Eirik Bjorheim Abrahamsen
University of Stavanger, Stavanger, Norway

Willy Røed
Proactima, Stavanger, Norway

A semi-quantitative approach for verification of Safety Integrity Level requirements

Keywords

safety integrity level, probability of failure on demand, uncertainty

Abstract

A Safety Integrity Level (SIL) is a measure of performance required for a safety instrumented function. The IEC 61508/61511 standards define four safety integrity levels, SIL1 to SIL4, where SIL4 is the level with the most stringent requirements. For each safety integrity level there are many design requirements, including requirements for the probability of failure on demand (PFD). Verification of the required failure probability is usually based on a quantitative analysis. In this paper we argue that such an approach is better replaced by a semi-quantitative approach. The approach acknowledges that the PFD requirement for a safety function cannot be adequately verified only by reference to an assigned probability number. There is a need for seeing beyond the probability number. The key aspect to include is related to uncertainty. Such an aspect is often ignored in verification of a safety integrity level.
The offshore oil and gas industry is the starting point, but the discussion is to large extent general.

1. Introduction

Safety instrumented systems (SIS) are important protection layers in the process industry. A SIS comprises input elements (e.g., pressure transmitters and gas detectors), logic solvers (e.g. relay based logic and programmable logic controllers), and final elements (e.g. valves, circuits breakers). A SIS is used to detect the onset of hazardous events and/or to mitigate their consequences to humans, the environment, and material assets. The international Standards IEC 61508 and IEC 61511 [7], [8] require that reliability targets for the SIS are defined and demonstrated. The reliability targets are assigned to each safety instrumented function (SIF) that is implemented into the SIS. The IEC standard use safety integrity level (SIL) as a measure for reliability. The safety integrity of a system is defined as the probability of a safety-related system performing the required safety function under all the stated conditions within a stated period of time [11].
Compliance to a SIL requires i.a. a quantitative analysis with a view towards a particular failure mode titled "failure to function on demand". The probability that a piece of equipment used to implement a SIF is referred to as the "probability of failure on demand" – PFD. This probability is calculated and compared with a target value. If the calculated PFD is higher than the target value, risk reducing measures should be implemented. Examples of such measures are shorter test intervals, better technology or more redundancy.
The traditional approach for verification of a quantitative SIL seems intuitively appealing. In this paper we do however argue that uncertainties should be taken into consideration more extensively than what is seen in the traditional approach. The assigned probability for failure on demand is conditioned on a number of assumptions and suppositions. They depend on the background knowledge. Uncertainties are often hidden in the background knowledge, and restricting attention to the assigned probabilities could camouflage factors that could produce surprising outcomes. By jumping directly into probabilities, important uncertainty aspects are easily truncated, meaning that potential surprises could be left unconsidered [2]. We find also similar ideas underpinning approaches such as the risk governance framework

[10], the risk framework used by the UK Cabinet Office [4] and a framework presented in [10].
In this paper we present and discuss an alternative approach, acknowledging that the calculated probability should not be the only basis for verifying the established quantitative SIL requirements. In the alternative approach the uncertainty aspects are given special attention, and are seen in relation to the assigned probabilities.
The paper is organized as follows. In Section 2 a short presentation of Safety Integrity Level is given. In Section 3 we review and discuss the traditional approach for verification of quantitative SIL requirements. Then, in Section 4, an alternative approach which gives more attention to the uncertainty dimension is presented. Finally, in Section 5, we draw some conclusions.

