



IEC 61508 – A PRACTICAL APPROACH TO ITS APPLICATION IN THE PROCESS INDUSTRY

Clive Charnock BEng CEng MIEE

AMEC Group Ltd, Sankey House, 130 Birchwood Boulevard, Warrington WA3 7WD

The new international standard IEC 61508 provides a generic framework for achieving functional safety through a risk reduction methodology. Because of the generic nature of the standard the challenge in the process industry has been to interpret these generic requirements in an appropriate manner. This paper explains why and how AMEC adopted and implemented the methodology and how it is being successfully applied in a practical manner on real projects

IEC 61508, risk-based, safety systems

INTRODUCTION

OVERVIEW OF THE STANDARD

IEC 61508 is an international standard for managing Functional Safety with regard to Electrical / Electronic / Programmable Electronic Safety Related Systems (referred to as E/E/PES). The standard has been in development for a number of years and the last of the seven parts were published in 2000. The standard is generic in nature and can be applied to a safety related application in any industry sector.

The standard defines a rational and consistent approach to achieving functional safety and uses the concept of the 'safety lifecycle' (from concept design, through hazard and risk analysis, specification, implementation, operation, maintenance to eventual de-commissioning) as a framework for addressing the phases to achieve functional safety in a systematic and auditable manner.

The standard is in seven parts. Parts 1, 2, 3 & 4 are normative and must be adhered to when claiming compliance with the standard. Parts 5, 6 & 7 are guidance documents providing suggestions for tools and approaches that may be used, if appropriate, to meet some of the requirements of the normative sections. This relationship between the individual parts is shown pictorially in Figure 1.

IEC 61508 is a "Basic Safety Publication" and is the basis for all sector-specific standards that are currently being developed. Due to the generic nature of IEC 61508 it can be difficult to interpret and sector-specific standards are being developed because:

- Each sector or industry having its own relevant and valuable experience that has built up over many years that needs to be captured;
- Each sector or industry has its own specific terminology and language.

The process industry sector specific standard IEC 61511 is currently in development, but will not be available for some time. Therefore, a detailed understanding of the generic standard IEC 61508 is currently required to achieve compliance.



WHY THE IEC 61508 METHODOLOGY WAS ADOPTED

AMEC are an established Engineering Contractor and have been involved in the Engineering, Procurement, Construction and Commissioning of many process plants / facilities that contain significant safety and environmental hazards.

Many chemical manufacturing companies now fall under the requirements of the Control of Major Accident Hazards (COMAH) Regulations. COMAH Regulations require submission of a report that identifies the major hazards and demonstrates the Safety Management Systems in place to mitigate those hazards. The methodology of demonstrable risk reduction through a formal risk management process is the same methodology that underpins IEC 61508. The resultant lifecycle documentation from a design, executed in accordance with the risk-based IEC 61508 methodology, would seamlessly integrate into a COMAH report.

It was also predicted that owner / operators would be citing compliance with the requirements of IEC 61508 in the technical sections of Request For Services documentation. This prediction has been vindicated as most enquiries now contain references to compliance with IEC 61508.

Compliance with the standard in the United Kingdom is NOT mandatory, but the view is that the standard represents current global best practice in achieving functional safety. Within the UK the Health and Safety At Work Act, 1974 places duties on employers, designers, suppliers, etc to provide safe equipment or plant that is 'so far as reasonably practicable', safe and without risk to health. Compliance with the standard would be a significant aid to demonstration of 'due diligence' in the delivery of a safe plant or facility.

AMEC have engineered many Safety Related Systems in the past using good engineering practice, Client engineering standards and guidance such as EEMUA Document Publication No. 160. Existing systems were in place, but were not risk-based and were difficult to audit through the lifecycle of engineering AMEC were involved in. Engineering safety related systems using the IEC 61508 risk-based approach offered the following significant advantages:

- Embracing current best practice to aid demonstration of 'Due Diligence' to mitigate legal risks;
- Understanding the implications of complying with IEC 61508 to aid mitigation of commercial risk;
- Minimising engineering, capital and operating costs on projects by utilising the risk-based approach;
- Demonstrating the capability to provide a marketing advantage.

Based on the above, the decision was made to adopt the IEC 61508 risk-based methodology into the engineering organisation, and is now being used successfully on all relevant projects.

HOW THE IEC 61508 METHODOLOGY WAS DEVELOPED

As outlined in the introduction IEC 61508 is a generic standard and as such it is a large and complex set of documents that introduces a whole new set of terminology and also presents concepts in a language that takes some level of interpretation when considering the process industry. These issues will be addressed, in many respects, when IEC 61511 is published, but the challenge was to be able to interpret the requirements of IEC 61508 to allow compliance with this base standard.

There have been many publications and articles that have discussed the standard and surrounding topics but there has, to date, been very little practical guidance as to the implementation of IEC 61508 on real process plant projects.

