Journal of Loss Prevention in the Process Industries 41 (2016) 333–343

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

# On the use of LOPA and risk graphs for SIL determination

Alejandro C. Torres-Echeverria [1]

*Risktec Solutions Inc., 1110 NASA Parkway, Suite 203, Houston, TX 77058, USA*

ARTICLE INFO

*Article history:*
Received 28 April 2015
Received in revised form
17 November 2015
Accepted 10 December 2015
Available online 13 December 2015

*Keywords:*
Safety instrumented systems (SIS)
Safety integrity level (SIL)
Layers of protection analysis (LOPA)
Risk graph
IEC 61508
IEC 61511

ABSTRACT

Safety Integrity Level (SIL), as defined in IEC 61511, is a widely used safety performance measure for safety instrumented functions. The standard IEC 61511 suggests several methods for SIL determination, ranging from fully quantitative methods to fully qualitative methods. The large number of safety functions to evaluate during plant design and the need to integrate multidisciplinary design and operation knowledge to achieve effective risk reduction has made necessary the use of multi-disciplinary-team workshop approaches.

Two widely used methods in the Oil & Gas industry for SIL determination are Layer of Protection Analysis (LOPA) and Risk Graphs. Each of these methods has their own advantages and disadvantages. LOPA allows the required risk reduction to be incorporated into the SIL values with higher precision. This enables a more detailed consideration of the available protection layers and leaves an objective traceable record of the decision-making process.

In contrast, the simplicity of Risk Graphs makes them convenient for screening a large number of safety functions. This can make Risk Graphs useful as a first screening pass prior to using LOPA. However, Risk Graphs are still widely used as a stand-alone method.

This paper seeks to explore the differences between LOPA and Risks graphs and to investigate whether the Risk Graphs method can provide the same level of SIL determination rigor as LOPA. The paper aims to determine if the simplicity of Risk Graphs can make that method more efficient for cases when the number of safety functions to evaluate is considerable.



## 1. Introduction

Two of the most widely used methods in the Oil & Gas Industry for determination of Safety Integrity Levels (SIL) of Safety Instrumented Functions are Layer of Protection Analysis (LOPA) and Risk Graphs. Each of these methods has their own advantages and disadvantages. Safety Integrity Levels are defined in the standards IEC 61508 (IEC, 2010a) and IEC, 61511 (IEC, 2003a). LOPA allows a more detailed consideration of layers of protection and required risk reduction, at the time that leaves a traceable record of the decision making process. The Risk Graph method is less intensive, and its relative simplicity makes it convenient for screening large number of SIFs. This paper makes a review of differences between LOPA and Risks graphs in order to determine whether the Risk Graphs method can provide the same level of SIL determination rigor as LOPA and if the Risk Graph method can be more efficient for cases when the number of safety functions to evaluate is considerable.

## 2. International standards' requirements

The international standard IEC 61508 (IEC, 2010a) addresses the requirements for safety related systems based on electrical, electronic and programmable electronic technology. This is a generic document, non-specific to any industry and relevant to a wide range of different sectors. The international standard IEC 61511 "*Functional safety: Safety instrumented systems for the process industry sector*" (IEC, 2003a) was created as a derivation of IEC 61508 to cover specifically the process industry. The standard ANSI/ISA-84.00.01 edition 2004 (ISA, 2004) later adopted the standard IEC 61511 in its entirety with some minimal modifications. Therein, any reference to IEC 61511 is equivalent to refer to ANSI/ISA-84.00.01 and vice versa.

A Safety Instrumented Function (SIF) is a safety protective function implemented by a Safety Instrumented System (SIS), and composed of any combination of sensors, logic solver and final elements (e.g. valves). A SIF must achieve a specific level of integrity,

*E-mail address:* alejandro.torres@risktec.com.
[1] Present address: 15810 Park Ten Place, Suite 100, Houston, TX 77084, USA.

http://dx.doi.org/10.1016/j.jlp.2015.12.007
0950-4230/

**Nomenclature**

| | |
|---|---|
| ANSI | American National Standards Institute |
| BPCS | Basic Process Control System |
| **C** | Consequence |
| CCF | Common Cause Failure |
| CCPS | Center for Chemical Process Safety |
| **F** | Occupancy |
| HAZID | Hazard Identification Study |
| HAZOP | Hazards and Operability Study |
| IEC | International Electrotechnical Commission |
| IPL | Independent Layer of Protection |
| ISA | International Society of Automation |
| LOPA | Layer of Protection Analysis |
| **P** | Probability of Avoiding a Hazard |
| $PFD_{avg}$ | Average Probability of Failure on Demand |
| QRA | Quantitative Risk Assessment |
| RRF | Risk Reduction Factor |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| **W** | Demand Rate |
| **W'** | Initiating Event Frequency |

represented by the Safety Integrity Level (SIL). Notice that the SIS, and thus the SIFs, is independent from the plant control functions performed by the Basic Process Control System (BPCS).

