

Safety Integrity Level Verification – Process and Problems

December 2000 Dr. William .M. Goble

The Safety Lifecycle

The safety lifecycle (SLC) is one of the fundamental concepts presented in the ANSI/ISA84.01 and IEC61508 functional safety standards. Once OSHA in the US stated that ISA84.01 is “a recognized and generally accepted good engineering practice for SIS,” the SLC got a lot of attention and many companies in North America have begun implementation. Likewise in the rest of the world. IEC61508 passed in Feb. 2000 and for the first time an international standard for functional safety existed. Many multinational companies in particular are reviewing their standards with a view toward IEC61508 reconciliation. Besides, the SLC is a good idea. The SLC helps optimize safety instrumented system (SIS) design by matching the SIS design to the risk reduction requirements of the process.

The SLC is a good common sense engineering procedure that can be summarized in three steps:

1. analyze the problem,
2. design the solution and
3. verify that the solution solves the problem.

This is illustrated in Figure 1. The problem analysis step involves hazard identification and risk analysis. Potential hazards with enough risk may warrant the design of a safety instrumented system (SIS). For those hazards, a target safety integrity level (SIL) is assigned according to risk reduction targets. In step 2 the SIS is designed to meet the SIL targets. This design process involves selecting the technology to be used, selecting particular pieces of equipment and configuring that equipment with enough redundancy to meet both the safety requirements and the process uptime (availability) requirements.

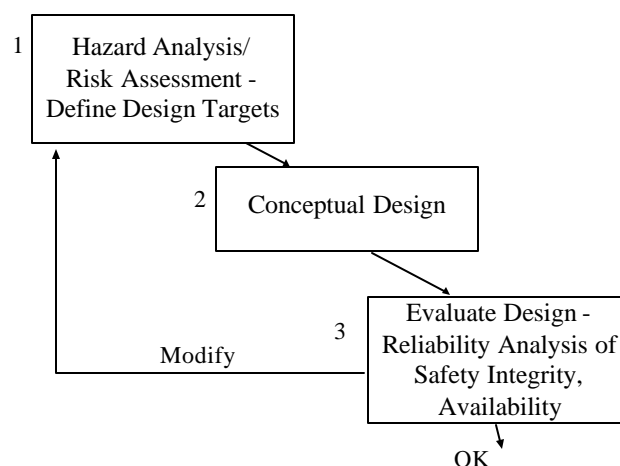


Figure 1: Three basic steps in the safety lifecycle.

SIL Verification

For any given SIS design, a failure probability calculation and risk reduction factor (RRF) calculation is done to verify that the SIS design meets the target. If the design does not meet the RRF goals, better equipment can be chosen or redundancy can be employed. If IEC61511 or IEC61508 compliance is also an objective, the Safe Failure Fraction (SFF) is also calculated. Different levels of redundancy are required for each target SIL depending on the SFF number regardless of the RRF calculation.

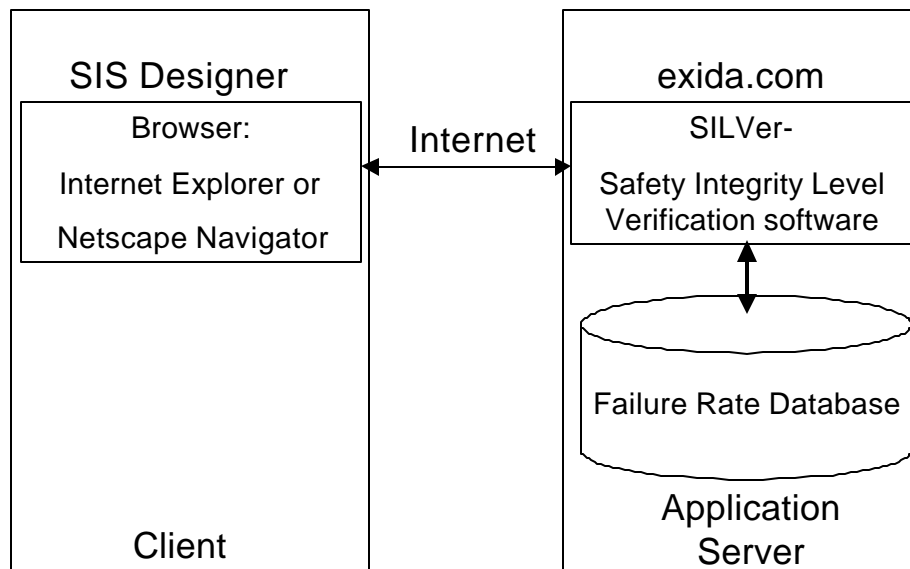
These RRF and SFF calculations seem easy enough. We have a brand Y pressure transmitter, a brand Z PLC and a brand X solenoid valve. One can just pull out the product data sheets and get the failure rate data. They should be printed just like any other specification. But a careful study of current product data sheets rarely shows anything. No problem, just call the sales engineer and get the failure rate data. Unfortunately in many cases, the sales engineer has never heard of safe failure rate, dangerous failure rate and diagnostic coverage factor. However, he will call the factory and get back to us. Several weeks and many hours of follow-up work later we are still looking for the data.

Even when failure data is obtained there is the issue of doing the calculations. Most Reliability Engineering textbooks have simple equations with good explanations of those equations but no mention of safe versus dangerous failure modes. Can those equations be applied to SIL verification? And how do we take into account the periodic inspection interval? How do we take credit for the automatic diagnostics built into the system? How do we adjust the calculations for different kinds of sensors on the same process variable? ISA is working on a technical report that covers the issues and ISA publishes a book on control systems safety that covers the subject. A study of that material is time consuming and often additional questions remain. Those equations look very long. And forget those Markov models.

These are just some of the realities of new engineering procedures. Not a good situation but things are getting better rapidly. Several equipment manufacturers who have equipment certified to IEC61508 by competent bodies like FM or TUV publish the failure rate data in much way as they publish temperature specs or accuracy ratings. It is true that the standards do not precisely specify how the failure rates are done. This means that one cannot compare numbers from different manufacturers. But for purposes of SIL verification these numbers are more than sufficient. Other manufacturers catering to the SIS market are working on providing the data as well.

There are several computer based SIL verification tools now available to help with the calculation. Some equipment vendors have programs available for use

with their equipment. Some independent tools are stand-alone WINDOWS applications. Others, like the new tool SILVer from exida.com, are available to use over the Internet from anywhere by using a browser. (Figure 2) The SILVer tool not only does the math but solves the other big problem, failure rate data. Exida maintains a database of failure rate, diagnostic coverage and safe failure percentage data from many major manufacturers. While not all products are there yet, if any user needs a particular piece of data, exida will either get the information from the manufacturer or estimate the value based on our experience with detail FMEDA (Failure Modes Effects and Diagnostic Analysis). The



database is constantly growing in content and accuracy.

Figure 2: Application Server – Client Architecture

The future of SIL Verification

Those who have tried to do SIL verification in the past know that it has been a frustrating process. It has been so frustrating that some have even questioned the whole SLC process. If the pain of the past continues, the SLC process will not show its real benefits. The lack of failure rate data and the complexity of calculation methods has been a serious impediment to SLC adoption. Fortunately SIL verification is getting much easier. With new databases, new SIL verification tools and on-line assistance via the Internet, the SLC process can progress. Hopefully the economic rewards of optimizing SIS designs will come to more and more companies as the ease of implementation increases.