SILMETRIC

Systematic Capability for Elements

The 61508 Association

18th June 2014

Functional Safety

TRAINING • CONSULTANCY • ASSESSMENT

www.silmetric.com

The Speaker...

Paul Reeve BEng CEng MIET MInstMC

Functional Safety Consultant

- **Silmetric Ltd** since 2011 providing training, consultancy and independent assessments to product and system designers in Europe, North America, Middle East, Asia and Far East
- Director of The CASS Scheme, www.cass.uk.net
- Previously 8 years at Sira Test & Certification (part of CSA International) as the senior functional safety assessor
- 21 years in product design and development (MTL Instruments, GE Medical Systems and The BBC)

SILMETRIC is a member of:

The 61508 Association

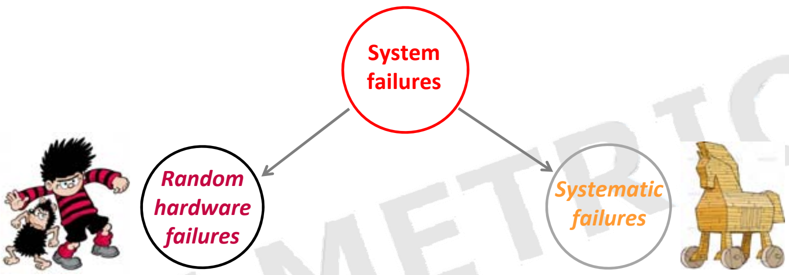
Member of BVAA

Institute of Measurement and Control Companion Company

Scope of this talk...

- We are familiar with the need for system *elements* to be assessed in terms of the reliability of their functions (to facilitate assessment of PFD, PFH, etc, of system level safety functions)
- IEC 61508 also states the elements need to have a '*Systematic Capability*' (SC), suitable for the SIL involved
- Advice about SC for element manufacturers and purchasers
- 61508 has rules (in regard to SC) about integrating systems with multiple elements

Random hardware and systematic failures



- Hardware can fail at predictable rates but at unpredictable (random) times
- Hence, random hardware failures can be quantified

- The events leading to systematic failures cannot easily be predicted
- Hence, systematic failures cannot be quantified

Addressing system failures

1. **Random hardware failures** are addressed by:
   - Design architecture, diagnostics, estimation (analysis) of probabilistic failures, design techniques and measures (to IEC 61508-7)

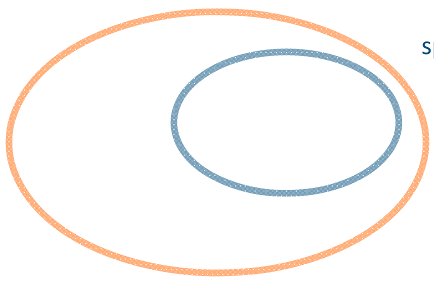
   a.k.a. Hardware Safety Integrity

2. **Systematic failures** are addressed by:
   - Correct and comprehensive specification, software design, testing, analysis, review, user documentation, system integration, validation, commissioning, operation, maintenance and modification (i.e., by attention to the 'Lifecycle')

   a.k.a. Systematic Safety Integrity

Systematic safety integrity and 'SC'

Systematic safety integrity: requirements for safety-related systems



Systematic Capability: specifically defined for elements

Definition of Systematic Capability

IEC 61508-4, clause 3.5.9 definition:

- 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

SC <no.> is related to SIL <no.>

SC 1 …	*meets the systematic safety integrity requirements*	… of SIL 1
SC 2 …		… of SIL 2
SC 3 …		… of SIL 3
SC 4 …		… of SIL 4

Example

A temperature sensor/transmitter has “SC 2”

Meaning:

the systematic safety integrity of the temperature measurement function* meets the requirements of SIL 2 when the unit is installed, used and maintained in accordance with the safety manual

<u>Safety Manual gives:</u>

- *Element safety function = to measure 0 to 100°C (± 2°C) via 4-20mA loop
- Numerical hardware failure data, etc
- Instructions for installation, use, maintenance, restrictions, etc…

