Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria

doi: 10.3850/ESREL2026061419_esrel26-p27816-cd

PFD calculation method for systems with high failure rates, long test intervals, and many components

Ondrej Osicka
TÜV Rheinland Safetec, Norway. E-mail: ondrej.osicka@safetec.tuv.com

Ragnar Aarø
TÜV Rheinland Safetec, Norway. E-mail: ragnar.aaro@safetec.tuv.com

Henrik K. Kortner
TÜV Rheinland Safetec, Norway. E-mail: henrik.kristian.kortner@safetec.tuv.com

Tor Onshus
Department of Engineering Cybernetics, Norwegian University of Science and Technology, Norway. E-mail: tor.onshus@ntnu.no

Safety Instrumented Functions (SIFs) in low-demand mode are key elements of risk reduction in the process industry. Their performance is commonly expressed through the average probability of failure on demand (PFD), forming the basis for compliance with Safety Integrity Level (SIL) targets. Current calculation methods, such as those presented in IEC 61508 and the PDS Method Handbook, rely on simplified formulas under a set of assumptions.
For systems with high failure rates, long proof test intervals, or a large number of components, some of these assumptions are violated. When $\lambda \cdot \tau$ is not "small enough," the resulting approximations may become overly conservative and, in some cases, produce unrealistic values (e.g., PFD > 100 %). Although such systems fall outside the applicability of IEC 61508 and IEC 61511 as they cannot meet even the lowest SIL 1 requirement, other guidelines (e.g., OG 00046) recognize the need to manage safety functions with requirements below SIL 1.
We propose a revised PFD calculation methodology which builds on the PDS Method framework but relaxes assumptions such as linearization of the time-dependent probability of failure on demand PFD(t) and the negligibility of simultaneous independent failures. The method offers improved validity for challenging cases while remaining considerably simpler than advanced approaches such as Markov models, yet more accurate and interpretable than current simplified formulas.
Numerical examples illustrate the differences between the proposed method and current simplified formulas, highlighting the importance of extending the validity range for reliability assessments. The revised methodology bridges the gap between theoretical rigor and practical usability, providing a basis for consistent management of all instrumented safety functions, irrespective of SIL.

Keywords: Probability of failure on demand (PFD), Reliability assessment, High failure rates, Long test intervals.

1. Introduction

Safety Instrumented Functions (SIFs) are essential elements of risk reduction strategies in the process industry, designed to mitigate hazardous events by automatically initiating protective actions when specific conditions are met. This paper focuses on SIFs operating in low demand mode, i.e., safety functions only performed on demand with the frequency of demands not exceeding one per year as defined by IEC 61508 (International Electrotechnical Commission 2010). The required performance of a SIF in low demand mode is typically defined by a Safety Integrity Level (SIL), which quantifies the maximum tolerable probability of failure on demand for the function.

The specification and design of a SIF are typically governed by a Safety Requirements Specification (SRS), which outlines functional and integrity requirements, including the target SIL. Furthermore, achieving and maintaining the required SIL throughout the operational life of the SIF requires systematic follow-up (commonly referred to as SIL follow-up) involving periodic assessment of reliability data and operational changes.

Note that a SIL requirement governs more than just the probability of failure on demand. It also includes architectural constraints for the SIF, as well as requirements related to its systematic performance. This paper, however, addresses only the calculation of the probability of failure on demand.

The probability of failure on demand is a time-dependent function, low immediately after a proof test and increasing as time since the last test passes. Each component in a SIF typically has an associated failure rate (λ_{DU})[a] and a proof test interval (τ), which together determine the contribution of that component to the overall probability of failure on demand. In many applications, it is sufficient to know the long-run average value, the average probability of failure on demand. It is the average value which is used for comparison with the target SIL during compliance assessments and operational follow-up. In the following, we use PFD to refer to the average probability of failure on demand, and PFD(t) to refer to its time-dependent counterpart.

The IEC 61508 standard (International Electrotechnical Commission 2010) presents the "reliability block diagram approach" to evaluation of the PFD as well as other, more complex, methodologies. The PDS Method Handbook (Hauge et al. 2013) proposes multiple modifications (for example, an extended version of the β-factor model) as well as further simplification (for example, the contribution from unavailability due to repair and testing is considered negligible, and detected dangerous failures are assumed to result in the system being brought to a safe state) of this approach. It is commonly referred to as the PDS Method and has been adopted by multiple guidelines (Offshore Norge 2023; Håbrekke et al. 2023) and is broadly used by practitioners (i.e., especially in Norway).

