HazAus2015/1507

Functional Safety: the Next Edition of IEC 61511

Mirek Generowicz
Engineering Manager
I&E Systems Pty Ltd
Level 2, 445 Hay Street
Perth WA 6000

Abstract

The functional safety standard IEC 61511 provides a framework for managing instrumented safety systems in the process sector.

The overall objective is to ensure that the systems reliably deliver sufficient risk reduction to reduce risk to acceptable levels.

IEC 61511 has remained essentially unchanged since 1996 when it was first released in the USA in the form ISA S84.

A revised edition of IEC 61511 has been prepared and is expected to be released by the end of 2015.

The revisions are still subject to some discussion and debate but there is basic agreement on the main changes.

This paper outlines:

- A brief history of the standard
- An overview of how the standard works to achieve reliable risk reduction
- The changes that are likely to be adopted and why those changes are necessary.

Application

Everybody involved in owning, operating, designing or building hazardous facilities has a **Duty of Care** under occupational health and safety legislation. We are obliged to:

- Identify appropriate standards
- Take reasonable steps to apply the standards
- Monitor compliance
- Demonstrate compliance

IEC 61511 is now a well-established in Australia and around the world.

It is the appropriate standard to apply wherever companies in the process sector choose to apply ‘safety instrumented functions’ to achieve risk reduction for workplace hazards.

IEC 61511 applies to all of us who are in a position to influence those hazards. It is not simply a standard for equipment suppliers or just for instrumentation and control engineers

Introduction

Safety instrumented systems have been delivering risk reduction for at least half a century.

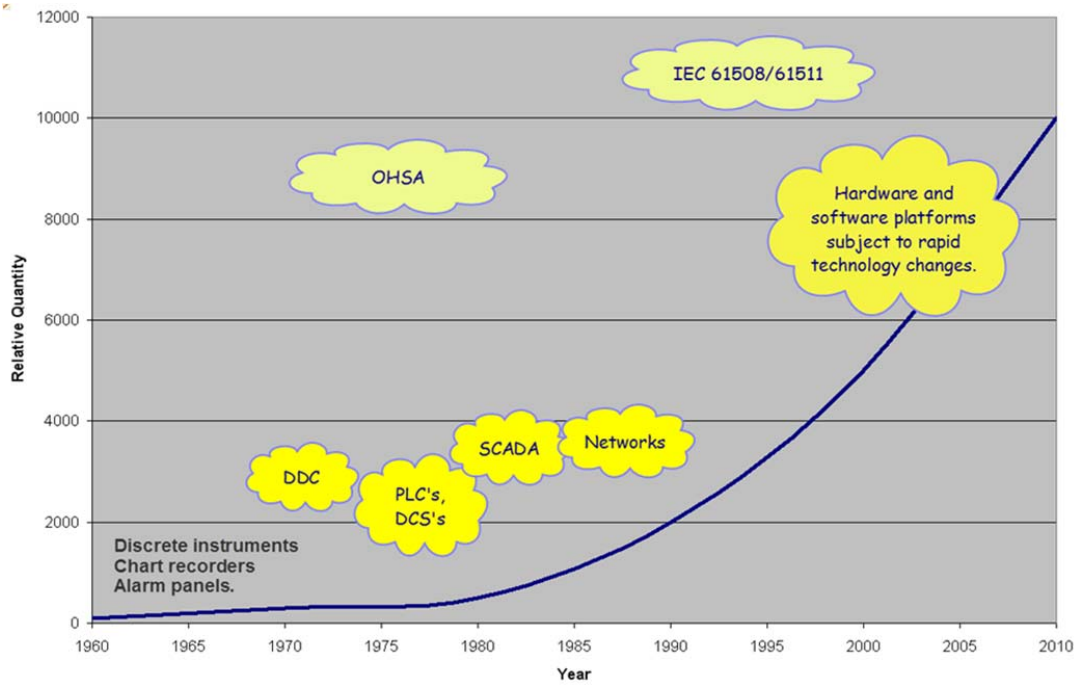
In the early years of automation after the Second World War safety instrumented functions were implemented using simple pneumatic, hydraulic or hardwired electrical circuits. These simple functions were easy to understand and had failure modes that were well defined. The behaviour under fault conditions could be completely determined and predicted.

