Towards Systematic Integrity

Abstract

Investigations into recent disasters such as Deepwater Horizon, Montara and Buncefield found multiple systematic problems at all levels across the many organisations involved.

The international standards on functional safety IEC 61508 and 61511 have 2 main objectives:

- Manage risk of random hardware failures
- Manage risk of systematic failures

Random hardware failure rates can be analysed mathematically. Engineers usually find it relatively easy to understand and to calculate random hardware failure rates.

It is significantly more difficult to embrace the management of ***systematic*** failures. This is about avoiding errors and failures due to the design, implementation and operation of the systems.

Systematic integrity is achieved through applying appropriate methods and techniques.

It is just as important to achieve systematic integrity as it is to control probability of random hardware failures in safety instrumented systems.

This presentation explains the concept of systematic integrity and outlines the steps that organisations need to take to achieve and maintain integrity.

Practical Exercise

The session will conclude with a short practical exercise. Participants will be guided in outlining a framework to manage systematic integrity in their own organisations.

Outline

The Problem: Multiple Systematic Failures

There is plenty of “disaster porn” for engineers. After each major disaster we have yet another report.

37 years ago we had Flixborough, then the Cullen report on the Piper Alpha followed by Longford, Buncefield, Deepwater Horizon (Macondo), Montara and others.

> ***disaster porn*** /dɪˈzɑːstə pɔːn/
>
> **Noun**. When the media puts horrific or tragic images on a 24 hour loop, constantly driving them into your head, and then refers to the events portrayed as an "unspeakable tragedy" . .. .despite the fact that they have 4 different talking heads analyzing it 24 hours a day.
>
> (from www.urbandictionary.com)

Buncefield Oil Depot explosions and fire, December 2005

From http://www.buncefieldinvestigation.gov.uk/:

> *In the early hours of Sunday 11th December 2005, a number of explosions occurred at Buncefield Oil Storage Depot, Hemel Hempstead, Hertfordshire. At least one of the initial explosions was of massive proportions and there was a large fire, which engulfed a high proportion of the site. Over 40 people were injured; fortunately there were no fatalities. Significant damage occurred to both commercial and residential properties in the vicinity and a large area around the site was evacuated on emergency service advice. The fire burned for several days, destroying most of the site and emitting large clouds of black smoke into the atmosphere*

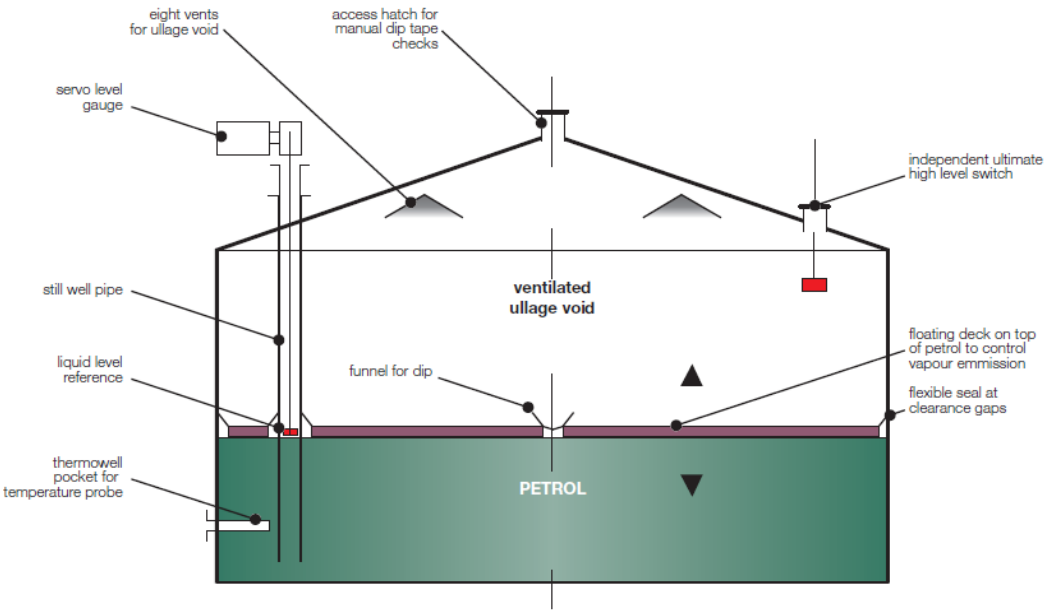
The initial event is described in the final report, Volume 1, p7:

> *“ Late on Saturday 10 December 2005 a delivery of unleaded petrol from the T/K pipeline started to arrive at Tank 912 in bund A at about 05:30 on 11 December. The*

safety systems in place to shut off the supply of petrol to the tank to prevent overfilling failed to operate. Petrol cascaded down the side of the tank, collecting at first in bund A. As overfilling continued, the vapour cloud formed by the mixture of petrol and air flowed over the bund wall, dispersed and flowed west off site towards the Maylands Industrial Estate."