Both the PDS Method and the IEC 61508 approach are subject to a set of assumptions with IEC 61508 explicitly listing 17 "underlying hypotheses". In some cases, these might be too restrictive, and the methods may not be applicable. There are other approaches which are more complex and allow for relaxation of some of the assumptions, including the Markovian approach, Petri nets or Monte Carlo simulation approach, which are discussed in IEC 61508-6 (International Electrotechnical Commission 2010). Bukowski (2005) compares simplified formulas (identical to those proposed by the PDS Method, only not considering common cause failures) and the Markovian approach with results obtained from classical probability techniques, and shows that the Markov models give the same results as the classical probability techniques, "when properly constructed and interpreted." Nevertheless, "the simplified formulas are still preferred by most practitioners, due to their simplicity" (Jin et al. 2013).

To provide a good approximation, several of the assumptions for the use of the simplified formulas require the failure rates λ_{DU} and/or the product of the failure rates and the proof test intervals τ being "small enough" (Hauge et al. 2013). In Fig. 1, Bukowski (2005) has shown the percentage error in PFD obtained by using the simplified formulas compared to the exact equations based on classical probability techniques, and its dependence on the value of $\lambda_{DU}\tau$. In case

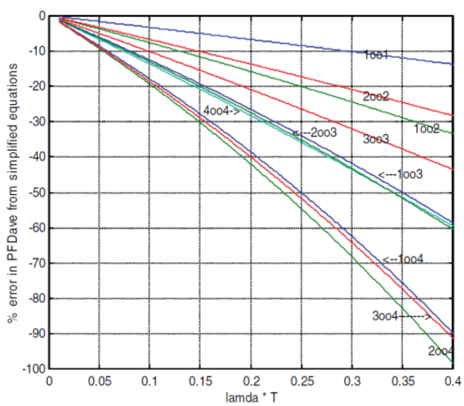

Fig. 1. Error in PFD from simplified formulas (Figure reprinted with permission from Bukowski (2005); © IEEE)

[a] When evaluating the probability of failure on demand, only the rate of dangerous undetected failures is relevant. Therefore, this paper uses notation λ_{DU} when referring to failure rates.

of the PDS Method, a specific requirement of $\lambda_{DU}\tau \leq 0.2$ is stated. Rausand (2014) suggests a value of 0.1 for this threshold, while Lundteigen and Rausand (2009) even mention a condition of $\lambda_{DU}\tau < 0.01$ for the underlying approximations not to be "too conservative".

The negative percentages in Fig. 1 mean that the simplified formulas consistently produce conservative approximations, i.e., the true PFD is less than the computed PFD.

The larger the value of $\lambda_{DU}\tau$ is and the greater the total number of components in the system, the more conservative the approximation provided by the simplified formulas becomes. However, at some point it will become overly conservative, which is evident in cases where the approximations result in failure probabilities exceeding 100 %. Applying the same parameters as used by Bukowski (2005) to produce Fig. 1 on a 11oo11 system (11-out-of-11; a voting logic configuration requiring all 11 out of 11 components to function), with $\lambda_{DU}\tau = 0.2$ ($\lambda_{DU} = 2 \cdot 10^{-5}\, hr^{-1}$ and $\tau = 10{,}000\, hours$) and a common cause failure parameter $\beta = 0\,\%$, one would arrive at a PFD value of 1.1, i.e., a 110 % probability that the system will fail to perform its safety function when required.

It may be difficult to interpret a calculated probability exceeding 100 %, but it would be reasonable to conclude that the true PFD would still be large. Systems with high probabilities of failure on demand fall outside the scope of IEC 61508 (International Electrotechnical Commission 2010) and IEC 61511 (International Electrotechnical Commission 2016). IEC 61508 explicitly states in the list of underlying hypotheses that "the resulting average probability of failure on demand for the system is less than 10^{-1}." If this condition is not met, the evaluated SIF cannot meet even the lowest SIL 1 requirement, and therefore lies beyond the applicability of both standards. In contrast, other guidelines such as OG 00046 (Health and Safety Executive 2014) or VDI/VDE 2180-1 (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik 2019) recognize the need for safety functions with SIL requirement below SIL 1. OG 00046 further emphasizes that management of all instrumented safety functions should be ensured, irrespective of the required risk reduction. With current PFD calculation methods in literature, this may be difficult to achieve.

