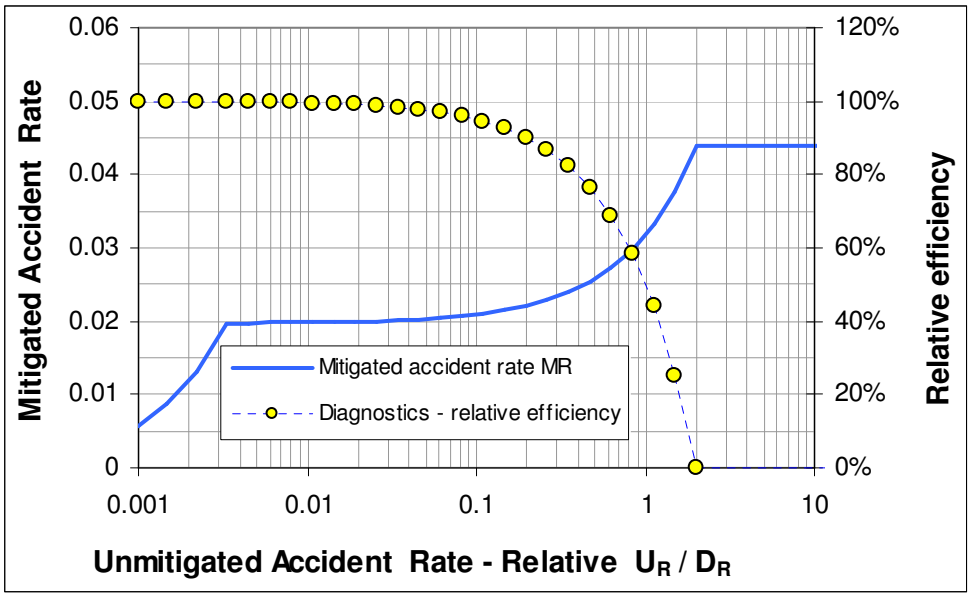

Figure 9 Relative Efficiency of the Diagnostic Test

The demand rate is normalized with respect to the diagnostic test rate DR. All other parameters are as in Figure 8.

8. Conclusions

The discussion above can be summarized as follows

- The rate of accidents, which are admitted by the unreliability of a protection function, can be described by two linear approximations. One of them applies to “low” demand rates, the other one to “high” demand rates. The respective operation mode for the protection function is “risk reduction” and “risk limiting”, respectively. The two approximations can be derived as special cases from a generalized statistical model.
- The linear approximations for a simple protection function can be used to derive linear approximations for more complex functions. The example of a function with diagnostics was discussed.
- A demand rate is “low” or “high” in the sense above depending on its ratio to the test rate of the protection function. A limit at “one demand per year” is statistically not conclusive.
- The “continuous demand” can be treated as a specific case of the “risk-limiting mode”. A distinction of “demand mode” versus “continuous mode” is not relevant in this context.
- A protection function can be validated against a specific risk target by using either of the two approximations. A positive result is valid, even if the “wrong” approximation was chosen. Conversely, a specification of PFH or PFD_{avg} is valid with respect to safety applications, even if the improper approximation was chosen. The requirement will rather be more stringent than necessary.
- In the “risk limiting mode”, the residual risk is given by the rate of undetected dangerous failures of the protection function F_R. Accidents occur as frequently as the protection function fails. The demand rate is not relevant in this respect and should not be used to specify the allowable failure rate. In particular, the exposure factor of people to a process hazards is ineffective in most applications with “high” demand rates.