From "The final report of the Major Incident Investigation Board, Volume 2":

The immediate cause of the incident at Buncefield was put down to failures in level instrumentation and in the overfill protection safeguarding systems. The hardware failures were exacerbated by multiple systematic failures in the design, installation, operation, maintenance and testing of safety systems.



Failures in instrumentation and safeguarding systems are involved in most of the disasters that we read about.

In each case the story and the pictures are different, but somehow they are all disturbingly similar. There are number of recurring themes:

- Weaknesses in the design of safety-related control systems
- Equipment poorly maintained
- Alarms and automatic shutdown systems not working properly
- Poor safety culture and a lack of leadership in safety
- Inadequate attention paid to personnel competencies – and in particular management competencies
- Lack of appreciation of organisational roles, responsibilities and interfaces
- Operators unaware of the significance of control systems as control measures against major accident events
- Inadequate control of modifications to critical systems
- Lack of documentation for safety systems
- *Multiple "systematic" failures*

The Solution: Systematic Capability

To address the problem of systematic failures the new 2010 edition of IEC 61508 introduced the new concept of "systematic capability".

This paper explains the meaning of the strange new term "systematic capability".

It describe es tools and resources that are available to assist in establishing and assessing systematic capability.

What is "Systematic Capability"?

According to the definition given in AS 61508.4—2011 / IEC 61508-4 Ed.2.0 (2010):

> **3.5.9**
> **systematic capability**
> measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element
>
> NOTE 1 Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).
>
> NOTE 2 What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.
>
> NOTE 3 A Systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

It seems to be another "made up" buzzword invented by a European committee.

To understand what this means we need to see it in the context of safety integrity:

Safety Integrity

One of the recommendations in the Buncefield report was that:

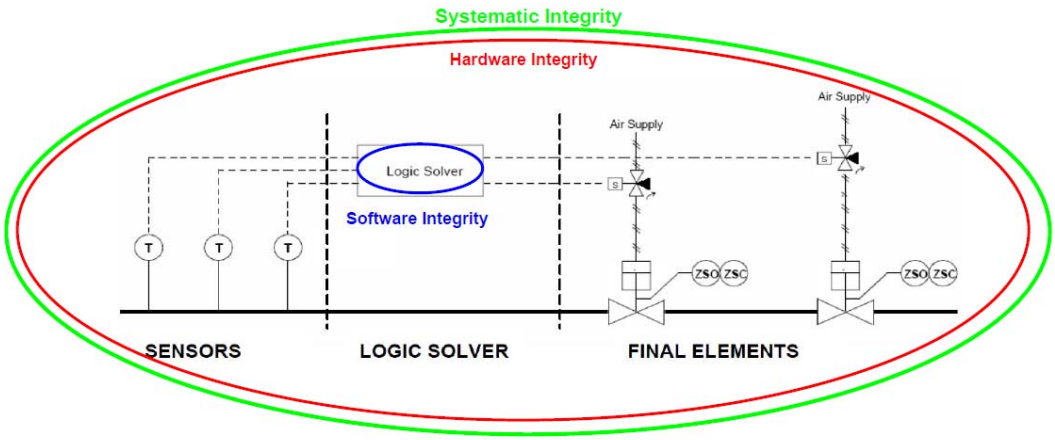
> *The [safety systems] should be **engineered, operated and maintained** to achieve and maintain an appropriate level of **safety integrity** in accordance with the requirements of the recognised industry standard for 'safety instrumented systems', Part 1 of BS EN 61511.*

Safety Integrity is defined as:

> **3.5.4**
> **safety integrity**
> probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time
>
> NOTE 4 Safety integrity comprises hardware safety integrity (see 3.5.7) and systematic safety integrity (see 3.5.6).

Safety Integrity is comprised of:

- Hardware Safety Integrity
- Systematic Safety Integrity (which includes Software Safety Integrity).



Hardware Safety Integrity is to do with the management of **random hardware failures**:

> **3.5.7**
> **hardware safety integrity**
> part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure

Systematic Safety Integrity (and Software Safety Integrity) is to do with the management of ***systematic failures***:

> **3.5.5**
> **software safety integrity**
> part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure that are attributable to software
>
> **3.5.6**
> **systematic safety integrity**
> part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure
>
> NOTE Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

Quantifying Safety Integrity Level (SIL)

3.5.8
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

The fundamental purpose of a Safety Instrumented System is to implement Safety Instrumented Functions (SIFs) as part of a company's overall risk management strategy.