In this paper, we propose a revised PFD calculation methodology which is valid for systems that include components with high failure rates and/or long proof test intervals.

Previously, other authors have challenged particular assumptions of the PDS Method and proposed alternative formulas to those presented by Hauge et al. (2013). For example, while the PDS Method considers constant failure rates and proof tests with perfect coverage (all elements "as good as new" after the test), Rogova et al. (2017) have proposed formulas for the case with non-constant failure rates with Weibull distribution, and Jin et al. (2013) have considered non-perfect proof testing.

2. PFD calculation with PDS Method

The probability of failure on demand, PFD(t), is a time-dependent function, low immediately after a proof test and increasing as time since the last test passes, as illustrated in Fig. 2. This function can be evaluated for individual components or for the entire system. Assuming an exponential failure rate, PFD(t) is defined as $1 - e^{-\lambda_{DU}t}$ over the interval $0 \leq t < \tau$, where λ_{DU} denotes the failure rate of the component or system, and τ is the proof test interval.

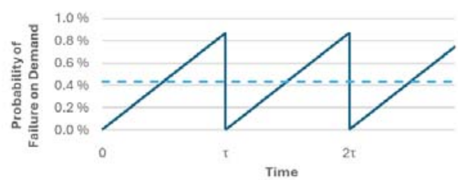

Fig. 2. The time-dependent probability of failure on demand (applied parameters: 1oo1 system; λ_{DU} = 1.00E-06 h^{-1}; τ = 8,760 h)

The long-run average value of PFD(t), indicated by the dashed line in Fig. 2 is referred to as the PFD. It represents the expected unavailability of the safety function upon demand, averaged over time.

For MooN (M-out-of-N; $M < N$) and NooN (N-out-of-N) systems, the PDS Method Handbook (Hauge et al. 2013) proposes the following approximative formulas for calculation of the PFD:

$$PFD_{MooN} \approx C_{MooN}\beta\frac{\lambda_{DU}\tau}{2} + \frac{N!}{(N-M+2)!\,(M-1)!}(\lambda_{DU}\tau)^{N-M+1} \quad (1)$$

$$PFD_{NooN} \approx N \frac{\lambda_{DU}\tau}{2} \quad (2)$$

Additionally, Hauge et al. (2013) acknowledge that the formulas may be "somewhat inaccurate when β is large, say $\beta > 5\ \%$ or when N is large (i.e., $N > 3$)" and propose also an alternative calculation method with proper consideration of common cause failures (CCF) with the following formulas (note that for $\beta = 0\ \%$, the formulas become identical):

$$PFD_{MooN} \approx C_{MooN}\beta \frac{\lambda_{DU}\tau}{2} + \frac{\binom{N}{N-M+1}\left((1 - H_N\beta)\lambda_{DU}\tau\right)^{N-M+1}}{N - M + 2} \quad (3)$$

$$PFD_{NooN} \approx (N - C_N\beta) \frac{\lambda_{DU}\tau}{2} \quad (4)$$

To account for CCF, the PDS Method utilizes the multiple beta-factor model originally proposed by Hokstad (2004). It is based on the idea of adjusting the CCF contribution based on the system's voting logic, offering a more realistic estimation than the standard beta-factor model presented in IEC 61508-6 (International Electrotechnical Commission 2010), which only considers simultaneous failure of all components. Although IEC 61508-6 also presents a multi-parameter shock model as an alternative approach to modelling partial-group failures, the PDS Method follows the multiple beta-factor model. For the use within the PDS Method, Hauge et al. (2013) proposed some adjustments and a different choice of parameters than used in the original work. For the definition of corresponding parameters C_{MooN}, C_N, and H_N, we thus refer to the PDS Method Handbook (Hauge et al. 2013).

For later reference, it is important to understand the interpretation of parameters C_{MooN} and H_N. According to Hokstad (2004) and Hauge et al. (2013), in a system with N components with probability Q of one component being in a fault state, $C_{MooN}\beta Q$ represents the probability that $N - M + 1$ or more components fail simultaneously due to CCF. Following the definition of H_N provided by Hauge et al. (2013), it can be shown that $(1 - H_N\beta)Q$ then refers to the probability of a single component failing independently of the common cause. This also highlights the key difference between the standard and multiple beta-factor models. In the standard model, either all components fail simultaneously due to a common cause or none do. In contrast, the multiple beta-factor model assigns a probability of failing due to a common cause to each subset of the N components, allowing for more nuanced modelling of partial common cause failures.