Electronic and programmable electronic systems came into use in safety functions during the 1970s.

Electronic and programmable electronic systems have indeterminate failure modes. They do not inherently fail into a safe state. They are subject to hidden or latent faults that can be difficult to eliminate. Failure modes and behaviours cannot be completely determined and predicted.

Programmable systems in particular have hidden complexity, and the complexity has been increasing exponentially for several decades. Complex systems are subject to the risk of systematic failures, failures caused by errors and failures in the design and implementation of the systems.

Engineering practices evolved over decades in response to increasing complexity.



Standards Evolution

Various standards were developed in the 1980s and 1990s to provide guidance in controlling the risk of both systematic failures and random failures:

- Health and Safety Executive (HSE UK) Guidelines - 1987
  'Programmable Electronic Systems in Safety Related Application'

- ISA S84 – 1996
  'Application of Safety Instrumented Systems for the Process Industry'
- IEC 61508 Ed. 1 – 1998, Ed. 2 - 2010
  'Functional safety of electrical/electronic/programmable electronic safety-related systems'
- IEC 61511 – 2003
  'Functional safety – Safety instrumented systems for the process industry sector' (virtually identical to ISA S84)

The content of IEC 61511 has remained essentially unchanged since it was first released in ISA S84 in 1996. Almost 20 years of experience has been gained since that first release.

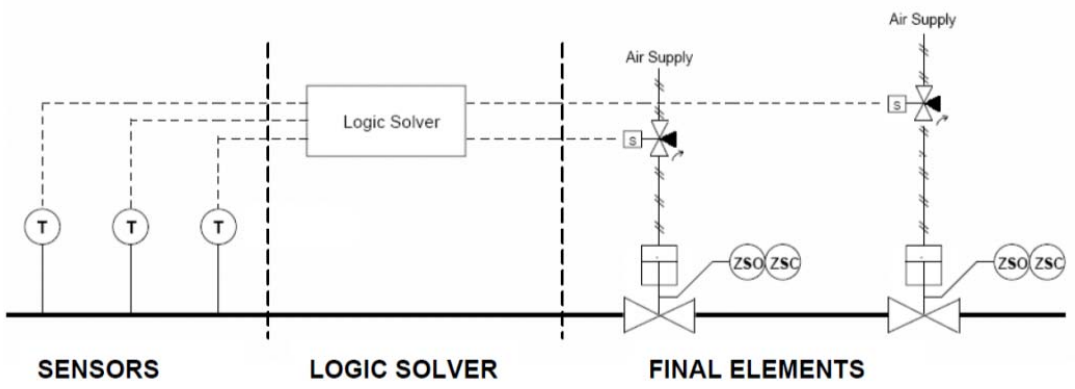
The Objectives of the Standard

Risk Reduction Factor

'Functional Safety' refers to "**Safety Instrumented Systems**" (SIS) that implement "**Safety Instrumented Functions**" (SIFs) as part of a company's **overall risk management strategy**.

Safety Instrumented Functions

- Respond to a specific, defined hazard
- Implement a specific action
- Put the equipment into (or maintain) a safe state
- Provide a defined degree of risk reduction



The risk reduction required from a function is characterised by the 'Safety Integrity Level' or SIL. To put it simply, each safety function is designed to deliver either 1, 2 or 3 orders of magnitude in risk reduction. SIL 1, SIL 2 and SIL 3 correspond to Risk Reduction Factors of at least 10, 100 and 1,000.

Reliable Risk Reduction

Safety functions can fail due to

- Systematic failures, caused by errors and failures in the design, implementation, operation and maintenance of the systems

OR

- Random hardware failures, those failures that can never be completely eliminated by controlling the design, implementation, operation and maintenance.