The objective of each SIF is to deliver a specific Risk Reduction Factor. This is to achieve one of the layers of risk mitigation within an overall risk management plan.

Each SIF has a Safety Integrity Level (SIL) that corresponds directly with the Target Risk Reduction Factor:

SIL1: RRF between 10^1 and 10^2

SIL2: RRF between 10^2 and 10^3

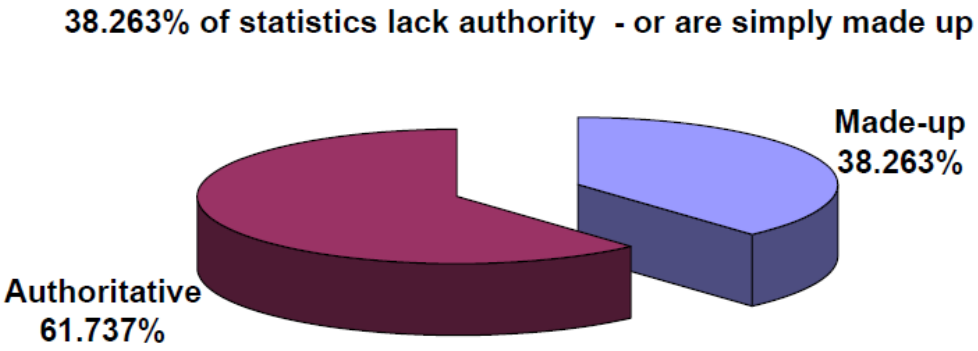
SIL3: RRF between 10^3 and 10^4

SIL4: RRF greater than 10^4

Assessing SIL is relatively easy; we can quantify Risk Reduction Factor and the Probability of Failure on Demand and we can assess the Hardware Fault Tolerance objectively.

The most difficult aspect is to deal with the uncertainty and ambiguity that is inherent in SIL studies. Some technologists find it hard to combine the heuristic and statistical methods that we need to quantify the SIL. We should worry when we see results such as RRF = 117.4

In risk management we can only work within orders of magnitude, SIL studies cannot be carried out with precision. Information on failure rates is always imprecise.



AS 61508.5—2011 / IEC 61508-5 Ed.2.0 (2010) gives examples of methods for the determination of safety integrity levels.

The idea of Safety Integrity Level applies only to each Safety Function as a whole; it is not a property of systems, subsystems, elements, components or of software.

"***Systematic Capability"*** is the equivalent measure that we use for system, subsystem, element, component and software

There is a one-to-one correspondence between Systematic Capability and Safety Integrity Level.

SC ≈ SIL

For a SIL *n* SIF we need SC *n* systematic capability in our engineering and in our software.

Quantifying Systematic Capability

It is easy to understand how we can quantify safety integrity with SIL. It is not so obvious how we can quantify systematic capability.

Random failures can be readily quantified (within an order of magnitude) but cannot be individually controlled. The target SIL is achieved by selecting equipment with quantified failure rates and by applying redundancy in the hardware architecture.

Systematic failures – failures in design, development, operation and maintenance – cannot be quantified but they can be readily controlled through appropriate engineering techniques and measures.

Systematic capability is achieved and assessed through applying techniques and measures for the **avoidance and control of systematic faults**.

3.5.9
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

NOTE 1 Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

NOTE 2 What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.

NOTE 3 A Systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

Systematic capability is quantified in the range SC 1 to SC 4 according to:

- which techniques and measures are applied

and

- the degree of effectiveness or rigour with which they are applied.

AS 61508.2—2011 IEC 61508-2 Ed.2.0 (2010) defines 3 routes for achieving systematic capability:

> **7.4.2.2** The design of the E/E/PE safety-related system (including the overall hardware and software architecture, sensors, actuators, programmable electronics, ASICs, embedded software, application software, data etc.), shall meet all of the requirements a) to e) as follows:
>
> c) the requirements for systematic safety integrity (systematic capability), which can be met by achieving one of the following compliance routes:
>
> – Route 1_S: compliance with the requirements for the avoidance of systematic faults (see 7.4.6 and IEC 61508-3) and the requirements for the control of systematic faults (see 7.4.7 and IEC 61508-3), or
>
> – Route 2_S: compliance with the requirements for evidence that the equipment is proven in use (see 7.4.10), or
>
> – Route 3_S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12;
>
> NOTE The "S" subscript in the above routes designates systematic safety integrity to distinguish it from Route 1_H, and Route 2_H for hardware safety integrity.

Route 1_S is the primary route that we will explore in this paper. Routes 2_S and 3_S are essentially retrospective, for existing systems.