The key steps that were identified to lead to implementation of IEC 61508 within AMEC were:

- Initial knowledge gathering through attendance at specific IEC 61508 training courses, reviewing the standard and associated articles and papers;
- Modification of Engineering Group Procedures and Work Instructions to reflect the safety lifecycle. Identification of specific safety reviews and relationships with respect to other reviews, eg. HAZOP, Layout, Hazardous Area Classification, etc;
- Development of Design Guidelines that interpret the requirements of IEC 61508 and present the practical ideas and approach in terms engineers working on process plant projects will more easily recognise;
- Develop pro-forma documents for capturing and presenting information and data throughout the project lifecycle in a consistent format.
- Develop default tools and methodologies for hazard and risk analysis;
- Define default parameter calibrations for the selected Risk Graph and Hazardous Event Severity Matrix tools that reflect the ALARP (As Low As Reasonably Practicable) principle;
- Development of MS Excel based tools for calculations to support Integrity Level Assessment / Verification;
- Purchase failure rate data (FARADIP 3 and SINTEF data sources);
- Purchase of a tool for detail calculation of Common Cause Failure percentages (although IEC 61508 - Part 6, Appendix D contains a methodology for calculating Beta values);
- Provision of training for Engineers undertaking the work and development of a detailed competency assessment framework;

TYPICAL PROJECT EXECUTION

SCOPE DEFINITION

The scope for an individual project is normally defined by a project Basis of Design, which reflects the scope and boundaries of a project as a technical and commercial basis. The Basis of Design and covers the physical scope and the scope of responsibilities.

In most instances the physical scope of a project will generally be defined by a set of Process Flow Diagrams (PFDs) or Process & Instrumentation Diagrams (P&IDs).

Given an agreed physical scope, figure 2 illustrates the main steps in the project safety lifecycle that AMEC, in an Engineering, Procurement, Construction Management role, are involved in. The diagram is not definitive and the scope of responsibilities can change from project to project. Therefore, it is essential that the scope of responsibilities for all parties are clear and understood at the outset of the project.

Figure 2 also shows a simplified linear view of the process. In actual detail project execution the process can involve a number of iterative steps to achieve the final engineered and tested facility.

Examples of this iterative process are:

- An initial safety review identifying major hazards leading to a requirement for modification of the process design;
- A legitimate process design change (eg. Process expansion, De-bottlenecking, etc);
- A protective function requiring re-design if, through the integrity verification, the function does not comply with the target integrity level.

Even though the process of engineering is shown completing at Site Acceptance Test / Commissioning the design and engineering must take into account the requirements for ease of operation and facilitation of ongoing maintenance and proof testing.

This whole lifecycle approach is imperative as poorly designed systems, with respect to ongoing maintenance and testing, can lead to poor quality proof testing (limited coverage) and significant additional operational costs.

HAZARD IDENTIFICATION

Hazard identification is undertaken at the preliminary P&ID development stage. The study will take the form of a high level desktop review of the process to identify the major hazards associated with the process. This process utilises methodologies such as brainstorming, what-if scenarios, checklists, etc. These major hazards are assessed in a preliminary coarse Hazard Analysis. The first step in this process is to review if the risks are minimised / removed by modification of the process design to achieve a process that is inherently safer.

By having this review process as early as possible in the project lifecycle it allows the process design to be challenged in a more open-minded and effective manner as the impact of any resultant changes will be minimised.



Additionally, the issue that a detailed HAZOP study is undertaken when the P&IDs are effectively finalised. Therefore, the expectation is that the implementation of all protective functions have already been defined, leading to the requirement for an earlier Hazard Identification and Risk Analysis process.

HAZARD AND RISK ANALYSIS

Each of the hazards identified from the initial review are studied in more detail within a detailed Hazard and Risk Analysis process. The review process is undertaken by a mixed AMEC / Client team generally comprising of the following disciplines:

- Safety
- Process
- Control & Instrumentation
- Machinery specialists (as required, e.g. Incinerators or large compressors)

The default methodology for risk analysis is the Risk Graph, as this method allows a number of risk factors to be taken into account. Where there are significant hazards and a number of independent safety systems in place (eg. mechanical devices in addition to a Safety Related E/E/PES) the use of a Hazardous Event Severity Matrix is considered.

Within the risk analysis process environmental and commercial risks are considered in addition to safety risks and the most onerous of these risks defines the integrity level requirement of the protective function.

It is essential that prior to the commencement of Hazard and Risk Analysis that the risk parameters for safety / environmental / commercial risk are discussed, agreed and documented. The parameters must be such that the risk graph calibrations reflect the values and culture of the operating company in addition to meeting any statutory requirements for tolerable risk levels.

Everyone in the study team must also understand the terminology and concepts as defined within IEC 61508. The Equipment Under Control (EUC) is the plant or facility with its normal process control system (DCS or PLC / SCADA) but WITHOUT any Safety Related E/E/PES. The Equipment Under Control includes Other Technology (OT) protection systems such as pressure relief or other mechanical systems. External Risk Reduction Factors (ERRFs) are systems such as blast walls, containment bunds and plant operating procedures. The relationships between the above are shown diagrammatically in figure 3.