Annex - Generalized Approach – Derivation and Formulas

In order to derive a representation of the mitigated accident rate M_R, which is valid over the entire range of "demand rates", the following approach is proposed

The definition of the risk reduction factor RRF is generalized with respect to equation (4):

(A1) $$RRF = U_R / M_R$$

In Figure 3 the probability of failing on demand PFD(t) is shown for a simple example as function of the calendar time. For the given example, this can be represented by a simple analytical equation:

(A2) $$PFD(t) = 1 - \exp\left(- F_R \cdot \mathrm{mod}(t, T_T)\right)$$

In order to predict, how effectively this function will prevent the next potential accident, one should know when this would occur. Other than the proof tests, the "potential accidents" do not occur in regular intervals. Instead, the expected time until the next accident is described by a probability density function $U_{PD}(t)$. This function describes for any time interval in the future, how likely it is, that the next "unmitigated accident" will fall in this interval.

Time intervals between random occurrences vary according to "Erlang distribution functions" /9/. In a statistical model with time independent accident rates, the "random time between two accidents" and the "random time to the next accident" have the same meaning. For this simple case, the basic equation is written as follows:

(A3) $$U_{PD}(t) \equiv Erl(t,1) \equiv t \cdot \exp(-a \cdot t)$$

The parameter "a" and a scale factor in equation (9) must be set in order to satisfy the following two conditions:

(A4) $$\int_{t=0}^{t=\infty} U_{PD}(t) \cdot \partial t = 1$$

(A5) $$\int_{t=0}^{t=\infty} t \cdot U_{PD}(t) \cdot \partial t = 1/U_R$$

With equation (A4) it is expressed, that the next demand is expected to happen certainly – at which time ever. Equation (A5) requires the distribution function to correspond to the correct "mean time between demands" $1/U_R$. This leads to:

(A6) $$U_{PD}(t) = 4 \cdot {U_R}^2 \cdot t \cdot \exp(-2 \cdot U_R \cdot t)$$

This function has a single free parameter, the unmitigated accident rate U_R. Graphs of the function are shown in Figure A1. This approach assumes the situation to be time independent and without memory. The time scale in Figure A1 is a relative time scale. “Now” in this graph is always at t=0.

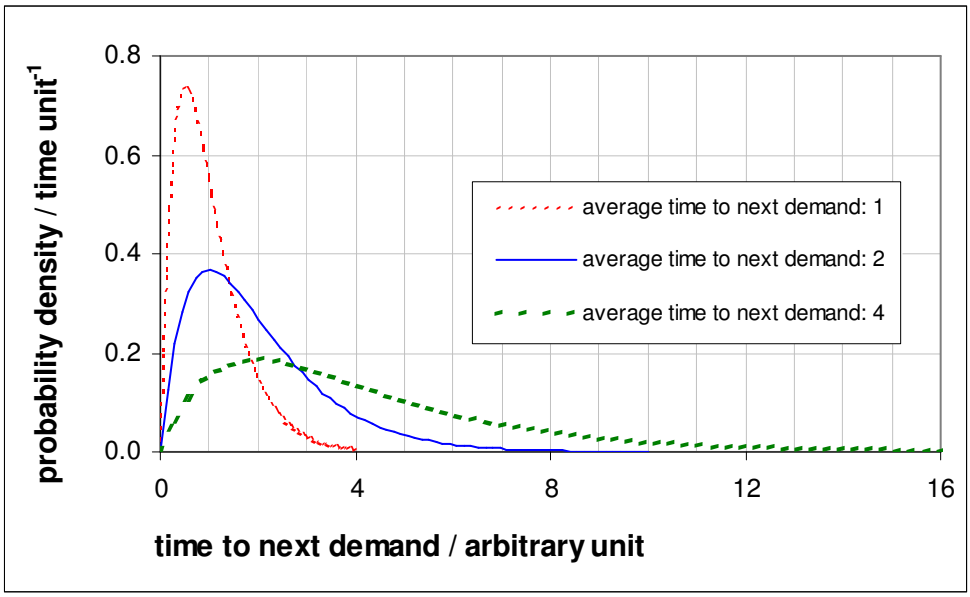

Figure A1 Erlang Probability Density Function

Graph of the probability density of the time to the next event, assuming that events occur randomly distributed in time at an average rate