Route 2_S is for equipment "proven in use". This route relies on "***adequate documentary evidence***":

> **7.4.10.1** An element shall only be regarded as proven in use when it has a clearly restricted and specified functionality and when there is adequate documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity levels of the safety functions that use the element is achieved. Evidence shall be based on analysis of operational experience of a specific configuration of the element together with suitability analysis and testing.

Route 3_S is for pre-existing software. It relies on reverse engineering and ***retrospective documentation*** to show that the software has the required integrity.

Avoidance and Control of Systematic Faults

Management Planning

To achieve avoidance and control of systematic faults in an objective and auditable way we need to start by managing the engineering and operation of the system using a formal plan.

Both AS/IEC 61508 and AS/IEC 61511 outline requirements for planning the management of functional safety. The objectives in management planning are to:

- Establish policies and strategies
- Define the Lifecycle Model, i.e. which parts within the overall lifecycle are relevant
- Define responsibilities
- Specify management and technical activities
  - including procedures, techniques and measures
- Establish the documentation framework
- Facilitate and demonstrate compliance to the standards
- Plan the verification, validation and assessment activities
- Provide a "live" planning document that can be maintained throughout the lifecycle
- Obtain acceptance of the plan from the risk owners

Resources for Management Planning

The requirements for management planning in the standards can be difficult to interpret and understand.

Useful guidelines are available on-line from the UK-based CASS Scheme Ltd, http://www.cass.uk.net and from the 61508 Association, http://www.61508.org

> CASS ("Conformity Assessment of Safety Related Systems") is run by The CASS Scheme Ltd, a not-for-profit company whose members are drawn from a wide range of organizations which use IEC 61508.
>
> The company develops and publishes the documentation necessary for carrying out the assessments as well as providing the criteria and procedure for assessing the competence of assessors. The company also licenses the use of the CASS logo by certification bodies which meet the CASS scheme requirements.
>
> CASS is a scheme for assessing the compliance of safety related systems with the requirements of IEC 61508 and associated standards.
>
> It provides a systematic approach to be used by certification bodies and others when assessing compliance at all stages from the specification of safety requirements through the design, development and manufacture of system components to integration, commissioning, operation and maintenance.
>
> At each stage CASS takes the conformity assessor through the logical steps of defining the scope of the assessment, the target of evaluation, the requirements to be met and the process of demonstrating and recording conformity.

About The CASS Scheme

CASS (Conformity Assessment of Safety-related Systems) is a methodology developed by industry for industry. The CASS methodology enables all sectors of industry to show compliance that can ultimately lead to accredited certification with IEC 61508, the international standard for functional safety of safety-related systems.

The CASS Scheme provides a rigorous and internationally acceptable structure under which consistent certification of safety related systems can take place. The scheme is operated through independent third-party certification bodies, that are accredited to the European and International accreditation standards.

The not-for-profit company is managed by a Board elected by the members who are associations representing manufacturers, designers, installers, users, certifiers or regulators of safety related systems. CASS covers all industry sectors including process, aerospace and transport.

CASS provides a Self-Assessment Workbook and guidelines to assist companies in establishing capability in functional safety management.

CASS Self-Assessment Workbook Outline:

> Part 1: Details of the owner

Part 2: Schedule of Activities

- Table 1 - Overall Activities Covered by the IEC 61508 Group of Standards
- Table 2 - Electrical / Electronic / Programmable Electronic Systems
- Table 3 - Software for Safety Instrumented Systems
- Table 4 - Functional Safety Management

Part 3: Functional Safety Management Self-Assessment Report

Sample CASS FSM Checklist – Part 2, Table 4 - Functional Safety Management

The CASS Scheme Ltd.

CASS Functional Safety Management Declaration
Lodged with CASS-appointed Body.

CASS32

Ref.	CASS Functional Safety Capability	Document	Evidence	Location	Comments
	Target of Evaluation (TOE)				
2.4.1	Functional Safety Management System				
2.4.2	Functional Safety Policy				
2.4.3	Organisation and Responsibilities				
2.4.4	Identification of relevant life-cycle phases				
2.4.5	Documentation structure and content policy				
2.4.6	Techniques and Measures conformance plan				
2.4.7	Corrective action procedure				
2.4.8	Competence assessment process				
2.4.9	Procedure for handling hazardous incidents & near misses				
2.4.10	Procedure for O&M performance analysis				
2.4.11	Functional safety audit process				
2.4.12	Modification process for safety related systems				
2.4.13	Procedures for maintaining information on hazards with respect to Safety-related systems or Safety Instrumented Functions with respect to Safety-Related Systems				
2.4.14	Configuration management procedures				
2.4.15	Procedures for provision of training and information for the emergency services				
2.4.16	Functional Safety Management System - Formal Reviews				
2.4.17	Supplier Assessment Process				
2.4.18	Functional Safety Assessment				

