



SIL Assessments - Identification of Safety Instrumented Functions

Dirk Schreier
Functional Safety Consultant
HIMA Australia Pty Ltd
L3, 37 St Georges Terrace
Perth WA 6000
Australia

INTRODUCTION

Since its release as an Australian standard in July of 2004, AS61511 is rapidly being accepted and applied on Safety Instrumented Systems throughout the process industry. AS61511 is a performance based standard with a risk-based approach to safety. Performance based standards are by nature very open to interpretation, and therefore allow for more than just one analysis technique. Some of the techniques currently applied in industry have some shortfalls in achieving the objective of the standard. This article looks at some common problems encountered during the analysis phase of the AS61511 safety lifecycle.

HAZOPS

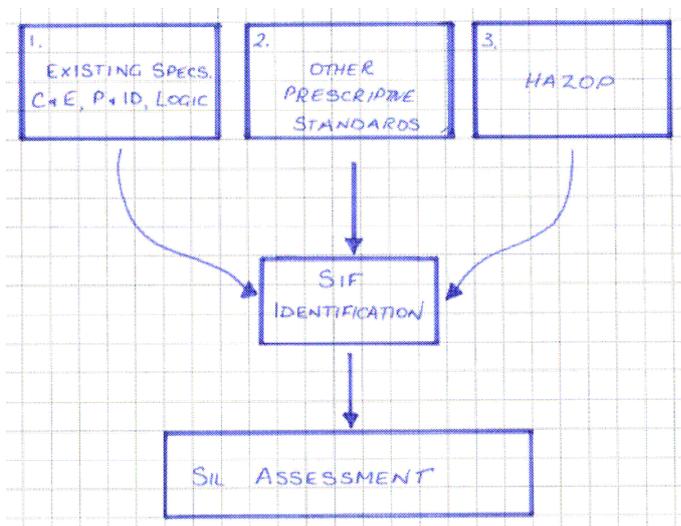
The safety lifecycle begins with a Process Hazard Analysis (PHA). The most common method of PHA used is the HAZOP. Whilst a HAZOP is a very effective way of identifying process hazards, it may be executed incorrectly, or without an awareness of the downstream activities such as the SIL assessment. In these instances, there is a real risk of Safety Instrumented Functions (SIFS) being missed or unclearly defined.

HAZOP leaders should be familiar with the requirements of AS61511 to ensure that the right information is available for further activities of the safety lifecycle. In one example a process contained many pressure vessels, however the HAZOP report did not identify any high-pressure hazards. Further investigation revealed that a fundamental HAZOP assumption that "pressure safety valves (PSV) installed on the vessels mitigated all high-pressure hazards", resulted in this information not being captured. The correct approach would have identified the high pressure as a hazard and noted the PSV as an existing protection layer. This information is essential for layer of protection analysis (LOPA) during the SIL assessment to determine if the PSV will provide sufficient risk reduction. An understanding of the downstream activities ensures that the outcomes from the HAZOP meet the objectives of AS61511.

Another issue arises when the SIL assessment is carried out as part of the HAZOP. Known as a modified HAZOP, this technique is an extension of the existing HAZOP process and the required experience and knowledge extends beyond simple understanding of the process operation. Experience has shown that the HAZOP is best kept as a separate activity and used to flag any SIFS that require further assessment. The HAZOP report together with other source documents is then used in a separate SIF identification process.

IDENTIFYING SAFETY INSTRUMENTED FUNCTIONS

Like all engineering processes, a SIL assessment requires pre-planning to ensure an effective outcome is achieved. Preparation for a SIL assessment includes; selection of the participants, determining the suitability of the end-users risk matrix, selection of the methodology to be used, and defining the SIFS to be assessed. One major item that may produce undesirable outcomes, and is often not very well defined, is the SIF identification process. To address this problem it is necessary to spend some time on the identification of SIFS. A modified HAZOP approach as discussed above, has an over simplistic approach to the SIF identification process, thereby resulting in SIFS that are either missed, or unclearly defined.



The following diagram illustrates a process of SIF identification that is based on building a list of SIFS based on various sources, not just the HAZOP.

Input 1 - Many applications are retrofit and already contain some form of protection. This provides a good starting point for identifying potential safety instrumented functions. Existing specifications, cause & effect (C&E) diagrams, P&ID's and Logic in most cases will identify shutdowns already in place.

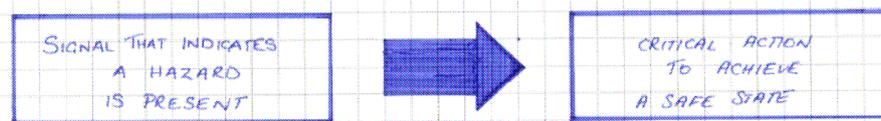
Input 2 - There is often also a requirement to conform to other prescriptive standards due to regulatory or customer requirements. This is a perfect opportunity to incorporate those requirements. Such as AS3814 and NFPA85 that contain requirements for safety-instrumented functions on burner management systems.

Input 3 - The HAZOP should identify any other potential safety instrumented functions not already identified in existing documents and standards.

By separating the SIF identification process from the HAZOP and drawing on other sources, to produce a list of SIFS to be assessed, the risk of missing a SIF is minimized, thereby resulting in an outcome that meets the objectives of this phase of the safety lifecycle.

FORMAT OF A SIF

When compiling a list of SIFS, it is also important to clearly identify what the safety function must accomplish. A safety-instrumented function can be compared to a balanced equation. Firstly, it must define a signal that identifies that a hazard is present, and secondly it must define the critical action to remove that hazard. E.g. High Separator Level -> Close Inlet Valve



SIFS are often documented on a C&E diagram, however it is often unclear which actions are critical, and which ones are secondary clean up actions. For this reason a C&E should not be used as the sole document identifying the SIFS. AS61511 has many other requirements such as a Safety Requirement Specification (SRS), and the C&E effectively becomes a summary of the SIFS.

CONCLUSIONS

Experience has shown that in many cases, SIFS are identified from sources other than the HAZOP. The HAZOP process may not completely address the requirements of AS61511, and we need to ensure that no SIFS are missed. By having an awareness of the SIL assessment process downstream of the HAZOP, we ensure that the outputs from the HAZOP meet the objectives of the AS61511 standard.

A formal SIF identification process during the planning phase of the SIL assessment reduces the chance of not identifying SIFS, and ensures that they are correctly documented. If a SIF is assessed and yields no SIL, it can easily be removed during the assessment. If a SIF is assigned an incorrect SIL, the protective function will still be effective, but provide a lower level of safety. However, if a SIF is missed altogether, and is not assessed, the potential consequences can be severe.

Dirk Schreier
Functional Safety Consultant
HIMA Australia Pty Ltd
www.hima.com.au