In Figure A2 the “unmitigated probability density for the next accident” $U_{PD}(t)$ is superimposed on the “probability of failing on demand” PFD(t) of the protection function. The multiplication of these two functions leads to yet another probability density, describing the chances of the next demand to meet the protection function in a failed state and to escalate to an accident. This is called the “mitigated accident probability density function” $M_{PD}(t)$. Hence:

(A7) $$M_{PD}(t) = U_{PD}(t) \cdot PFD(t)$$

The probability of the next ”demand” to escalate to an accident is given by the overall integral of the “mitigated accident probability density”. This is inverse to the risk reduction factor of the protection function in the given scenario:

(A8) $$\int_{t=0}^{t=\infty} M_{PD}(t) \cdot \partial t \quad = \quad \int_{t=0}^{t=\infty} U_{PD}(t) \cdot PFD(t) \cdot \partial t \quad = \quad 1/RRF \quad = \quad M_R / U_R$$

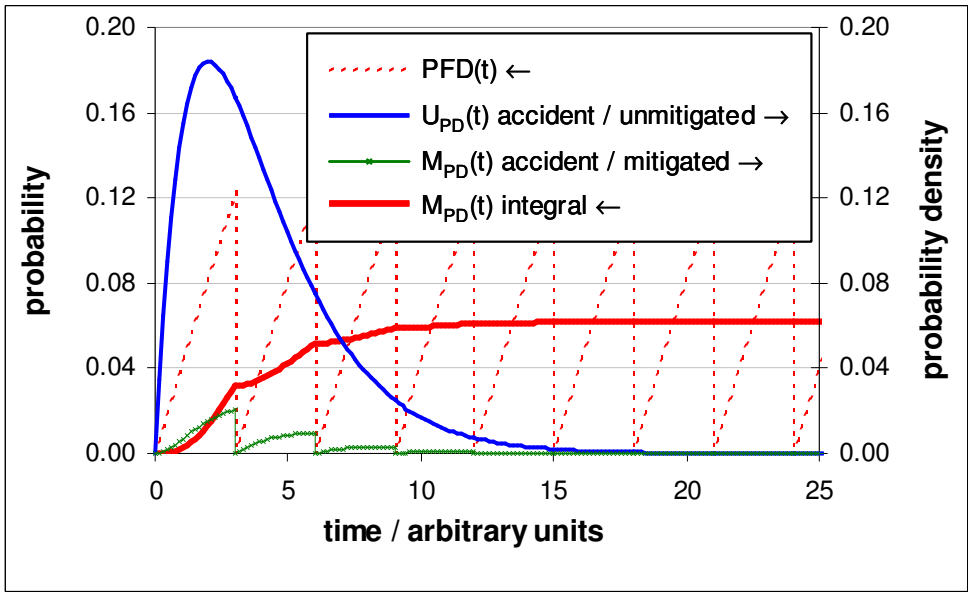

Figure A2 Calculation of the Expected Accident Rate MR

Determination for a specific demand rate, using the probability density function for the next demand. See in the text for further explanation

The "mitigated accident probability density function" $M_{PD}(t)$ is not anymore normalized. Its overall integral is different from 1. It is not expected, that the next demand will lead to an accident with certainty. This probability should be less than 1.

The chances of the protection function to prevent the **next** accident are as high as its chances to prevent any accident. Equation (A8) assumes only, that PFD(t) is zero at time zero for $U_{PD}(t)$. Note, that the time scale for PFD(t) is fixed in relation to calendar time, while the time scale for $U_{PD}(t)$ is only relative with respect to "now" and always extends into the future. The condition "t equals zero" for both is strictly valid for any instant, where just a test was completed with positive result. By substituting equation (A6) in equation (A8), one obtains:

$$(A9) \quad M_R / U_R = \int_{t=0}^{t=\infty} 4 \cdot U_R{}^2 \cdot t \cdot \exp(-2 \cdot U_R \cdot t) \cdot PFD(t) \cdot \partial t$$

