7

SIF Verification Process

The Conceptual Design Process

The conceptual design process for a safety instrumented function begins with a Safety Requirements Specification (SRS). The SRS is an important document. It should contain complete specifications for designing all the safety instrumented functions. For each SIF the following information should be included:

- the hazard and its consequences
- the demand frequency for the hazard
- a reference to the appropriate P&ID drawing
- a definition of the process safe state
- a description of the safety instrumented function
- a description of the process measurements and trip points
- a description of the output response required for both primary equipment and auxiliary/secondary equipment
- the relationship between process measurements and outputs, including logic, mathematical functions and any required permissive – this must be specified for all modes of operation, e.g., startup, normal, abnormal, emergency, shutdown, etc.
- the required safety integrity level
- target proof test intervals
- maximum allowable spurious trip rate
- maximum response time requirement for the SIF
- requirements for manual activation of the SIF
- requirements for reset of the SIF (latching or automatic reset)

- SIF response to diagnostic faults (automatic shutdown, alarm only or other)
- requirements for human interface – What variables must be displayed? What variables must be input?
- maintenance override capability requirements
- estimates for mean time to restore, startup time after a trip, etc.
- expected environmental conditions during normal operation and emergency situations

Other items may be required for specific applications including any local regulatory requirements (must meet NFPA85 [Ref. 1] for example), references to company specific requirements or other requirements.

Given the design objectives in the SRS, the designer must choose equipment, determine if redundancy is needed, determine SIF testing techniques and perform a set of calculations to determine if various metrics are within the range for the desired SIL level. A diagram of the process is shown in Figure 7-1.

