Whitepaper on the topic of how to manage safety instrumented functions (SIFs) classified as high-demand mode

Mary Ann Lundteigen (NTNU), Solfrid Håbrekke (SINTEF), Shenae Lee (SINTEF)

Date: 25.9.25

This memo builds on further work from the following two presentations:

1. *Lundteigen, M.A (NTNU), Cought in the middle: High-demand SIFs. PDS forum 22-23. October 2024*
2. *Lundteigen, M.A (NTNU). and Kvam, E. (Safetec). High/low demand – Når kan PFD brukes. 19-20 March 2025.*

1 High-demand mode in IEC 61511

In safety-critical industries, the design and operation of Safety Instrumented Systems (SIS) demand careful consideration of failure probabilities and overall system reliability. A key distinction in the IEC 61511 standard is between low-demand, high-demand, and continuous modes of operation of a safety-instrumented function (SIF), defined as:

- low-demand mode, where the SIF is performed only on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than once per year;
- high-demand mode, where the SIF is performed only on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than once per year;
- Continuous mode, where the SIF retains the process in a safe state as part of normal operation.

Although not formally defined in IEC 61511, the term demand can be interpreted as a predefined process state or event that requires a response from SIF. To highlight that low- and high-demand conditions depend on the demand rate, the term demand mode has been introduced, as illustrated in Figure 1.

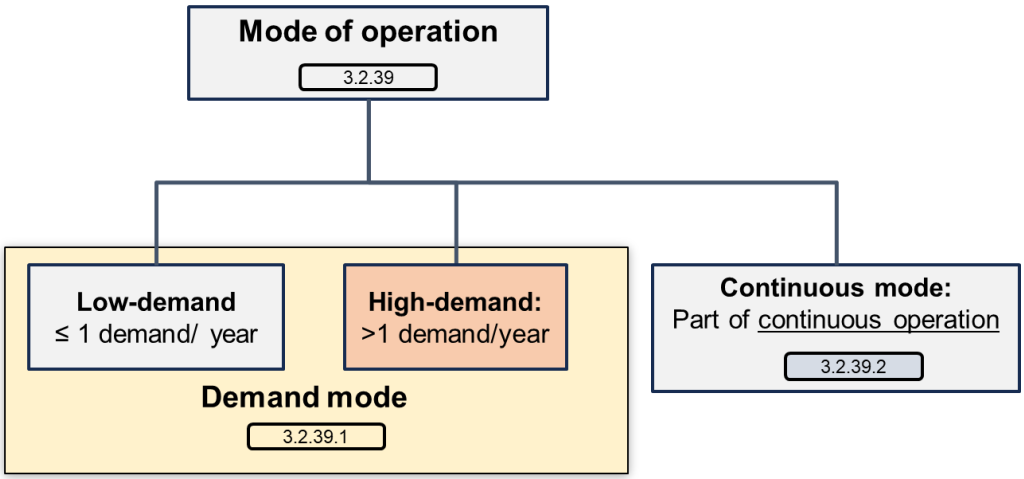


Figure 1. Classification of modes of operation of a SIF per IEC 61511

2 Choice of reliability measure for an SIF

IEC 61511, in alignment with IEC 61508, recommends the use of the average Probability of Failure on Demand (PFD) as a reliability measure for low-demand mode and the average Probability of Failure per Hour (PFH) for continuous mode. However, for high-demand mode, both PFD and PFH are permitted; however, IEC 61511 does not provide guidance on how to choose between them, leaving uncertainty about which measure is most appropriate in a given context.

Table 1 Choice of reliability measures in IEC 61511

SIL	Low demand	High demand	Continuous
	PFD	PFH (per hour)	
4	1E-5 ≤ PFD < 1E-4	1E-9≤ PFH < 1E-8	
3	1E-4 ≤ PFD < 1E-3	1E-8 ≤ PFH < 1E-7	
2	1E-3 ≤ PFD < 1E-2	1E-7 ≤ PFH < 1E-6	
1	1E-2 ≤ PFD < 1E-1	1E-6 ≤ PFH < 1E-5	

The purpose of this guidance is to explore the criteria for selecting PFD or PFH and to examine the implications this choice has for system design and ongoing operational follow-up.

3 Implications of being in high-demand mode

IEC 61511 does not provide different sets of requirements for design, work processes, and follow-up for the three modes of operations, except for the minimum hardware fault tolerance (HFT) requirements outlined in Table 2 (IEC 61511-1): In case of a SIL 2 requirement, a

minimum HFT of 1 is required for high-demand and continuous mode of operation, whereas a minimum HFT of 0 is sufficient for low-demand mode.