The process control system is used for the normal safe operation of the process plant. The control system is not designated as 'Safety Related' as the control system, in many cases, is the source of demand for a particular hazard. It could be possible, in certain cases, to claim that the control system can provide a layer of protection against a hazard. The implications of classifying a control system as 'Safety Related' normally leads to the more conservative approach of providing a separate, independent protective measure.

Within the Hazard and Risk Analysis process the plant is analysed, taking each individual hazard in turn and considering:

- What is the consequence of the hazard occurring based on the operating regime, physical features and layout of the plant (EUC) ?
- What conditions could cause the hazard to occur ?
- What is the frequency of occurrence of these conditions ?
- What measurements could be provided to detect the onset of the hazardous conditions ?
- What terminating devices could be provided prevent or mitigate the hazard ?
- Are the process dynamics such that an operator could manually detect and prevent the hazard from occurring ?
- Are there facilities and clear procedures to allow operators to detect a potential hazard and manually prevent it from occurring, or effectively evacuate the area ?
- If a protective function were provided what would be the effect of spurious tripping, and what target reliability needs to be achieved ?

By answering the above questions in the structured risk-based approach the requirement for a Safety Related E / E / PES can be determined for a particular hazard. The safety requirement is defined in terms of target Integrity Level (most onerous of Safety / Environmental / Commercial Integrity Levels) and functional operation (cause and effect). Figure 4 shows the Integrity Level Calculation Sheet, which is used to capture the information with respect to a particular hazard and forms the basis of the Safety Requirements Specification (SRS).

Where a target Integrity of SIL3, or above, is identified for a particular hazard the approach is to insist on re-examination of the process design to investigate if the risk can be reduced. If it not possible to effectively reduce the target Integrity Level then independent 3rd party assessment would be applied through the safety lifecycle for the particular hazard.

The Safety Lifecycle defined within IEC 61508 refers to a 'Safety Requirements Allocation' stage which is distinct from the Hazard and Risk Analysis. Theoretically, this is the stage where the decision is made as to what contribution is made to overall risk reduction by Other Technologies (OT), External Risk Reduction Factors (ERRFs) and Safety Related E/E/PES to achieve Functional Safety.

In practical situations the 'Safety Requirements Allocation' is an integrated part of the Hazard and Risk Analysis study process, for example:

- The demand rate for a Reactor Overpressure hazard is reduced by a factor of a least 10 due to the pressure safety relief valve that is correctly sized for the particular case.
- The consequence of reactor explosion due to overpressure is reduced by a factor of at least 10 due to the provision of a correctly design blast wall.



The above considerations are taken into account when assessing the resultant risk (and target Integrity Level for the Safety Related E/E/PES) and are identified / recorded on the Integrity Level Calculation sheets as Safety related Items.

SYSTEM REALISATION

The documentation resulting from the Hazard & Risk Analysis process forms the basis of the Safety Requirements Specification (SRS) which then requires realisation into an engineered system. The complete Safety Requirements Specification is not contained within a single comprehensive document, but rather within a coherent set of related documents that are developed through the engineering phase of the project. These documents provide an amplification / extension of the base requirements (target Integrity Level and functional requirements) to define the detailed realisation requirements, and include:

- Safety System User Requirements Specification (performance criteria, reset requirements, maintenance overrides, communication links, Human Machine Interfaces, environment, etc);
- Safety System Input / Output Schedules (including ranges & set-points);
- Safety System Trip Matrix Definitions (including and sequential and timing requirements).

This collection of documents that form the Safety Requirements Specification is used as the basis for verification phase of the project, therefore, no unauthorised deviations from the approved specifications are allowed unless a formal change has been raised, reviewed, approved and implemented under strict revision control.

Where the consequences of spurious tripping of a Safety Related E/E/PES may cause significant commercial loss (eg production downtime or situations such as a product setting solid in a reactor vessel) or further downstream hazards there may be a requirement to achieve a specific Spurious Trip Rate target for the protective function. These situations require implementation of architectures (such as 2 out of 3 voting) which are robust to revealed failures.

Instrumentation and valves must be selected that are appropriate for the duty in terms of fouling, plugging and material compatibility.

Proof testing is an essential part of maintaining the integrity of Safety-Related systems and the design, where possible, is implemented to facilitate effectiveness and ease of proof testing, eg. Test pots for high level switches, isolate / vent valves for pressure instruments and facilities for by-passing or partial stroking of shut-off valves.

The internally developed Design Guides address these detailed realisation issues and provide practical advice for engineers during this phase of the lifecycle.

AMEC's engineering systems facilitate the very stringent requirements for the management of change through the safety lifecycle by employing engineering database tools that utilise the single point data entry paradigm. Therefore, a single instrument tag stored in the database is linked to the graphical representation on the P&ID, associated with an I/O definition and associated with a protective function. A Revision history tracking process is automated and operated down to individual tag level.

E / E / PES SAFETY RELATED SYSTEM VERIFICATION

To achieve functional safety the E / E / PES Safety Related System must perform specific actions with a certain degree of certainty to reduce the risks resulting from the EUC to an acceptable level. The system must be considered from the sensors through to the final terminating devices, ie. The 'Pipe to Pipe' concept.

