# A NEW APPROACH FOR VERIFICATION OF SAFETY INTEGRITY LEVELS

**E.B. Abrahamsen**
University of Stavanger, Norway
e-mail: eirik.b.abrahamsen@uis.no

•

**W. Røed**
Proactima AS, Norway
e-mail: wr@proactima.com

## ABSTRACT

The IEC standards 61508/61511 require that reliability targets for safety instrumented functions are defined and verified. The reliability targets are given as one out of a possible four safety integrity levels. For each safety integrity level there are many design requirements, including requirements for the probability of failure on demand. Verification of the requirements for the probability of failure on demand 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 probability of failure on demand requirement 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.

## 1 INTRODUCTION

A Safety Instrumented System (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) for the purpose of bringing the plant or an equipment to a safe state if a hazardous event occurs (Lundteigen, 2009). Each SIS has one or more Safety Instrumented Functions (SIF), where every SIF within an SIS has a Safety Integrity Level (SIL). The IEC standards 61508/61511 define four safety integrity levels (SIL 1-SIL 4). The higher the safety integrity level, the more stringent become the requirements. For each safety integrity level there are many design requirements, including requirements for the Probability of Failure on Demand (PFD). The probability of failure on demand for each SIL is given in the IEC standards as shown in Table 1. The levels depend on whether the demand mode of operation is low or high/continuous. Low demand mode embraces systems where the frequency of demands for operation made on safety-related systems is not greater than one per year and not greater than twice the proof-test frequency; otherwise it is classified as a high demand system (IEC, 2003a). An example of a low demand application in subsea production is a down-hole 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 (Rolén, 2007).

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 IEC standards 61508/61511 require that safety integrity levels for the different safety instrumented functions are verified. Verification of the quantitative part (PFD) of the SIL level for a safety instrumented function is usually done by a calculation of PFD and then by a comparison with the criterion established. If the calculated PFD is higher than the target value, risk reducing measures should be implemented.

This traditional approach for verification of a quantitative SIL seems intuitively appealing. Firstly, a criterion for the probability of failure on demand is given. Then the probability of failure on demand is calculated and compared with the criterion established.

In this paper we do, however, argue that uncertainties should be taken into consideration more extensively than 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 (Aven, 2008). See also Abrahamsen and Aven (2011) and Abrahamsen et al. (2010). We also find similar ideas underpinning approaches such as the risk governance framework (Renn, 2008) and the risk framework used by the UK Cabinet Office (Cabinet Office, 2002).

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 we review and discuss the traditional approach for verification of quantitative SIL requirements. Then, in Section 3, an alternative approach which gives more attention to the uncertainty dimension is presented. Finally, in Section 4, we draw some conclusions.

## 2 THE TRADITIONAL APPROACH FOR VERIFICATION OF SAFETY INTEGRITY LEVELS

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 the isolation of subsea well example presented in the OLF-070 Guideline (OLF, 2004).

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 (with reference to Figure 1):

- 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 seabed
- Down Hole Safety Valve(s) (DHSV) including actuator(s), located in the well (below seabed)

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 seabed, the XT is located on the seabed, 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 the PMV or PWV and CIV, the same logic as the one described above follows; see Figure 1.

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 $10^{-3}$.