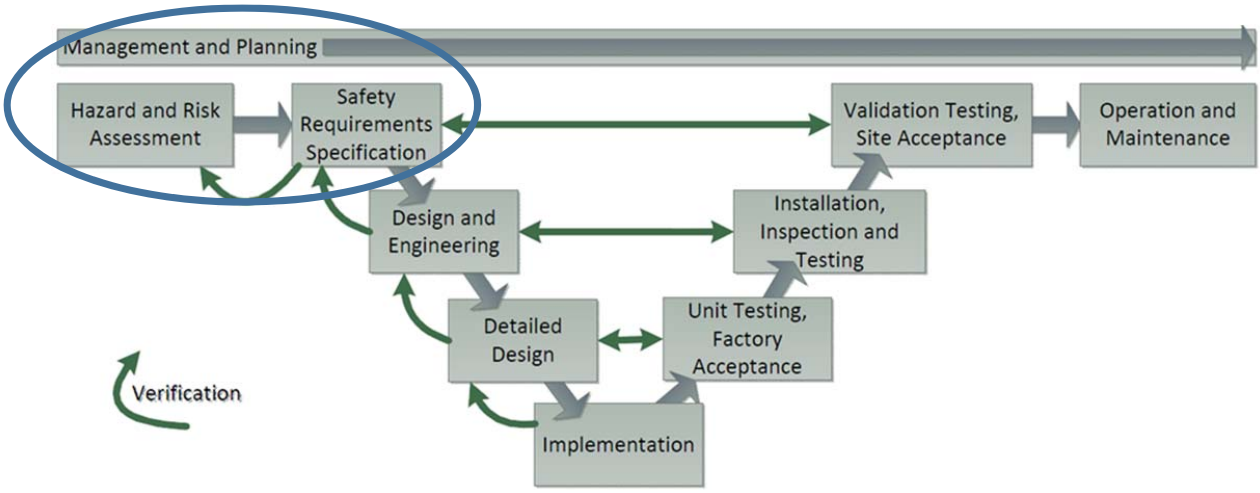
Systematic Integrity

IEC 61511 outlines well defined and detailed quality management practices to avoid or to control the risk of systematic failures.

The degree of attention to detail and the level of effectiveness in the techniques applied depend on the risk reduction required.

SIL 3 safety functions need to be 100 times as reliable as SIL 1 safety functions. Design, checking, inspection and testing techniques need to be proportionately more effective.

IEC 61511 defines a '**safety lifecycle**' (similar to a quality process):



Safety requirements are defined in objective terms to achieve measurable risk reduction.

The hazard and risk assessment and the safety requirements derived from it form the basis for the whole system. Management and planning provide a framework to ensure systematic integrity and dependability.

The safety lifecycle applies traceability, verification and validation to ensure that the requirements are fulfilled.

The owners, end users and process designers play a vital role in the IEC 61511 safety lifecycle because they are ultimately accountable for the risk management.

Hardware Integrity

To deliver a risk reduction factor of 10, the probability of failure on demand must be less than 0.1

To deliver a risk reduction factor of 1000, the probability of failure on demand must be less than 0.001

IEC 61511 and the related standard IEC 61508 describe techniques to evaluate the probability of random hardware failure.

The probability of failure of a function can be reduced by increasing the coverage and/or frequency of regular testing. It can be reduced by selecting devices with lower failure rates. It can also be reduced by applying a fault tolerant design – which means that the function can continue to function successfully with one or more failed components. For instance if two block valves are used in series the probability that both will fail is lower than the probability of a single valve failing.

Minimum Acceptable Fault Tolerance

When the standards were developed it was recognised that the there was a great deal of uncertainty in the failure rate statistics and in the assumptions made in the design.

To compensate for the uncertainty the standards set minimum levels of fault tolerance for each part of a safety function.

The level of fault tolerance that is appropriate increases with the risk reduction required. IEC 61511 defines minimum **hardware fault tolerance** (HFT) requirements for the sensors, logic solvers and final elements that make up each safety function.

Lessons Learned in Practice

Systematic Integrity Not Well Understood

The long history of major accident events shows that many users have failed to understand and apply the requirements for managing quality or 'systematic integrity'.