2. Safety Integrity Levels

Safety integrity is a fundamental concept in IEC 61508 and is defined as the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time (see IEC 61508, sect. 3.5). The safety integrity is classified into four discrete levels called safety integrity levels (SIL), where the highest SIL rating states the lowest probability that the SIS will fail to perform the required SIF.
The safety integrity levels are expressed in terms of the probability of the SIS to fail to perform the requested SIF upon demand, often referred to as the PFD (probability of failure on demand). The PFD may be interpreted as the average fraction of times the system will be in a dangerous failure mode and not work as a SIF on demand.
Depending on whether the demand mode of operation is low or high/continuous, the range of the levels differ as shown in Table 1. Low demand mode embrace systems where the frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof-test frequency, otherwise it is classified as a high demand system (IEC 2003). An example of a low demand application in subsea production is a downhole safety valve (DHSV), which remains in open position until a demand occurs. An application in high demand mode can for example be the brake system in a car.
The relation between SIL and the PFD is shown in *Table 1*.

Table 1. Safety integrity levels for safety functions

SIL	Low demand mode	High demand or continuous mode
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
4	$< 10^{-4}$	$< 10^{-8}$

The SIL concept can only be applied to an entire safety instrumented system performing one or more safety functions. Since the safety integrity requirements relate to the safety function, it is not correct to refer to any individual item (such as a sensor) as having a safety integrity level [3].
The SIL also determines several other constraints, for example requirements on the design of a safety instrumented system. Generally speaking, the higher the SIL, the more stringent the requirements to comply with the IEC 61508 standard.

3. The traditional approach for verification of SIL requirements

An example from the offshore oil and gas industry is used in this section in order to illustrate the main ideas of the traditional approach for verification of SIL requirements. The example is strongly related to one of the examples presented in the OLF-070 Guideline [9].

Example: Isolation of subsea well

Isolation of a subsea well is defined as the system needed to isolate one well. For a standard subsea well, the system normally consists of:

- The emergency shut down node(s) (ESD), located topside
- Hydraulic bleed down solenoid valves in the hydraulic power unit (HPU), located topside
- Electrical power isolation relays located in the electric power unit (EPU), located topside
- Directional control valves located in the subsea control module (SCM), located topside
- Production wing valve (PWV), production master valve (PMV) and chemical injection valve (CIV) (including actuators) located on the christmas tree (XT) on the sea bed
- Down Hole Safety Valve(s) (DHSV) including actuator(s), located in the well (below sea bed)

Isolation of a subsea well can be activated through a hydraulic power unit (HPU) and/or through an electric power unit (EPU), ref. Figure 1.
In the above-mentioned design, the DHSV(s) is/are located in the well below the sea bed, the XT is located on the sea bed, and the SCM, HPU, EPU and ESD node systems are located topside. The signals are transferred through an umbilical integrated in the production riser. Activation of the safety function will occur if one of the following valve systems is activated:

- DHSV
- PMV
- PWV and CIV

In order to close the DHSV, the directional control valve for DHSV (DCV_{DHSV}) in the control module must be activated. The DCV_{DHSV} is activated from one of the solenoid valves in the hydraulic power unit. The solenoid values are activated from the ESD Node.
To close PMV or PWV and CIV the same logic as the one described above follows, see Figure 1.

SIL requirement

From the OLF-070 Guideline the requirement for the function "ESD isolation of one subsea well" is SIL category 3, which means that the probability of failure on demand (PFD) should not be higher than 10^{-3}, i.e. SIL 3 can be claimed for the safety function presented if the PFD can be demonstrated to be in the range 10^{-4} to 10^{-3}.