Therefore, the verification process consist of two distinct parts:

Integrity Verification – A defined level of certainty that a function will operate as required.

Functional Verification – The function performs specific actions (eg. Close valve V1) when specific conditions (eg. Vessel V3 High Level) occur.

INTEGRITY LEVEL VERIFICATION

IEC 61508 defines four discrete levels for Safety Integrity Level (SIL 1 to SIL 4 - SIL 4 having the highest level of integrity). The Safety Integrity Level is expressed as a numerical range of values that are expressed as:

Probability Of Failure On Demand (PFD) – Low Demand Rate Systems

Probability of Failure Per Hour (PFH) – High Demand or Continuous Demand Systems

Applications within the Process Industry tend to mainly fall within the category of low demand systems.

The dangerous failure of a protective function can be caused by:

- Random Hardware failures;
- Systematic failures (software failures, design process failures, etc.)

Quantitative predictions of protective function PFD / PFH due to random hardware failures can be effectively calculated to assess performance. It is generally not possible to calculate PFD / PFH due to systematic failures using fully quantitative methods. Therefore, in the case of software based systems, it is necessary to ensure specific design methods / checking / review / test measures are undertaken for different target Integrity Levels.

To calculate the Integrity of a safety function, a block diagram of the complete function (from initiators to terminating devices needs to be defined). This block diagram is broken down into the three sub-system sections as shown in figure 5.



IEC 61508, Part 6 Has multiple tables to allow the user to look-up a PFD or PFH value for a sub-system. The multiple tables allow a selection of the following parameters:

Configuration:	One out of One (1oo1) One out of Two Voting (1oo2) Two out of Two Voting (2oo2) One out of Two Voting Reverting to One out of One (1oo2D) Two out of Three Voting (2oo3)
Proof Test Interval:	6 months, 12 months, 2 years & 10 years (Low demand) 1 month, 3 months, 6 months and 12 months (High demand)
Failure rates:	0.1, 0.5, 1, 5, 10 & 50 failures per million hours
Diagnostic Coverage:	0%, 60%, 90% & 99%
Beta Values:	1%, 5% & 10%

The tables also assume that:

Mean Time To Repair: 8 hours

Dangerous Failures: 50% of total failures

Beta Values for Detected Failures = 0.5 x Beta value for undetected failures.

Failure Rate Data

The most accurate failure rate data for any operational plant would be data collected by the plant operator from maintenance records or incident reports. The problem is that many operational sites do not effectively collect historical data in a consistent format that could be used as a basis for use in calculations.

In most instances the default data sources utilised for analysis purposes are recognised data sources such as FARADIP 3 and SINTEF.

Extreme care must be exercised when making a judgement on percentage of failures to a dangerous mode. The duty and failure mode of the specific device in the context of the safety function must be clearly understood.

Diagnostic Coverage

There is little practical guidance for assessing diagnostic coverage for a sub-section, and again, careful engineering judgement must be exercised in understanding what facilities have been engineered into the sub-system to detect faults and make faults visible to the operator.

Beta Values

To make an accurate assessment of Common Cause Failure fractions it is necessary to not only have a detailed understanding of the complexity, environment and design features of the system, but an understanding of the safety culture of the organisations involved with respect to procedures, training and competency. The methodology used is an enhancement of the partial BETA model known as the BETAPLUS model.

Proof Test Interval

The proof test interval is agreed following discussions with the plant operator to understand the operating and maintenance regimes and experience with specific types of instrumentation and equipment. The normal approach would be to agree a short proof test interval in the first instance, and once satisfactory experience of the equipment is gained then the proof test interval can be review and increased given that the PFD / PFH figure for the complete safety function remains acceptable.

The tables may be acceptable as a 'first-pass' as the tabular results are based on specific assumptions that may not be applicable to the specific sub-system, and there are limited choices for other parameters that may not be suitable. Due to these limitations, Microsoft EXCEL tools have been developed by AMEC (based on reliability block diagram models) to allow the PFD or PFH to be calculated for a sub-system with specific values rather than pre-determined fixed value choices or coarse assumptions. An Figure 6 shows an example output.

A summary assessment sheet is set up such that the effective block can be modelled and the individual sub-system details added. The PFD or PFH for the complete safety function is calculated and compared against the numerical target value. The percentage contribution from each section is calculated to identify the dominant component that should be addressed if the target PFD or PFH is not met. An example output is shown in Figure 7.

Spurious Trip Rate

The summary assessment sheet contains a second sheet that calculates the spurious trip rate for the protective function and percentage contribution from each sub-system. Where applicable, the calculated spurious trip rate is compared with the target spurious trip rate as defined on the Integrity Level Calculation Sheet.