2.1. *Limitations of the simplified formulas*

The simplified formulas presented in the PDS Method Handbook are suitable for most applications and are widely used by practitioners. However, the extensive list of underlying assumptions in the Handbook indicates that the formulas have certain limitations. To overcome specific limitations, other authors have proposed alternative formulas. For example, Rogova et al. (2017) introduced formulas for systems with non-constant failure rates modeled using the Weibull distribution, while Jin et al. (2013) considered the impact of non-perfect proof testing.

In this paper, we focus specifically on the assumptions that limit the formulas' applicability to systems with high failure rates, long test intervals and a large number of components. These are discussed individually in the following paragraphs.

It is important to note that all of the assumptions discussed below can be justified and are generally valid when the parameters $\lambda_{DU}\tau$, β and N are sufficiently low.

2.1.1 *Linear approximation of PFD(t)*

In the derivation of the PDS Method formulas, it is assumed that the time-dependent function for the probability of failure on demand, $1 - e^{-\lambda_{DU}t}$, can be approximated by a linear function $\lambda_{DU}t$ on interval $0 \leq t < \tau$. This approximation is commonly obtained by expanding the exponential function as a Taylor series and only retaining the term of lowest order (Bukowski 2005; Rausand 2014), while Simpson and Kelly (2002) use a different derivation technique to arrive at the same equations.

While this linear approximation is generally acceptable for components and systems with low values of $\lambda_{DU}\tau$, it may become inaccurate in cases involving high failure rates, long test intervals or systems with many components. Fig. 3 illustrates PFD(t) for such a system (blue), its approximation (green), and their respective average PFD values (dashed lines).

This is a conservative assumption which, for systems with high failure rates, long test in-

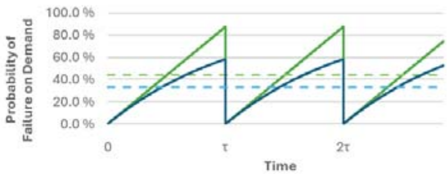

Fig. 3. The time-dependent probability of failure on demand of a system with high failure rates and many components, and its linear approximation (applied parameters: 10oo10 system; λ_{DU} = 1.00E-05 h^{-1}; τ = 8,760 h)

tervals and many components, can lead to a substantial overestimation of PFD.

2.1.2 *Negligibility of simultaneous independent failures*

The simplified formulas consider most simultaneous failures negligible (except for those attributed to a common cause described by parameter β). This is most evident in Eq. (2), where PFD_{NooN} is calculated as $N \cdot PFD_{1oo1}$, despite the failures on demand of different elements in a NooN system not necessarily being mutually exclusive. Eq. (4) accounts for CCF and adjusts the PFD accordingly, but like Eq. (2), it does not consider simultaneous failures due to different causes (i.e., not described by β). In Eq. (1) and (3), the second term includes only simultaneous failures of the lowest order, while neglecting all higher-order combinations.

This is a conservative assumption which, for systems with high failure rates, long test intervals and many components, can lead to a substantial overestimation of PFD.

2.1.3 *Negligibility of simultaneous independent and common cause failures*

The multiple beta-factor model used within the simplified formulas introduces the possibility of common cause failures affecting only a subset of components, rather than all simultaneously. In a MooN system where $M < N$, this means that a common cause may lead to the failure of some components while the system continues to function, as long as at least M components remain operational, i.e., a common cause failure affecting up to $N - M$ components.

However, what the simplified formulas fail to capture is the probability of a common cause failure affecting up to $N - M$ components combined with simultaneous independent failures of additional components. Such combinations can lead to the total number of failed components reaching or exceeding $N - M + 1$, hence causing the system to fail.

This is a non-conservative assumption which can lead to an underestimation of the PFD.

3. Proposed PFD calculation method

To overcome the limitations presented in the previous section and to better account for systems with high failure rates, long test intervals and a large number of components, we derive alternative formulas to Eq. (3) and (4). These revised formulas aim to improve the accuracy of PFD estimations under conditions where the assumptions of the simplified PDS Method formulas no longer hold.

It is important to note that, aside from the specific assumptions discussed in the previous section, the original assumptions of the PDS Method Handbook still apply.