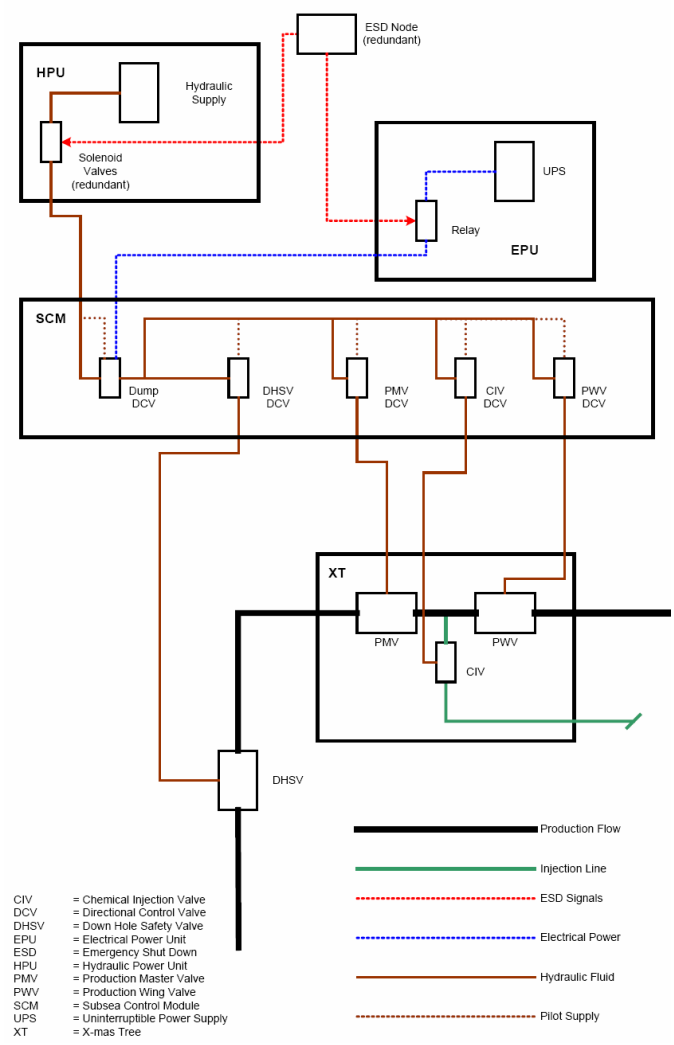

Figure 1. Components included to ensure isolation of one subsea well (typical design based on the OLF-070 Guideline).

Traditional approach for verification of SIL requirement

The safety function "ESD isolation of one subsea well" can be represented by a Reliability Block Diagram as shown in *Figure 2* [9].

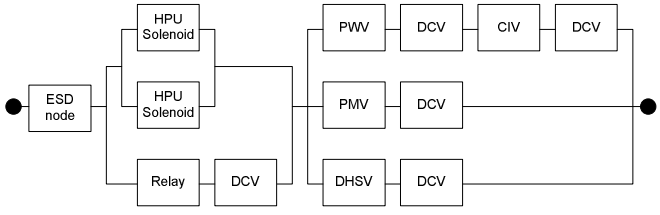

Figure 2. Reliability block diagram for "ESD isolation of subsea well"

To calculate the PFD values, several methods exist, see e.g. appendix F in the OLF 070 guideline and the PDS method [6]. Such methods have in

common that they are based upon traditional reliability theory, in combination with historical observations documented in databases such as e.g. the OREDA database. Some of the methods also allow for updated PFD calculations based on field specific historical observations and information about technical and operational aspects of the system in focus. We will not elaborate on such methods in this paper, since the key aspects of the paper is relevant for all PFD calculation methods. An example of component PFD calculation results is presented in *Table 2*, based on the OLF 070 document [9].

Table 2. Summary of component reliability values used in example calculations.

Component	Component redundancy	Calculated PFD
ESD logic	Duplicated	$2.20 \cdot 10^{-4}$
HPU Solenoid	Duplicated	$2.00 \cdot 10^{-4}$
PMV/PWV	Single	$2.20 \cdot 10^{-4}$
CIV	Single	$8.80 \cdot 10^{-4}$
DHSV	Duplicated	$5.50 \cdot 10^{-4}$
DCV	Single	$2.20 \cdot 10^{-4}$
Relay	Single	$1.18 \cdot 10^{-3}$

Based on the reliability block diagram in Figure 2 and the component PFDs, the system unreliability may be calculated. In the above example, the calculated system unreliability is $2.2 \cdot 10^{-4}$. Compared to the values presented in *Table 1* we conclude that the safety function is within safety integrity level 3, as the calculated PFD is less than 10^{-3} and greater than 10^{-4}.