Hardware Integrity

In addition to meeting the requirement for compliance with a target PFD or PFH value the sub-system requires assessment of the hardware integrity. The sub-system hardware integrity is dependent upon the hardware diagnostic coverage and fault tolerance. Tables 2 & 3 within IEC 61508 part 2 define the requirements for Type A and Type B sub-systems respectively. Type A systems are simple, well understood and proven in the field, whereas Type B systems are complex, with behaviour that cannot be not fully determined and is not proven in the field.

An example is a single trip valve sub-system that has the following attributes:

- Simple, well understood and proven operation in the field (Type A sub-system)
- No diagnostic coverage
- No fault tolerance (ie. A single fault could cause a dangerous failure)

Using Table 2 results in a sub-system hardware integrity that is applicable to SIL 1 applications. Regardless of the failure rate data or proof test interval the sub-system can only be applied in a safety function that has a target Integrity Level of SIL 1, eg. If the complete safety function had an input section rated at SIL 2, logic solver at SIL 3, and output section rated at SIL 1 then the complete safety function would be limited to SIL 1.

Terminology used within the industry such as a 'SIL 2 pressure transmitter' must be treated with caution, as the term is specific to the device in terms of the device having the hardware integrity applicable to SIL 2. Using this specific device within the sub-system of a complete safety function DOES NOT guarantee that the complete safety function will comply with the requirements appropriate to SIL 2.

FUNCTIONAL VERIFICATION

To ensure that all of the protective functions perform the necessary actions as defined within the Safety Requirements Specification (SRS) it is necessary undertake rigorous testing of the system. These tests are usually split into two phases, namely:

- Factory Acceptance Tests;
- Site Acceptance Tests.

The factory acceptance tests are carried out against a pre-approved test specification that reflects the Safety Requirements Specification (SRS).

The Site Acceptance Tests are performed at the pre-commissioning phase of the project and are normally the final proof tests undertaken prior to plant start-up. At this stage all installation checks have been made, the systems fully energised and instrumentation fully calibrated.

It is sensible to perform the Site Acceptance Tests utilising the actual proof test procedures that will be utilised during the operational lifetime of the plant. This approach has the benefit of validating the procedures prior to start-up. It is extremely important to agree early in the project lifecycle who will be responsible for the production of these procedures as it can be a significant task that needs to be well planned and carefully executed. Last minute development of these procedures can lead to shortcomings in the testing leading to a reduction of achieved integrity.

CONCLUSIONS

Adoption of the IEC 61508 has required a significant amount of work and commitment with the organisation going through a steep learning curve. The benefit of adopting the risk-based methodology is that it has driven the organisation to a more rigorous, consistent, auditable and holistic way of achieving functional safety.

By successfully delivering projects using the methodology AMEC have a detailed understanding of what is required and ensure that the necessary resources are taken into account, thus minimising risk to the project.

It has been noted in some cases on recent projects that application of the risk-based methodology has led to cases where a Safety Related E / E / PES, that previously would have been included (because of custom and practice or engineering judgement), has been found not to be required to achieve functional safety. By applying the methodology the number of Safety Related E / E / PESs can be reduced, allowing savings in capital, operating and maintenance costs that are achieved through the lifetime of the plant. This general reduction of the number of protective functions allows resources and effort to be concentrated on the legitimate protective functions, which will reap benefits in terms of maintaining functional safety through the complete lifecycle of the plant.

FUTURE PLANS

The plans for the future are to gain formal recognition of AMEC's ability to conform with the requirements of IEC 61508. The Conformity Assessment for Safety Systems (CASS) Scheme is an initiative recently launched in the UK and provides a common framework for companies involved in the Safety Lifecycle to demonstrate compliance with IEC 61508. The intention is to demonstrate compliance at management system level through what is known as a "Functional Capability Safety Assessment" (FSCA), which requires an audit process through a UKAS accredited assessment company.

REFERENCES

IEC 61508	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems – Parts 1 – 7.
IEC 61511 (Draft)	Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Parts 1 – 3.
EEMUA	Publication 160. Safety Related Systems for the Process Industries.
FARADIP.THREE	Failure Rate and Failure Mode Databank and Failure Mode and Effect Analysis Package. Technis, Tonbridge, Kent UK.
BETAPLUS	Common Cause Failure (Partial Beta model) Analysis Package. Technis, Tonbridge, Kent UK.
SINTEF	Industrial Management Safety and Reliability. Reliability Data for Control and Safety Systems. 1998 Edition.