PART 3:FUNCTIONAL SAFETY MANAGEMENT SELF-ASSESSMENT REPORT

Item	Target of Evaluation (TOE)	Requirement (for all SILs)	Systems and procedures in place	Documentary evidence	IEC 61508 2nd edition clause references	Notes
1	Functional Safety Management	**Purpose** To specify all management and technical activities that are necessary to ensure that the E/E/PE safety-related systems achieve and maintain the required functional safety (1/6.1.1) The activities specified as a result of 1/6.2.1 shall be implemented and progress monitored			Part 1 clause 6 Particularly – 1:6.2.1 to 1:6.2.12 inclusive including evidence for all the relevant sub-clauses and 1:6.2.16	
2	Functional Safety Policy	**Purpose** The policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organisation to ensure a culture of safe working There should be a top level policy statement that reflects the safety goals and objectives of the organisation.			Part 1 clause 6 Particularly – 1:6.2.2 and Figures 2, 3 and 4, Table 1, and 1:6.2.1 first bullet	

Item	Target of Evaluation (TOE)	Requirement (for all SILs)	Systems and procedures in place	Documentary evidence	IEC 61508 2nd edition clause references	Notes
3	Organisation and Responsibilities	**Purpose** Identification of the persons, departments and organisations who perform or review safety lifecycle activities and allocation of responsibilities for those activities. To ensure that all those named, nominated, specified or identified as responsible for management of functional safety activities are informed of the responsibilities assigned to them. The allocation of responsibilities must be documented, and shall cover all of the scope of the person's functional safety activities.			Part 1 clause 6 Particularly – 1:6.2.3 and Figure 2, 3 and 4, Table1.	
4	Identification of relevant lifecycle phases	**Purpose** The overall E/E/PES or software safety lifecycle phases to be applied The documented plan shall show that there is an understanding of where all persons involved in functional safety fit within the overall safety lifecycle.			Part 1 Clause 6 Particularly – 1:6.2.1 first bullet and Figures 2, 3 and 4, Table 1.	
5	Documentation structure and content policy	**Purpose** There is a clear definition of the way in which information is to be structured and the extent of information to be documented.			Part 1 clause 6 Particularly – 1:6.2.4 and 1:5.0	
6	*Table continues….*					

Techniques and Measures

Much of the low level detail in functional safety management can be covered by specifying procedures, techniques and measures.

The 61508 standard includes detailed tables that outline procedures, techniques and measures to be used for the avoidance and control of systematic failures:

> AS 61508.2—2011
> IEC 61508-2 Ed.2.0 (2010)
>
> Annex A (normative) Techniques and measures for E/E/PE safety-related systems – control of failures during operation...
>
> Annex B (normative) Techniques and measures for E/E/PE safety-related systems – avoidance of systematic failures during the different phases of the lifecycle .....
>
> AS 61508.3—2011
> IEC 61508-3 Ed.2.0 (2010)
>
> Annex A (normative) Guide to the selection of techniques and measures
>
> Annex B (informative) Detailed tables
>
> Annex C (informative) Properties for software systematic capability

AS 61508.7—2011 / IEC 61508-7 Ed.2.0 (2010) provides detailed descriptions of the techniques and measures.

In the 2010/2011 edition the techniques and measures in Parts 2, 3 and 7 have been updated with minor amendments. 61508.3 Annex C is completely new. It introduces new concepts to support software systematic capability.

61508.2 Annex A

61508.2 Annex A outlines techniques and measures to ***control*** failures:

- Table A.15 – Techniques and measures to control systematic failures caused by hardware design
- Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences
- Table A.17 – Techniques and measures to control systematic operational failures
- Table A.18 – Effectiveness of techniques and measures to control systematic failures

61508.2 Annex B

61508.2 Annex outlines techniques and measures to ***avoid*** failures:

- Table B.1 – Requirements specification
- Table B.2 – Design and development
- Table B.3 – Integration
- Table B.4 – Operation and maintenance procedures
- Table B.5 – Safety validation
- Table B.6 – Effectiveness of techniques and measures to avoid systematic failures

61508.3 Annex A

61508.3 Annex A provides techniques and measures for managing ***software integrity***:

- Table A.1 – Software safety requirements specification
- Table A.2 – Software architecture design
- Table A.3 – Support tools & programming language
- Table A.4 – Software detailed design
- Table A.5 – Software module testing & integration
- Table A.6 – Hardware and software integration
- Table A.7 – System safety validation
- Table A.8 – Modification
- Table A.9 – Software verification
- Table A.10 – Functional safety assessment

61508.3 Annex B

61508.3 Annex B provides detailed techniques and measures for software:

- Table B.1 – Design and coding standards
- Table B.2 – Dynamic analysis and testing
- Table B.3 – Functional and black-box testing
- Table B.4 – Failure analysis
- Table B.5 – Modelling
- Table B.6 – Performance testing
- Table B.7 – Semi-formal methods
- Table B.8 – Static analysis
- Table B.9 – Modular approach

Choosing appropriate techniques and measures

The tables provide guidance on the techniques and measures that are appropriate according to the required SIL - and therefore the required Systematic Capability.