How SC is demonstrated

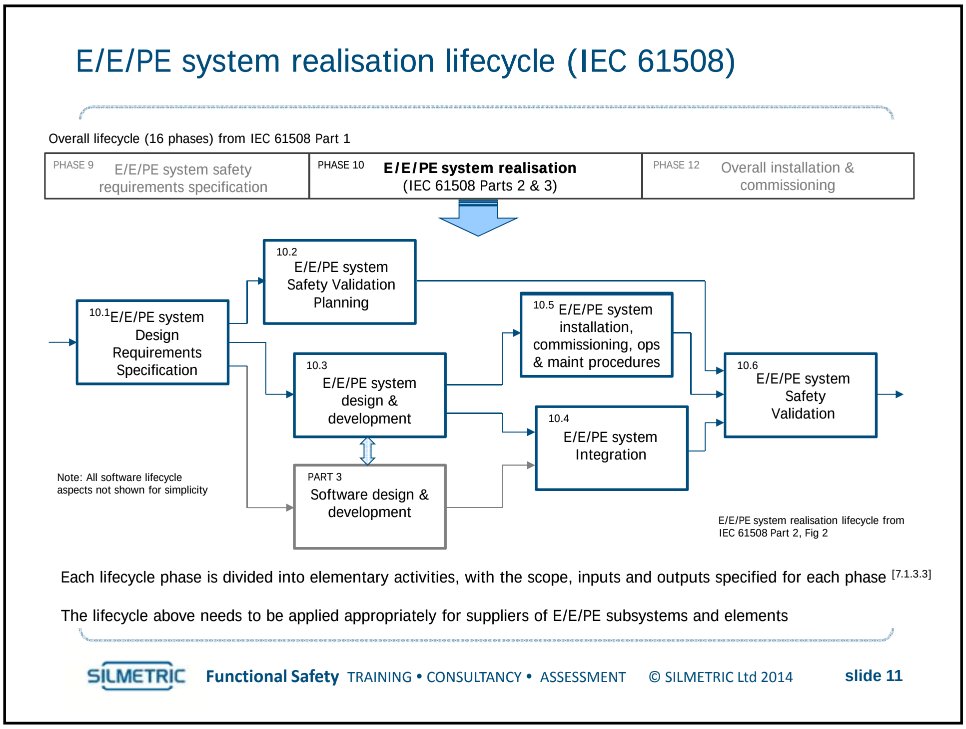
61508-2, 7.4.2.2 gives the following methods:

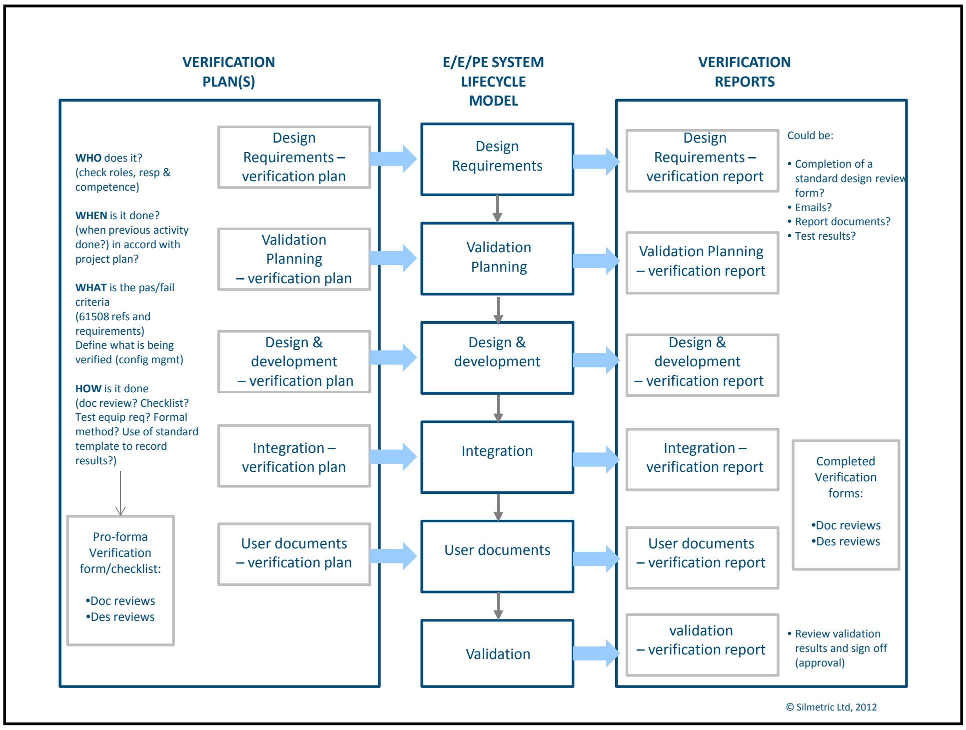
- Route 1_S: by a realisation lifecycle with ‘techniques and measures’ and documentation
- Route 2_S: by a ‘proven-in-use’ justification of the element safety function reliability performance
- Route 3_S: (pre-existing software), compliance with 61508-3, 7.4.2.12