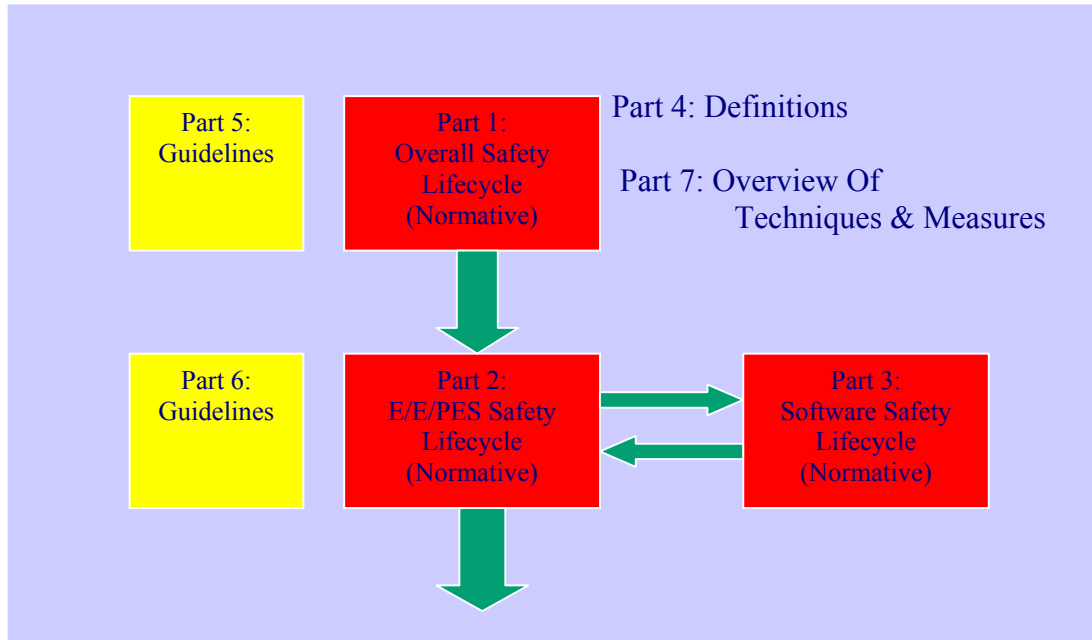


Figure 1 – Relationship Between The Seven Sections of The IEC 61508 Standard

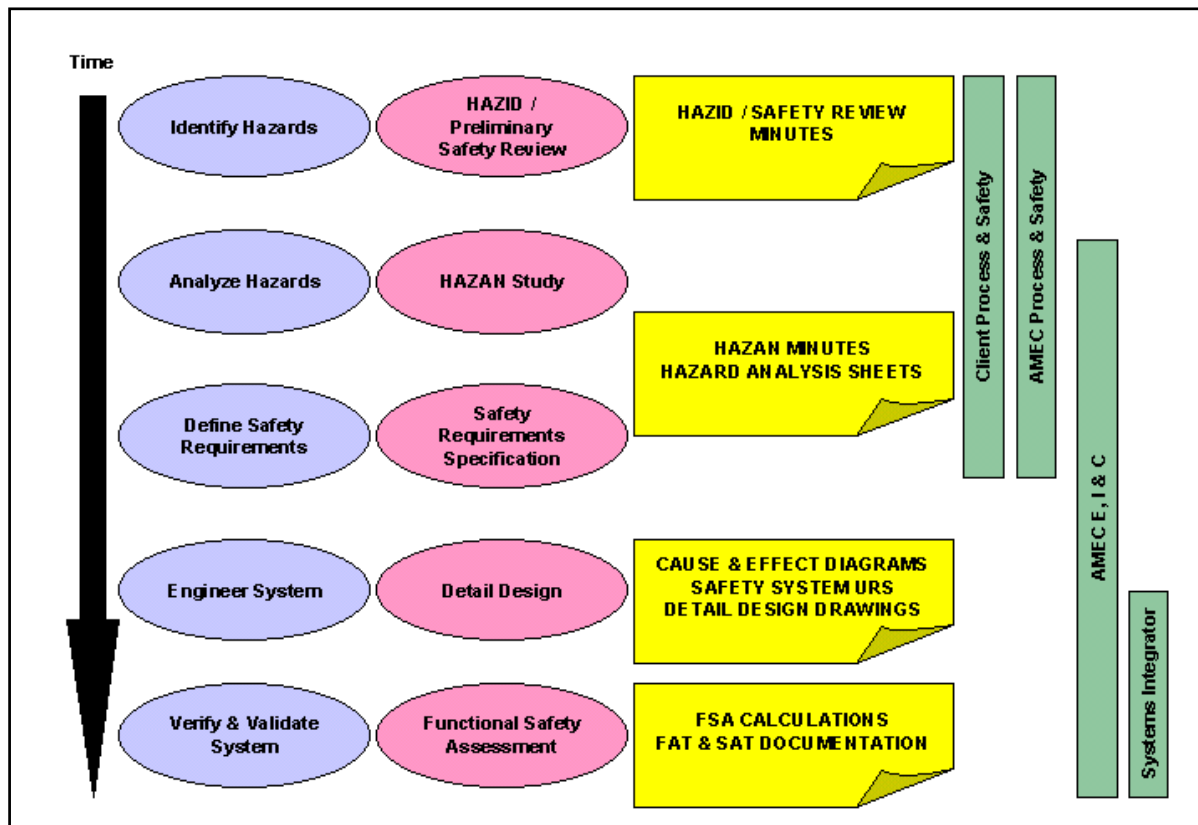


Figure 2 – Simplified View of The Safety Lifecycle Applicable to Design & Engineering

