

# Implementing IEC61508 in the Process Industries

Dr. Eric W. Scharpf  
Partner, [exida.com](http://exida.com)  
[escharpf@exida.com](mailto:escharpf@exida.com)

Dr. William M. Goble  
Principal Partner, [exida.com](http://exida.com)  
[wgoble@exida.com](mailto:wgoble@exida.com)

## Abstract

*IEC61508 and its process-specific companion IEC61511 are providing new codification to safety-instrumented systems and their application to the process industry. Setting the structure of the safety lifecycle and clarification of the safety integrity level generally enable companies to follow good engineering practice more readily. Experience shows that this clarification can uncover potential stumbling blocks in obtaining accurate failure rate data and insuring the competence of personnel involved throughout the safety lifecycle. Fortunately, solutions and guidance through these issues with improved databases, training, and official qualifications are becoming available via certification bodies and specialty consultants.*

## 1. Introduction

The final parts of IEC61508 [IEC98] were passed in February 2000. This standard resulted from many years of work by many of the world's experts and represents a consensus on the best methods to use when designing and operating a safety critical system. Although IEC61508 is an "umbrella" standard meant to cover many industries; chemical, petrochemical, oil and gas, etc. This can readily be seen by looking at the company affiliations of committee members. IEC61511 is the process specific standard, recently out of committee. It is expected that this standard will become dominant for process control industry users, while IEC61508 remains the standard for use in equipment and engineering company certification.

There is a great deal to be learned from IEC61508, especially for application in the process industries. From this material, two things stand out from our perspective. The first is the use of a well-defined "safety lifecycle" that requires risk-based design targets for safety to be established. The second is that these targets are order-of-magnitude targets called "safety integrity levels."

The safety integrity levels (SILs) from both the ISA84.01 [ISA96] standard and the IEC61508 standard establish order of magnitude targets for risk reduction. Although the standard covers both "continuous or high demand mode" and a "low demand" mode, for the process industries the low demand mode is most relevant. This comes from the classification of the continuously operating electric/electronic/programmable electronic (E/E/PE) control systems that maintain the normal, safe process operating conditions as part of the process itself, rather than as part of the safety instrumented system. Thus the E/E/PE devices in the safety instrumented system only become active on demand, and are therefore classified as low demand mode. For the low demand mode, the standards use the terms "probability of failure on demand," "probability of failure to function on demand," or "probability of dangerous failure." These terms are abbreviated as "PFD." This is the probability that a system designed to prevent an accident will fail to prevent the accident when needed. Risk reduction of a system critical system is related to PFD. Figure 1 shows the safety integrity levels from the international standards, with the defined probability of failure on demand and risk reduction factor.

Safety integrity level	Probability of failure on demand (PFD <sub>avg</sub> )	Risk reduction factor (ÄR)
4	$10^{-4} > \text{PFD}_{\text{avg}} > 10^{-5}$	10,000 ÄR < 100,000
3	$10^{-3} > \text{PFD}_{\text{avg}} > 10^{-4}$	1,000 ÄR < 10,000
2	$10^{-2} > \text{PFD}_{\text{avg}} > 10^{-3}$	100 ÄR < 1,000
1	$10^{-1} > \text{PFD}_{\text{avg}} > 10^{-2}$	10 ÄR < 100

Figure 1. IEC61508 safety integrity levels

## 2. The safety lifecycle

Another fundamental principle of IEC61508 is the “safety lifecycle (SLC)” defined in the document. Clearly, the SLC comes across as good engineering practice—almost common sense. But one important aspect of this SLC is that when risks and hazards are identified, they are evaluated and a target design SIL is established. In many companies in the process industries, this is not standard procedure.

The target design SIL is established based on the needed risk reduction. Risk reduction in the process industries is typically accomplished using more than one mechanism and more than one type of technology. A number of individual protection mechanisms, each with a risk reduction factor, may be required to reach the total risk reduction factor requirement. Some risk reduction mechanisms reduce the probability of an event. Others reduce the consequences of an event. These risk reduction mechanisms are known as “layers of protection.” This is illustrated in Figure 2.

