

↵  
↵  
↵  
↵  
↵  
**STATE-OF-THE-ART SAFETY VERIFICATION**  
↵  
↵

**Dr. Eric W. Scharpf and  
Dr. William G. Goble**

↵  
↵  
**Partner, exida.com, escharpf@exida.com and  
Principal Partner, exida.com, wgoble@exida.com**

↵  
↵  
↵  
**Abstract:** The past few years have brought significant changes to the control safety field in both technology (i.e., fieldbus) and regulation (i.e., IEC 61508). Globalisation has further compounded the increased challenges of keeping pace and the consequences of falling short. Experience in this environment has shown the value of recently developed Web-accessible database and analysis tools to assess and verify the Safety Integrity Level (SIL) of existing and proposed systems. Similarly, improved communications technology has allowed process industry firms to tap into a broader range of specialised expertise for both identifying and addressing critical risk management issues.

↵  
**Keywords:** Safety, Database, SIS, SIL, IEC 61508.

↵  
↵  
↵  
↵  
**1. Introduction**  
↵

The controls technology revolution has made its impact in the field of safety just as strongly as in the other specialties. On the equipment side, we face the task of properly assessing the safety and reliability of the many new—and thus unproven—systems. One of the technology-driven challenges facing the safety community has been the debate over control and safety system segregation. The new controls technology is consolidating more and more functions into single modules, while the safety standards and philosophy strongly support a segregation of functions (IEC, 2000). This apparent conflict has led to questions over where the control system ends and the safety system begins; answers differ depending on the perspective of the observer. Thus end users are faced with having to justify their choices in an ambiguous and increasingly litigious environment.

The standards and framework committees also have been generating significant change. Standards are now driven largely on the international level, rather than by the more traditional efforts of national organisations in individual countries and markets. Today, one often finds that DIN xxx and ISA yyy are superseded by IEC zzz. Many of the new

international standards attempt to guide users toward an overall safety life cycle approach, but the language and details are not always clear.

As if these rapid developments in technology and standards provided insufficient change, the business and trade communities have added to the mix. Increased freedom in world trade has made for intense competition across previously segregated markets, thus significantly raising the standards for performance and price. This globalisation has had two main related effects. The first is industry consolidation, as evidenced by the large number of recent corporate takeovers and mergers. The second is the additional push toward standardisation driven by the single global platform programs within many of the surviving firms.

Despite the eventual clarification that these business and regulatory trends should produce, we are now near the point of maximum flux in the overall situation. The industry consolidations are not yet fully integrated. There is still a lack of clarity in what product lines will be consolidated and what will remain as well as an uncertainty in which firms will focus on which regional markets. Also, although the primary international safety standard IEC 61508 has been issued, many other supporting standards remain in progress and acceptance at the national level is by no means consistent or universal. Thus we are currently experiencing the both the curse and the blessing of “living in interesting times.”

## 2. Safety Analysis Techniques and Tools

### 2.1 The Safety Life Cycle

└

The recently released IEC 61508 standard attempts to facilitate the development of more specific standards for different application sectors as well as to provide support for safety system development where no specific sector standards exist. (IEC, 2000) It presents a generic safety life cycle (SLC) structure including phases from “concept” through “decommissioning.” The key themes of the IEC 61508 SLC are to analyse, design, verify, and document. There is some leeway in the precise execution of the life cycle phases, but the stated measure of compliance is that the resulting safety-related system meets the requirements in the standard (IEC, 2000). Experience has shown these requirements can be achieved most readily through adherence to the standard’s key themes, as shown in Figure 1.

