SIS Design Basis Report Methodology

The industry consensus standard ANSI/ISA 61511 requires a Safety Integrity Level (SIL) be selected for each Safety Instrumented Function (SIF) used within a Safety Instrumented System (SIS) and that the SIL achieved by the selected equipment be verified through quantitative calculations. However, the standard does not prescribe what analytical methods or techniques should be used to accomplish the SIL Selection task. Rather, the standard allows each organization that applies the standard the flexibility to establish a SIL selection method, and the ISA standard provides some guidance on example SIL Selection methods. This allows flexibility so that users can tailor their SIL selection method so that it is consistent with other risk management processes within the organization. This is consistent with other governmental organizations that allow a great deal of flexibility in implementing industry safety standards such as OSHA Process Safety Management 29 CFR 1910.119.

Safety integrity level selection is an exercise in risk analysis. In general, the goal of risk analysis is to determine the risk, as a function of consequence and likelihood of an unwanted event and compare that against a benchmark to determine if any risk reduction is required. A variety of techniques for SIL selection have been described in the literature, including five in the informative appendices to the ANSI/ISA 61511 standard. These techniques all generally follow the process outlined in the section below, but vary in terms of the detail and resolution that is applied to each individual task.

Most techniques begin with a qualitative approach to risk analysis, typically considering consequence and likelihood in order-of-magnitude bands. This general type of approach is often referred to as Layer of Protection Analysis (LOPA). In some cases, the simple qualitative techniques do not provide enough insight into the risk scenario to properly assign the required risk reduction. In these cases, more advanced techniques are applied to assist in the assignment of likelihood and consequence, and ultimately required risk reduction.

As noted above, specific procedures for SIL selection vary from organization to organization, and even from site to site within an organization. These procedures must be tailored to meet the needs of a specific site in terms of staff needs and preferences and existing site procedures for risk analysis and tolerable risk criteria. The specific procedure that was used for SIL selection for the study described in this report can be found in *Appendix B*.

1 SIL Selection Methodology

Most SIL selection techniques are procedures that begin with more qualitative processes for estimating consequence and likelihood. These procedures consider order-of-magnitude bands instead of specific numerical data or completely qualitative judgment. This type of analysis is often referred to as Layer of Protection Analysis (LOPA).

SIL selection processes generally follow the following steps.

1. Define hazard under analysis (the hazard that the SIF under consideration is preventing)

2. Estimate consequence of the hazard and its severity

3. Estimate likelihood of the hazard, considering all initiating events and all protection layers and mitigating circumstances

4. Measure the risk of the hazard as a function of consequence and likelihood

5. Compare risk against tolerability criteria to determine risk reduction requirements.

6. Select the appropriate Safety Integrity Level (SIL) that will achieve tolerable risk.

While all techniques generally follow the steps outlined above, there may be considerable variability in the detail and degree of resolution between those steps within different organizations that apply the ANSI/ISA 61511 – 2018 standard.

Step 1. – Define Hazard

Definition of the hazard is a critical step in the SIL selection process. Errors in this step will propagate and may result in poor overall results of the study. The definition of the hazards prevented by a specific safety instrumented function will be defined in the instrumented protective function list which can be found in *Appendix B* and in the referenced hazard risk analysis / SIL Selection.

Step 2. – Estimate Consequence

Estimation of consequence is typically performed in a qualitative fashion. Consequence is assigned a category based on its magnitude. While all SIL selection techniques require an analysis of safety impacts, some techniques supplement safety consideration with consideration of environmental and commercial impacts.

Step 3. – Estimate Likelihood

Likelihood is often considered in a more detailed fashion than consequence, but is still typically limited to order-of-magnitude bands. Some techniques simply categorize the overall likelihood of the consequence without considering the impact of the instrumented protective function (IPF) that is under consideration or other protective safeguards. Other techniques explicitly consider that an unwanted accident is the result of an initiating event in combination with the failure of other independent protection layers.

Step 4. – Measure Risk

Most organizations represent risk in terms of a matrix where event likelihood and consequence are the two axes and the magnitude of the risk is defined inside the matrix for each consequence-likelihood pair. Some organizations prefer explicit numerical representation of risk, either to the maximum-exposed individual or to a group.

Step 5. – Compare Risk Against Tolerable Risk Criteria

The degree to which risk can or should be tolerated is not a topic that is addressed in OSHA safety standards or industry consensus standards from ISA. In the US, this topic remains an area where each user of the ISA standard must establish organizational criteria for risk tolerance. Risk tolerance criteria are usually established in one of three ways. Organizations that use risk matrices can choose to assign a required risk reduction to each consequence-likelihood pair within the matrix. The risk reduction usually takes the form of a number of orders of magnitude reduction in the risk that need to occur to achieve a tolerable risk level. This has the advantage of integrating into a more holistic analysis of engineered safeguards using Layer of Protection Analysis (LOPA). Organizations that use fully quantitative measures of risk can also use LOPA, but risk tolerance criteria is usually handled in one of two ways. Some organizations prepare a table of "tolerable event frequency" that is a function of the severity category that is selected for the consequence. Other organizations have general criteria for individual risk of fatality to the maximum-exposed individual (or societal risk criteria). When quantitative risk tolerance criteria are used, the required risk reduction is explicitly calculated as a function of the unmitigated accident frequency and the tolerable frequency of the event.