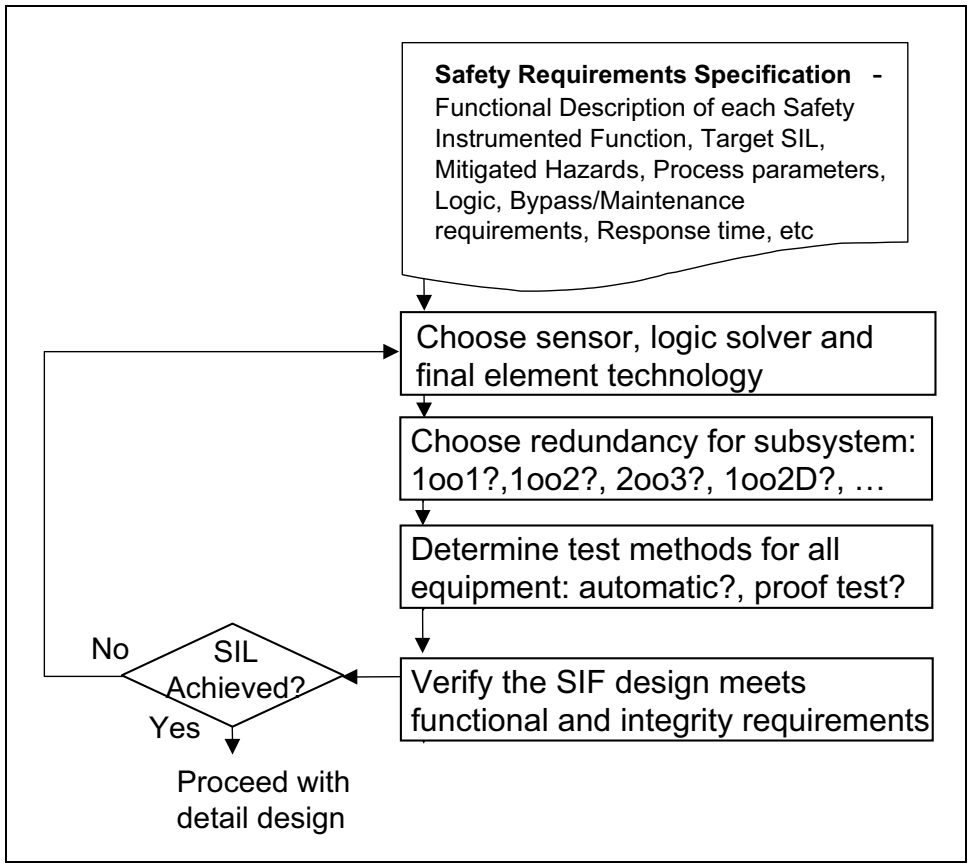

Figure 7-1. Conceptual Design Process

It is during this conceptual design step that probabilistic calculations are done to show that any given design meets the performance requirements of the SIL level. These calculations are the key to a performance based standard like IEC 61508 (Ref. 2) or ANSI/ISA 84.00.01-2004 (IEC 61511) (Ref. 3). This performance-based approach was done as an alternative to a set of very prescriptive rules that embody specific design practices. Instead of listing what each designer must do in terms of specific equipment choices and levels of redundancy, the engineer doing the conceptual design is given the freedom to choose equipment, choose redundancy levels and make tradeoffs between equipment types, testing and even cost. The conceptual design process must be taken seriously. Because with the freedom of a performance based standard, comes the responsibility to properly model the probabilistic performance of the design.

The standards allow any internationally accepted methodology for the purpose of performing the probabilistic calculations and the most common methods are described in this book -- simplified equation, fault trees and Markov models.

Equipment Selection

Equipment used in a safety instrumented function must be carefully chosen. The instrumentation must be fully capable of performing the functional requirement. All equipment must be justified so that the end user is totally confident that the instrumentation will properly perform in the intended application.

Materials used in the instruments must be compatible with process materials if the instrumentation sees process wetted service. Process environmental conditions must not exceed the instrumentation ratings. The functional safety of the instrument must be assessed. All justification decisions must be documented as part of project records.

Special attention must be paid to the support systems; e.g. power supplies, air supplies, wiring methods. For energize to trip designs, these systems become safety critical since they have a direct impact on safety.

Equipment Functional Safety Assessment

ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) requires that equipment used in safety instrumented systems be chosen based on either IEC 61508 certification to the appropriate SIL level or justification based on “prior use” criteria (ANSI/ISA-84.00.01-2004 (IEC 61511Mod), Part 1, Section 11.5.3). However the ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) standard does not give specific details as to what the criteria for “prior use” means. Most agree however that if a user company has many years of documented successful experience (no dangerous failures) with a

particular version of a particular instrument this can provide justification for using that instrument even if it is not safety certified.

Most agree also that prior use requires that a system be in place to record all field failures and failure modes at each end user site. Version records of the instrument hardware and software must be kept as significant design changes may void prior use experience. Operating conditions must be recorded and must be similar to the proposed safety application.

Many users have asked instrument manufacturers to help with justifications. In turn, manufacturers have had different levels of assessment performed by third party assessors. Such assessments are normally done by third-party experts like exida, TÜV or FM. Often, two or more assessor companies will team together to do the assessment as requested by the instrument manufacturer.

Assessments can help reduce the burden of documentation when an end user attempts to justify an instrument for use on safety applications. In the marketplace three basic levels of assessment have been done on instrumentation products with variation between assessment companies.

FMEDA Assessment of an Instrument

A hardware analysis called a Failure Modes Effects and Diagnostics Analysis (FMEDA) can be done to determine the failure rates and failure modes of an instrument (Ref. 4). This is done to provide the safety design engineer with the data needed to more accurately perform probabilistic analysis.

A FMEDA is a systematic detailed procedure that is an extension of the classic FMEA procedure developed and proven decades ago. The technique was first developed for electronic devices and recently extended to mechanical and electro-mechanical devices (Ref. 5). This analysis for hardware devices provides the required failure data needed for SIF verification.

Some assessors also do a useful life analysis to provide the safety instrumentation engineer with knowledge of any wear out mechanisms and the time periods until wear out. Preventative maintenance programs can be established to replace instruments at the end of their useful life knowing this information. Some FMEDA analyses are also extended to evaluate the effectiveness of proposed proof test methods. This provides the safety instrument engineer with proof test coverage factors used for more realistic PFH/PFD/PFDavg calculations.

Note that an FMEDA alone should not be considered sufficient justification for selecting a product.