For the specific function shown in Figure 3 with PFD(t) according to equation (A2) this gives:

$$(A10) \quad M_R / U_R = \int_{t=0}^{t=\infty} 4 \cdot U_R{}^2 \cdot t \cdot \exp(-2 \cdot U_R \cdot t) \cdot \left\{1 - \exp\left[- R_U \cdot \mathrm{mod}(t, T_R{}^{-1})\right]\right\} \cdot \partial t$$

Equation (A9) represents the “overall model”, which relates the “risk reduction factor” to the reliability parameters of the protection function in a single approach, valid for the entire numerical ranges of input parameters. This is a general form for any type of PFD(t) function. Equation (A10) is the specific form of for the simple “example protection function” according to Figure 3.

In Figure A2 the calculation of the inverse risk reduction factor RRF^{-1} is illustrated for a single data point. In Figure 7 in the main text the data are displayed for a series of data points in the plot of “mitigated accident rate” as function of “unmitigated accident rate”. It is shown, which rate of accidents would have to be expected as function of the “demand rate”, assuming a specific protection function as installed and effective.

The model calculation verifies, what could be inferred already from Figure 6: The “mitigated accident rate” M_R as a function of the demand rate U_R is a hyperbolic function, which switches smoothly from one linear branch to another linear branch. “Low demand” and “high demand” represent indeed two specific cases of a general problem with a general solution. Equation (A9) above is one of the possible representations for this “general solution”.

The form of the probability density function for the next demand $U_{PD}(t)$ according to equation (A6) is not even critical for obtaining the result according to Figure 7. It is visually evident, that long “demand periods” will interact with an average of the function – see Figure A3.

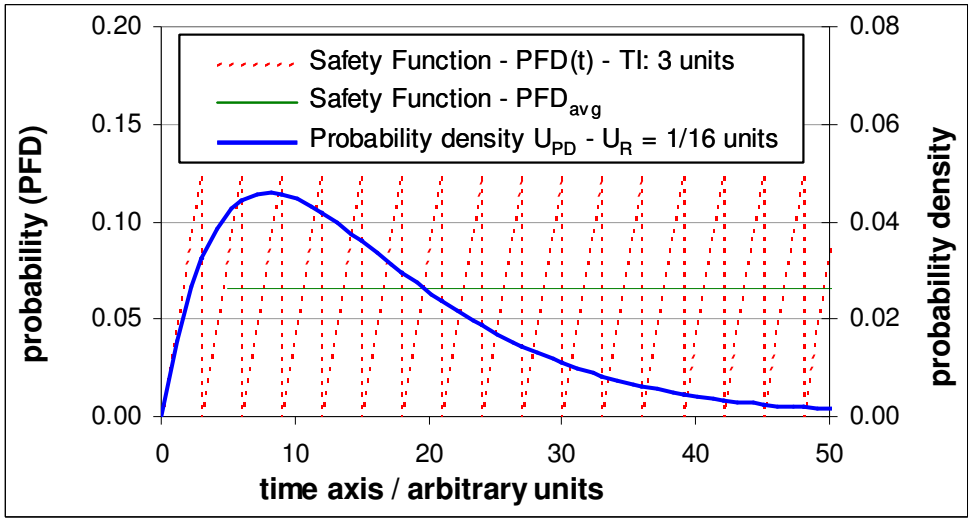

Figure A3 Variation of PFD(t) in Relation to "Long" Demand Periods

The probability density of the next demand averages PFD(t) over extended periods

With respect to short demand periods, i.e. high demand rates, the probability of failure can be expressed as linear function of time – see also Figure A4

(A11) $PFD(t) = F_R \cdot t$

Equation (A8) takes the following form:

(A12) $M_R / U_R = \int_{t=0}^{t=\infty} U_{PD}(t) \cdot F_R \cdot t \cdot \partial t \quad = \quad F_R \cdot \int_{t=0}^{t=\infty} U_{PD}(t) \cdot t \cdot \partial t$

Substituting equation (A5) in (A12) simply yields:

(A13) $M_R = F_R$

The failure rate F_R of the protection function becomes identical with the mitigated accident rate M_R in the boundary case of a high demand rate, irrespective of which probability density function describes the "next demand".

