

Selecting the Right Safety Equipment
Safety Control and Instrumentation Systems Conference
Singapore, March 2008
Eric Scharpf, Ray Wright, and David Ong



Text

ABSTRACT

This paper presents various solutions to the problem of safety equipment selection faced by system designers and plant project teams. It begins with a discussion of how it is often possible to meet plant safety requirements without SIL rated safety functions. Then for cases where SIL rated safety functions are needed, it looks at the differences between equipment selected on “proven in use” criteria and fully 61508 certified equipment with an eye toward finding the best match between cost, hassles, requirements and practicality. This includes considerations about how to reduce risk from systematic failures and what to look for in certification reports.

INTRODUCTION

Electrical and electronic controls are being used in more and more applications throughout the process and manufacturing industry, in both regular control and safety service. That means the traditionally obvious hazards from poor safety equipment selection are now joined by an increasing number of not-so-obvious safety equipment hazards. Unfortunately these not-so-obvious hazards can lead to frightening consequences, with millions and in some cases even billions of dollars in damage plus many lives lost.

As you might expect, there are a number of new standards in use to help manage these hazards. As you might not expect, there is a lot of value underneath all of the bureaucratic language that helps you set your risk management targets and actually achieve them as effectively and efficiently as possible. The IEC standards 61508, 61511, and 62061 put forward a very useful process called the safety lifecycle to help companies identify risks, develop electronic safety controls to manage those risks, and run their plants and factories with minimal chance of accidents.

SAFETY LIFECYCLE AND EQUIPMENT SELECTION

Overall considerations:

The overall philosophy of the safety lifecycle is similar to the ISO 9000 quality idea of planning the work, executing the work, measuring the results, and fixing the things that fall short. This provides a very powerful way to manage both random hardware failures from equipment operated within its design guidelines and the various systematic failures that can creep in throughout the planning, design and operation phases. It is worth noting that many of the recent major accidents in the process industry are the result of systematic failures. One dramatic example of this is the 2005 BP disaster in the US where the subsequent investigation by the Baker Panel found serious concerns about safety management, oversight and a “longstanding deviations from good safety practice”. [Baker et. al. 2007] Systematic failures are defined where there is a clear deterministic error that could have been corrected by modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors. Specification errors, poor maintenance procedures, incorrect equipment selection or installation errors are classic examples of systematic failures.



Selecting the Right Safety Equipment

Safety Control and Instrumentation Systems Conference

Singapore, March 2008

Eric Scharpf, Ray Wright, and David Ong

Text Continued



Look for simple solutions first:

The other item to note is that electronic safety controls are only part of overall process and machine safety. In fact it is often easier (and more effective) to solve a safety problem at the process or mechanical equipment level rather than trying to fix it with a more complex electronic safety system. Fortunately the standards not only allow this, they directly encourage it.

A detailed layer of protection analysis (LOPA) is one of the most effective ways to look at what risk reduction methods and equipment you have already and what additional elements you might need to manage risk. LOPA basically identifies and estimates the effectiveness of all of the different safeguards that reduce the chance of a potential accident. The result is typically an estimate of the frequency of the potential accident along with the target SIL for potential safety instrumented functions to reduce the risk to a tolerable level. With this focus on specifying SIL rated functions, they may miss some valuable non-SIS opportunities. It is usually possible with a minimum of additional effort to take a wider perspective that includes a specific focus on improving existing non-SIS risk reduction and identifying new non-SIS layers of protection. With this wider perspective, it is usually possible to reduce the requirements for any more complex SIL-rated functions and often eliminate a number of those functions entirely. The end result is the optimum combination of mechanical, process and intrinsic safety measures along with the SIL-rated functions to give the best balance of low cost, simple operation, and low risk from both systematic and random failures.

SIL rated equipment requirements:

For the more complex SIL-rated safety functions, you have to make sure that they are designed with the correct equipment to properly detect or sense that harm is imminent, decide what action to take, and then carry out that action to bring the process or machine to a safe state. The performance of each function is defined by its SIL along with a whole host of related equipment and procedure requirements to ensure that the overall safety function actually meets its SIL-rated performance for both random hardware failures and systematic failures.

