Safety & Risk Management Services

Safety Integrity Level (SIL) Studies

Germanischer Lloyd – Service/Product Description
Safety Integrity Level (SIL) Studies

Service Title: Safety & Risk Management Services
Lead Practice: GL Safety & Risk (UK)

Contents

Page 3 Service Description and Values Generated

Pages 4 - 9 Detailed Method Statement
The detailed method statements explain how the work is conducted, which inputs are required and which outputs and results can be expected.

a: Data Gathering and Review
b: Process Hazard Analysis
c: SIF Definition
d: SIL Classification
e: SIL Verification
f: Safety Requirements Specification
g: Performance and Testing
h: Management of Change
i: Gap Analysis and Reporting

Pages 10 - 11 Case Studies and Examples

a: Reliability Assessment of Overpressure Protection Systems
b: Tankfarm SIL Assessment
Service Description and Values Generated:

A Safety Integrity Level (SIL) assessment determines the effectiveness of safety systems based on the probability of tolerable incidents that can occur within a number of processing demands. With many years of experience in the management of safety, hazard and risk, Germanischer Lloyd (GL) are extremely well placed to deliver SIL assessments. Our understanding of major hazards and their consequences and the evolvement of tools and methodologies, as our knowledge has enhanced over the past 30 years to where it is today, is fundamental to our business and the services we provide.

The determination of Safety Integrity Levels (SIL) for safety components and systems is part of GL’s overall Quantitative Risk Assessment (QRA) service.

SIL assessments are a formal classification method which provide a record of a quantified assessment of the probability of failure on demand of a safety system taking account of the consequences of the failure of the Safety Instrumented Functions (SIFs).

Initially a review of safety documentation will be carried out in order to identify relevant information required for the project. The documents to be reviewed will include safety studies and HAZOPs. A complete list of the Safety Instrumented Functions (SIFs) is prepared prior to the SIL classification being developed. The project is completed with verification of instrument and system specifications, including reliability data and a formal recording of a Safety Requirements Specification (SRS).

This is one of a series of formalised specialist methods for calculating numerical individual, environmental, employee and public risk level values for comparison with regulatory risk criteria.

GL conduct SIL studies in accordance with International standard IEC 61511 and have conducted studies for numerous customers over a wide range of projects.
a. Data Gathering and Review

The initial stage of this type of project will be to gather the data required for the study. This will include, but will not be limited to:

- All relevant studies (HAZOPs, QRAs, etc)
- P&IDs
- Cause and effect charts
- Current maintenance and shutdown details
- Relevant operational information

It is also anticipated that visits will be required to the operational plant facilities.

GL will require access to key site personnel during the visits (e.g. Instrument engineers, mechanical engineers). The purpose of these visits will be to obtain a clear understanding of the actual instrumented systems being studied and any constraints on proof testing.

A review of the documents will be carried out in order to identify relevant information required for the project. The documents to be reviewed will include safety studies and HAZOPs, but will also extend to:

- Drawings of the process and ESD systems.
- Documents detailing design and operation philosophy, as required.
- The client risk matrix.

A record of documents received and reviewed will be retained for inclusion in the reports to the client.
b. Process Hazard Analysis

A Hazard Identification (HAZID) workshop will be conducted for the plant facilities in order to formally define the fire and gas hazards present on the facilities (including toxic hazards). This HAZID can then be used, in conjunction with a Quantified Risk Assessment (QRA) to define the level of risk reduction that would be required from the fire and gas systems present on the facilities.

The HAZID will be carried out on a location basis and at each stage the provision of fire and gas detection systems will be identified. Where a shortfall in the provision of fire and gas systems is identified, this will be detailed in the HAZID report.

The client will need to provide personnel for the HAZID workshop who understand the nature of the fluids present at each location and the fire and gas systems.

Based on the review carried out in Activity (a), a methodology will be defined that will allow the HAZOP studies to be used in the definition of Safety Instrumented Functions and assignment of Safety Integrity Levels.

c. SIF Definition

Based on the work carried out in Activities (a) and (b), a complete list of Safety Instrumented Functions (SIFs) will be prepared. This list will be provided to the client in a draft report for review. Following receipt of comments, the report will be updated to provide a definitive list of SIFs. This list will be used to define those systems that need to be assessed in all subsequent activities.

During the definition process, where loops provide identical functionality and have the same design, this will be identified in order to avoid repetition of analysis work.
d. SIL Classification

Following the definition process, a Safety Integrity Level (SIL) target will be assigned to each SIF. This SIL target will be assigned using a methodology that will be agreed with the client. The methodology will take account of both Layers of Protection Analysis (LOPA) and risk matrix approaches as appropriate.