Table 2 Minimum hardware fault tolerance requirements in IEC 61511-1

SIL	Mode	Minimum HFT
1	All	0
2	Low demand	0
2	**High demand or continuous**	**1**
3	All	1
4	All	2

This requirement for SIL 2 functions is not impacted by whether PFD or PFH is selected for reliability analysis. However, as will be demonstrated later, the decision to use either PFD or PFH can result in a different SIL requirement during the SIL allocation process. This choice can indirectly influence follow-up practices, such as the intervals between regular proof tests

4 Deriving the SIL requirement

The SIL allocation process is applied to derive the maximum tolerated PFD or PFH of an individual SIF, considering the risk acceptance criteria and the impact of other layers of protection. The layers of protection analysis (LOPA) is a tailor-made method for identifying SIL requirements for SIFs operating in the low-demand mode. In contrast, the maximum tolerated PFH for high-demand SIFs can be determined directly from the risk acceptance criterion, if last-in-line defense. If not last in line, it may be possible to introduce the high-demand SIF as an initiating event in LOPA, and calculate the maximum tolerated PFH value, after taking into account the probability of failure of subsequent independent (and low-demand) protection layers.

Simplified, we may explain how the maximum PFD and maximum PFH of a SIF are derived in the following way, given a maximum tolerated hazardous event frequency (TF) and only one layer (the SIF). Then,

- If using PFD: $TF \geq HR_{SIF} = DR * PFD_{SIF}$
- If using PFH: $TF \geq HR_{SIF} = PFH_{SIF}$

Here, DR is the demand rate, and HR_{SIF} is the hazard rate caused by SIF failure, the PFH. PFH, TF, and HR must have the same unit of measurement (e.g., per hour). We notice that the required PFD of SIF will decrease if the DR increases, to maintain the HEFSIF less than the TF. In contrast, the required PFH is not impacted by the DR. Depending on how much the demand rate increases, the corresponding SIL requirement for a low-demand SIF may increase compared to the SIL requirement for a high-demand SIF.

Considering two protection layers as shown in **Figure 2**, one being SIF1 operating in the high-demand mode and another non-instrumented safety function (SF2) operating in the low-demand mode, not necessarily an SIF.

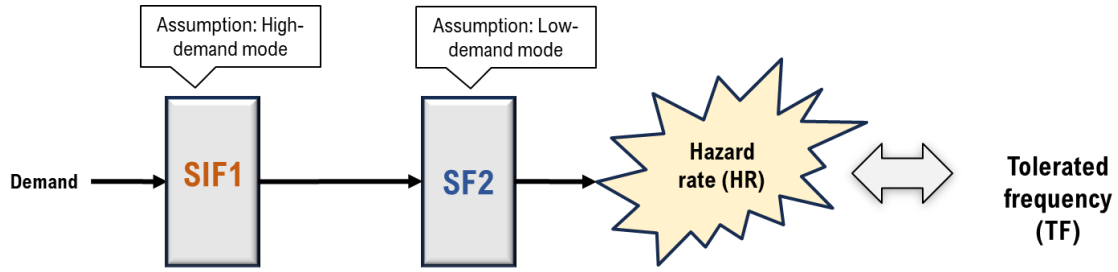


Figure 2. Two layers of protection

Figure 3 visualizes the corresponding formulas and how an increasing DR will result in a decreasing value for the required PFD of SIF1, if we assume that the probability of failure of SF2 (PSF2) is constant and that the maximum allowed HR is set equal to the tolerable frequency of a risk acceptance criteria. The same figure also show that the required PFH remains unaffected by the demand rate. It has been assumed that the probability of failure of SF2 is kept constant.