The conclusions from many reports include these recurring systematic failures:

- Lack of appreciation of organisational roles, responsibilities and interfaces
- Poor safety culture and a lack of leadership in safety
- Inadequate attention paid to personnel competencies – and in particular management competencies
- Equipment poorly maintained
- Alarms and automatic shutdown systems not working properly
- Inadequate control of modifications to critical systems
- Safeguards bypassed – or not even commissioned
- Lack of documentation for safety systems

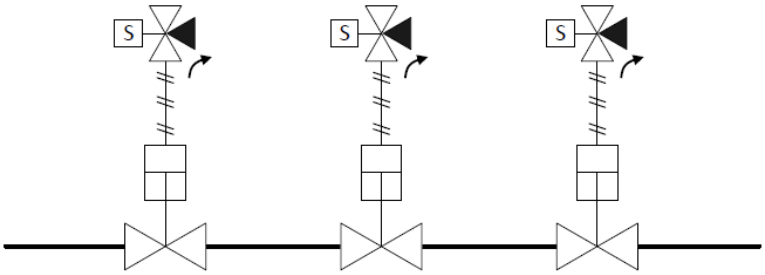
Minimum Acceptable Fault Tolerance Impracticable

The hardware fault tolerance required by IEC 61511 has been too onerous to achieve in practice. Most users have found it difficult to comply with the standard. The methods of assessing the HFT requirements are complicated and difficult to use.

To minimise the HFT requirement to a practicable level users need to obtain extensive evidence about the suitability of the devices being used. Users also need to ensure that the majority of failures are to a safe state or that dangerous failures are promptly detected and repaired.

Actuated valves are commonly used as final elements in safety functions, but the dominant failure mode of actuated valves is dangerous. The most common failures cause the valves to stick or jam in a dangerous state.

In the existing IEC 61511 standard a risk reduction factor of 1,000 or more (SIL 3) requires at least three block valves in series as final elements – unless continuous automatic diagnostic functions can be implemented:



In many cases this is impracticable, and non-compliance is widespread. The most common practice is to use only two valves in series in a double block or double block and bleed arrangement. Installing a third block valve not only increases the cost; it also increases the risk of spurious trip and loss of production. Continuous automatic diagnostic functions are not usually practicable in the process sector.

The Changes in the New Edition

The new edition of IEC 61511 will include:

- New requirements for systematic capability
- New requirements for formal functional safety management systems
- New requirements for formal procedures to manage competence
- New security risk assessments, relating to deliberate malicious interference
- More detailed requirements about planning for verification
- Clarification of requirements for risk reduction is spread across multiple SIFs
- New annexes with detailed guidance
- Simplified requirements for hardware fault tolerance
- Requirements for better substantiation of the failure rate data and of uncertainties in the data
- Revised software development requirements
- Additional requirements for bypasses
- Formal review by operations and maintenance of the hazard and risk assessments
- Independent assessment of modifications to systems before implementation.

Systematic Capability

The concept of systematic capability was introduced in the 2010 edition of IEC 61508. Systematic capability is essentially a measure of the effectiveness of quality management techniques applied to components. Requirements for systematic capability are included in the new edition of IEC 61511.

Functional Safety Management Systems

The purpose of a functional safety management system is to achieve systematic integrity.

Functional safety management has been poorly understood and largely ignored throughout the process sector, particularly by the end users or plant owners.

Any organisation with responsibility for one or more phases in the lifecycle must now demonstrate a functional safety management system as well as a quality management system.

This requirement applies just as much to end users and owners as it does to designers and suppliers.

The operation and maintenance of a safety instrumented system must be managed under a formal system of functional safety procedures.

Competency

More emphasis has been put on competency requirements for all parties involved in designing, developing, implementing, operating and maintaining SIS.

The wording in the standard has been changed from describing factors that '***should***' be addressed when considering competence to factors that '***shall***' be addressed.

A new sub-clause has been added requiring formal procedures to manage competence and requiring periodic assessments of competence of individuals with respect to their responsibilities.

There are competency requirements for those in charge too: Managers and leaders need to have adequate knowledge, ability and experience relating to the activities for which they are accountable.