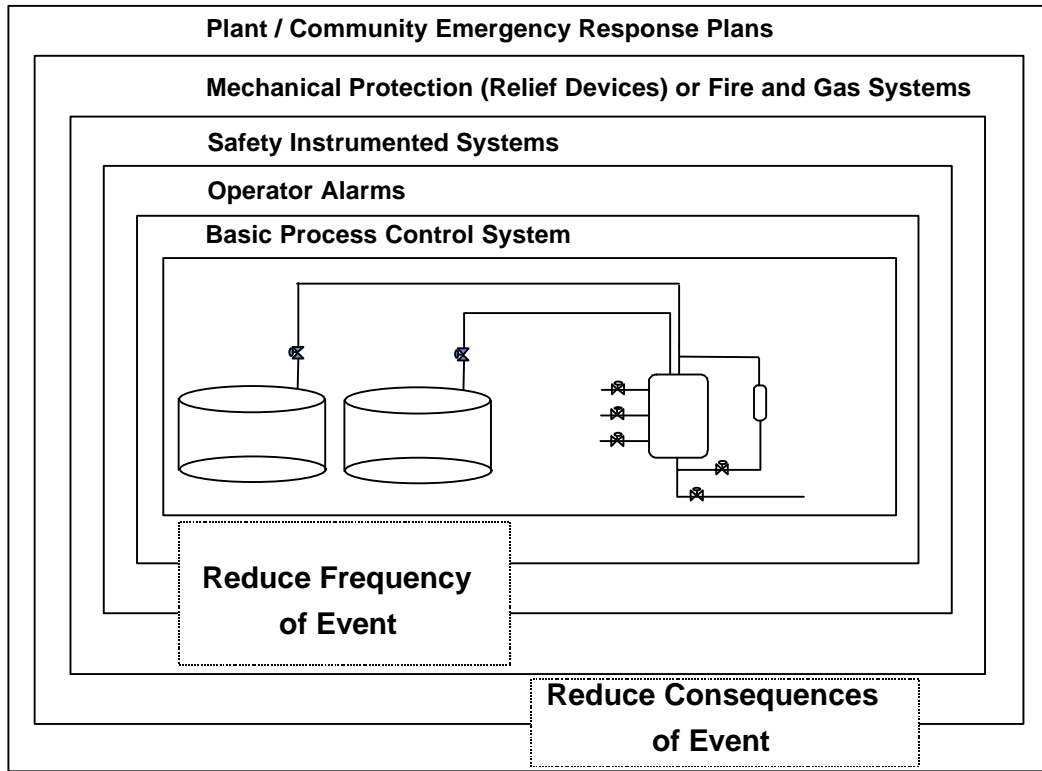


Figure 2. Layers of protection

The risk reduction factor from each independent layer can be combined to obtain the total risk reduction factor. This process is known as “layer of protection analysis (LOPA)” and is becoming commonly used to establish the target design SIL for the safety critical system.

The safety lifecycle process (Figure 3) further includes safety system design and, most importantly, design verification. The PFD for each section of the safety system hardware is calculated. Then, based on the

SIL chart, each design must meet or exceed the requirements established during risk and hazard analysis. This aspect of the SLC provides a “closed loop” checking system that helps make sure designs are optimal for the need. Overkill designs with too much redundancy are identified, and in most cases changed. Designs lacking the needed safety integrity are also identified and strengthened to meet design goals.