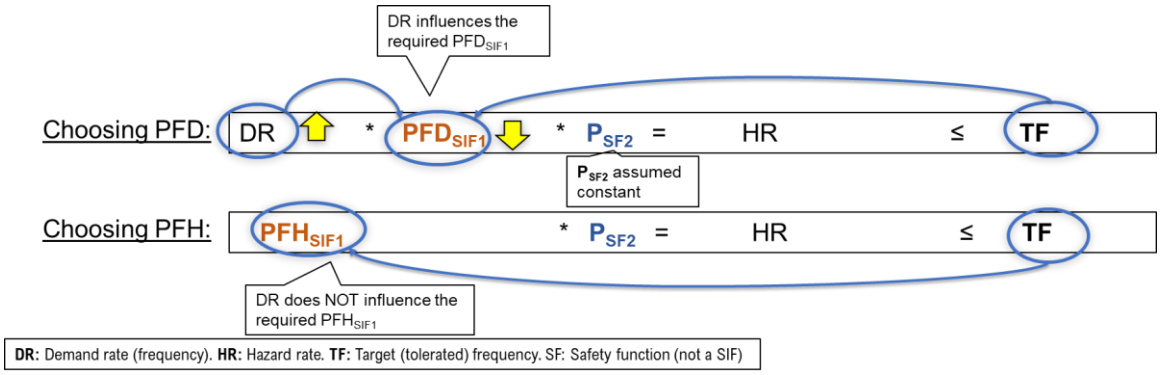


Figure 3. Impact of choosing PFD or PFH.

5 Implications for follow-up and testing

The choice of PFD and PFH may impact the follow-up of SIFs, including how often the SIFs are subject to regular testing. Some of the explanations can be found in the formulas used to calculate PFD and PFH of a SIF, considering the subsystem voting and device failure rates.

- PFH is calculated as an average over a period T. There are no definitions or restrictions mentioned in IEC 61511 about the length of T; however, the following guidance has been identified in other standards:
    - IEC 62061 (2021) on functional safety of machinery defines T with reference to the useful lifetime of SIF components, which may be claimed as high as, e.g., 20 years. Some consider this to be the same as the period when a renewal or overhaul is needed, to regain a state as good as new of the system.
    - IEC 61508 (2010) suggests formulas for PFH formulas where the underlying assumption is that no more than one failure of each subsystem may occur during T. Under this assumption, the resulting formulas indicate that T has a limited influence on the PFH value, for both single subsystems and redundant ones, as long as CCFs are incorporated in the latter. This has led to the misinterpretation that T is unimportant. Unfortunately, it is not generally possible to determine a required (maximum tolerated) T for a given PFH requirement using the PFH formulas.
    - IEC 61508 (1998) had a second criterion for distinguishing low-demand from high-demand/ continuous mode of operation: A SIF would operate in the high-demand/continuous mode if DR > 2*1/T, otherwise it would be defined as low-demand. A subject to at least two proof tests per period between demands would be described as low-demand mode, meaning in practice that proof tests are efficient ways to reveal failures in due time before the following demands. Some may argue that such a criterion could imply.
- PFD is also calculated as an average, but in this case, an average of the failure probability for the regular proof test interval. To separate the meaning of T in PFH from the regular proof test interval for PFD calculations, the Greek letter τ (tau) is used instead of T.
    - IEC 61511 does not provide formulas for calculating PFD, but common practice is to apply formulas in IEC 61508-6, or similar formulas. Here,
    - The proof test interval has a significant impact on both single and redundant systems. Consequently, determining the required τ (tau) is possible.

Therefore, by choosing PFD, the corresponding PFD formulas define a maximum proof test interval more often than the rate of demands. The case study presented later will illustrate that the rate of regular proof tests increases compared to the rate of demands remaining constant when the TF is kept constant, while it increases with increasing TF. Considering the extra wear and operational challenges from frequent proof testing, i.e., many times per year, it seems

reasonable to have a testing strategy that credits successful responses in combination with regular proof tests, regardless of whether PFD or PFH is used.

It is therefore recommended to develop some industry practice or guideline on this topic, as IEC 61511 Part 2, an IEC or ISA technical report, or similar international guidance. This may be a topic for further discussion, and corresponding formulas could be developed. A starting point can be to build on the approach suggested in the PDS method handbook (2014); however, other approaches may also be available for consultation and further development.

6 Case study

Consider a flare system shown in **Figure 4** covering the flare knockout drum that receives gases from process systems that need to be depressurized. The flare drum outlet is locked until a certain pressure level is exceeded, where gas is sent to the flare header and ignited. The following assumptions are made:

- **Hazardous event:** Flare knockout drum outlet remains closed when it should be opened.
- **Demand:** The pressure reaches the setpoint for triggering the SIF, here named high-high (PSHH)
- **Demand rate:** 2–5 times per year
- **SIF1:** One pressure transmitter (PSHH), a logic solver, and a normally closed (fail-to-open) emergency safety valve (ESV)
- SF2: A normally closed mechanical pressure safety element (PSE).

