

Summary of Draft IEC 61511 Standard for Functional Safety: Safety Instrumented Systems for the Process Industry

Rachel Amkreutz
Reliability Engineer, exida.com
Sellersville, PA 18960
+215-453-1720

IEC 61511 has been developed as a Process Sector implementation of the international standard IEC 61508: "Functional safety of electrical / electronic / programmable electronic safety-related systems." The standard has two concepts, which are fundamental to its application; the safety lifecycle and safety integrity levels (SIL). The safety lifecycle forms the central framework which links together most of the concepts in this international standard. It is a good engineering procedure for safety instrumented system (SIS) design. In the safety lifecycle, process risks are evaluated and SIS Performance requirements are established (availability and risk reduction). Layers of protection are designed and analyzed. Finally, a SIS (if needed) is optimally designed to meet the particular process risk. Safety integrity levels are order of magnitude levels of risk reduction. There are four SIL's defined in this standard, just as in IEC 61508. SIL1 has the lowest level of risk reduction. SIL4 has the highest level of risk reduction. The standard suggests that applications which require the use of a single safety instrumented function of SIL 4 are rare in the process industry and that they shall be avoided where reasonably practicable. The standard is primarily concerned with safety-instrumented systems for the process industry sector (sensors, logic solvers and final elements are included as part of the safety instrumented system). It also deals with the interface between safety-instrumented systems and other safety systems in requiring that a process hazard and risk assessment be carried out.

This draft consists of three parts:

Part 1: Framework, definitions, system, hardware and software requirements
(Version CDV, 26/05/00)

Part 2: Guidelines in the application of IEC 61511-1
(Version 2.3, 18/05/00)

Part 3: Example methods for determining safety integrity in the application of Hazard & Risk Analysis. (Version CDV, 06/07/00)

1 Part 1: Framework, definitions, system, hardware and software requirements

Part 1 specifies requirements for system architecture and hardware configuration, application software, and system integration. This includes sections on management of functional safety, safety lifecycle requirements, verification, process hazard and risk analysis, and allocation of safety functions to protection layers. These last two sections only contain general requirements and no detailed requirements.

Furthermore, there are sections on SIS safety requirements specification, and SIS design and engineering, and requirements for application software (including selection criteria for utility

software). This section contains a detailed safety lifecycle overview for application software. Finally there are sections on factory acceptance testing, SIS installation and commissioning, SIS operation and maintenance, SIS decommissioning, and information requirements. Parts 1, 2, 3, and 4 of IEC 61508 have thus been combined into part 1 of IEC 61511. IEC 61511-1 furthermore has sections on: scope, references, abbreviations and definitions (process sector specific), and conformance.

The relationship between IEC 61508 and IEC 61511 is also defined in Part 1, as shown in figure 1. The key differences between IEC 61508 and IEC 61511 are discussed in Part 1, Annex A.

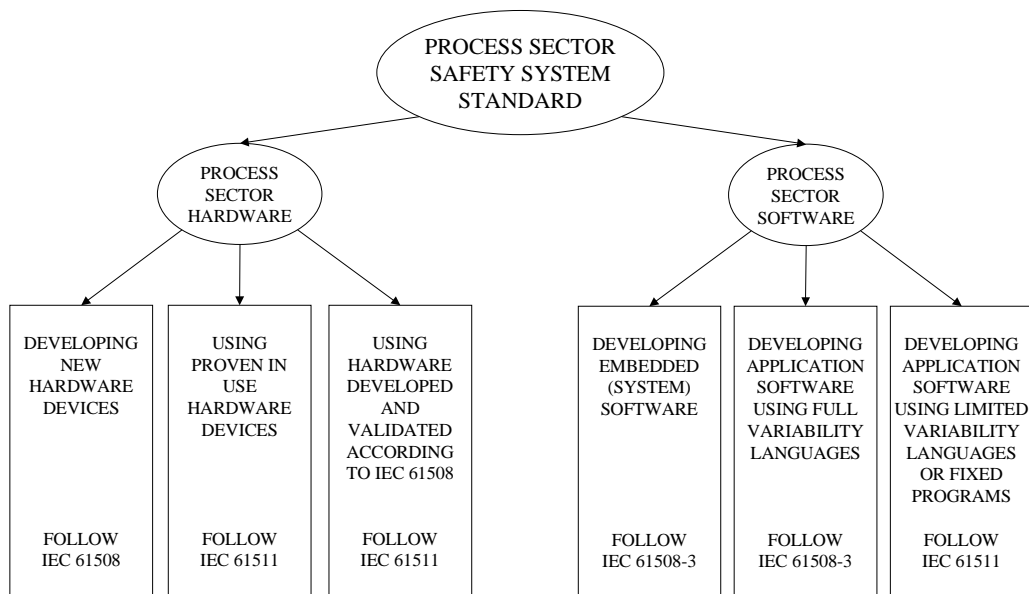


Figure 1

2 Part 2: Guidelines in the application of IEC 61511-1

Part 2 contains sections on scope, definitions and abbreviations (same apply as for part 1), and 6 informative annexes. Part 2 generally contains information and guidelines on IEC 61511, Part 1. Annex A gives a brief overview of the requirements of clause 5 (functional safety management), 6 (safety lifecycle requirements) and 7 (software requirements) of IEC 61511 Part 1 and sets out the functional steps in their application. In this way, this part of IEC 61511 corresponds to part 6 of IEC 61508.