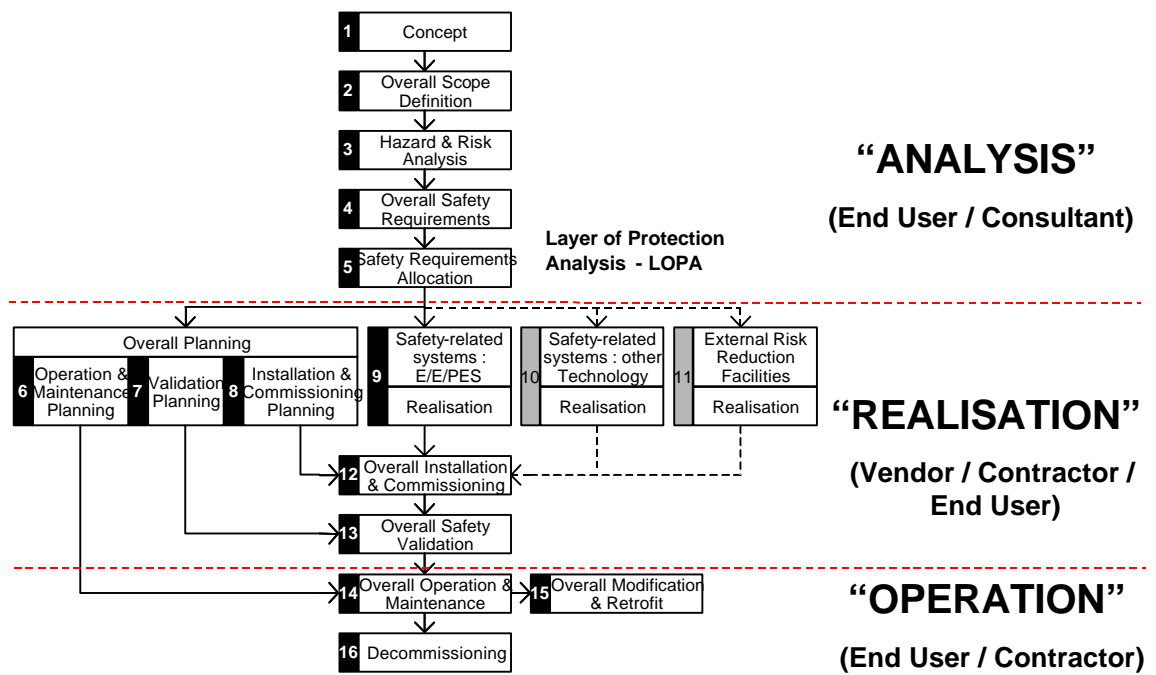


Figure 3. IEC61508 safety lifecycle

The SLC process includes maintenance planning. A periodic test plan is created showing what components of the safety systems are to be tested on what schedule. The periodic testing schedule is calculated as part of the design verification. Operation, maintenance, and even decommissioning complete the SLC.

### 3. Experience, problems, solutions

While the SLC concept detailed in IEC61508 seems so logical and so much like common sense, there have been a number of problems uncovered in helping several companies implement IEC61508. The main issues uncovered to date involve failure rate data and personnel competency.

The design verification step in IEC61508 requires that a  $PFD_{avg}$  calculation be made for the hardware in each safety instrumented function (safety loop) in the system. Using the SIL chart, a “design SIL” is established and compared to the target SIL. Designs with too much redundancy are usually updated to increase availability or decrease cost. Designs lacking sufficient safety integrity must be upgraded to reach goals. (Although some cases have resulted in a review of the target design SILs!)

To calculate a  $PFD_{avg}$  for a collection of safety hardware, failure rates, failure mode distributions, and possibly the self-test diagnostic test, coverage factors must be obtained for each component. While there are

industry databases available with failure rates and failure mode distributions, these are somewhat generic and should be adjusted for specific site conditions. Occasionally, the user company has a good database, and site-specific data is always preferable to generic database numbers. In some cases, there is little data available and the analyst must take the best data they can find and use it.

Fortunately, things are getting better. Equipment manufacturers that have their equipment third-party certified for IEC61508 applications (by organizations such as TUV Product Service, IQSE [Fal96], or Factory Mutual Research Corporation [FMR99]) will have failure rate, failure mode, and diagnostic coverage data available. This analysis is being done using consistent, conservative methods [Bel84]. This data should be published by the equipment manufacturer. Although this data also should be adjusted to take into consideration site-specific operating conditions, this is a substantial improvement in data. Databases are being compiled of this new data and other data sources [Exi00] to provide quickly accessible information to cut the cost of IEC61508 compliance. The AIChE Centre for Chemical Process Safety (CCPS) also has established a process equipment reliability database (PERD) project to help companies collect and share better equipment reliability data.

## 4. Personnel competency certification

Another big issue faced by companies that implement IEC61508 is the verification of personnel competency. Personnel who design, implement, maintain, and operate safety-instrumented systems are required to be competent in the activities they have been assigned. Although this requirement is self-evident, it is also codified into national and international standards: "...ensuring that applicable parties involved in any of the overall E/E/PE or software safety lifecycle activities are competent to carry out activities for which they are accountable." [IEC 61508, Part 1, Paragraph 6.2.1 (h)]. IEC61508 also states in Part 1, Appendix B: "All persons involved in any overall, E/E/PES, or software safety lifecycle activity, including management activities, should have the appropriate training, technical knowledge, experience, and qualifications relevant to the specific duties they have to perform." That makes good common sense, but how does one verify that? Another statement in IEC61508 reads, "The training, experience and qualifications of all persons involved in any overall, E/E/PES, or software safety lifecycle activity, including any management of functional safety activities, should be assessed in relation to the particular application." Many companies are concerned that there has been no guidance on how this assessment should be done. There is concern over consistency, cost, and liability.

The need to insure the right level of knowledge and skill of all persons working on safety systems is a problem for everyone, not just operating companies. It is easy to imagine potential liability issues of engineering companies. One would think that the operating companies might even demand IEC61508 compliance statements from the engineering companies.