If SIF1 fails, SF2 shall open at a slightly higher pressure, calibrated with a self-opening mechanism, at a setpoint higher than that of SIF1.

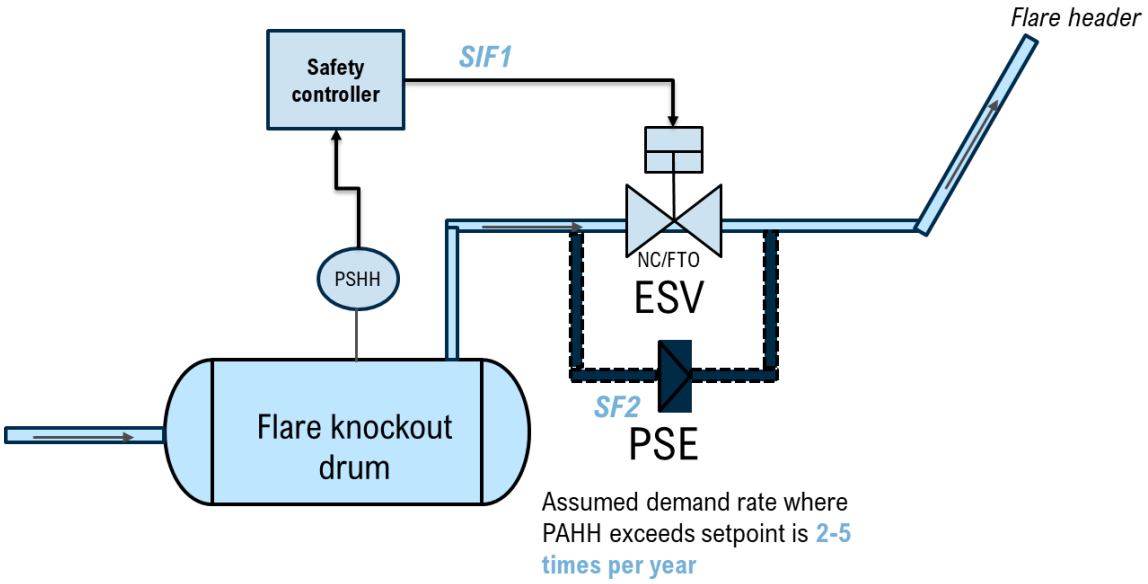
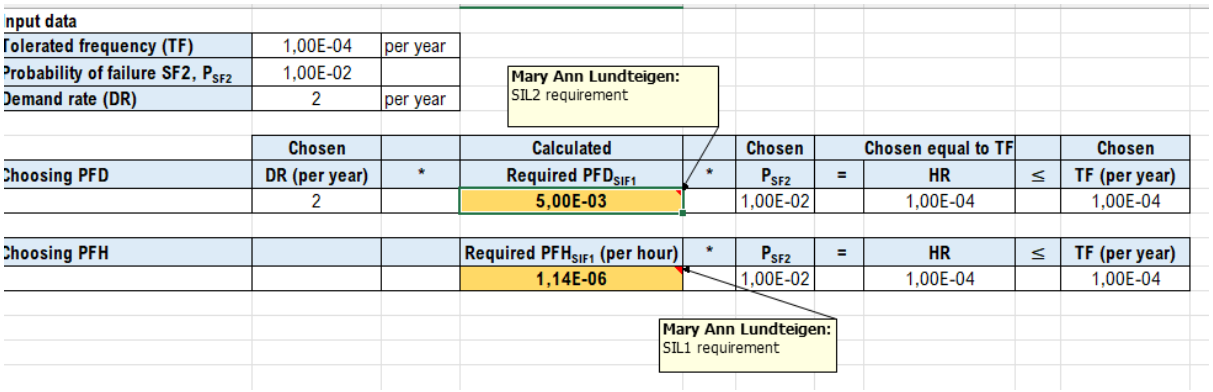


Figure 4. Flare system with safety functions.

6.1 Deriving the required PFD and PFH from the tolerable frequency

The required PFD and PFH for SIF1 may be calculated as follows:



Input data		
Tolerated frequency (TF)	1,00E-04	per year
Probability of failure SF2, P_{SF2}	1,00E-02	
Demand rate (DR)	2	per year

Mary Ann Lundteigen:
SIL2 requirement

	Chosen		Calculated		Chosen		Chosen equal to TF		Chosen
Choosing PFD	DR (per year)	*	Required PFD_{SIF1}	*	P_{SF2}	=	HR	≤	TF (per year)
	2		5,00E-03		1,00E-02		1,00E-04		1,00E-04

Choosing PFH			Required PFH_{SIF1} (per hour)	*	P_{SF2}	=	HR	≤	TF (per year)
			1,14E-06		1,00E-02		1,00E-04		1,00E-04

Mary Ann Lundteigen:
SIL1 requirement

We may investigate how the required PFD of SIF1 is affected when the demand rate increases further, considering the four cases presented in the table below.

