

***Instrumented Safety Reliability – One Approach to Optimising the Design Reliability and Maintenance Proof Testing Relationship.***

***BP Exploration & ABB Eutech***

**Authors:**

Stuart Nunns

ABB Eutech, UK

Craig Mason,

BP Exploration, UK

**Contact Details:**

Stuart Nunns

ABB Eutech

PO Box 99

Belasis Hall Technology Park

Billingham

Cleveland TS23 4YS

Tel: 01642 372134

Fax: 01642 372111

E-mail: [stuart.nunns@gb.abb.com](mailto:stuart.nunns@gb.abb.com)

***Introduction***

In the process industries it is becoming increasingly unacceptable to operate in a way which risks hurting people or damaging the environment. Companies that cannot assure Safety, Health or Environmental (SHE) compliance are subject to regulatory or legal sanctions and loss of public support, leading to what could be catastrophic effects on reputation and revenue. In a highly competitive, cost sensitive sector, this compliance must be achieved in an effective, economic manner

This paper will explore the need for compliant reliable instrumented safety systems, which are cost effective through design and optimising the level of maintenance required whilst still providing adequate safety mitigation.

## ***BP Perspective***

As a major operator in both the historical North Sea and in multiple developing countries worldwide, BP plays a significant role in the oil and gas industry. At the heart of its operations lies its ethic of:

*“no accidents, no harm to people and no damage to the environment”*

Achieving this ethic is partly reliant on the successful application of IEC61508<sup>1</sup> and latterly IEC 61511<sup>2</sup>. To be considered successful this application needs to be ***consistent*** and ***auditable***, covering all of BP's existing operations and new projects, and involve both BP engineers and vendors/contractors working on and specifying Instrument Protective Systems on behalf of BP.

Out with the successful application of these standards the design of Instrument Protective Systems, and once installed, their testing frequency to maintain plant integrity and reliability is an optimisation problem.

For a new build we have two cases: On one hand we have a simple system costing little up front but requiring regular maintenance and testing, resulting in a high life time cost. At the other end is the complex system costing a lot upfront but requiring little testing and maintenance, but still with an overall high life time cost. The optimum lies somewhere in between these two cases, but where?

For existing operations there is the ever present drive to reduce costs, this results in a squeeze on people, processes and technology. The ongoing testing of Instrument Protective systems is a significant cost on any operating asset and being able to minimise this cost whilst maintaining plant integrity/reliability would be of real benefit. But how to do this?

As can be seen both the new build case and the existing ops case talk about the balance between costs and maintaining equipment integrity and reliability. IEC 61508 and IEC 61511 provide the foundation to enable this balance to be found, however they also require the operator to demonstrate that IL requirements of the standards are being met.

BP developed an in-house software tool 'Trip Testing Interval Calculator' (TTIC) to enable these optimums to be located and through the use of hardcopy signoff sheets the tool also provided an auditable trail enabling BP to demonstrate the achievement Integrity Level (IL) protection.

As with many tools/software products the development started in a small corner of the company (BP Chemicals at Hull) and slowly spread to other sites/engineers. Then through continual use, modification and reuse the functionality and usability improved until it was a robust and commonly used tool. However, BP is not a software owner and at this point sought an external partner to commercialise the software, proving BP with a fully supported tool and the external company with a commercial product, a win-win situation! ABB-Eutech was selected as the commercial partner.

The commercialisation of the tool enabled it to be developed fresh, from the 'ground up', utilizing BP's operating experience and ABB-Eutech's software and safety systems expertise. The experience of the two partners and the re-basing of the tool enabled several new benefits to be realised.

- Firstly the tool was moved into a secure software environment leading to a fully auditable electronic system
- Secondly the new software uses a client server architecture enabling single point storage of IL assessments for a whole asset/region
- Thirdly the new architecture results in a single database of Instrument MTBF data facilitating the use of the tool for knowledge management

Overall the partnership development of the commercial TRAC tool was highly successful due to both operator and vendor involvement, with both parties openly bringing their experience and expertise to the table. Through this open approach a tool was developed and delivered that exceeded the original expectations of the project and has gone on to deliver significant business benefit.

## *The Current Environment*

Trip and Alarm system compliance features in several standards and directives for the prevention of harm to people and the environment. Typical guidance for compliance can be found within the following documents:

- Pressure Equipment Directive
- Machinery Directive
- Seveso II/ COMAH<sup>3</sup>
- IEC 61508 / IEC 61511

In general operating plants are required to have a safety management system in place, which prevents hazardous events or losses of containment.

A key element within such a functional safety management system will be the approach to the trip and alarm protection philosophy.

Normally, this can be seen in relation to every plant, factory and office building employing a safety system of risk mitigation, often described as a 'layer of protection', designed to protect people – both employees and the public, the environment and, of course, its own productivity, equipment and assets.

An integral part of a process industry manufacturing plants' 'layer of protection' is the instrumented protective system, made up primarily of trips and alarms.

To provide an adequate level of reliability the design engineers and subsequent operating and maintenance teams need to consider relevant key themes for both reliability performance and safety integrity. This will normally involve providing documented evidence in the following areas:-

- Design basis documented and traceable
- Testing for functionality and reliability by the appropriate methods
- Testing at the required intervals
- Manage repairs appropriately

- Maintain technical records for the instrumented safety loop
- Conduct analysis of failures and corrective actions

One framework to aid delivery of compliance for these important activities is the use of the lifecycle strategy and supporting guidance that is found within IEC 61508 for the Functional Safety of Electrical, Electronic and Programmable Electronic Safety Related Systems.