4. An alternative approach for verification of quantitative SIL requirements

The assigned probability provides useful insight to decision makers, but there is a need for a broader reflection of uncertainties. The point is that the above calculations express conditional probabilities. In mathematical terms this can be expressed as P(A|K) where A includes the PFD and K is the background information and knowledge. The background knowledge covers historical system performance data, system performance characteristics and knowledge about the phenomena in question. Assumptions and presuppositions are an important part of this information and knowledge. The background knowledge can be viewed as frame conditions of the analysis, and the produced probabilities must always be seen in relation to these conditions. Thus, different analysts could come up with different values, depending on the assumptions and presuppositions made. The differences could be very large. Hence uncertainty needs to be considered, beyond the assigned probability number.

The assigned probability (P) for the safety function should be seen in relation to uncertainties (U). The point is that probability is a tool to express uncertainty. It is however not a perfect tool, and we should not restrict verification of SIL only to the probabilistic world. The probabilities are conditional on specific background knowledge (K), and they could produce poor predictions. Surprises relative to the assigned probabilities may occur, and by just addressing probabilities such surprises may be overlooked.

We argue that there are important aspects of uncertainty that should be taken into consideration when it is concluded on the SIL level. In particular there are uncertainties on the non-technical aspects that are not taken into consideration in the PFD calculation methods applied by the industry. In the common implementation, there is a close link between the PFD calculation results and the SIL level conclusion. We argue that uncertainties should be taken into consideration before it is concluded on the SIL level. In practice, this could be done qualitatively in a workshop subsequent to the quantitative SIL verification analysis, but prior to the SIL level conclusion. This principle is presented in *Figure 3* below illustrating both the traditional approach and the approach suggested in this paper. We will come back on an example of how information about the uncertainties could be taken into consideration.

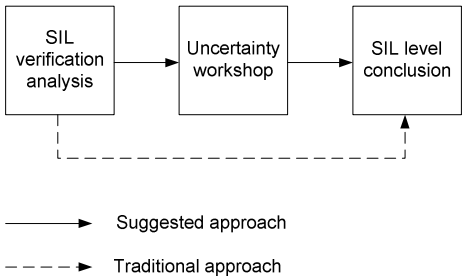

Figure 3. Main principles of the suggested approach

To reflect the uncertainties to the decision makers we recommend that the uncertainties should be classified within one of the three categories: high, medium or low. The categorisation process should be based on some guidelines or criteria to ensure consistency. The following descriptions could serve as a guideline [5]:

Low uncertainty:
All of the following conditions are met:

- The assumptions made in calculations of P are seen as very reasonable
- Much reliable data are available
- There is broad agreement among experts

High uncertainty:
One or more of the following conditions are met:

- The assumptions made in calculations of P represent strong simplifications
- Data are not available, or are unreliable
- There is lack of agreement/consensus among experts

Medium uncertainty:
Conditions between those characterising high and low uncertainty

Note, that the degree of uncertainty must be seen in relation to the effect/influence the uncertainty has on the assigned probability. For example, a high degree of uncertainty combined with high effect/influence on the assigned probability number will lead to a conclusion that the uncertainty factor is high. However, if the degree of uncertainty is high but the assigned probability number is relatively insensitive to changes in the uncertain quantities, then the uncertainty classified in the diagram could be low or medium.

As already mentioned, the uncertainty evaluations should be carried out in a workshop. An example of how the results from the workshop could be presented, is shown in Table 2.

Based on the discussion in the workshop, documented in Table 2, many aspects with high uncertainty have been identified. The uncertainty factor which is considered most important is 'experience with subcontractors'. The calculated probability number (PFD) is based on the assumption that the subcontractors have high experience from Norwegian Continental Shelf. This is not necessarily the case. Changes in assumptions related to this factor will have a significant influence on the calculated probability number. The calculated probability may be considered to be less than 10^{-3} even for small changes in the assumptions related to the factor 'experience with subcontractors'.