For $\beta = 0\,\%$, a formula for the time-dependent PFD(t) of a MooN configuration (where $1 \leq M \leq N$) can be stated as follows:

$$PFD_{MooN}(t) = \sum_{j=N-M+1}^{N} \binom{N}{j} \left(1 - e^{-\lambda_{DU} t}\right)^{j} \left(e^{-\lambda_{DU} t}\right)^{N-j} \tag{5}$$

Using classical probability techniques, Eq. (5) calculates the probability of $N - M + 1$ or more components being in a fault state at time t.

For configurations 1ooN, NooN as well as some common configurations, Eq. (5) can be simplified as:

$$PFD_{1ooN}(t) = \left(1 - e^{-\lambda_{DU} t}\right)^{N} \tag{6}$$

$$PFD_{NooN}(t) = 1 - e^{-N\lambda_{DU} t} \tag{7}$$

$$PFD_{2oo3}(t) = 1 - 3e^{-2\lambda_{DU} t} + 2e^{-3\lambda_{DU} t} \tag{8}$$

$$PFD_{2oo4}(t) = 1 - 6e^{-2\lambda_{DU} t} + 8e^{-3\lambda_{DU} t} - 3e^{-4\lambda_{DU} t} \tag{9}$$

$$PFD_{3oo4}(t) = 1 - 4e^{-3\lambda_{DU} t} + 3e^{-4\lambda_{DU} t} \tag{10}$$

When $\beta > 0\,\%$, the probability of CCF should be considered in the calculation. We adopt the multiple beta-factor model in line with the PDS Method (i.e., using the same underlying parameters). A general formula for PFD(t) for MooN configurations where $1 \leq M \leq N - 1$ and any value of β can then be defined as follows:

$$PFD_{MooN}(t) = (1 - C_{NooN}\beta) \sum_{j=N-M+1}^{N} \binom{N}{j} \left(1 - e^{-\lambda_{DU}t}\right)^j \left(e^{-\lambda_{DU}t}\right)^{N-j} + \sum_{k=M+1}^{N} \left(C_{kooN} - C_{(k-1)ooN}\right)\beta\left(1 - e^{-\lambda_{DU}t}\right) \sum_{j=k-M}^{k-1} \binom{k-1}{j} \left(1 - e^{-\lambda_{DU}t}\right)^j \left(e^{-\lambda_{DU}t}\right)^{k-j-1} + C_{MooN}\beta\left(1 - e^{-\lambda_{DU}t}\right) \quad (11)$$

Eq. (11) calculates the probability of failure on demand at time t while accounting for independent (with no shared cause) failures of $N - M + 1$ or more components (first term of Eq. (11)), CCF of $N - M + 1$ or more components (third term of Eq. (11)), as well as for any combination of CCF of less than $N - M + 1$ components and independent failures adding up to a total of at least $N - M + 1$ components simultaneously in a fault state (second term of Eq. (11)). While, according to Hokstad (2004) and Hauge et al. (2013), $C_{kooN}\beta Q$ (Q being probability of one component being in a fault state) refers to the probability of $N - k + 1$ or more components failing due to a common cause, the applied expression $\left(C_{kooN} - C_{(k-1)ooN}\right)\beta Q$ refers to the probability of exactly $N - k + 1$ components failing due to a common cause.

For NooN configurations, CCF of any number of components results in a failure of the function. Therefore, the second term does not have to be considered and the formula becomes:

$$PFD_{NooN}(t) = (1 - C_{NooN}\beta) \sum_{j=1}^{N} \binom{N}{j} \left(1 - e^{-\lambda_{DU}t}\right)^j \left(e^{-\lambda_{DU}t}\right)^{N-j} + C_{NooN}\beta\left(1 - e^{-\lambda_{DU}t}\right) \quad (12)$$

By applying the binomial theorem, this can be also reformulated as

$$PFD_{NooN}(t) = 1 - C_{NooN}\beta e^{-\lambda_{DU}t} - (1 - C_{NooN}\beta)e^{-N\lambda_{DU}t} \quad (13)$$

For $\beta = 0$ %, one can notice that both Eq. (11) and (13) are identical to Eq. (5).