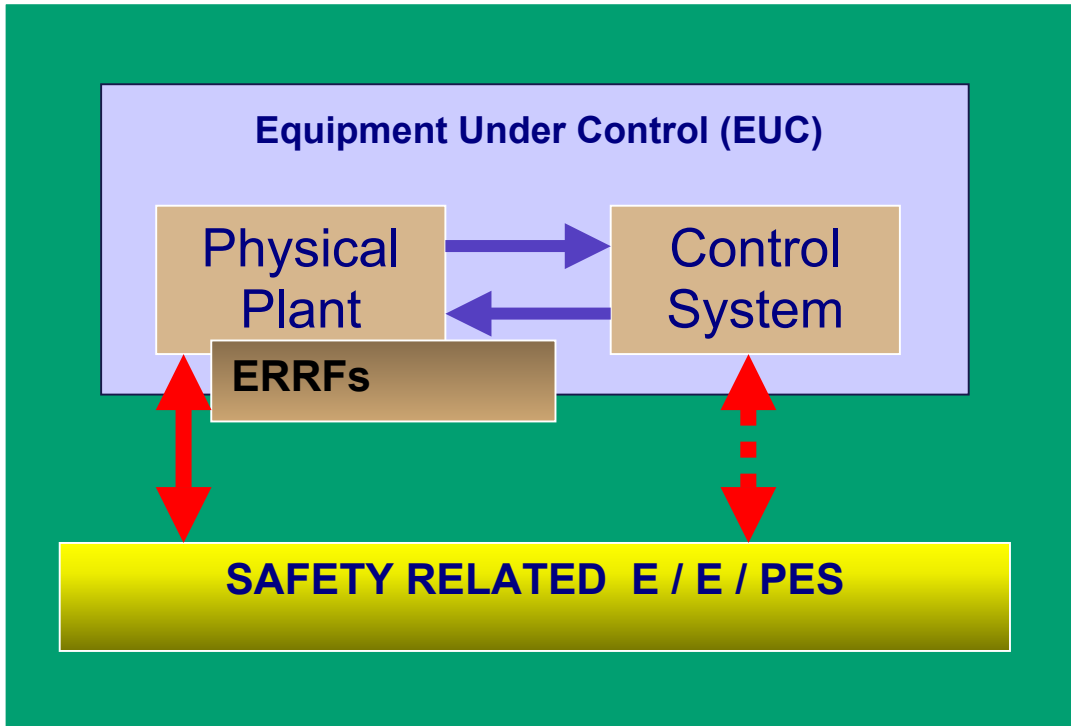


Figure 3 – Diagram of a Process Plant Entity

The screenshot shows a Microsoft Word document titled "Hazard Analysis Proforma.doc (Preview)". It displays two pages of an integrity level calculation form. The left page, labeled "Integrity Level Calculation", includes fields for project details, hazard identification, and a table for termination tags. The right page, also labeled "Integrity Level Calculation", includes risk graphs for safety and environmental assessments, a commercial assessment table, and a consequence factor table. Both pages include a table for integrity levels and a section for notes.

Figure 4 – Example of an Integrity Level Calculation Sheet

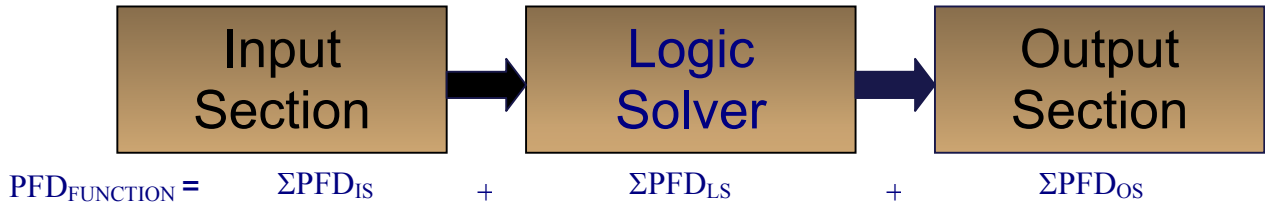


Figure 5 – Block Diagram Representing Sub-systems and Contribution to total PFD

SAFETY INTEGRITY ASSESSMENT (1 OUT OF 1 ARCHITECTURE) - LOW DEMAND MODE

This assessment sheet covers only a single part of the safety function, ie. Initiator, Logic Solver or Terminating device having a 1 out of 1 (simplex) architecture.

Tag Reference / Identifier (If applicable) **XV 1234**
 Section Type (Initiator, Logic Solver or Terminating device) **Terminating Device**

General Details **Single Shut-off Valve Failing to Closed Position**

Mean Time To Repair (MTTR) **8** Hours (Normally assume 8 hours)
 Proof Test Interval (T) **8760** Hours (3 months - 2190, 6 months - 4380, 1 year - 8760, 2 years - 17520)
 Percent Diagnostic Coverage (For Whole Section) **0%**

Component	Component 1	Component 2	Component 3
λd	3.00E-06 per hour	6.00E-06 per hour	0.00E+00 per hour
Component Description	Pilot Solenoid Valve	Actuator / Butterfly Valve Assembly	
Failure Rate (Failures per million hours)	6	10	
Percentage of failures to a dangerous mode	50.0%	60.0%	
Data Source	Faradip 3	Faradip 3	
Total Dangerous Failure Rate	9.00E-06 per hour		

Assessed Hardware Integrity For Section **SIL 1**

Total PFD for the Section **3.94E-02**

Spurious Trip Rate **1 trip every 16.3 years**

NOTES
 1. The PFD calculation is assumed to be valid if the proof test interval is at least FIVE times less than the demand rate on the overall protective function.