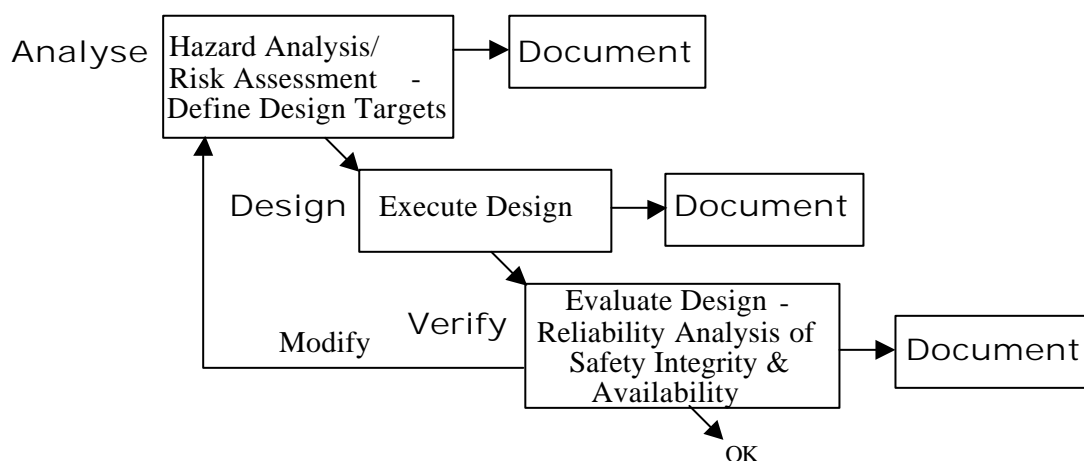


Fig 1. Key Safety Life Cycle Themes.

Many examples of SIS over-design (too much redundancy), SIS under-design (not enough risk reduction), and SIS design mismatch (single sensors and TMR logic solvers) have wasted money. These are exactly the problems that the safety lifecycle approach was designed to catch. Designers recently trained in the use of the technique have been able to

save both time and money with more optimal SIS designs. The primary result of the safety lifecycle process is this kind of optimal SIS design that matches risk reduction with process risk while maintaining internal design consistency.↵

## 2.2 Safety Integrity Level Selection

↵

Assessment of the frequency and magnitude of hazards is vital to the analysis and verification components of the life cycle, and numerous potential options for this assessment are broadly described in the standard. Methods for assessing hazard frequency range from qualitative risk graph techniques, which can be very subjective and imprecise, to semi-quantitative and fully quantitative processes, such as event tree, fault tree, and Markov analyses. Methods for assessing hazard consequences also vary significantly, mostly based on the type of hazard being assessed. The results of these analyses help identify the required Safety Integrity Level (SIL) for a specific Safety Instrumented Function (SIF). The appropriate calculation and selection of this SIL, and its follow-through during the execution and operation phases, is what stands between a safe facility and an industrial catastrophe.

For the low demand mode relevant to the process industry, the four SIL levels are defined based on the required risk reduction factor or probability of failure on demand for the safety instrumented function (IEC, 2000). These definitions are summarised below in Figure 2.

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

Fig 2. IEC 61508 Safety Integrity Levels.

To be faithful to the overall safety goal in the most effective and economical way, these calculation methods must accurately take into account the benefits of other layers of protection that may be present for a specific hazard. In some cases, these layers of protection can sufficiently reduce the overall risk to a tolerable level on their own, thus eliminating the need for an additional safety related system and its accompanying expense and complexity. Therefore the proper identification of these layers of protection, the assessment of their contributions and common modes of failure, and their translation into an appropriate level of risk reduction are formally classified as Layer of Protection Analysis or LOPA. This has become an essential technique in safety assessment.

Event tree analysis is becoming the favoured method for LOPA and SIL selection because of its balance of quantitative accuracy and relative ease of use in an industrial setting (exida.com, 2000). The mathematics behind this method come from Bayes's Theorem of Conditional Probabilities, which is well suited for calculating the frequency of outcomes based on multiple condition sequences. The conditional probabilities input for this analysis come from a combination of site-specific experience for the systems in question supported by referenced external data for comparable systems. One of the challenges with the site-specific input for this analysis is the assessment of the common cause failure components of the conditional probability values. In many cases this part of the assessment will have a component of engineering judgement involved and thus must be justified as part of the

documentation. As will be discussed in Section 3, it is also not necessarily an easy task to collect the appropriate external referenced data.

### 2.3 Safety Integrity Level Verification

┘

Once the SIL has been selected and safety system design begins, additional analytical work is required to characterise any proposed Safety Instrumented System (SIS) to verify whether it meets the required SIL. This method has some commonalities with the conditional probabilities approach used in LOPA. However, there are some key differences related to assessing the appropriate contributions of internal system diagnostics and safe vs. unsafe failure modes through a detailed failure modes and effects analysis. In addition, common cause failures in redundant equipment, equipment test intervals, the completeness of those tests, offline repair times, and numerous other vital details also contribute to the calculation. Figure 3 shows the relationship between diagnostic coverage and RRF. Figure 4 shows the relationship between PFDavg and common cause. (Goble, 1998) The magnitude of the change is often surprising.