DR (per year)	Required PFD_{SIF1}	Corresponding SIL requirement
2	**5,00E-03**	SIL2
5	**2,00E-03**	SIL2
10	**1,00E-03**	SIL2
20	**5,00E-04**	SIL3

6.2 Determining the required PFD for proof test interval

In both the PFD and PFH formulas, dangerous failures undetected (DU) failures are the most significant contributors to unreliability. In contrast, dangerous detected (DD) failures have a relatively minor impact, provided that the diagnostics are effective and the device is promptly restored or triggers a forced transition of the process to a safe state within the process safety time.

SIF is here assumed to have a single pressure transmitter, logic solver, and final element, so the PFD of the SIF becomes:

$$PFD_{SIF1} \approx \frac{\lambda_{DU,PT}\tau}{2} + \frac{\lambda_{DU,LS}\tau}{2} + \frac{\lambda_{DU,ESV}\tau}{2}$$

Reliability data suggested for the case study are “hypothetical”, but still not far from values found in e.g., PDS data handbook.

Input data:	Failure rate	
Sensor (1oo1)	1,00E-06	Per hour
Logic Solver (1oo1)	1,00E-07	Per hour

Final element (1oo1)	3,00E-06	Per hour

The following required proof test interval “tau” has been calculated with demand rates ranging from 2 to 20 demands per year. 20 demands per year is outside the scope of the case study; however, it is included just to illustrate the effect of such a high demand rate.

DR	Req PFD	Required tau (hours)	Proof test per year	Factor tau:DR
2	5,00E-03	2439	3,6	1,8
5	2,00E-03	976	9,0	1,8
10	1,00E-03	488	18,0	1,8
20	5,00E-04	244	35,9	1,8

We notice from the results that at least 1.8 regular tests per period between demand is required to meet TF < 1E-4 per year. If the TF is reduced from 1E-4 per year to 1E-5 per year, the factor changes to 18 as shown below.

DR	Req PFD	Required tau (hours)	Proof test per year	Factor tau:DR
2	5,00E-04	244	35,9	18,0
5	2,00E-04	98	89,8	18,0
10	1,00E-04	49	179,6	18,0
20	5,00E-05	24	359,2	18,0

Even if PFD formulas can provide a required value for tau, it is not realistic to implement such frequent proof testing. Besides the operational challenges, the testing would most likely have a negative impact on the reliability of the devices, due to additional wear of the tests themselves.

To clarify the increase in Factor tau in the above table, the demand rate (DR) can be expressed as:

$$DR = \frac{HR}{P_{SF2}} \cdot \frac{1}{PFD_{SIF1}}$$

Given P_{SF2} is constant and $PFD_{SIF1} \propto \tau$, it follows that

$$DR \propto HR \cdot \frac{1}{\tau}$$

Assuming that DR and HR are independent,

$$\tau \propto \frac{HR}{DR}$$

Therefore, if the hardware fault rate (HR) is reduced by a factor of 10, e.g., due to changes in technical failure (TF) requirements, while the demand rate (DR) is assumed to remain unchanged, the value of τ is consequently reduced by a factor of 10. This results in an increase in the frequency of proof testing by a factor of 10.

If the outdated criterion from IEC 61508 (1998) on distinguishing low-demand from high-demand based on the PFH, it would call for at least two regular proof tests per year per demand period. In practice, the requirement becomes unrealistic, considering that demands may also be credited as tests.

6.3 Implications of the required PFH for proof test interval

Assuming the same SIF1, the corresponding formula for PFH becomes:

$$PFH_{SIF1} \approx \lambda_{DU,PT} + \lambda_{DU,LS} + \lambda_{DU,ESV}$$

We notice that the renewal interval is not reflected in the formula. This would change with redundancy, but the impact is negligible when also common cause failures (CCFs) are considered. For high-demand, it may be necessary to introduce some other criteria to determine the renewal period T, where tests/inspections are carried out to reveal and restore the SIF to as good as new state, considering that some credit is made to how the SIF has responded to demands.