Safety Instrumented Systems in EPC Project Lifecycle

Shivendra Kapoor

This simplified article is an attempt to help engineers working in the EPC/ detail engineering sector to understand the first two stages of the ‘Analysis’ phase of the Safety Instrumented Systems (SIS) lifecycle (as per IEC 61511) and effectively consider the same in their overall project lifecycle so as to successfully complete the project including the HSE perspective and holistically as well.

The author while dealing with various engineering companies as a part of implementing SIS was almost always posed with these questions: Can the SIS lifecycle be understood in a simplified manner? How do we consider it appropriately in our project lifecycle?

This article is written in a similar fashion to IEC 61511 standard i.e. non-prescriptive way as it will help readers relate more to the standard.

Shivendra Kapoor is Manager- Functional Safety with Chola MS Risk Services in Mumbai, India. He is a Instrumentation Engineer and a Certified Functional Safety Professional from TÜV SÜD. He has +13 years of industry experience covering a variety of sectors like: Oil and Gas, Mines and Minerals, Chemicals, etc. He is also a freelance writer at heart and has many short fictional and non-fictional stories published globally in reputed publications.
Introduction

PCs and detail engineering companies over the years have mastered the art of efficient and optimized engineering of various types of industrial plants. However, with huge increases in the scale, production capacities and complexity, high end automation had to be introduced in plants. Even though a lot of automated safety measures are implemented, there is a long list of catastrophic industrial disasters occurring quite frequently and the numbers are ever increasing. Operating companies are facing the heat from government, the general public and insurance companies to improve process safety. Accordingly, HSE studies like: HAZOP, SIL, FERA, Vent and dispersion, Alarm Rationalization, Human Factors, etc. have become very popular; whether it is for greenfield/brownfield projects or for existing installations. Some of these studies were conducted earlier as well, but now, it is with more vigor and involvement.

Overall SIS lifecycle

Figure 1 depicts the SIS lifecycle phases as given in IEC-61511, Part-1. As can be seen from the figure, the entire lifecycle is divided primarily into 3 phases:

Analysis, Realization, Operation.

Each phase is equally important and depending on the type and size of a project and an engineer’s competence and scope of work, he/she may either be involved in one or more phases of the lifecycle.

This article will be limited to the first two stages of the Analysis phase.

The ‘Analysis’ phase includes: Initial Planning, Identification and Specification activities. The key focus of this phase is the SIL selection process.
First Two Stages of the Analysis Phase:

“HAZARD AND RISK ASSESSMENT”
and
“ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS”

(BEGINS with: Conceptual Process Design)

Ends with: Safety Requirements Specifications (SRS)

Details

The lifecycle begins by conceptualizing the initial design of the process and by definition of the project’s scope and purpose in terms of goals and measurable outcomes. This is done to avoid ambiguity amongst team members involved in the project. Critically, it should address the limits of the process and equipment as well as any other boundaries that will be addressed further during hazard and risk analysis.

During hazard and risk analysis, the first task is identification of hazards and hazardous events that may potentially occur in the operation of the process. This is usually carried out by way of a PHA study (Process Hazard Analysis) such as HAZOP.

The required risk reduction will determine which SIL should be selected for the SIF in question. The SIF if used to reduce the risk of the process from intolerable region to the tolerable region becomes one of the layers of protection. There could possibly be other non-SIS layers of protection, for e.g. mechanical relief devices, alarms, etc. that may protect against the same hazard.
Key points

After the P&IDs are developed and stamped as ‘Approved for Design/Detailing’, they are considered ready for HAZOP. HAZOPs are well understood and incorporation of recommendations usually follows by marking the same on the P&IDs /other relevant documentation. These form the basic inputs for the SIL selection study that begins after the HAZOP.

It is of utmost importance that sufficient time is given to the engineering team to prepare and conduct the HAZOP. Subsequently, adequate time shall be given to incorporate all HAZOP findings on the P&IDs and relevant documentation so that technically clear and precise information is available to the SIL selection team. Failure to do so usually results in a lot of confusion during the SIL selection study. The ‘Target SIL’ that is defined during the SIL selection study should be developed in accordance with the HAZOP study findings. A mismatch will result in a Safety Instrumented System that is either over-rated/designer or under-rated/designer.

Identification of hazards and potential SIFs are completed and then the hazards are characterized in terms of ‘magnitude of their consequences’ and ‘likelihood of their occurrence’. Likelihood analysis is done using various methods of which Layers of Protection Analysis (LOPA) is the most popular. With all the information available and the tolerable risks known, one can determine whether a SIS is required to perform the SIF under consideration. The required risk reduction will determine which SIL should be selected for the SIF in question. The SIF is used to reduce the risk of the process from intolerable region to the tolerable region becomes one of the layers of protection. There could possibly be other non-SIS layers of protection, for e.g. mechanical relief devices, alarms, etc. that may protect against the same hazard.

The EPC personnel shall consider the following points while planning and executing the HSE study:

• Arranging all pre-requisite documentation for conducting the required study including coordinating with the end-user/operating company for active participation with their operations/maintenance team
• Team members participating in the study shall be competent and well trained to give valuable inputs during the study; else the purpose of the study is lost
• Review and comment on the reports generated by the HSE consultant based on agreed review/comment cycle
• Inter-disciplinary squad check of the reports (as per the type of report)
• Resolution of comments, implementation of recommendations in consultation with the HSE consultant

• Close out of all open points and acceptance by the operating company/end-user

All of the above consume reasonable man hours and resources and same shall be budgeted in the overall project.

The Analysis phase ends with documenting all the above efforts and results in a structured manner in a Safety Requirement Specification (SRS). The SRS forms the key input for the next phase of the lifecycle i.e. Realization phase as SRS is the document that exactly specifies what is required if the safety system is to be designed, installed and operated.

Summary

In this article, we saw the first two stages of the Analysis phase of the safety lifecycle. Some of the subsequent phases/stages of the safety lifecycle also require similar involvement in the overall project lifecycle; which will be covered in forthcoming articles.

It is worth reiterating that it is important to give full justice to any project and same can only be achieved if adequate allocation of budget, man-hrs and trained resources is given for HSE studies during planning and execution stages of a project. The safety lifecycle concept is usually embraced by companies, but when it comes to actual project execution, the application of the safety lifecycle concept comes in conflict with the overall project planning and then the project goes haywire. This should strictly be avoided as once the safety lifecycle phases are bypassed; they merely become a piece of formality and difficult to correct/manage errors start creeping in all the subsequent phases of the safety lifecycle.

The ‘Analysis’ phase is probably the most crucial phase in the lifecycle, as if the team fails to identify the correct hazards, then there will not be a need for a safety function in place to reduce the potential risk associated with the hazards.

References

IEC-61511 standard: Safety Instrumented Systems for the process industry sector.

Safety Integrity Level Selection by Edward M. Marszal and Eric William Scharpf.