As with all instrumentation and control applications, each equipment element used in a safety system must meet the specific application requirements as a first line of defence against systematic failure. However for SIL-rated applications there are three additional things that must be true. First, the entire safety function must meet the SIL requirements for probability of failure on demand (PFDavg) to protect against random hardware failures. Second, the voting configuration of the function hardware elements must meet the architectural fault tolerance constraints for that given SIL and equipment safe failure fraction. And third, each instrument's design and design process must meet a sufficient safety integrity level (SIL) to also manage systematic failures. Since fit-for-service application requirements are usually well understood, and the calculation tools to determine the PFDavg and architectural constraints are generally available commercially, the focus is on the less understood design and design process requirements for each instrument in a SIL-rated application.

Selecting the Right Safety Equipment

Safety Control and Instrumentation Systems Conference

Singapore, March 2008

Eric Scharpf, Ray Wright, and David Ong

Text Continued



The design requirements for SIL-rated elements can be confirmed by one of two methods. The first is a “prior use” assessment done by the end user. Although the standards do not provide much detailed guidance, the idea is to prove that a component has demonstrated its performance long enough and under enough different conditions to justify relying on it as part of a SIL rated safety instrumented function. This method is fine for simple elements like the piping to an emergency vent system. Here it is very easy to send out a simple mechanical spec and for the supplier to provide pipe that clearly meets that specification and will perform as needed in the field. In such simple cases, there is no need to make things any more difficult. This idea can be extended to slightly more complex equipment. However, you must then assess the performance of each aspect of the equipment under a full range of expected operating conditions with a high enough level of confidence to sign up to the responsibility for each component to perform properly in each application. For anything much more complex than a solenoid, this method is usually not the best choice.

Component Type	Number of different 61508 certified components	SIL Capability
Pressure Transmitter/Switch	7	2-3
Temperature Transmitter/Switch	3	3
Level Transmitter/Switch	7	2-3
Flow Transmitter	2	3
Gas Detectors	1	3
Flame Detectors	1	3
PLC	15	3
Fire and Gas Controllers	3	2
Solenoid Valves	9	3
ESD Partial Stroke Monitors	6	3
Actuators	8	3
Ball Valves	4	3
Butterfly Valves	2	3
Globe Valves	4	3
Specialty Valves	4	3

Table 1: IEC 61508 Certified Components (All recognized certifying organizations)
(<http://www.exida.com/applications/sael/index.asp>)

Selecting the Right Safety Equipment
Safety Control and Instrumentation Systems Conference
Singapore, March 2008
Eric Scharpf, Ray Wright, and David Ong
Text Continued



The second method to confirm an equipment item for SIL-rated applications is third party assessment of the device's design "in accordance with" IEC 61508. Here the cost of the detailed assessment is built into the equipment price, but it is effectively shared by every company that also purchases the same equipment so any one company's additional cost can be quite low. While prior use assessment was the only alternative for most instruments some years ago, now instruments of most every category are available with IEC 61508 certification. (See Table 1.) However, there are still a number of hidden fish hooks to avoid in order to use such equipment properly.

Other Important considerations:

It is important to remember that the purpose of equipment certification is to reduce the risk of systematic design failures to a negligible level. Also the definition of "negligible" becomes more and more strict, the higher the SIL. For example a component certified for use in SIL 3 applications will need to have a hundred times lower risk of systematic design and application errors than a component certified for use in a SIL 1 function.

A proper 61508 assessment includes the failure modes, fail-safe vs. fail-danger, any automatic diagnostics claimed and internal redundancy. The result of the assessment is typically a set of quantitative failure rates used by the control system engineer to verify a particular safety function design along with a "SIL capability" rating and any associated restrictions. SIL capability means that an instrument may be used in a design up to the capability level. Note that this alone does not ensure that the entire safety function will meet that given SIL.