REV	BY	CHKD	APPD	DESCRIPTION	DATE
A	CC			FOR DESIGN	

PROJECT NO: 99996
 PROJECT TITLE: Hazards XV1
 CLIENT: Make It Safe Chemicals

amec logo

DOC NO: 99996-0000-32-09-6101

REV: A
 SHT 1 OF 1

Version 1.01 Copyright Amec

Figure 6 – Integrity Assessment Calculation Result of a 1 Out Of 1 Architecture

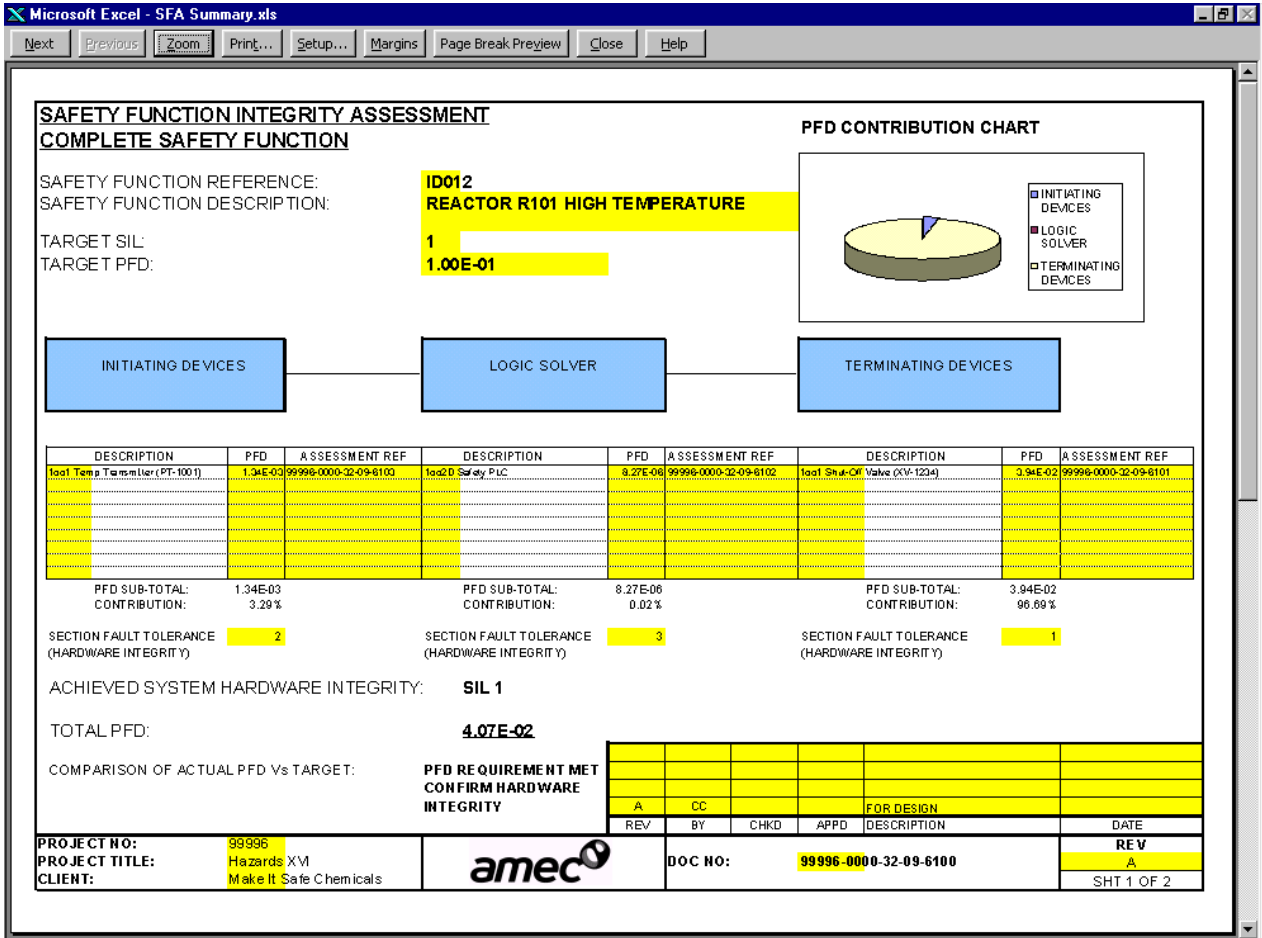


Figure 7 – Integrity Assessment Calculation Result for a Complete Safety Function