For some common configurations, Eq. (11) and (13) can be simplified as (C_{MooN} values from Hauge et al. (2013) applied: $C_{1oo1} = 1$, $C_{1oo2} = 1$, $C_{2oo2} = 1$, $C_{1oo3} = 0.5$, $C_{2oo3} = 2$, $C_{3oo3} = 2$):

$$PFD_{1oo1}(t) = 1 - e^{-\lambda_{DU}t} \quad (14)$$

$$PFD_{1oo2}(t) = 1 - (2 - \beta)e^{-\lambda_{DU}t} + (1 - \beta)e^{-2\lambda_{DU}t} \quad (15)$$

$$PFD_{2oo2}(t) = 1 - \beta e^{-\lambda_{DU}t} - (1 - \beta)e^{-2\lambda_{DU}t} \quad (16)$$

$$PFD_{1oo3}(t) = 1 - (3 - 2.5\beta)e^{-\lambda_{DU}t} + (3 - 4.5\beta)e^{-2\lambda_{DU}t} - (1 - 2\beta)e^{-3\lambda_{DU}t} \quad (17)$$

$$PFD_{2oo3}(t) = 1 - 2\beta e^{-\lambda_{DU}t} - (3 - 6\beta)e^{-2\lambda_{DU}t} + (2 - 4\beta)e^{-3\lambda_{DU}t} \quad (18)$$

$$PFD_{3oo3}(t) = 1 - 2\beta e^{-\lambda_{DU}t} - (1 - 2\beta)e^{-3\lambda_{DU}t} \quad (19)$$

From PFD(t), the average probability of failure on demand PFD can be calculated as follows:

$$PFD = \frac{1}{\tau}\int_0^\tau PFD(t)\,dt \quad (20)$$

Integrating the general formula (Eq. (11)) might be challenging, however, for Eq. (13) as well as for each of the simplified formulas (Eq. (14)-(19)), the calculation of PFD is rather straightforward resulting in the following PFD formulas:

$$PFD_{NooN} = 1 - \frac{1 + (N-1)C_{NooN}\beta - NC_{NooN}\beta e^{-\lambda_{DU}\tau} - (1 - C_{NooN}\beta)e^{-N\lambda_{DU}\tau}}{N\lambda_{DU}\tau} \quad (21)$$

$$PFD_{1oo1} = 1 - \frac{1 - e^{-\lambda_{DU}\tau}}{\lambda_{DU}\tau} \quad (22)$$

$$PFD_{1oo2} = 1 - \frac{3 - \beta - (4 - 2\beta)e^{-\lambda_{DU}\tau} + (1 - \beta)e^{-2\lambda_{DU}\tau}}{2\lambda_{DU}\tau} \quad (23)$$

$$PFD_{2oo2} = 1 - \frac{1 + \beta - 2\beta e^{-\lambda_{DU}\tau} - (1 - \beta)e^{-2\lambda_{DU}\tau}}{2\lambda_{DU}\tau} \quad (24)$$

$$PFD_{1oo3} = 1 - \frac{22 - 11\beta - (36 - 30\beta)e^{-\lambda_{DU}\tau} + (18 - 27\beta)e^{-2\lambda_{DU}\tau} - (4 - 8\beta)e^{-3\lambda_{DU}\tau}}{12\lambda_{DU}\tau} \quad (25)$$

$$PFD_{2oo3} = 1 - \frac{5 + 2\beta - 12\beta e^{-\lambda_{DU}\tau} - (9 - 18\beta)e^{-2\lambda_{DU}\tau} + (4 - 8\beta)e^{-3\lambda_{DU}\tau}}{6\lambda_{DU}\tau} \quad (26)$$

$$PFD_{3oo3} = 1 - \frac{1 + 4\beta - 6\beta e^{-\lambda_{DU}\tau} - (1 - 2\beta)e^{-3\lambda_{DU}\tau}}{3\lambda_{DU}\tau} \quad (27)$$

3.1. *Limitations of the proposed method*

The proposed methodology improves the validity of simplified PFD calculations for systems with high failure rates, long proof test intervals, or large number of components. However, some limitations remain and should be considered when calculating PFD.

The underlying multiple beta-factor model assumes calculation of the C_{MooN} factors independent of the value of β. Although not explicitly stated by Hokstad (2004) or Hauge et al. (2013), the model is not applicable for combinations of large N and large β where $C_{NooN}\beta >$ 100 %. This can occur, for example, for combinations $N = 16$ and $\beta = 5$ %, or $N = 11$ and $\beta = 10$ %. In such cases, Eq. (11) may produce incorrect and misleading results.

The proposed methodology only considers groups of identical components in a MooN configuration. In practice, a typical SIF consists of multiple component types - initiators, logic solvers, and final elements. PFD calculation for the entire SIF is not addressed here, as this paper focuses only on groups of components of the same type.