Per IEC 61511, definition of any SIFs must be based on a previous risk assessment. The risk assessment would determine the current level of risk presented by the facility. This would be compared against a tolerable risk level. The gap between the actual risk level and the tolerable risk is the required level of risk reduction (Fig. 1), also called the Risk Reduction Factor (RRF). The RRF is the relation of the actual risk presented by the facility and the risk that must be achieved as a target based on the acceptance criteria:

RRF = Actual Risk / Tolerable Target Risk

An important consideration is that the tolerable risk level to be used as baseline for risk assessment must be set by each individual organization specific to each process or facility as their Corporate Risk Criteria (CCPS, 2001; De Salis, 2011).

## 3. Safety integrity level concept

SIL stands for "Safety Integrity Level", which is a discrete performance measure that indicates the range of maximum acceptable probability of failure of a SIF to perform its intended function upon a demand to do so. The SIL levels are defined in terms of the average Probability of Failure on Demand ($PFD_{avg}$) for systems working on demand mode of operation, as presented in Table 1.

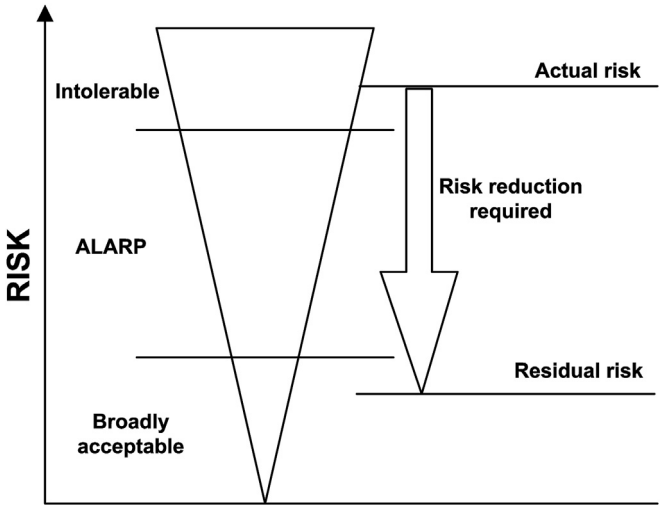


**Fig. 1.** Risk reduction factor concept.

**Table 1**
Safety integrity levels for demand mode (IEC 61511 (2003a)).

| SIL | $PFD_{avg}$ | Risk reduction factor |
|---|---|---|
| 4 | $\geq 10^{-5}$ to $<10^{-4}$ | >10,000 to ≤100,000 |
| 3 | $\geq 10^{-4}$ to $<10^{-3}$ | >1000 to ≤10,000 |
| 2 | $\geq 10^{-3}$ to $<10^{-2}$ | >100 to ≤1000 |
| 1 | $\geq 10^{-2}$ to $<10^{-1}$ | >10 to ≤100 |

## 4. SIL determination methods

SIL Determination refers to the activity of selecting the required SIL for a SIF. SIL determination is usually done after the risk assessment has been performed and the SIFs required in the plant have been defined. There are several methods suggested in IEC 6511 and IEC 61508 for SIL determination. These methods range from quantitative, semi-quantitative to qualitative. The most rigorous and comprehensive methodology is based on a fully quantitative analysis (see IEC 61508 Part 5 Annex D (IEC, 2010b), and IEC 61511 Part 3 Annex B (IEC, 2003b)), such as a Quantitative Risk Assessment (QRA). However, this method is not frequently used because it is resource intensive. Three widely used approaches in the Oil & Gas industry are Layers of Protection Analysis (LOPA), Risk Graphs and Safety Layer Matrix. The latter is briefly explained next, while LOPA ad Risk Graphs are fully described in Sections 5 and 6 respectively.

**Risk Matrix.** This is a qualitative method described in IEC 61508 Part 5 Annex G (IEC, 2010b) and ISA IEC 61511 Part 3 Annex D (IEC, 2003b). IEC 61511 calls it Safety Layer Matrix, while IEC 61508 names it Hazard Event Severity Matrix. This method is based on qualitative knowledge of the likelihood and consequences of hazardous events, as well as the number of layers of protection available. It is based on the assumption that each added protection layer provides a risk reduction of one order of magnitude. The matrix is presented Fig. 2. The factors used in the matrix are:

- Severity rating
- Likelihood of the hazardous event
- Number of independent protection layers for the specific hazardous event.

## 5. Layer of protection analysis (LOPA)

Layer of Protection Analysis (LOPA) is a simplified semi-quantitative risk analysis methodology. This method is presented in both IEC 6508 Part 5 Annex F (IEC, 2010b) and IEC 61511 Part 3 Annex F (IEC, 2003b). LOPA is described comprehensively in CCPS (2001). The LOPA method consists on identifying (semi-