Only a portion of the tables and the techniques and measures will apply to our individual scope. We need to review all of the techniques and measures and choose which should be applied.

There are no “correct answers”, an individual review and judgement needs to be made for every application. The rationale needs to be recorded for management review and approval and to justify that we are doing enough to achieve integrity.

AS IEC 61511

61511.1 requires the use of appropriate techniques and measures but it does not give specific detailed requirements.

> **6.2.3** For all safety life-cycle phases, safety planning shall take place to define the criteria, techniques, measures and procedures to
>
> - ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
> - ensure proper installation and commissioning of the safety instrumented system;
> - ensure the safety integrity of the safety instrumented functions after installation;
> - maintain the safety integrity during operation (for example, proof testing, failure analysis);
> - manage the process hazards during maintenance activities on the safety instrumented system.
>
> **12.4.3.3** The set of methods and techniques used to develop the application software should be identified and the rationale for their choice should be justified.
>
> NOTE These methods and techniques should aim at ensuring
>
> – the predictability of the behaviour of the SIS subsystem;
> – the fault tolerance (consistent with the hardware) and fault avoidance, including redundancy and diversity.

Full compliance with the techniques and measures in 61508 is required for only SIL4. For SIL3 the standard leaves the choice of techniques and measures open.

The reason that 61511 has been left more open is because it restricts software to Limited Variability Languages or to Fixed Program Languages.

AS 61511.1:

> **12.1.2.4** Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to
>
> - minimize the risk of introducing faults into the application software;
> - reveal and remove faults that already exist in the software;
> - ensure that the faults remaining in the software will not lead to unacceptable results;
> - ensure that the software can be maintained throughout the lifetime of the SIS;
> - demonstrate that the software has the required quality.
>
> NOTE The selection of methods and techniques should depend upon the specific circumstances. The factors in this decision are likely to include
>
> – amount of software;
> – degree of complexity;
> – safety integrity level of the SIS;
> – consequence in the event of failure;
> – degree of standardization of design elements.

AS IEC 61511.2 (Guidelines for the application of AS IEC 61511.1) provides detailed guidance for clause 12.1.2.4 but without specific requirements.

Under the heading “12.4 Application software design and development” it advises:

> **12.4.2.2** With regard to guidance on selection of application software design methods and techniques, systems with a safety requirement up to SIL 3 should be designed in accordance with the instructions given in the supplier’s Safety Manual as part of a system conforming with IEC 61508. For SIL 4 systems, the developer should additionally confirm that the selected methods do conform with the requirements of IEC 61508-3.
>
> With regard to guidance on selection of application software test and verification methods and techniques, systems with a safety requirement up to SIL 3 should be verified in accordance with the guidance given in 12.7. For SIL 4 systems, the verifier should also confirm that the selected methods do conform with the requirements of IEC 61508-3.

Although 61511 does not require strict compliance with the tables in 61508.2 and 61508.3 the tables provide a useful basis.

The techniques and measures selected still need to be planned and documented and the rationale in selecting them needs to be recorded.

Sample table:

