tonyfrederickson@msn.com

Guidance for SIS definition in accordance with standards SIL levels.

We are looking for clear guidance on how to properly define in accordance with local and international standards SIL levels and select the appropriate SIS systems for both new projects as well as existing site installations. We are in the process to define guidelines for safety / process designers to set the SIL levels, and for defining guidelines to instrument engineers / designers to match this required SIL with the appropriate cost effective SIS system.

Anton A. Frederickson, Mr., *Dr.* (prepared answer)
Independent Consultant – member of Safety Users Group Network
01 April, 2002

SIL Determination

The determination of the safety integrity level (SIL) for each Safety Instrumented Function (SIF) in a Safety Instrumented System (SIS) is dependent on the following factors:

1. The Corporate Standard for the tolerable risk after applying all the layers of protection. This tolerable risk may be a function of the cost of reducing the residual risk. The IEC 61508-5 Standard – Example of methods for the determination of safety integrity levels, discusses the general concept of risk and safety integrity in Annex A and the concepts of ALARP and tolerable risk in Annex B.
2. The overall risk from the unprotected hazards that can occur. The Layers of Protection Analysis (LOPA) provides a methodology for determining the overall risk from data determined in a Hazard and Risk Analysis (HAZOP). The LOPA methodology is discussed in Answer #C.
3. The risk reduction provided by all of the non-SIS protection layers. LOPA also provides a methodology for analyzing the risk reduction from various non-SIS protection layers.

The residual risk remaining can be computed from the unprotected risk and the risk reduction provided by the non-SIS protection layers. If the residual risk is greater than the tolerable risk, a SIS is required to provide the final required risk reduction. The average probability of failure on demand of each safety instrumented protection function, PFDavg, is equal to the necessary risk reduction the protection function must provide. The necessary risk reduction is computed by dividing the tolerable risk by the residual risk remaining before the application of the safety instrumented function. The SIL for each safety function can be determined from Table 2 in IEC 61508-1 by use of the required PFDavg. Annex C in IEC 61508-5 discusses this method of determining the required safety integrity level and includes example calculations.

Annexes D and E in IEC 61508-5 describe two qualitative methods for determining the SIL. Annex D outlines the risk graph method, and Annex E describes a hazardous event severity matrix method.

It should be noted that the PFDavg and the corresponding SIL must be computed for all safety functions required within the Safety Instrumented System.

SIS Selection

The user should determine the appropriate safety standard to be used to develop their guidelines. In most countries, the IEC 61508 standard must be used for current applications. In the United States, the user can follow the ANSI/ISA S84.01 standard as well as the IEC 61508. Since it is anticipated that IEC 61511 standard will be formally issued in 2002, users in the process industry should be developing guidelines that will conform to IEC 61511. The IEC 61511 standard requires all components and subsystems necessary to achieve a safety instrumented function to be designed in

accordance with IEC 61508 or to meet the requirements for a component to be proven-in-use. Clause 11.5.3 in the draft IEC 61511-1 specifies the requirements for proven-in-use. Clause 11.5.3 requires many years of operational experience with a component or device, so the random hardware failure rates can be determined to a single sided lower confidence limit of at least 70%. Most users will probably purchase logic solvers from manufacturers that have developed logic solvers designed in accordance with IEC 61508 and certified by an independent certification body like TÜV.

The guidelines for selection of the logic solver required to implement a complete SIS that performs many safety instrumented functions should consider the following factors:

1. The IEC 61511 standard requires manufacturers and suppliers of devices for safety instrumented systems to conform to the IEC 61508 standard. Hence the manufacturer of the logic solver should follow the IEC 61508 standard.
2. The logic solver portion of the SIS should be suitable for implementing the SIF requiring the highest SIL.
3. The logic solver manufacturer should provide a safety manual that details all restrictions and operating requirements for the logic solver and it's associated tools that are appropriate for the SIL required. The IEC 61511 standard requires a safety manual for the logic solver.
4. If the user or the user's system integrator selects a logic solver that was not designed in accordance with IEC 61508, the logic solver must the requirements for proven-in-use.
5. The hardware fault tolerance requirements in Clause 11.4 in IEC 61511-1 must be followed when selecting the logic solver.
6. The spurious trip rate of the logic solver, MTTFspurious, should also be considered since a spurious trip can disrupt production and result in significant lost production costs.

Since very few sensors and final elements have been designed to be in accordance with IEC 61508, most users will be required to select sensors and final elements that have been proven-in-use.
The guidelines for selection of the sensors and final elements required to implement safety instrumented functions should consider the following factors:

1. The sensor and final element process interfaces should be included when determining the failure rates and failure modes of the subsystem.
2. The sensor and final element subsystem redundancy required to implement the various safety instrumented functions should be determined by calculation of the PFDavg for each subsystem.
3. The sensor and final element hardware common cause should be included in the calculation of PFDavg.
4. The hardware fault tolerance requirements in Clause 11.4 in IEC 61511-1 must be followed when selecting the sensor and final element redundancy.

This document has been prepared by: **Anton A. Frederickson, Mr. *Dr.***
For more information see full contact details in Safety Users Group Directory