Prior Use Assessment of an Instrument

The primary function of Prior Use assessment is to obtain a level of comfort regarding systematic (design) faults. One must develop confidence that a product does not have inherent design flaws. Sometimes the data gathered in a Prior Use assessment is used to calculate failure rates but this must be approached with caution whenever it is suspected that all failures are not reported.

Prior use assessment is the responsibility of an end user. However some manufacturers are working to help their customers in prior use evaluations by providing information. Some manufacturers have had a third party assessment of the field failure records that exist for a device. Failures attributable to both hardware and software are considered. As part of this process an assessment must also be made of the field return data gathering procedures and the product modification process.

Sufficiently detailed procedures must exist within a manufacturer to insure a reasonable level of quality in the data. The field data must show environmental limitations and application limitations. Since the manufacturer does not actually "use" the equipment, this information must be obtained from end users' data. Methods for collecting, reporting and analyzing this data should be critically reviewed. Typically field failure records are used to calculate failure rates and these are compared to the failure rates from a FMEDA. If they are significantly lower than the FMEDA numbers there is evidence that significant design flaws do not exist. Field failure rate numbers from this data should not be used for SIL verification. Remember that field failures are notoriously under-reported to the manufacturer.

All field failure data must be reviewed keeping in mind design revisions. When significant design changes are made, then field experience with previous designs should not be considered.

An end user may consider the data provided by the manufacturer but it is much better if the end user has their own detailed failure records that provide statistically significant failure information about a product.

Full Assessment according to IEC 61508

A complete IEC 61508 assessment includes a FMEDA, a study of Prior Use and adds an assessment of all fault avoidance and fault control measures during hardware and software development as well as detail study of the testing, modification, user documentation and manufacturing processes. The objective of all this effort is to provide a high level of assurance that an instrument has sufficient quality and integrity for a safety instrumented system application. This is clearly more important for products containing software as many end users have the strong opinion that software is "bad

for safety systems." This attitude comes from experience where products have failed due to software faults.

A full assessment according to IEC 61508 is the most comprehensive functional safety assessment available. It is becoming more necessary as software content grows in our instrumentation equipment. Field failures due to design faults (systematic errors) are increasing. These are mostly software faults. This type of failure is very unlikely to be reported to the manufacturer, as "repair" is often a "software reset" or power cycle. This type of failure is often not even recorded in the end user maintenance system since no "replacement" needs to be made. Hence "prior use" or field failure evaluation techniques based on returns to the manufacturer are not sufficiently effective and very few end users have the failure recording systems needed to assure a high level of integrity.

Many of the requirements of IEC 61508 focus on the elimination of systematic faults. In order to demonstrate compliance with all requirements of IEC 61508, the design and development process used to create an instrument must show extensive use of many techniques for "fault control" and "fault avoidance." The IEC 61508 standard defines a set of practices that represent good software and hardware engineering. Most experts believe that these methods are the best techniques available to provide high design quality.

Another benefit of having instrumentation products that are 61508 certified is that they have demonstrated higher levels of design quality and software quality. Given the number of failures due to software in instrumentation equipment, this is a top priority for many end users. It should be noted that the quality within a product is directly proportional the to "SIL Capability" rating assigned to the product. A SIL3 capable product is generally considered to have an order of magnitude higher quality than a SIL2 capable product.

Full compliance with the requirements of IEC 61508 is seen when a product does not have any significant "restrictions" on usage as documented in the product "Safety Manual." A large safety manual with a long detailed list of instructions on how to make the product "safe" is a sure sign the manufacturer does not meet requirements unless these restrictions are implemented by the end user.

The primary differences in the assessment techniques are summarized in Table 7-1.

Redundancy

After equipment is selected, the next step in the conceptual design process is the decision to use multiple instruments to serve the same purpose – redundancy. Redundancy is configured to provide continued system operation even though one or more specific instruments may fail – fault tolerance. Some redundant architectures provide fault tolerance against a

false trip. Some redundant architectures provide fault tolerance against a dangerous failure and some architectures can provide fault tolerance against multiple failure modes. Detailed explanations of various redundant architectures can be found in Appendix F.