The methodology will also be consistent with and take account of any existing client risk matrix, the risks as quantified in existing QRAs and relevant client guidance. The SIL classification methodology will take account of the consequences of the failure of the SIF in relation to:

- The safety of people
- The environment
- Asset damage and production loss
- Company reputation

The typical SIL target levels that will be defined in the methodology are:

- **SIL 0** - no safety requirement for the function
- **SIL A** - risk reduction of less than a factor of 10 required from the function
- **SIL 1** - Probability of failure on demand between $10^{-1}$ and $10^{-2}$.
- **SIL 2** - Probability of failure on demand between $10^{-2}$ and $10^{-3}$.
- **SIL 3** - Probability of failure on demand between $10^{-3}$ and $10^{-4}$.
- **SIL 4** - Probability of failure on demand between $10^{-4}$ and $10^{-5}$.

Though SIL 4 will be defined within the methodology, no single SIF will be allowed to have a target of SIL 4 as maintaining this level of reliability in a single system is generally impracticable. If SIL 4 assignments are given, then the SIF will be identified as one where multiple independent SIFs are required with recommendations indicating how this might be achieved being provided to the client.

The SIL classification methodology will be reviewed with the client within workshops to ensure a consensus view has been achieved. GL will provide the facilitator and secretary for these workshops and it is assumed that the client will make personnel available for these workshops.

A report will be prepared that provides the SIL classification for each SIF along with:

- The methodology
- The parameters selected to arrive at the classification
- How the demand rate was determined and what causes a demand on the system
- Details of other risks reduction measures considered in the classification
- The manning assumptions and consequence studies used
e. SIL Verification

The next stage of the project will be to determine the SIL that the installed systems can achieve based on:

- The equipment, (e.g. sensor, logic unit) used in the SIF
- Appropriate reliability data
- Specific proof testing intervals

Reliability data specific to the client and plant/process will be used in the assessment if this readily available, otherwise either manufacturers’ data or generic industry data will be employed. It should be noted that caution should be used in applying manufacturers’ data as they may only consider the element they provide and not the associated cabling, hydraulic supply etc. Reference to industry data will always therefore be made to ensure that overly optimistic data is not used. Where significant deviations from generic data are observed, this will only be used if there is sufficient justification provided by the manufacturer.

In addition to the manufacturers’ industry data sources GL will also refer to the following publications:


These references provide an interpretation of the OREDA data (Offshore Reliability Data) in conjunction with other published data. These references also provide valuable guidance on common cause factors and dangerous failure and spurious trip fractions.

The method used for calculating both the overall reliability and spurious trip frequency and SIL of components will depend on the complexity of the system. For simpler systems, approaches such as the use of reliability block diagrams will be used. More complex systems are likely to be analysed using fault tree analysis. GL will use an appropriate software package to carry out any fault tree analysis.

Proof test intervals of one, two and three years will be used in the analysis and the maximum proof test interval that will still meet the SIL target will be detailed.

Where the verification shows that the SIL target cannot be met with the one year proof test interval, recommendations will be provided that detail system improvement options that will allow the target to be met. These recommendations will focus on the elements of the system that contribute most to the overall probability of failure.

Typically a report will be prepared that will detail all the inputs and outputs of the verification process and describe the methodology used.
f. Safety Requirements Specification

Safety Requirements Specifications (SRS) will be prepared for all SIFs. As required by the client and these SRSs will typically contain:

- A description of the SIF, how it works and related devices
- The assigned SIL
- Reference to the Cause & Effect charts
- Calculated SIL values for proof test intervals considered
- Recommended response time based on a high level understanding of functional requirements
- Trip settings and whether the system is energised or de-energised on trip
- Safe state
- Test requirements (tasks, not frequency)
- Operator interfaces (including manual initiation)

The SRSs will be tabulated in a standard format and provided to the client in a report.
g. Performance and Testing

Performance standards will be prepared for each SIF describing the functionality, reliability and survivability of the function. They will also detail the proof tests that should be carried out on each system, the steps associated with the proof test and the relevant regulations.

The performance standards will be consistent with the requirements of the client's technical integrity or quality assurance guidance documents.