Annex B refers to example techniques for calculating the probabilities of failure on demand, either from IEC 61508, Part 6 Annex B or ISA TR84.0.02. Annex C provides an example of the application of IEC 61511, Part 1 in a chemical company, i.e. a typical SIS architecture development.

Annex D provides three examples of the application of IEC 61511, Part 1, related to various aspects of application programming. It gives information on attributes of a programming language for SIS, an example of the development of application code for a process sector programmable electronic SIS, and an example that illustrates how a major SIS logic solver manufacturer/integrator develops safety application software for customers. Annex E provides

an example of a safety PLC manufacturer's approach in developing a programmable logic solver certified to IEC 61508 for the process sector.

Annex F contains an overview of relevant safety techniques and measures relevant to Parts 1, 2, and 3 of this standard, shortly stating, aim, description and reference of the specific technique. It only gives an overview of additional process sector references. For other techniques it refers to IEC 61508, Part 7.

3 Part 3 Guidelines in the Application of Hazard & Risk Analysis

This part of IEC 61511 contains guidelines in the area of selecting safety integrity level (SIL) in hazards and risk analysis, and in this way corresponds to Part 5 of IEC 61508. The information is intended to provide a broad overview of the wide range of global methods used to do hazards and risk analyses. It provides information on the underlying concepts of risk and the relationship of risk to safety integrity and a number of methods that should enable the safety integrity levels for the Safety Instrumented Functions to be determined.

IEC 61511, Part 3 consists of a clause on the underlying concepts of risk and the relationship of risk to safety integrity (general guidance), see figure 2. Furthermore there are several informative annexes, of which Annex A covers the ALARP principle (As Low As Reasonably Practicable) and tolerable risk concepts.

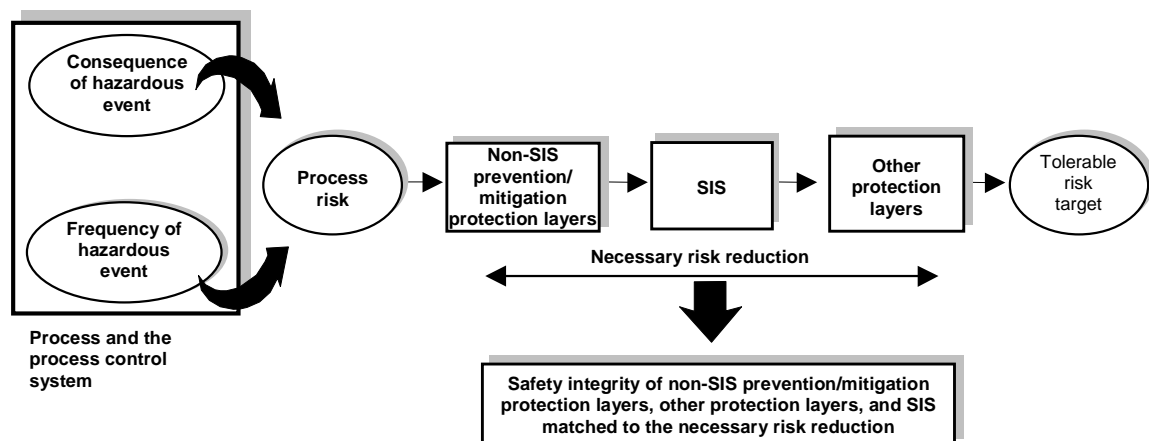


Figure 2 Risk and safety integrity concepts

Part 3, Annex B through F cover both quantitative and qualitative approaches to SIL selection. These include a qualitative method (the Safety Matrix Method), a Calibrated risk graph (semi-quantitative), a risk graph (qualitative), and Layer Of Protection Analysis (semi-quantitative) are described. All methods have been simplified in order to illustrate the underlying principles. The information provided is not of sufficient detail to implement any of these approaches.

Overall, IEC 61511 is considered a standard for users. Figure 1 even shows that. It is expected that engineering companies and instrumentation users will find the most value from this document.

exida.com is an internet based knowledge company focusing on automation safety and reliability. Training courses on all aspects of IEC 61511 are available. Manuals, books and self-study guides are available on our website, www.exida.com. Coaching and consulting services to cost effectively implement IEC 61511 are proudly offered.