Safety Integrity Level (SIL) Assessment as key element within the plant design

Tobias WALK
ILF Consulting Engineers GmbH
Germany

Abstract

Special attention has to be provided to safety instrumented functions during the plant design and their classification within the safety integrity levels (SIL). The classification has a direct effect on the plant safety, its operability as well as on the investment costs. During the pipeline design phase various safety review studies - e.g. Hazards and Operability Analysis (HAZOP), Quantitative Risk Analysis (QRA), Project Health, Safety, Environmental Review (PHSER) - are required and the determination of the SIL is ranked as one element within the safety aspects design workflow. The approach how to determine the proper integrity level is demonstrated in detail on risk graphs. The risk graph approach is not only limited to safety aspects as it is more and more common to use these also for environmental and commercial aspects. This requires a proper calibration of the risk graphs which big oil & gas operators define within their company standards.

The article provides examples for a SIL review assessment including its reporting and flags the required input data. It refers to the relevant norms and standards and explain how pipeline operators are calibrating the risk graphs for the environmental and commercial aspects within their company standards.

ILF Consulting Engineers is involved as a designer within many international Oil & Gas projects for more than 40 years. Acting as an independent owners engineer various types of plant safety systems had to be specified, procured and commissioned depending on the project specific process conditions and environmental requirements.

1. Introduction

The boundary conditions for the safe operation of an industrial plant are already identified and mitigated within the project define phase. During the Basic Design (or Front-End Engineering & Design) of an industrial plant all safeguards and Layers of Protection needs to be properly identified and defined. The various process protection layers are illustrated within the figure 1 and 2. The Safety Instrumented Function (SIF) forms the third protection layer. The SIF is required to interfere in case the basic process control system as well as the process alarms could not bring back the process values under normal control. Within that respect the SIF initiates on critical process demand a unit trip to avert further process escalation and mitigate hazardous process conditions. Therefore an adequate and unambiguous SIF definition is very important.
The SIF definition is mandatory necessary and important for every Safety Integrity Level (SIL) classification. An incorrect definition easily leads to over or under engineering.

---

**Figure 1: Process Protection Layers**

**Figure 2: Risk Reduction by Process Protection Layers**
Obviously, the intention of a safety function is to prevent or mitigate the consequences of a hazardous event. Therefore, it needs to function properly and it needs to be reliable. Adequate definition of a safety function can only be achieved if a full understanding of its demand scenarios, design intent and consequences of failure on demand are known:

1. The ‘demand scenario’ describes the initiating events (e.g. failure of control instruments or failure of equipment), which will ultimately lead to a demand on the SIF.
2. The ‘design intent’ specifies the released hazard to be averted (e.g. loss of containment).
3. The ‘consequences of failure on demand’ describe the ultimate consequences (of a SIF failure) and the way they are achieved.

During the ‘Hazard and Operability’ (HAZOP) study potential out-of-control process situations are identified, by analyzing variations of process parameter values (e.g. more / less / none / negative pressure). Variations can cause a potential hazardous situation which can lead to a hazardous event (e.g. leakage of toxic products, explosion, fire, etc.). The consequences of the hazardous event can have an impact on human safety, environmental pollution, damage to the installation, production loss and other negative effects. As a result the HAZOP study identifies the required safeguards for the process.
In a SIL classification the demand scenario frequency and the severity of the consequences of the hazardous event are used to establish the Safety Integrity Level (see also the generic norm for safety IEC 61508 and the adapted safety norm for process industry IEC 61511), which determines the required level of risk reduction. The SIL indicates the minimum probability that the equipment will successfully do what it is desired to do when it is called upon to do it. As soon as the required risk reduction is known, it can be converted into a Probability of Failure on Demand (PFD) which is required for the SIF and which results into the SIL.

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Probability of Success on demand</th>
<th>Risk Reduction Factor (RRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>99,99 – 99,999 %</td>
<td>10.000 – 100.000</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>99,9 – 99,99 %</td>
<td>1.000 – 10.000</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>99 – 99,9 %</td>
<td>100 – 1.000</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>90 – 99 %</td>
<td>10 – 100</td>
</tr>
</tbody>
</table>

*Table 1: SIL Definition (for Low Demand Application) as per IEC 61508-1*

The norms are focused primary on personnel safety and do not provide any quantitative values for tolerable risk. The tolerable risk has to be defined by company standards and/or local authorities. Many companies have developed their own internal standards which provide the necessary quantitative values for the tolerable risk. Furthermore these company standards are not only focused on personnel safety issues as they adapt the same risk reduction methods also for environmental issues (Environmental Integrity Level, EIL) and asset loss issues (Asset Integrity Level, AIL).