3.1. *Comparison with the PDS Method*

Table 1 presents PFD values calculated for different configurations as well as for different parameters β and $\lambda_{DU}\tau$ applying the PDS Method formulas and the proposed methodology.

As observed in Table 1, for $\beta = 0$ %, compared to the proposed methodology, the PFD calculation according to the PDS Method is increasingly more conservative with increasing value of $\lambda_{DU}\tau$. This is in line with the observations of Bukowski (2005) described in the introduction.

For $\beta > 0$ %, the PFD calculation according to the PDS Method is especially conservative for NooN configurations. In fact, replacing C_N in Eq. (4) by $NH_N - C_{NooN}$ according to the definition of H_N presented by Hauge et al. (2013), one would arrive at:

$$PFD_{NooN} \approx N(1 - H_N\beta)\frac{\lambda_{DU}\tau}{2} + C_{NooN}\beta\frac{\lambda_{DU}\tau}{2} \tag{28}$$

This corresponds to calculation of PFD by summing all probabilities of independent failures and probability of any CCF as if the events were mutually exclusive. On the other hand, mutual exclusivity is not assumed in the definitions of C_N and H_N resulting in $H_N < C_{NooN}$ for $N \geq 3$. For larger β values, this inconsistency leads to considerable overestimation of the PFD for NooN configurations with large number of components N.

A similar conclusion of overestimating the PFD due to assumption of mutual exclusivity of

Table 1. Comparison of calculated PFD according to the PDS Method and to the proposed methodology (Rel. diff. shows the relative error of the PDS Method calculation as compared to calculation according to the proposed methodology)

MooN	PDS Method	Proposed method	Rel. diff.	PDS Method	Proposed method	Rel. diff.	PDS Method	Proposed method	Rel. diff.
	$\lambda_{DU}\tau = 0.01$								
	$\beta = 0$ %			$\beta = 5$ %			$\beta = 10$ %		
1oo1	5.00E-03	4.98E-03	+ 0.3 %	5.00E-03	4.98E-03	+ 0.3 %	5.00E-03	4.98E-03	+ 0.3 %
1oo2	3.33E-05	3.31E-05	+ 0.8 %	2.80E-04	2.81E-04	- 0.2 %	5.27E-04	5.28E-04	- 0.2 %
2oo2	1.00E-02	9.93E-03	+ 0.7 %	9.75E-03	9.69E-03	+ 0.7 %	9.50E-03	9.44E-03	+ 0.7 %
1oo3	2.50E-07	2.47E-07	+ 1.2 %	1.25E-04	1.27E-04	- 1.6 %	2.50E-04	2.54E-04	- 1.6 %
2oo3	1.00E-04	9.88E-05	+ 1.3 %	5.86E-04	5.87E-04	- 0.3 %	1.07E-03	1.08E-03	- 0.3 %
3oo3	1.50E-02	1.49E-02	+ 1.0 %	1.44E-02	1.39E-02	+ 3.7 %	1.38E-02	1.29E-02	+ 6.8 %
	$\lambda_{DU}\tau = 0.1$								
	$\beta = 0$ %			$\beta = 5$ %			$\beta = 10$ %		
1oo1	5.00E-02	4.84E-02	+ 3.4 %	5.00E-02	4.84E-02	+ 3.4 %	5.00E-02	4.84E-02	+ 3.4 %
1oo2	3.33E-03	3.09E-03	+ 7.7 %	5.51E-03	5.36E-03	+ 2.8 %	7.70E-03	7.62E-03	+ 1.0 %
2oo2	1.00E-01	9.37E-02	+ 6.8 %	9.75E-02	9.14E-02	+ 6.7 %	9.50E-02	8.91E-02	+ 6.6 %
1oo3	2.50E-04	2.22E-04	+ 12.6 %	1.45E-03	1.64E-03	- 11.8 %	2.65E-03	3.06E-03	- 13.3 %
2oo3	1.00E-02	8.84E-03	+ 13.1 %	1.36E-02	1.28E-02	+ 6.0 %	1.72E-02	1.67E-02	+ 2.9 %
3oo3	1.50E-01	1.36E-01	+ 10.2 %	1.44E-01	1.27E-01	+ 12.9 %	1.38E-01	1.19E-01	+ 16.0 %
	$\lambda_{DU}\tau = 0.2$								
	$\beta = 0$ %			$\beta = 5$ %			$\beta = 10$ %		
1oo1	1.00E-01	9.37E-02	+ 6.8 %	1.00E-01	9.37E-02	+ 6.8 %	1.00E-01	9.37E-02	+ 6.8 %
1oo2	1.33E-02	1.15E-02	+ 15.9 %	1.70E-02	1.56E-02	+ 9.1 %	2.08E-02	1.97E-02	+ 5.5 %
2oo2	2.00E-01	1.76E-01	+ 13.8 %	1.95E-01	1.72E-01	+ 13.6 %	1.90E-01	1.68E-01	+ 13.4 %
1oo3	2.00E-03	1.58E-03	+ 26.6 %	4.08E-03	4.63E-03	- 11.8 %	6.23E-03	7.67E-03	- 18.8 %
2oo3	4.00E-02	3.14E-02	+ 27.5 %	4.42E-02	3.76E-02	+ 17.6 %	4.89E-02	4.38E-02	+ 11.6 %
3oo3	3.00E-01	2.48E-01	+ 21.0 %	2.88E-01	2.33E-01	+ 23.6 %	2.75E-01	2.17E-01	+ 26.6 %

