LISTEN. THINK. SOLVE.®

Safety in numbers

A 7 step guide to functional safety

The management of electrical, electronic and programmable electronic systems is governed by IEC61508. Where functional safety in the process industry is concerned, IEC61511 offers guidelines on the application of IEC61508.

IEC61511 is not a design standard, but a standard for safety management. Compliance is the result of risk assessments that lead to the allocation of Safety Integrity Levels (SILs).

1 *Requirements for compliance with IEC61511*

Because the standard is non-prescriptive, compliance is never straightforward: it isn't possible to buy 'SIL certified components' and assume this is adequate. Compliance requires the implementation of procedures for the management of Functional Safety, and demonstration that the lifecycle approach has been adopted, and that lifecycle activities are planned, resourced and verified.

2 *What is a Safety Integrity Level (SIL)?*

A SIL is a measure of the performance needed for a safety function to reduce the risk of a process hazard to a tolerable level. There are 4 SILs. SIL4 provides the highest level of safety integrity and the greatest amount of risk reduction, and SIL1 the lowest. Determining a SIL target is based on the assessment of the likelihood of a hazard and the severity of its consequences.

3 *Safety Requirement Specification*

Hazard and Risk Assessment allows the specification of safety requirements for the Safety Instrumented System (SIS). The Safety Requirement Specification (SRS) facilitates the Design and Engineering of the SIS by not only specifying the target SIL and the hardware reliability measure but also performance requirements to ensure that the SIF can act quickly enough to protect the plant.

4 *SIL targets*

A compliant SIS design must meet not only the specified SIF probability of failure for each safety function, but also the requirements for fault tolerance based on levels of redundancy and the effectiveness of available diagnostics. In addition, all SIS components must be demonstrated to be suitable for use in a safety function at the specified SIL and the application software must follow an appropriate development methodology and use suitable languages, coding standards and development tools.

5 *Functional Safety Management*

Appropriate Functional Safety Management is essential over all of the safety lifecycle. This requires the implementation of procedures for all safety lifecycle activities, the clear definition and communication of roles and responsibilities and the selection of staff based on competence. Functional safety audits should be planned and carried out at appropriate points in the project.

6 *Suitability of Components*

It is not essential to only use 'SIL Certified' components and subsystems but it is essential to demonstrate that the components and subsystems that are used, are suitable for use in a SIS. Suitability can be demonstrated either by certification, by assessment of compliance to IEC61508 or by field performance based on the volume of operating experience in similar environments and applications.

7 *SIL Verification*

SIL Verification is carried out against the SRS. It provides a calculation of the achieved target reliability measure, the probability of failure, and also the achievement of the requirements for hardware fault tolerance based on Safe Failure Fraction (SFF). The verification also enables the development of a maintenance philosophy that determines the maximum proof test interval that allows the SIL targets to be achieved.

The question to ask is, if an incident occurs and there's an injury or worse, can you demonstrate that you did everything that would be reasonably expected of you?

Download 'Process Safebook 1' to get the full story on SILs and what they mean for your business, get your copy of the NUMBER ONE GUIDE TO PROCESS SAFETY.

Publication SAFETY-QR008A-EN-E - November 2015

Rockwell Automation

Allen-Bradley • Rockwell Software