Obviously, it is of key importance that the allocated safeguarding measures can realize the required level of risk reduction. Therefore, their functionality and their reliability need to be defined properly.
2. Example

The pressure sensor of the separator vessel detects high pressure that may lead to the hazardous event ‘rupture of the separator’ and to the consequences ‘oil and gas leakage to the environment which could ignite’. The shutdown system receives the pressure sensor trip signal and close the ESD Valve on the inlet side. The SIF consists of the entire loop, the high pressure sensor, the Shutdown System and the ESD valve actuator. The entire SIF loop needs to be implemented in accordance with the defined SIL.

3. SIF definition process

Based on experience, based on the initial basic design, the process design is detailed including protection systems, safety instrumented functions, mechanical devices, mitigating measures, etc. A HAZOP study has been carried out already to verify if all protection layers are provided and, if required, additional protection layers needs to be added.

As far as SIF are concerned the design is mainly reflected in Piping & Instrumentation Diagrams (P&ID) and Cause & Effect Charts (C&E). Therefore, the starting point of a SIL assessment is often a set of P&ID and C&E, detailing the SIF envisaged. It is an interdisciplinary team approach to derive from these information the hazardous situations and events that the SIF intent to detect and prevent. Those
hazardous situations are often not specifically defined in design memoranda and HAZOP reports. The interdisciplinary team mainly consists of a safety engineer, process engineer, operation expert, instrumentation and control engineer and other skilled people (e.g. machinery expert) who can distribute on this exercise. It is common practice to nominate an independent experienced chairman for the SIL assessment who is not directly involved within the project. The chairman will guide the exercise and generate the SIL assessment report.

There are two common methods for selection of the Integrity Level (IL):

- **Risk Graph** method: it relates consequence severities to demand rates considering possibilities of avoiding the hazard (one risk graph for each consequence category). Using the risk graph is a semi-quantitative method. It can be applied quickly to large numbers of SIFs, but it is a conservative approach.

  ![Risk Graph from IEC 61508 / 61511](image)

  *Figure 5: Risk Graph from IEC 61508 / 61511*

- **Layer Of Protection Analysis (LOPA)** method: to be conducted for all SIFs with an IL of 3 or higher. The LOPA method is more complex that the Risk Graph
method and it can mitigate Integrity Level after analysis of protection layers. Typically the LOPA method reduces the IL category by 1 class compared with the Risk Graph method.

In case the LOPA method result is still indicating an IL 3 or 4 a detailed quantitative analysis would be required which is using fault trees to estimate the frequency of the undesired event and event trees to understand all possible outcomes including their frequencies. The use of the above mentioned methods are illustrated within the following flow chart (refer to figure 6).

![Figure 6: usage of IL methods](image)

The results of all identified Integrity Levels (for Safety, Environmental and Asset Loss) are compared with each other and the most stringent has to be chosen for the SIF. The SIL assessment report is documenting all the findings including the description of the description of the demand scenarios and consequences of failures on demand of each SIF. The report will be updated during the entire lifetime of the plant and it will be also used to determine the proper maintenance cycles for all SIF loops as more frequent maintenance cycles would have a positive effect on the probability of success on demand.
CV of the author

As a native German, Tobias Walk studied Electrical Engineering and Information Technology at the Technical University in Munich with special focus on Automation and Control Systems. In 1996 he received his Diploma and he started 1997 to work as project engineer for ILF Consulting Engineers within the Oil & Gas market. Over the past 13 years, he has held a number of positions of increasing responsibility within ILF. Since 2008 he is the ILF Director for Electrical Engineering, Automation and IT-Systems. Furthermore, end of 2009 he was nominated as Corporate Director for the ILF Russia Oil & Gas activities.

He has been deeply involved as owners engineer within the design and commissioning of various international pipeline projects (amongst others: BTC Crude Oil Pipeline, ADCOP Habshan - Fujairah Pipeline, Bourgas-Alexandroupolis Crude Oil Pipeline, ESPO Pipeline, Revamp of Janaf Crude Oil Pipeline) during the last decade. Within these projects he was also responsible for the design of various process control and safety systems. Furthermore he was involved as an external expert or chairman within various SIL review workshops to identify and validate the required integrity level.

Contact
Tobias Walk
ILF Consulting Engineers GmbH
Werner-Eckert-Street 7
D-81829 Munich

phone: +49 (0)89 – 25 55 94 – 244
fax: +49 (0)89 – 25 55 94 – 44 244
eMail: Tobias.Walk@ilf.com