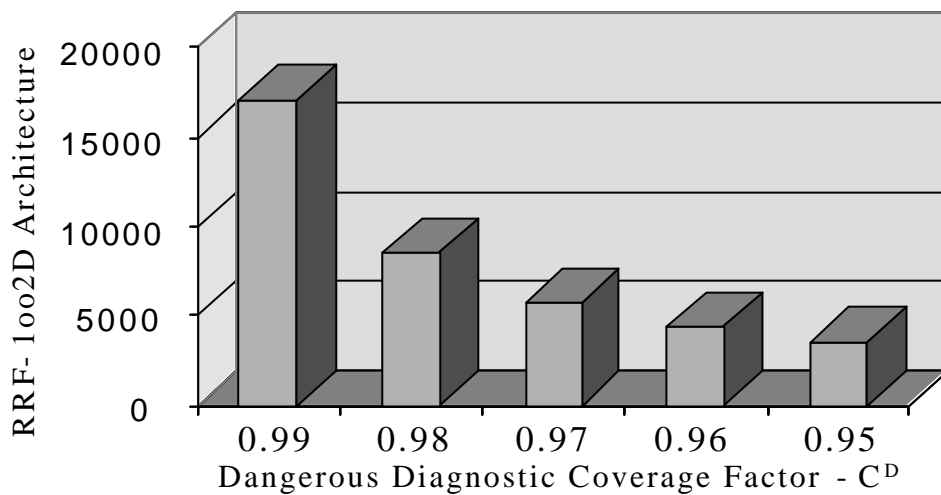


Fig 3. Effect of Diagnostic Coverage on Risk Reduction Factor for 1oo2D Architecture (Goble, 1998)

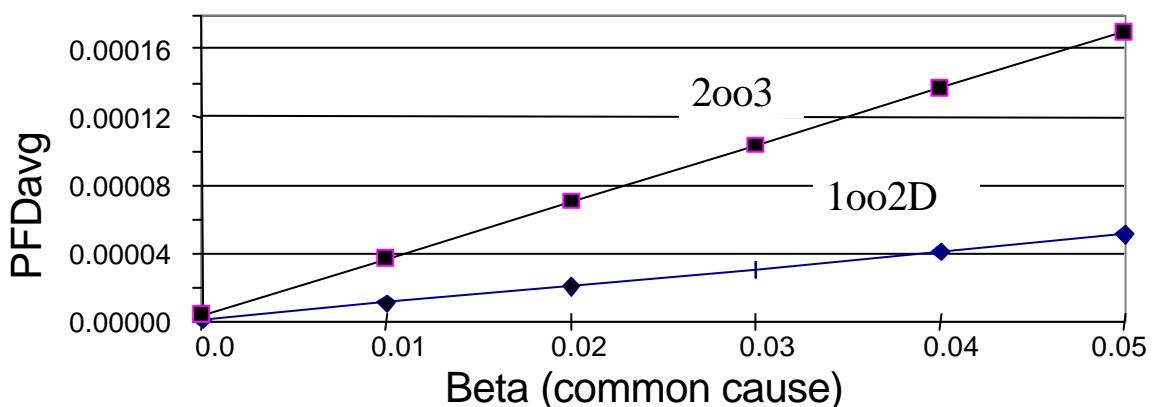


Figure 4 PFDavg versus common cause Beta factor.

As with many process plants, especially those that have been in operation over a number of years, there may be partially redundant systems in place with some shared, redundant, and/or parallel but diverse equipment configurations. These stumbling blocks further contribute to the complexity faced by those at the plant charged with responsibility for SIL verification.

An additional key issue in SIS design and SIL verification that often raises significant debate is the difference between safety and non-safety equipment and their segregation in total system design. Despite the desire of industrial users to use non-safety equipment for safety instrumented systems, the results are often disappointing. The basis for this poor performance is rooted in the much higher reliability, safe failure fraction, and diagnostic levels required of SIL certified safety systems (AS, 2000; IEC, 2000). By utilizing non-safety specific equipment designed to lower standards, one effectively degrades the overall system integrity to that of a system designed entirely from non-safety grade components. This degradation becomes readily apparent in proper SIL verification analysis, again underlining the importance of a robust analytic method.

As mentioned earlier with respect to SIL selection, developing and maintaining the procedures and tools capable of suitably rigorous analysis can be quite demanding and expensive. This high level of additional cost typically is difficult to justify, except perhaps by the largest process industry firms.