Table 7-1. Assessment Techniques

Assessment Criteria	FMEDA only	Prior Use	IEC 61508 Certification
Detail analysis of hardware failure modes	X		X*
Detail analysis of hardware diagnostic capability	X		X*
Analysis of hardware useful life	X*		X*
Analysis of proof test effectiveness	X*		X*
Assessment of operational hours based on manufactured units		X	X
Assessment of Configuration Management system per requirements of IEC 61508		X	X
Assessment of Field Failure Return System - field failures corrected		X*	X
Assessment of Field Failure Return System - notification to users of safety issues		X*	X
Assessment of design revision history - few revisions based on design faults		X*	X
Assessment of hardware design process			X
Assessment of hardware testing techniques			X
Assessment of software requirements			X
Assessment of software criticality			X
Assessment of software design techniques			X
Verification of Safety Manual per IEC 61508			X
Assessment of software testing techniques			X
Assessment of product testing techniques including environmental testing			X
Assessment of manufacturing process			X

* Depends on assessment agency - not all third-party agencies perform the same analysis

SIF Testing Techniques

The safety and availability of a set of equipment used for a safety instrumented function may benefit from testing. However, that depends on redundancy and how often the demand occurs. Three modes of operation have been defined in IEC 61508 for equipment providing a safety instrumented function: continuous demand mode, high demand mode and low demand mode. This book will use the IEC 61508 definitions to designate those three different situations.

These three modes have been defined because SIF testing may or may not be given credit depending on the level of redundancy and the mode. The probability of failure on demand is calculated differently for each mode. The essential differences are due to the relationship between the dangerous condition (the demand) and the diagnostic testing.

Three time intervals must be known to define what credit may be taken for automatic diagnostic testing and manual proof testing. These three time intervals are the average demand interval, the manual proof test interval and the automatic diagnostic test interval (usually the worst-case time is considered). The three modes and their relationships are shown in Table 7.2.

Table 7-2. SIF Modes and Time Interval Relationships

Mode	Demand Interval versus Automatic Diagnostic Interval	Demand Interval versus Manual Proof Test Interval	Probability Measure
Continuous Demand	DI <= ATI	DI <= PTI	PFH
High Demand	DI >> ATI	DI <= PTI	PFH
Low Demand	DI >> ATI	DI >> PTI	PFDavg

Continuous Mode

In continuous mode, the demand is effectively always present. Dangerous conditions always exist and a dangerous failure of the safety instrumented function will immediately result in an incident. There are no safety benefits that can be claimed for manual proof testing or even automatic on-line diagnostics in a single channel system (1oo1). By the time the diagnostics detect the fault and initiate action, it is too late. Therefore, in continuous demand mode probability evaluation cannot take credit for any diagnostics except in redundant systems.

The probability evaluation is done by comparing the calculated probability of failure per hour (PFH) against the PFH table shown in Figure 7-4.

High Demand Mode

In high demand mode, the dangerous condition is not always present but does occur frequently. We can define the "high demand" mode by stating that it occurs when a demand occurs nearly as often as or more often than any practical manual proof test interval but considerably slower than the automatic diagnostic test and response time. The exact demand rate is not important. It is the ratio of demand rate to manual proof test rate and automatic diagnostic and response rate that defines the region. The threshold between continuous demand and high demand depends on the ratio of the demand rate to the automatic test rate. The reason to distinguish these modes is that one may take credit for automatic diagnostics in high demand mode even in a single channel (1oo1) system.

If automatic diagnostics complete execution at a frequency two or more times the expected average demand rate and the system responds to a diagnostic fault by initiating a move to the safe state, then safety could be improved and some credit can be taken in the probability of failure modeling. If automatic diagnostics are not done many times faster than the demand rate then detailed probability models showing the demand probability and deterministic diagnostic time periods must be done. Repair time must be carefully modeled if the safety instrumented function is not programmed to automatically initiate safety action upon detecting a dangerous fault within the instrumentation equipment. This level of modeling is complicated and many choose to simply classify these safety instrumented functions in the continuous mode category.