The rest of this talk will be considering Route 1_S

Achieving SC: Route 1_S

- Following the full ***REALISATION LIFECYCLE*** (see 61508 Parts 2 & 3)
  - including software
  - including the right user documentation (safety manual)
- Using the correct ***TECHNIQUES AND MEASURES*** throughout the *lifecycle(s)* to *avoid introducing* systematic failures (see Part 2, Annex B and Part 3 Annexes A & B)
- Using the correct ***TECHNIQUES AND MEASURES*** in the *design* to *control* systematic failures (see Part 2, Annex A, A.15-A.18)
- Don’t forget the ***MANAGEMENT*** of the above! (FSM)


E/E/PE system realisation lifecycle (IEC 61508)
Overall lifecycle (16 phases) from IEC 61508 Part 1
PHASE 9 E/E/PE system safety requirements specification
PHASE 10 E/E/PE system realisation (IEC 61508 Parts 2 & 3)
PHASE 12 Overall installation & commissioning
10.1 E/E/PE system Design Requirements Specification
10.2 E/E/PE system Safety Validation Planning
10.3 E/E/PE system design & development
PART 3 Software design & development
10.4 E/E/PE system Integration
10.5 E/E/PE system installation, commissioning, ops & maint procedures
10.6 E/E/PE system Safety Validation
Note: All software lifecycle aspects not shown for simplicity
E/E/PE system realisation lifecycle from IEC 61508 Part 2, Fig 2
Each lifecycle phase is divided into elementary activities, with the scope, inputs and outputs specified for each phase [7.1.3.3]
The lifecycle above needs to be applied appropriately for suppliers of E/E/PE subsystems and elements
SILMETRIC
Functional Safety TRAINING • CONSULTANCY • ASSESSMENT
© SILMETRIC Ltd 2014
slide 11


VERIFICATION PLAN(S)
E/E/PE SYSTEM LIFECYCLE MODEL
VERIFICATION REPORTS
WHO does it? (check roles, resp & competence)
WHEN is it done? (when previous activity done?) in accord with project plan?
WHAT is the pas/fail criteria (61508 refs and requirements) Define what is being verified (config mgmt)
HOW is it done (doc review? Checklist? Test equip req? Formal method? Use of standard template to record results?)
Pro-forma Verification form/checklist:
•Doc reviews
•Des reviews
Design Requirements – verification plan
Validation Planning – verification plan
Design & development – verification plan
Integration – verification plan
User documents – verification plan
Design Requirements
Validation Planning
Design & development
Integration
User documents
Validation
Design Requirements – verification report
Validation Planning – verification report
Design & development – verification report
Integration – verification report
User documents – verification report
validation – verification report
Could be:
• Completion of a standard design review form?
• Emails?
• Report documents?
• Test results?
Completed Verification forms:
•Doc reviews
•Des reviews
• Review validation results and sign off (approval)
© Silmetric Ltd, 2012