#### ***2.4 Documentation and Resources***

↓

Similarly important is the sufficiency and clarity of the documentation for SIL selection and verification to insure that functional safety is ultimately achieved. Methods must be consistent, logical, and verifiable. One of the best ways to insure this completeness and clarity is through an established, documented, and proven procedure. For SIL selection that procedure preferably should include a detailed, quantitative LOPA. Starting from this base, all aspects become more straightforward and, as a consequence, more consistent and more easily documented. This is even further the case when a proven computer-driven template with embedded calculations is available. In these situations it is vital that the calculations behind the software are well understood by an expert on the safety evaluation team so that nothing is assessed improperly.

Developing and maintaining an efficient and accurate safety program demand significant dedicated resources. In the current lean corporate environment this is only possible at the largest of the multi-nationals. Nearly all organisations can sustain dedicated controls expertise in their inherent technical specialty. However, safety often is a specialty focus and employing a complete, fully-dedicated safety staff simply is not always economically viable.

### **3. Reliability Data and Databases**

↓

Another, often challenging, piece of both SIL selection and verification procedures is finding accurate data for the calculations. This includes information on the sensors, logic control system, actuators, and final control elements that make up the safety system. Time-tested, site-specific data is the best but typically least available option. Next best, and increasingly more available in recent years, is specific data from manufacturers. The challenge with manufacturers' data is in the work to find, collect, and collate the information from different sources. Although vendors typically provide information only for their own products, one recent answer to this difficulty is the multiple-listing database. The AIChE Center for Chemical Process Safety has put together a notable database and is working on procedures for a more complete database (PERD, 2000). Also third-party safety service firms such as exida.com also maintain well-populated, up-to-date files.

At a minimum these files should contain probability of failure data and failure mode data for sensor, actuator, and final elements commonly used in safety and control systems. Ideally

these sources also should contain detailed information on the various logic boxes. At a minimum, this information also should include the type of system architecture used, different I/O types available, diagnostic coverage level, and safe failure fraction.

An additional question present in all of this is, “How reliable is the reliability data itself?” The best way to insure data reliability is to look for the original source. TÜV, Factory Mutual, and specialty companies like exida.com use consistent methods including detailed failure modes, effects and diagnostic analysis (FMEDA) that provide conservative and comparable data. Their evaluation, documentation and testing procedures for equipment are rigorous and the data resulting from this level of work can be treated with confidence.

#### 4. Applications and Conclusions

↓

The process industry is faced with a clear need and code-required call for rigorous, documented safety analysis based on solid techniques and solid data. In the current competitive environment and rapidly changing regulatory climate, it is a significant stretch for many moderately sized organisations to properly address this need. As a result, several third-party safety specialist organisations have emerged that provide these services.

As a leader in this field, exida.com has pioneered the use of these safety tools, databases, and personal expert support and delivers these services via the Web. These systems have the advantage of accessibility from any telephone, assurance of up-to-the-minute revision, ease of use, and individual support through video, telephone, email, and in-person contact. The users automatically link directly to both the tools and databases, as shown in Figure 5.

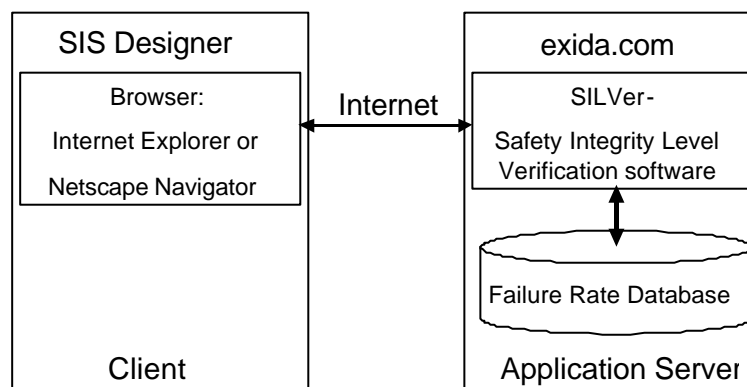


Fig 5. exida.com Software Function, Use, and Support Configuration

Thus control engineers at a production facility are able to use their desktop computers to access directly the tools, data, knowledge and expertise of an entire team of safety specialists.

#### 5. References

Australian Standard 3814, *Industrial and commercial gas fired appliances*, (2000).

exida.com, “Probe™ Layer of Protection Analysis”, [www.exida.com/services/articles](http://www.exida.com/services/articles), (2000).

International Electrotechnical Committee 61508, *Functional safety of Electrical / Electronic / Programmable Electronic Safety Related Systems Part 1*, (2000).

Goble, W.M., *Control System Reliability and Safety*, ISA, (1998).