If the automatic diagnostics complete execution many times faster than the average expected demand rate and automatic safety action is initiated, then the probability models can be simplified and the effects of diagnostics can be given full credit even in a single channel (1oo1) system. IEC 61508 suggests that a number of ten times be used (Part 2, 7.4.3.2.2, e, Note 3). In order to determine this, the time period of the automatic diagnostics must be known.

In high demand mode, the probability evaluation is done by comparing the calculated probability of failure per hour (PFH) against the PFH table shown in Figure 7-4.

Low Demand Mode

In low demand mode, a dangerous condition is expected very infrequently. The threshold for classification between high demand and low demand should be determined by the ratio of any planned manual proof test interval to the average interval between demands. IEC 61508 states that the proof test interval must be no greater than half the expected average demand interval or greater than one year (Part 4, Clause 3.5.12). Detailed probabilistic modeling will show that manual proof test diagnostics can and should be given credit when the average demand

EXAMPLE 7-1

Problem: A set of non-redundant (1oo1) equipment is used to implement a safety instrumented function. Within the equipment, automatic diagnostics complete execution every one second. The instrument is programmed to take the process to a safe state when an internal failure of the equipment is detected. A dangerous condition occurs every one minute on average. What is the mode of operation and can the automatic diagnostics be given credit in the probability of failure calculation?

Solution: The automatic diagnostics perform their function sixty times during the average demand period and perform an automatic process shutdown. A detailed probability model showing the exact effect of deterministic automatic diagnostics is not necessary as it would show diagnostics are effective in improving safety. This SIF would be classified as high demand mode.

interval exceeds twice the manual proof test interval. Simplified equations that do not specifically account for the demand period will give an optimistic result unless the average demand period is ten times greater than manual proof test interval.

EXAMPLE 7-2

Problem: Layer of protection analysis has indicated that a demand would occur every 5 years on average for a particular process hazard. Although most automatic diagnostics execute every minute, the worst-case time period for automatic diagnostics within the equipment is once per week. A proof test interval of one year is proposed for a manual test and inspection. Would this SIF be classified as low demand?

SOLUTION: Automatic diagnostics are performed many times within the expected average demand interval. The proof test is done at least two times within the expected average demand period so the SIF would be classified as low demand.

Fortunately in most situations in the process industries, especially when independent layers of protection (Ref. 6 and 7) are properly designed and considered in the demand rate analysis, average demand intervals are very high. Often the average demand interval will exceed one hundred years.

In low demand mode safety instrumented functions, the person performing the SIF verification calculations must:

1. define the proposed proof test procedures and
2. estimate the effectiveness of all procedures via an estimate of proof test diagnostic coverage.

That information is needed along with other parameters to perform an accurate average probability of failure on demand calculation.

EXAMPLE 7-3

Problem: A pressure transmitter is needed for a safety instrumented function. What proof test procedures should be performed and what coverage factors should be used for those procedures?

Solution: Many manufacturers recommend proof test procedures for low demand safety instrumented system applications. The information is found in the "safety manual." That document may be part of another manual or may be a separate document. Referring to the safety manual section of a pressure transmitter (Ref. 4), proof test options with associated coverage factors are given (Figure 7-2). The test titled "Five Year Proof Test" has a manual proof test coverage of 65%. The test titled "Ten Year Proof Test" has a manual proof test coverage of 99%.

Reliability and Safety Metric Calculation

Probabilistic calculations are done to determine if the design meets the safety integrity requirement after:

1. equipment is chosen,
2. redundancy designs are completed and
3. the automatic test capabilities / manual proof testing goals are established based on SIF demand mode,

The calculations may be done with simplified equations, fault trees, Markov models or other techniques depending on the complexity of the model and the demand mode of operation.

SIF Identification

The first step in the calculation process is to properly identify the equipment required for each safety instrumented function. All equipment associated with a particular SIF must be classified into "primary" – equipment needed to provide the required protection against the identified hazard and "auxiliary" – equipment that provides useful functionality but not required to protest against the hazard. This classification is important because only primary equipment is included in the PFDavg analysis and the SFF analysis.