Security Risk Assessment

In the section of the standard dealing with process hazard and risk assessment, a new sub-clause has been added requiring a security risk assessment. This relates to security of the systems from deliberate malicious interference, as distinct to the risk assessment of materials, process and equipment.

Verification

A new sub-clause has been added with more detailed requirements about what should be covered in planning when verification is to include testing.

A new sub-clause has been added specifically requiring verification that non-safety functions that are integrated with safety function do not interfere with the safety functions. Lack of separation between safety functions and non-safety functions has been a widespread problem which compromises safety integrity.

Multiple SIFs

A new sub-clause clarifies that if risk reduction is spread across multiple SIFs within the same SIS, then the safety integrity achieved must meet the overall risk reduction requirement taking into account dependencies.

Risk Reduction > 10 000

The requirements for achieving four or more orders of magnitude reduction in risk are specified in much more detail.

In IEC 61511-3 there is a new Annex J that provides very detailed guidance on the evaluation of dependencies between multiple safety systems or functions. This annex is particularly relevant to where high levels of risk reduction are achieved by splitting risk reduction across multiple systems.

Hardware Fault Tolerance

The requirements for HFT have been simplified and aligned with the method 'Route 2_H' that was introduced in the 2010 edition of IEC 61508.

The level of hardware fault tolerance required has been reduced with the justification that failure rate with increased confidence levels will be used.

SIL 3 can now be claimed with only two block valves in series (fault tolerance of one). An increased level of confidence in the failure data is required. The proposed IEC 61511 edition stops short of specifically requiring the 90% confidence level required by IEC 61508, but it does require an equivalent demonstration of confidence in the data.

The 'systematic capability' of components and subsystems must be demonstrated. That means that the quality control must be appropriate for the level of SIL claimed.

New sub-clauses have been inserted into the section on 'Quantification of random failure' requiring better substantiation of the failure rate data and of uncertainties in the data.

The calculated probability of failure will need to consider faults that might never be detected, and failures that might be caused by periodic testing.

Software Development

The clause on application software has been completely re-written, though there are no obvious or significant changes in requirements.

The new clause is shorter.

The application program development lifecycle is now integrated into the overall safety lifecycle. In the earlier edition it was described separately.

Control of Bypasses in Operation

History has shown us that the application of bypasses and overrides has contributed to the cause of many disasters.

A new sub-clause has been added requiring additional risk management where SIS devices are bypassed in continuous operation.

A new sub-clause requires all bypasses to be authorised and logged.

A new sub-clause requires spare parts to be identified and made available to minimise bypass duration.

Operations and Maintenance Review of Hazard and Risk Assessment

There has often been a lack of communication between the designers and those responsible for operation and maintenance.

A new sub-clause requires those responsible for operations and maintenance to review the assumptions made in hazard and risk assessment.

SIS Modification

A new sub-clause emphasises the need to update documentation affected by a modification.

A new sub-clause requires independent assessment of the functional safety before any modification is implemented.

Annexes

IEC 61511 parts 2 and 3 include many annexes that provide guidance on implementing the standard.

Extensive changes, deletions and additions have been proposed for the annexes in the new edition.

Summary

The changes in the new edition are primarily aimed at improving systematic safety integrity.

The objective is to prevent the recurring systematic failures that have been evident for many years throughout the process sector. These failures are all preventable.

The requirements for hardware fault tolerance have been reduced, but the failure rate data used in calculations must be more reliable. The quality and suitability of components must be demonstrated.

The guidance and support material has been enhanced in the standard to assist safety and design engineers, safety assessors, and operators.

Over the past 20 years the standard has been applied widely and shown to be practicable. The changes make the standard simpler and should improve the level of compliance that can be readily achieved.

Regulators now expect a reasonable level of compliance to the standard.

Our Duty of Care requires us to be able to demonstrate compliance with IEC 61511.

Owners, end users and EPC/EPCM contractors will need to improve and to formalise the way they execute engineering activities in order to comply with the standard requirements.

For more information on functional safety visit: http://www.iesystems.com.au/publications/