



Mary Kay O'Connor Process Safety Center
2005 International Symposium
Beyond Regulatory Compliance, Making Safety Second Nature
October 25-26, 2005

Failure Conundrum

Michaela Gentile, Ph.D.
Design Consultant
SIS-TECH Solutions, LP
12621 Featherwood, Suite 120
Houston, Texas 77034

Angela E. Summers, Ph.D., P.E.
President
SIS-TECH Solutions, LP
12621 Featherwood, Suite 120
Houston, Texas 77034

During the hazard & risk assessment, a safety integrity level (SIL) is assigned to each safety instrument function (SIF) in the safety instrumented system (SIS). The SIL is related to the amount of risk reduction required to mitigate the process risk to the risk criteria. As with any other protective system, SISs can fail and the SIL provides the benchmark for acceptable performance.

IEC 61511 (ANSI/ISA 84.00.01-2004) stresses the importance of minimizing failures through design, operating, and maintenance practices. However, to understand its lifecycle requirements, it is first necessary to understand their nature and the effects on the SIS. Although several technical standards and other specialized literature address the topic, it is still a “fuzzy” matter, subject to misunderstanding and discussion.

In general, SIS-related failures include random, systematic, and common cause faults. IEC 61511 requires a functional safety management system to minimize the systematic failures related to hardware and software components throughout the SIS lifecycle. For the random hardware failures, IEC 61511 Clause 11.9 requires that the SIL be verified using quantitative analysis. This analysis should include common cause failures that are random in nature and should not include those that are systematic.

Therefore, the standard has specific requirements for each type of failure, whether common cause, random, or systematic. The person verifying the SIL should therefore understand the various types of failures and how each is treated within IEC 61511. This paper will briefly discuss the different types of failures with the goal of clarifying differences in consequences on the SIS system. It will then apply the concepts presented to introduce the current modeling techniques used to assess common cause failures in the SIS.