Choose methods that are mandatory or recommended for the SIL

61508.2 Table B.2 – Recommendations to avoid introducing faults during E/E/PES design and development

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4	Applies to IES?	Remarks
	Observance of guidelines and standards	B.3.1	M high	M high	M high	M high	Y	IES Framework PROJPS02, complying with IEC 61511 / 61508
	Project management	B.1.1	M low	M low	M medium	M high	Y	IES EMS Procedures apply, certified to ISO 9001. For SIL 3 medium effectiveness shall be achieved through validation independent from design; project monitoring; standardised validation procedure and configuration management.
	Documentation	B.1.2	M low	M low	M medium	M high	Y	IES Framework PROJPS02, complying with IEC 61511 / 61508 (satisfies "high" effectiveness).
	Structured design	B.3.2	HR low	HR low	HR medium	HR high	Y	IES PROJGL21, System Architecture Specification Guideline shall be applied where applicable to scope. High effectiveness achieved through DAD design for systems hardware, traceability to specification, tag naming to aid traceability.
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high	Y	IES PROJGL21, System Architecture Specification Guideline shall be applied where applicable to scope. Medium effectiveness through re-use of well-proven modules; easily comprehensible modules
	Use of well-tried components	B.3.3	R low	R low	R medium	R high	Y	IES PROJGL21, System Architecture Specification Guideline shall be applied where applicable to scope
	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high	Y	Logic / function block diagrams shall be used. Cause & Effects tables shall be used
	Checklists	B.2.5	– low	R low	R medium	R high	Y	The use of IES verification checklists is recommended. Use detailed checklists for all lifecycle phases for high effectiveness where SIL 3 is required, i.e. use PROJFM19 checklists when verifying each deliverable. For SIL 1 & 2 the Milestone checklists will suffice.
	Computer-aided design tools	B.3.5	– low	R low	R medium	R high	N	
	Simulation	B.3.6	– low	R low	R medium	R high	Y	Emulation testing is dary transitions
	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	– low	R low	R medium	R high	Y	IES checking proce e design. Supply & fabricatior procedure PROJGL21 and fulf ependent from the supplier.
	Formal methods	B.2.2	– low	– low	R medium	R high	N	

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required. For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in table B.5 shall be used.
NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding table B.1.
NOTE 2 Most of these measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.
NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

Record the rationale for methods chosen and for methods not used

The recommendations given in the IEC 61508 tables are signified as follows:

M: The technique or measure is required (mandatory) for this safety integrity level.

HR: The technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed

R: The technique or measure is recommended for this safety integrity level.

-: The technique or measure has no recommendation for or against being used

NR: The technique or measure is positively not recommended for this safety integrity level. If this technique or measure is used then the rationale behind using it shall be detailed

Any deviations from HR and NR should be discussed and agreed during functional safety planning with the functional safety assessor.

The required effectiveness is signified as follows.

Low: If used, the technique or measure shall be used to the extent necessary to give at least low effectiveness against systematic failures;

Medium: If used, the technique or measure shall be used to the extent necessary to give at least medium effectiveness against systematic failures;

High: The technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures

Table 61508.2 B.6 gives examples of 'high' and 'low' effectiveness.

New: 61508.3 Annex C – Properties and Rigour

Annex C gives guidance on assessing how techniques and measures will confer properties for ***software systematic capability:***

Annex C
(informative)

Properties for software systematic capability

C.1 Introduction

Given the large number of factors that affect software systematic capability it is not possible to give an algorithm for combining the techniques and measures that will be correct for any given application. The purpose of Annex C is:

– to give guidance on selecting specific techniques from Annexes A and B to achieve software systematic capability;
– to outline a rationale for justifying the use of techniques that are not explicitly listed in Annexes A and B.

Annex C is supplementary to Annexes A and B tables.

The tables in Annex C correspond one-for-one with tables in 61508.3 Annexes A and B:

- Table C.1 – Software Safety Requirements Specification
- Table C.2 – Software Architecture Design
- Table C.3 – Support tools and programming language
- Table C.4 – Software design and development – detailed design
- Table C.5 – Software module testing and integration
- Table C.6 – Hardware and software integration
- Table C.7 – Software aspects of system safety validation
- Table C.8 – Software modification
- Table C.9 – Software verification
- Table C.10 – Functional safety assessment

Detailed tables:

- Table C.11 – Design and coding standards
- Table C.12 – Dynamic analysis and testing
- Table C.13 – Functional and black-box testing
- Table C.14 – Failure analysis
- Table C.15 – Modelling
- Table C.16 – Performance testing
- Table C.17 – Semi-formal methods
- Table C.18 – Properties for systematic safety integrity – Static analysis
- Table C.19 – Modular approach

Degree of Rigour R1 to R3

The tables in 61508.2 Annexes A and B define the degree of "effectiveness" that is needed according to the SIL.

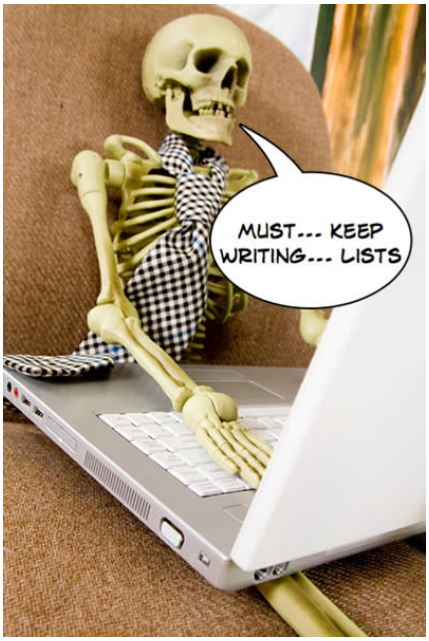
Higher SIL needs higher effectiveness.