the events could be made for MooN configurations with $M < N$ and $\beta > 0$ %. However, this conservative assumption is also accompanied by a non-conservative simplification by neglecting the probability of simultaneous CCF of less than $N - M + 1$ components and independent failures of the remaining components (second term of Eq. (11)). As seen in Table 1, this combination can lead to both overestimation and underestimation of PFD.

4. Conclusion

Current simplified PFD formulas work well within their intended assumptions. However, for systems with high failure rates, long proof test intervals, or a large number of components, some of these assumptions are violated. The methodology presented here extends the validity range of simplified formulas by relaxing assumptions that do not hold under these conditions. While the new formulas are not as simple as those in the PDS Method, they remain straightforward enough to be implemented in most tools used by reliability engineers today, including spreadsheets like Microsoft Excel that support basic functions and simple numerical integration. This balance between accuracy and usability makes the approach suitable for challenging cases while remaining accessible for everyday engineering practice.

There are still limitations that point to potential future work. The underlying multiple beta-factor model may produce misleading results for combinations of large N and large β, and the current approach only considers homogeneous components in a MooN configuration. Extending the methodology to handle heterogeneous component types and more complex configurations, and refining the beta-factor model would further improve its applicability.

References

Bukowski, J.V. (2005). A comparison of techniques for computing PFD average. *Annual Reliability and Maintainability Symposium, 2005: Proceedings*, 590-595.

Hauge, S., T. Kråkenes, P.R. Hokstad, S. Håbrekke, and H. Jin (2013). *Reliability Prediction Method for Safety Instrumented Systems: PDS Method Handbook - 2013 Edition* (report no. A24442). SINTEF Technology and Society.

Health and Safety Executive (2014). *OG 00046: Management of instrumented systems providing safety functions of low / undefined safety integrity.*

Hokstad, P. (2004). A Generalisation of the Beta Factor Model. In: C. Spitzer, U. Schmocker, and V.N. Dang (Eds.), *Probabilistic Safety Assessment and Management,* pp. 1363-1368. Springer.

Håbrekke, S., S. Hauge, and M.A. Lundteigen (2023). *Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase* (report no. 2023:00107). SINTEF Digital.

International Electrotechnical Commission (2010). *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems* (2.0 ed.).

International Electrotechnical Commission (2016). *IEC 61511: Functional safety - Safety instrumented systems for the process industry sector.*

Jin, H., M.A. Lundteigen, and M. Rausand (2013). New PFH-formulas for k-out-of-n:F-systems. *Reliability Engineering & System Safety 111*, 112-118.

Lundteigen, M.A. and M. Rausand (2009). Reliability assessment of safety instrumented systems in the oil and gas industry: a practical approach and a case study. *International Journal of Reliability, Quality and Safety Engineering 16(2)*, 187-212.

Offshore Norge (2023). *Guideline 070: Recommended Guidelines for Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL Requirements)* (Rev. 06).

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications* (1st ed.). Wiley.

Rogova, E., G. Lodewijks, and M.A. Lundteigen (2017). Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231(4)*, 373-382.

Simpson, K.G.L. and M. Kelly (2002). Reliability Assessments of Repairable Systems - Is Markov Modelling Correct? *Safety and Reliability 22(2)*, 19-39.

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (2019). *VDI/VDE 2180-1: Functional safety in the process industry - Introduction, terms, conception.*