The International Standard, IEC 61508 covers the functional safety of electrical, electronic and programmable electronic systems and constitutes good practice for instrumented protective systems. The standard is a pre-cursor to a more robust approach for industry to demonstrate that appropriate reliability, functionality and performance are built into equipment and that it is maintained effectively. IEC 61511 will be used as the vehicle to interpret the framework of IEC 61508 specific to the process industries.

### ***Instrumented Protective Systems***

As instrumented systems play such a crucial role in controlling potential accident hazards, it is vital that the trip and alarm systems themselves do not malfunction.

Appropriate design and installation is necessary, and it is normally obligatory to maintain the system effectively and undertake functional testing at regular intervals, to reveal any covert failures of the system and satisfy the integrity and risk acceptability criteria of the installation.

### ***Reliability as Part of the Compliance Process***

Within IEC 61508, a set of key criteria is required to be met by a plant to demonstrate that appropriate reliability and functionality is built into the trip and alarm equipment, and that it is maintained effectively.

Utilising the IEC 61511 lifecycle approach a key area in determining the appropriate reliability and the eventual maintenance testing regime of the instrumented protective systems is the process of SIL (Safety Integrity Level) determination.

On most process plant the majority of the instrumented protective functions will be SIL 1. The safety functions at a SIL 3 rating are normally very rare, therefore the maintenance proof testing and resultant cost of maintaining the reliability of these functions will reside with the bulk of the SIL 1 systems i.e. typically 80-90% of the safety functions will be classified as SIL 1 or Ungraded.

Key aspects to the process of SIL determination should cover the following attributes:

- Utilise appropriate reliability data
- Optimise test intervals, appropriate for the EUC and are cost effective
- Use Qualitative and Quantitative methods
- Justify of techniques and measures used
- Document the decision basis
- Define competencies by team composition

and SIL rigour is important!

Testing should verify the end-to-end performance of the safety loop. No section of the trip loop should be untested, even if it means testing the inputs and outputs of the loop at differing times.

Optimising the component architectures to meet both the SIL reliability rigour and practical maintenance proof testing frequencies in accordance with industry good practice is paramount in today's legislative environment.

To help in this process, Industry has highlighted the requirement to provide a level of automation for SIL determination in accordance with IEC 61508's principles, to assist instrument designers and operations teams, where the majority of instrumented protective systems are SIL 1 and where complex loop design and corresponding test methods are not the norm.

## *Automating SIL Determination*

Building on the successful development of the BP TTIC software tool both ABB Eutech and BP collaborated to develop the TTIC tool further in accordance with the good practices identified within IEC 61508. The result of this collaboration is a software tool named 'TRAC', Trip Requirement and Availability Calculator.

Recognising that IEC 61508/IEC 61511 would become the benchmark standard for instrumented protective systems then any support tools would need to be developed using IEC 61508/IEC 61511 terminology and drawing upon recommended SIL determination techniques such as calibrated risk graphs.

Accordingly the TRAC software program specification was jointly developed and designed to assist project design and maintenance engineers in determining the optimum reliability design configuration and required SIL, including the periodic test intervals of a plant's instrumented protective system including trips and alarms.

Advisory software such as TRAC is designed to provide repeatable calculations from a set of consistent process industry based failure data, which ensures effective and appropriate functionality to maintain the required level of safety, environmental and/or asset protection.

By focusing on the relevance of the instrumented protective system, consequences of failure on demand and using reliability and IEC 61508 Risk Graph methodologies, an optimum range of test intervals for the trip and alarm system can be calculated, set against the projected annualised cost. The instrumented protective systems architecture can be configured to meet the desired test intervals while still achieving the target integrity level.

TRAC is designed to fundamentally support design and maintenance features such as:

- IEC 61508 risk graph methodologies for SIL determination
- Safety function architectural configurations
- SIL related calculations
- Reliability data
- Analysis and reclassification of existing safety functions

- Choice of beta factor and process/environmental conditions

The benefits in automating the SIL process for the majority of the plants instrumented protective functions is a significant reduction in the overall design and maintenance burden whilst retaining compliance with regulatory and organisational requirements, with supportable auditable documentation.

A further feature of TRAC is that it can be used on existing instrumented protective functions where there is pressure to reduce ongoing maintenance costs. By demonstrating that the target integrity level is retained, 'What If' scenarios can be undertaken to evaluate extending the test intervals to an appropriate frequency, such as to coincide with a plant shutdown for maximum convenience, generating proof testing labour savings.

### ***Conclusions***

The advent of TRAC has culminated in the design of a software tool with the ability to provide a means to optimise of trip testing intervals relative to cost and reliability, in accordance with the principles of IEC 61508/IEC 61511 and the surrounding regulatory framework.

TRAC provides an example of successful collaboration between two major international organisations that seek to maintain instrumented protective system reliability whilst maximising asset effectiveness.

TRAC is geared to provide multiple architectural solutions for the testing of inputs and outputs within target SIL bands of the required maximum & minimum allowable probability of failure on demand.

For each test interval scenario a cost of testing is calculated from known annual testing costs. Results are displayed graphically and a comprehensive report is issued with full traceable and archived decision processes.

TRAC is one element of industries desire to fully automate the IEC 61508/IEC 6511 functional safety lifecycle in order to drive down CAPEX and OPEX spend and ultimately '*Profit Through Safe Systems*'.

### ***References***

1	IEC 61508 - Functional Safety of Electrical/Electronic and Programmable Electronic Safety Related Systems
2	IEC 61511 – Functional Safety – Safety Instrumented Systems for the Process Industry Sector
3	Seveso II/COMAH – European Union Directive 92/86/EC- SEVESO II & UK Control of Major Accident Hazards Regulations 1999.