The SIL capability should take into account the complete component design process including specification methods, design methods, design tools, testing methods, review techniques and documentation. The instrument manufacturer's change process is also included as many design faults are made when the original design is modified. This is important for all products including simple mechanical devices as design mistakes can cause dangerous failures, but it is more important for products that contain complex integrated circuits and software. The results should present a "Safety Case" which describes how an instrument manufacturer meets each requirement of IEC 61508. The safety case should be summarized in a certification report that is openly available to all prospective buyers.

What to look for with certified equipment:

Fortunately, if you are buying equipment designed for safety applications with a 61508 compliance certificate from a good third-party certification firm, this information will be accurately determined, relatively easy to find, and in a form that is relatively easy to use. However, it is important to be careful here since all certifications are not created equal.

Selecting the Right Safety Equipment

Safety Control and Instrumentation Systems Conference

Singapore, March 2008

Eric Scharpf, Ray Wright, and David Ong

Text Continued



The first problem is how much should you believe the information for your particular application. You will need to look at both the certification report and the equipment safety manual to confirm that the values are good. Remember that process control applications and safety instrumented system applications are different and that instrumentation does not behave the same in those different applications. Consider a valve. In a process control application, the valve is likely to move frequently. In a safety instrumented system close to trip application, the valve likely sits in a static (full open) position for long periods of time. Data gathered in one application must be carefully considered as it may not be applicable to the other application. You will need to check how the failure rate information was evaluated and confirm that it matches how you will be using the equipment.

Another problem is that most equipment does eventually get a certificate. For reputable certification firms, this means that lower performance equipment will have a large number of restrictions on how it can be used in different SIL-rated applications. These restrictions will be clearly documented in both the equipment safety manual and in the certification report. For example, one product manufacturer might require the use of two sets of input and output modules for safety applications in the safety manual. Duplicate equipment may be impractical and will certainly be costly. Before you make a purchase, be sure to look at the certification report and equipment safety manual to confirm they provide you with all of the information you need, and that any restrictions do not prevent you from effectively using the equipment in your application.

Once you have the equipment and you can verify by calculation and validate by testing that the whole safety function meets the SIL requirement, you can begin operation. However now that the equipment is in service and throughout the operating life of the plant, you must be able to intelligently compare the actual field performance data against the data you used to show that the equipment would meet the SIL requirements during the design verification phase. This is another case where the information you have about your safety system components is critical and it should be considered before you select equipment with either incomplete or incompatible failure rate, operating and testing information

Selecting the Right Safety Equipment
Safety Control and Instrumentation Systems Conference
Singapore, March 2008
Eric Scharpf, Ray Wright, and David Ong
Text Continued



SUMMARY

The safety lifecycle can provide valuable support in using electronic safety systems to manage risk. With proper risk analysis activities up front, you can identify the most effective balance between mechanical devices, process modification, inherently safe designs and SIL-rated safety functions to reduce your risk to a tolerable level. Then with a solid design process, coupled with an understanding of what to look for with certified and non-certified equipment, you can get the safety system you need. For the more basic component you may seek "Prior Use" justification, document the corresponding safety case, and take on the corresponding responsibility. For more complex components you may seek equipment that is certified to be SIL capable at various levels. Here you will need to make sure that the safety manual and certification report are from a reliable third party and that they make it easy for you to get the information you need for design and that there are no restrictions that prevent you from using the equipment as needed. Then once you install and validate the system, you still need to follow up with good operation and maintenance practice to confirm the equipment does what it is supposed to and you are able to fix any problems before they turn into accidents.

Although there is a lot to consider with safety instrumented systems, with a clear focus on the right equipment and the right information for the right application you can dramatically reduce the chance of blowing up your plant.

REFERENCES

[Baker et. al. 2007] "The Report of the BP U.S. Refineries Independent Safety Review Panel" By James Baker, et. al. (January 2007) p viii.

Selecting the Right Safety Equipment

Safety Control and Instrumentation Systems Conference

Singapore, March 2008

Eric Scharpf, Ray Wright, and David Ong

Exercise / Discussion



List methods within your plant or project experience that are likely to be successful in managing systematic failures.

List methods within your plant or project experience to show that the selected equipment and any applicable software is sufficiently free of systematic errors.