61508.2 Table A.18 and B.6 give guidelines on how to asses the effectiveness of techniques and measures to control and avoid systematic failures.

Similarly, 61508.3 Annex C introduces the concept of rigour.

Higher SC needs higher rigour.

Higher rigour is achieved through increasing objectivity and more detailed and systematic documentation.



Annex C Table C.1 also ranks on an informal scale R1/R2/R3 the effectiveness of specific techniques in achieving these desirable properties.

Technique/ Measure		Properties					
		Completeness with respect to the safety needs to be addressed by software	Correctness with respect to the safety needs to be addressed by software	Freedom from intrinsic specification faults, including freedom from ambiguity	Understandability of safety requirements	Freedom from adverse interference of non-safety functions with the safety needs to be addressed by software	Capability of providing a basis for verification and validation
1a	Semi-formal methods	R1 Application-friendly or domain specific specification method and notation used by domain experts	R1 Application-friendly or domain specific specification method and notation used by domain experts	R1 Method and notation that helps avoid or detect internal inconsistency, missing behaviour or mathematically inconsistent expressions.	R1 Defined notation that restricts opportunity for misunderstanding R2 Application of complexity limits in specification	–	R2 Defined notation that reduces ambiguity in specification

A technique may achieve one of several R1/R2/R3 rankings relating to a particular property, depending on the level of rigour that the technique satisfies.

[…]

The confidence that can be placed in the software safety requirements specification as a basis for safe software depends on the rigour of the techniques by which the desirable properties of the software safety requirements specification have been achieved. The rigour of a technique is informally ranked on a scale R1 to R3, where R1 is the least rigorous and R3 the most rigorous.

R1	without objective acceptance criteria, or with limited objective acceptance criteria. E.g., black-box testing based on judgement, field trials.
R2	with objective acceptance criteria that can give a high level of confidence that the required property is achieved (exceptions to be identified & justified); e.g., test or analysis techniques with coverage metrics, coverage of checklists.
R3	with objective, systematic reasoning that the required property is achieved. E.g. formal proof, demonstrated adherence to architectural constraints that guarantee the property.
–	this technique is not relevant to this property.

[…]

Finally, in addition to defining R1/R2/R3 criteria, it is useful for guidance purposes to make an informal link between (1) the increasing level of rigour of the R1 to R3 progression and (2) an increased confidence in the correctness of the software. As a general and informal recommendation, the following minimum levels of rigour should be aimed for when Annex A requires the corresponding SIL performance:

SIL	Rigour R
1 / 2	R1
3	R2 where available
4	highest rigour available

Summary

Buncefield Report (2008):

Recommendation 4:
*The [safety systems] should be **engineered, operated and maintained** to achieve and maintain an appropriate level of **safety integrity** in accordance with the requirements of the recognised industry standard for 'safety instrumented systems', Part 1 of BS EN 61511*

- To achieve Safety Integrity as a whole, achieving Systematic Safety Integrity is just as important as achieving Hardware Safety Integrity.
- It is not obvious how Systematic Safety Integrity can be quantified. To address this issue the new 2010 edition of IEC 61508 introduced the new concept of systematic capability.
- To avoid and control systematic faults we apply:
  - Management planning
  - Techniques and measures
- Systematic capability is quantified in the range SC 1 to SC 4 according to:
  - which techniques and measures are applied

    and
  - the degree of effectiveness or rigour with which they are applied.
- SC1 – 4 corresponds with SIL1 – 4

- The selection of techniques and measures has to be appropriate according to the systematic capability required. Just as in determining SIL, a degree of judgement is needed. There are no “correct” answers.
- Because of the uncertainty and ambiguity in this process it is important to record the rationale and reasoning made in choosing how to apply techniques and measures.
- Tools are available to support users in developing systematic capability:
  - CASS Self Assessment checklists – for management planning
  - 61508.2 and 61508.3 annex tables – for techniques and measures

Ask for help when you need it in using these tools. You can seek advice and assistance from an independent functional safety assessor such as I&E Systems (www.iesystems.com.au) or from user support groups such as:

- TUV Functional Safety Professionals, Engineers and Experts group on LinkedIn
- 61508 Association http://www.61508.org
- CASS Scheme Ltd http://www.cass.uk.net

Exercise

The exercise for this presentation is to examine any one of the following tools:

- CASS FSM Checklist
- 61508.2 Table B.2 – Design and development
- 61508.2 Table B.4 – Operation and maintenance procedures
- 61508.3 Table C.8 – Properties for systematic safety integrity – Software modification

Participants will form into groups of 3 or 4 with a common interest and will take 5 to 10 minutes to review how to apply the chosen checklist.

Questions and suggestions will then be discussed in an open forum.