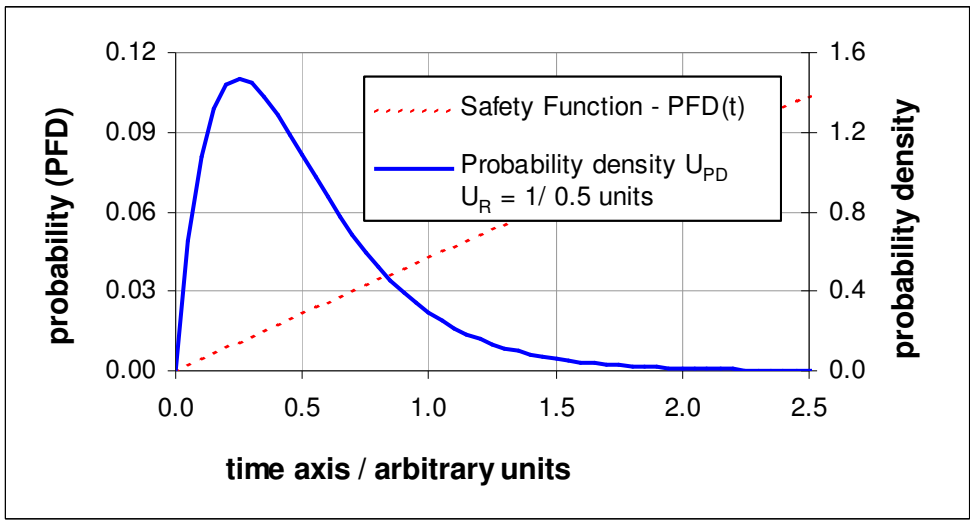

Figure A4 Variation of PFD(t) in Relation to "Short" Demand Periods

The probability density of the next demand interacts with PFD(t) as linear increasing function

The derivation above is transferable to protection functions with more than a single channel as well. These architectures are all characterized by functions PFD(t) in the shape of a saw-tooth curve – very similar to Figure 3. For complex protection functions comprising several elements with different architectures and testing regimes, the overall relation $M_R = f(U_R)$ can be developed by applying the linear approximation according to equation (6) to the single constituent subsystems. In text section 7 an example is given for a single channel function with diagnostics.

References

/1/ IEC 61508; Functional safety of electrical / electronic / programmable electronic safety related systems; 1st edition 1998-12

/2/ IEC 61508; Functional safety of electrical / electronic / programmable electronic safety related systems; 2nd edition 2010

/3/ IEC61511, Functional safety – Safety instrumented systems for the process industry sector; 1st edition 2003-01

/4/ IEC 62061; Safety of Machinery - Functional safety-related electrical / electronic and programmable electronic control systems; 1st edition 2005-01

/5/ VDI/VDE 2180; Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT); April 2007

/6/ ISO 13849; Safety of machinery - Safety-related parts of control systems; Part 1: General principles for design; 2007-07

/7/ VDMA-Einheitsblatt 4315-1; Turbomaschinen – Anwendung der Prinzipien der Funktionalen Sicherheit – Teil 1 Verfahren zur Ermittlung der notwendigen Risikoreduktion, to be published 2011.

/8/ A. Belzner; Demand Mode and Target Failure Measure for Protection Functions - A Generalized Approach; in Proceedings of the 37th ESReDA Seminar; Asset Optimization and Maintainability: Challenges in a New World Order; Baden, Switzerland, October 22, 2009

/9/ Wikipedia, entry “Erlang distribution”; 2009-09-03