Step 6. – Select SIL for the Safety Instrumented Function

The risk reduction requirements that are determined in the step above can then be allocated to a safety instrumented function (or potentially a non-SIS protection layer). In general, the integrity level assigned to an SIF is equal to the number of orders of magnitude of risk reduction that are required.

2 SIL Verification Methodology

The industry consensus standard ANSI/ISA 61511 requires a Safety Integrity Level (SIL) be selected for each Safety Instrumented Function (SIF) used within a Safety Instrumented System (SIS). Further, verification that the specified SIL has been achieved is required, based on a quantitative analysis that considers the equipment selected, architecture, voting, diagnostic capabilities, and testing schedules. Each SIF will have a specified SIL. Therefore, each SIF requires a SIL Verification analysis. This involves use of a reliability/availability model for the SIF and selection of appropriate data to use in that model.

Procedures for determining the achieved SIL are based on calculations of performance of a SIF. Performance is based on the metric known as average Probability of Failure on Demand (or PFD_{avg}, which is defined below). Procedures for SIF performance calculations have been standardized are described in industry technical reports, including ISA Technical Reports entitled: Safety Integrity Level (SIL) Evaluation Techniques, ISA-TR84.00.02-2015.

2.1 Model Selection

Several reliability/availability models are available for analyzing SIF performance. Those models utilize calculations which typically consider the following information:

- Failure rate data of the individual components that comprise a SIF

- A statistical model that calculates the overall performance of a SIF based on the known performance of the components that are used in the SIF,

- A definition of the minimum necessary and sufficient actions that a SIF must take under one or more pre-determined input conditions, and

- A description of how SIF components are logically related, or the architecture of the SIF.

Collectively these techniques are called “fault propagation models”. Common fault propagation models include fault tree analysis, event tree analysis, reliability block diagrams, and Markov models.

Kenexis selects the model that is most appropriate for the specific SIF being analyzed. In most cases, a model based on Simplified Equations is adequate to determine PFD_{avg}, and Kenexis defaults to calculation methods based on Simplified Equations in its SIS Design Toolkit™.

In some cases, the architecture required for a particular Safety Instrumented Function is more complex than the packaged SIS analysis software tools are capable of analyzing. In these situations, Kenexis will build a model of the SIS using a Fault Tree Analysis (FTA). Fault Tree Analysis is performed using Fault Tree+ from Isograph. Although rarely required, Kenexis is also able to employ Markov analysis using the Fault Tree+ tool if specified by client needs. In Kenexis’ experience this level of analysis is neither required nor is advantageous to use in applications.

These procedures were used to calculate PFD_{avg} results that are referenced in this report. Details can be found in ISA TR84.00.02-2015.

2.2 Failure Rate Data

The quality of the SIL Verification analysis depends on the failure data that was used to calculate PFD_{avg}. The data needed for a component is represented in terms of four variables: overall failure rate, % Safe Failures, Diagnostic coverage of safe failures (Cs), and Diagnostic coverage of dangerous failures (Cd).

Obtaining accurate equipment failure rates requires historical information on how equipment has failed in a process plant environment. The best source of data is records of equipment failures, repairs, and maintenance, which are taken from the process plant that is being evaluated. This information is preferred because the data best describes the actual conditions under which the equipment is being used. Unfortunately, data in a usable format is often not available, and other data sources are needed to conduct SIL Verification analysis.

In cases where site-specific data is unavailable, industry-average data is typically used. Kenexis has compiled a database of equipment-specific failure records. This database allows for quantification of equipment failure rates, and percent safe failure. The database is collected from public and confidential sources within industry. Some of the major public sources are listed below.

- Offshore Reliability Data Handbook (OREDA)
- Instrumentation, Systems, and Automation Society (ISA) Technical Reports
- Institute of Electrical and Electronic Engineers (IEEE)
- Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE)
- United States Nuclear Regulatory Commission

- Reliability, Maintainability, and Risk, D.J. Smith
- Non-Electric Parts Database (NPRD-95) and Electronics Parts Reliability Database (EEPD-97)
- Publicly-available technical reports
- FMEDA Reports from Equipment Manufacturers

In many cases, public data is suitable and is preferred. However, in other cases public data is not adequate. In these situations, Kenexis has deemed it preferable to include data from confidential sources, which is obtained from companies in the oil and gas industry, petroleum refining, petrochemical, specialty chemicals, and pharmaceutical industries.

Kenexis selected the most appropriate data from the various sources and combined them on a consistent basis for many types of process equipment and services. Failure rate data used in this study are provided in the appendix that contains detailed calculation information.

Although Kenexis has provided data for use in SIL Verification calculations, it is the responsibility of the customer to verify that equipment failure rates that are used in this analysis are consistent with equipment failure histories in the field.