If required, a document will be prepared that provides all relevant information for uploading the testing requirements into the client’s database for maintenance management.

h. Management of Change

It is important that once this SIL study has been completed that changes are only made with the full understanding of any implications for the SIFs. A change management procedure will therefore need to be prepared that is consistent with the existing change management processes used by the client (e.g. Management of Engineering Change). In this manner, the change management process could be incorporated within the client’s existing procedures.

The change management process will include the procedures that should be used if there is any erosion of the SIF performance below SIL target levels. This could include, for example, provision of special protection measures.

i. Gap Analysis and Reporting

The final stage of a project will be to collate all gaps found between the target requirements and specifications of the standards and the actual equipment installed.

Where gaps have been identified, recommendations on how this gap could be closed will be provided.

The summary of gaps and recommendations would be provided in a report to the client.
a. Reliability Assessment of Overpressure Protection Systems

**Date:** 2007  
**Customer:** Onshore Gas Storage Facility, UK  
**Benefit:** Confidence to the HSE that protection systems would operate as per the design

**Issue:**

GL were requested by an Onshore Gas Storage Facility in the UK to undertake a detailed analysis of the Safety Instrumented Systems that are to be used to protect a number of critical areas of plant against overpressurisation.

**Work:**

The work included:

- Providing a robust determination of the frequency of overpressurising the critical plant areas in the absence of the Safety Instrumented Systems.
- Determining the potential consequences of overpressurisation using updated results from a full QRA of the site that had previously been undertaken by GL.
- Determining the reliability (i.e. achieved SIL rating) of the Safety Instrumented Systems that included both ESD and HIPPS systems. Fault tree analysis was used to determine the reliability of the systems.
- Calculating the risk in terms of PLL (Potential Loss of Life) as a result of overpressurising the critical plant areas.
- Showing that the risks were ALARP.

**Output:**

The proposed design of the safety systems changed a number of times during the project and required re-working of reliability and ALARP calculations. However, the work was still completed on time against a tight schedule and enabled the Storage Facility to meet important commitments made to the HSE.
**b. Tankfarm SIL Assessments**

**Date:** 2008  
**Customer:** Major Asian National Operator  
**Benefit:** Understanding of safety systems which do not meet the required standard

---

**Issue:**

To conduct a risk analysis of the Tank Farm facility, comprising:

- A Quantitative Risk Assessment (QRA).
- An assessment of the safety systems in place using a calculation of the appropriate Safety Integrity Level (SIL) approach.

This case study focuses on the review of the safety systems.

---

**Methodology & Results:**

Information supplied by the client that describes the safety systems on the facilities was reviewed in order to assess their adequacy in terms of their reliability and performance. This study utilised a similar approach to the Safety Integrity Level (SIL) methodology as defined in IEC 61508 and 61511 and provided recommendations, based on international standards, on areas for improvements to the instrumented systems. The approach was to identify the hazardous events that could occur as a result of failure of the safety instrumented systems and evaluate the consequences in terms of the safety, environmental and security of supply from the facility.

**Benefits:**

The assessment showed that the majority of the safety systems on site met the required safety integrity level. However, a few areas were identified that did not meet required SIL and recommendations for improvement were provided.
Safety & Risk Management Services

Safety Case and Compliance Consultancy
Hazard Identification Studies (HAZID)
Hazard Operability Studies (HAZOP)

- **SIL Studies (Safety Integrity Level)**
  
  Consequence Evaluation (Fire, Release, Explosion, Dispersion), Including CFD
  
  EER Analysis (Escape, Evacuation, Rescue) (GL-Aeneas)
  
  Quantitative Risk Analysis (QRA)
  
  Decision Support (Risk Based Layout Studies)
  
  Performance Standards
  
  Large Scale Hazards Testing (Spadeadam)
  
  Incident Investigation

**Germanischer Lloyd Industrial Services GmbH**

Oil and Gas
Steinhöft 9
20459 Hamburg, Germany
Phone +49 40 36149-7700
Fax +49 40 36149-1781
glis@gl-group.com

www.gl-group.com/glis

---

Germanischer Lloyd does not warrant or assume any kind of liability for the up-to-date nature, accuracy, completeness or quality of the information provided. Liability claims against Germanischer Lloyd arising out of or in connection with material or non-material loss or damage caused by the use or non-use of information provided, including the use of incorrect or incomplete information, are excluded unless such loss or damage is caused by the proven wilful misconduct or grossly negligent conduct of Germanischer Lloyd.

All offers are subject to alteration and are non-binding. Germanischer Lloyd expressly reserves the right without notice to change, supplement or delete parts of the pages or the entire offer or to stop the publication temporarily or definitively.