Table 2. Uncertainty evaluation example

Main categories	**Sub-categories**	**Evaluation**	**Uncertainty categorization**
Human aspects (M)	Competence and experience	Well-educated personnel. But some operations have never been carried out before by the present crew	High
	Operator training	Operators will be trained in advance to operations being carried out	Medium
Technical aspects (T)	Environmental aspects	Harsh climate at location	Medium
	Internal: Fluid composition	High uncertainties on fluid composition. May result in corrosion and other challenges	High
	New or well-known technology	New equipment: Limited experience with the equipment to be installed subsea	High
	Well characteristics	Challenging well due to high pressures and unknown reservoir characteristics	High
Operational aspects (O)	Experience with subcontractors	New subcontractor (first operation). Limited experience from Norwegian Continental Shelf	High
	Maintenance	No specific challenges identified	Low
	Documentation	No specific challenges identified	Low

With no attention on the uncertainty dimension, we conclude that the SIL requirement is within SIL 3 as the calculated probability number is within the range 10^{-4} to 10^{-3}. Taking the uncertainty dimension into account, the safety integrity level for the safety function considered may be judged not to be within SIL 3, even if the calculated probability is within this category, ref. *Figure 4.* In this case additional risk reducing measures should be implemented prior to the operation. This could be measures in order to reduce the PFD or means to reduce the uncertainty factors to such extent that an updated evaluation concludes on SIL3.

Figure 4. Application example

5. Conclusion

The common approach for verification of a safety function's safety integrity level is usually based on probability calculations only. In this paper we argue that such an approach is better replaced by an approach including uncertainty assessment qualitatively in a workshop. This approach acknowledges that the probability requirement for a safety function cannot be adequately verified only by reference to an assigned probability number. There is a need for seeing beyond the probability number. The key aspect to include is related to uncertainty. An example has been included in order to illustrate the ideas.

Acknowledgement

The authors are grateful to the Research Council of Norway for financial support.

References

[1] Abrahamsen, E.B., Aven, T. & Iversen, R.S. (2009). An integrated framework for safety management and uncertainty management in petroleum operations. *Journal of risk and reliability*. To appear.

[2] Aven, T. (2008). *Risk analysis – Assessing uncertainties* beyond expected values and probabilities. Wiley. NJ.

[3] Brown, S. (2000). Overview of IEC 61508 – Design of electrical/electric/programmable electronic safety-related systems. *In Computing and Control Engineering Journal* 11: 6-12.

[4] Cabinet Office. (2002). Risk: improving government's capability to handle risk and uncertainty. Strategy unit report. UK.

[5] Flage, R. & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Risk & Reliability – Theory & Application* 2009; 2(13): 9-18.

[6] Hauge, S., Lundteigen, M.A., Hokstad, P. & Håbrekke, S. (2010). *Reliability prediction method for safety instrumented systems*. PDS method Handbook 2010 edition. SINTEF, ISBN 978-82-14-04850-6.

[7] IEC – International electrotechnical commission. (2003a). IEC 61508. Functional safety of electric/electronic/programmable electronic safety-related systems. International Electrotechnical Commission; Geneva.

[8] IEC - International electrotechnical commission. (2003b). IEC 61511. Functional safety – safety instrumented systems for the process industry. International Electrotechnical Commission; Geneva.

[9] OLF – The Norwegian oil industry association (2004). OLF-070. Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. Technical report, The Norwegian Oil Industry Association, Stavanger, Norway.

[10] Renn, O. (2008). *Risk governance: coping with uncertainty in a complex world.* London: Earthscan.

[11] Smith, D.J. & Simpson, K.G.L. (2005). *Functional safety – s straightforward guide to applying the IEC 61508 and related standards*. Burlington, UK.: Elsevier