In the process industries, work has indeed been done on this problem as well. There has been a pioneering effort by members of the IICA in Australia, and a detailed method of competency evaluation was created. Based on this and other input, TÜV Product Service, IQSE, has announced their new "Certified Functional Safety Expert" program [exi00a]. The certification process involves a review of an individual applicant's background and the satisfactory completion of a proficiency exam. The background review includes proof of completion of relevant training, review of relevant professional experience, and statements from professional references. Successful applicants will receive a certificate of competency in one of three disciplines: 1) *Application Engineering*. Personnel who are involved in implementing safety instrumentation at end-user facilities and processes should be certified in application engineering. End-user facility personnel, engineering firms, and systems integrators typically perform application engineering tasks. 2) *Development Engineering*. Personnel who are involved with the

design of electric, electronic, or programmable electronic devices for use in safety applications should be certified in development engineering. Equipment vendor development personnel typically perform development engineering tasks. 3) *Safety Lifecycle Management*. Personnel who are involved with scheduling, budgeting, and oversight of development and application of instrumented systems in safety applications should be certified in safety lifecycle management. Safety lifecycle management applies to both the equipment development and application processes for vendors and users.

There are three certification exams, corresponding to the three categories of competency. Each of the tests contains multiple questions. The participant is only required to answer a subset of the questions: typically those that are most relevant to the test-taker's experience and job responsibilities. For many companies, this represents a consistent and inexpensive way to comply.

## 5. Conclusion

The IEC61508 had parts approved in 1998 and the final sections approved in 2000. In the short time since its approval, several companies in the process industries have embraced the concepts from that document and have begun programs to comply even though the industry specific standard, IEC61511, is not yet complete. Initial projects have shown that benefits in design optimisation are valuable. The assurance that risks and safety system design are matched is another solid benefit. This performance-based standard permits the flexibility to do the optimal job.

While there are clearly problems in getting failure data, insuring the competency of personnel, etc., solutions are becoming available through certification bodies and specialty consultants.

## 6. References

[Bel84] "Reliability Prediction Procedure for Electronic Equipment," *Bellcore Technical Advisory* TA-000-23620-84-01, Bell Communications Research, Redbank, NJ, USA, 1984.

[exi00] Failure rate database for industrial equipment, [www.exida.com/databases](http://www.exida.com/databases), exida.com LLC, Sellersville, PA, USA, 2000.

[exi00a] Certified functional safety expert paper, [www.exida.com](http://www.exida.com), exida.com LLC, Sellersville, PA, USA, 2000.

[Fal96] R. Faller, "Aspects of TÜV Type Certification and Safety-Related Application of Programmable Electronic Systems," *Safety in the Process Industry, Yesterday, Today and Tomorrow, Proceedings*, Eindhoven University of Technology, Netherlands, September 1996.

[FMR99] Factory Mutual Research Corporation, "Approval Report—Quadlog/ProSafe PLC comprising CCM, CDM and SAM," Siemens Process Automation Solutions, Spring House, PA, USA, 1999.

[Gob98] W. M. Goble, *Control Systems Safety Evaluation and Reliability*, 2d ed., ISA, Research Triangle Park, NC, USA, 1998.

[IEC98] IEC61508, *Functional Safety of electrical / electronic / programmable electronic safety-related systems*, IEC, 1998, 2000.

[ISA96] ISAS84.01, *Application of Safety Instrumented Systems for the Process Industries*, ISA, Research Triangle Park, NC, USA, 1996.

## 7. Author information

Dr. Eric W. Scharpf has a Ph.D. in Chemical Engineering from Princeton University, USA. He has spent much of his career working on process optimisation, new process design, and risk analysis in the chemical processing industry. Dr. Scharpf has authored numerous patents on various operating and process efficiency improvements. He is now a partner in exida.com, a company that does consulting, training, and provides support for safety-critical and high-availability process automation. Dr. Scharpf is based near Dunedin, New Zealand, and teaches at the University of Otago. Email: [escharpf@exida.com](mailto:escharpf@exida.com). Phone/fax: +64 3 472 7707.

Dr. William M. Goble is currently a principal partner in exida.com, a company that does consulting, training, and provides support for safety-critical and high-availability process automation. He has over 25 years of experience in the research and development of control systems doing analogue and digital circuit design, software development, engineering management, and marketing. Dr. Goble has a Ph.D. from Eindhoven University of Technology in Eindhoven, Netherlands. He is an adjunct professor at the University of Pennsylvania and has authored the ISA book *Control Systems Safety Evaluation and Reliability*. Dr. Goble is an ISA fellow member and a member of the ISA's SP84 committee on safety systems. Email: [wgoble@exida.com](mailto:wgoble@exida.com). Phone: +1 215 896 7170. Fax: + 1 215 257 1657.