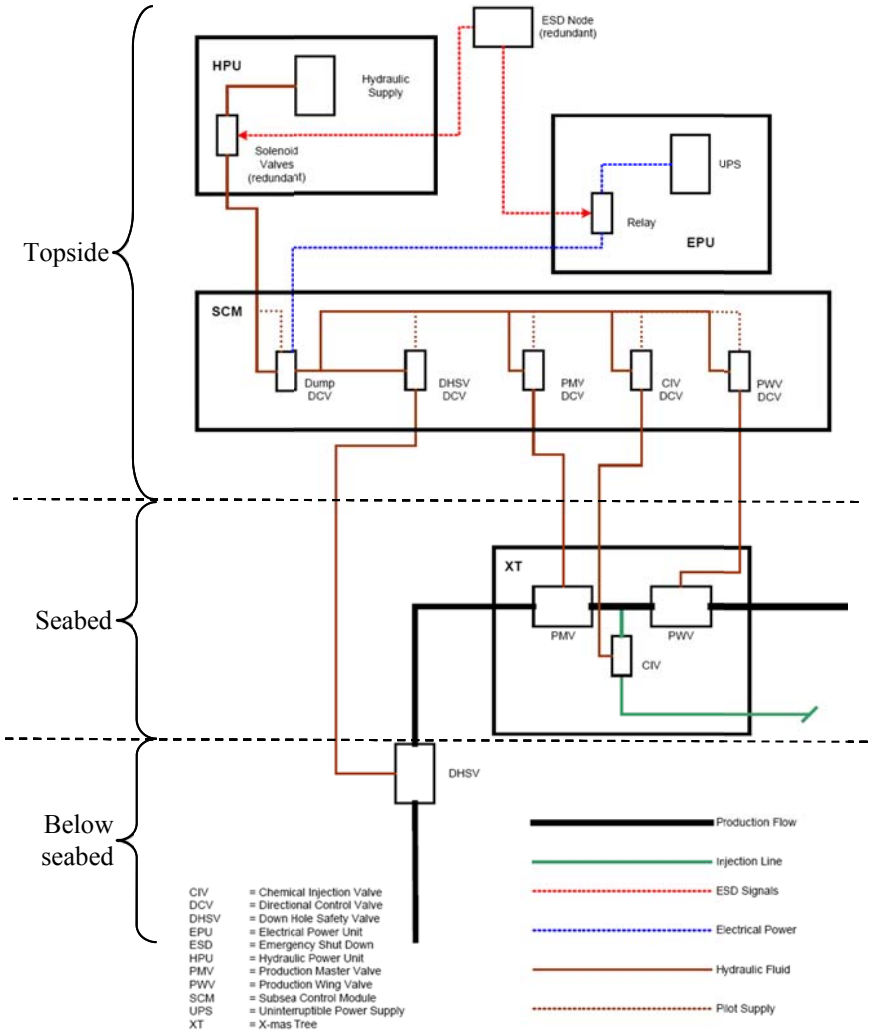


**Figure 1.** Components included to ensure isolation of one subsea well (typical design based on the OLF-070 Guideline)

The safety function "ESD isolation of one subsea well" can be represented by a reliability block diagram as shown in Figure 2 (OLF, 2004).

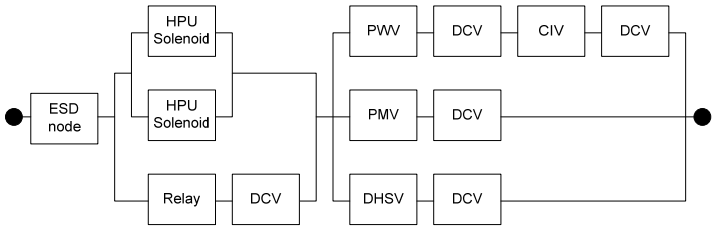


**Figure 2.** Reliability block diagram for "ESD isolation of subsea well"

Assume that the reliability values for the components included in Figure 2 are as shown in Table 2.

Table 2. Component reliability values used in example calculations (OLF, 2004).

| 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 | $1.18 \cdot 10^{-3}$ |

By using the method shown in the OLF guideline, 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 $10^{-4}$.

There are other traditional approaches as well. See for example the approach presented by Hauge et al. (2010). The main idea for verification of the quantitative part of the SIL level is, however, equal; attention is given to the calculated PFD and then compared with a target value.

## 3 A NEW APPROACH FOR VERIFICATION OF SAFETY INTEGRITY LEVELS

The assigned probability provides a useful insight for 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(failure on demand|K) where 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 a conclusion is made 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 a conclusion is made 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 to an example of how information about the uncertainties could be taken into consideration.

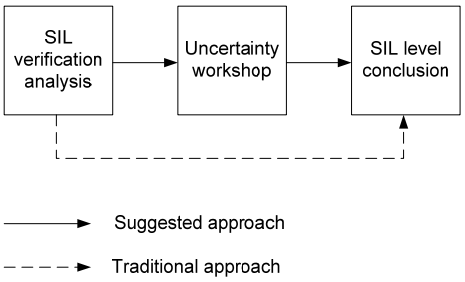


**Figure 3.** Main principles of the suggested approach

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 (Flage and Aven, 2009):

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 3.

Based on the discussion in the workshop, documented in Table 3, 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 a high level of experience from the 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 3. Uncertainty evaluation example

| **Main categories** | **Sub-categories** | **Evaluation** | **Uncertainty categorisation** |
|---|---|---|---|
| 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. These could be measures in order to reduce the PFD or means to reduce the uncertainty factors to such an extent that an updated evaluation concludes on SIL3.

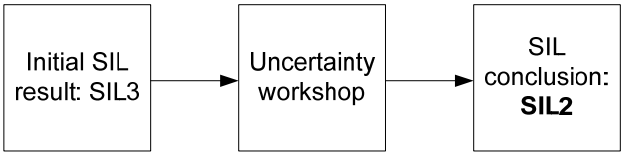


**Figure 4.** Application example

## 4 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 work on the paper has been funded by the Research Council of Norway through the RAMONA research programme. The financial support is gratefully acknowledged.

## REFERENCES

1. Abrahamsen EB, Aven T. 2011. Safety oriented bubble diagrams in project risk management. International Journal of Performability Engineering 7(1): 91-96.
2. Abrahamsen EB, Aven T, Iversen RS. 2010. Integrated framework for safety management and uncertainty management. Journal of Risk and Reliability 224(2): 97-103.
3. Aven T. 2008. Risk analysis – Assessing uncertainties beyond expected values and probabilities. Wiley: N.J.
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 2(13): 9-18.
6. Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. 2010. Reliability prediction method for safety instrumented systems, PDS method Handbook 2010 edition. SINTEF.
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. Lundteigen MA. 2009. Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation. Doctoral thesis at NTNU.
10. 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.
11. Renn O. 2008. Risk governance: coping with uncertainty in a complex world. London: Earthscan.
12. Rolén H. 2007. Partial and imperfect testing of safety instrumented functions. Master thesis at NTNU.