Techniques and measures – Table B.5

Techniques to avoid faults/failures in the E/E/PE system safety validation

Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
Functional testing	B.5.1	HR High	HR high	HR high	HR high
Functional testing under environmental conditions	B.6.1	HR high	HR high	HR high	HR high
Interference surge immunity testing	B.6.2	HR high	HR high	HR high	HR high
Fault insertion testing (when required diag coverage > 90 %)	B.6.10	HR high	HR high	HR high	HR high
Project management	B.1.1	M low	M low	M medium	M high
Documentation	B.1.2	M low	M low	M medium	M high
Static analysis, dynamic analysis and failure analysis	B.6.4, B.6.5, B.6.6	- low	R low	R medium	R high
Simulation and failure analysis	B.3.6, B.6.6	- low	R low	R medium	R high
Worst-case analysis, dynamic analysis and failure analysis	B.6.7, B.6.5, B.6.6	- low	- low	R medium	R high
Static analysis and failure analysis	B.6.4, B.6.6	R low	R low	NR	NR
Expanded functional testing	B.6.8	- low	HR low	HR medium	HR high
Black-box testing	B.5.2	R low	R low	R medium	R high
Fault insertion testing (when required diag coverage < 90 %)	B.6.10	R low	R low	R medium	R high
Statistical testing	B.5.3	- low	- low	R medium	R high
Worst-case testing	B.6.9	- low	- low	R medium	R high
Field experience	B.5.4	R low	R low	R medium	NR

SILMETRIC **Functional Safety** TRAINING • CONSULTANCY • ASSESSMENT © SILMETRIC Ltd 2014 slide 13

Techniques and measures – Table B.6

Effectiveness of techniques & measures to *avoid* systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Project management	B.1.1	Definition of actions and responsibilities; scheduling and resource allocation; training of relevant personnel; consistency checks after modifications	Validation independent from design; project monitoring; standardised validation procedure; configuration management; failure statistics; computer aided engineering; computer-aided software engineering
Documentation	B.1.2	Graphical and natural language descriptions, for example block diagrams, flow-diagrams	Guidelines for consistent content and layout across organization; contents checklists; computer-aided documentation management, formal change control
Expanded functional testing	B.6.8	Test that all safety functions are maintained in the case of static input states caused by faulty process or operating conditions	Test that all safety functions are maintained in the case of static input states and/or unusual input changes, caused by faulty process or operating conditions (including those that may be very rare)
Fault insertion testing	B.6.10	At subunit level including boundary data or the peripheral units	At component level including boundary data
etc	etc	etc	etc

SILMETRIC **Functional Safety** TRAINING • CONSULTANCY • ASSESSMENT © SILMETRIC Ltd 2014 slide 14

Techniques and measures – Table A.16

Techniques & measures to control systematic failures caused by environmental stress

Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	A.8	M low	M medium	M medium	M medium
Separation of electrical energy lines from information lines	A.11.1	M	M	M	M
Increase of interference immunity	A.11.3	M low	M low	M medium	M high
Measures against physical environment (e.g. temperature, humidity, water, vibration, dust, corrosive substances)	A.14	M low	M high	M high	M high
Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
Failure detection by on-line monitoring	A.1.1	R low	R low	R medium	R high
Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
Code protection	A.6.2	R low	R low	R medium	R high
Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
Diverse hardware	B.1.4	- low	- low	- medium	R high
Software architecture	7.4.3 of 61508-3	See Tables A.2 and C.2 of IEC 61508-3			

Techniques and measures – A.18

Effectiveness of techniques & measures to *control* systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Failure detection by on-line monitoring	A.1.1	Trigger signals from the EUC and its control system are used to check the proper operation of the E/E/PE safety-related systems (only time behaviour with an upper time limit)	E/E/PE safety-related systems are retriggered by temporal and logical signals from the EUC and its control system (time window for temporal watch-dog function)
Tests by redundant hardware	A.2.1	Additional hardware tests the trigger signals of the E/E/PE safety-related systems (only time behaviour with an upper time limit), this hardware switches a secondary final element	Additional hardware is retriggered by temporal and logical signals of the E/E/PE safety-related systems (time window for temporal watchdog); voting between multiple channels
Standard test access port and boundary-scan architecture	A.2.3	Testing the used solid-state logic, during the proof test, through defined boundary scan tests	Diagnostic test of solid-state logic, according to the functional specification of the E/E/PE safety-related systems; all functions are checked for all integrated circuits
etc	etc	etc	etc

Key safety related documents

Typical documents (not including software) to consider are:

- Design requirements specification
- Architecture description
- Detailed design (schematics, drawings, BoMs, design descriptions)
- Techniques & Measures plan
- Verification & validation (V&V) plan / results
- Safety Manual
- Manufacturing documentation
- Monitoring field failure performance

NOTE: Evidence of all design/document reviews should be kept

The safety manual

The safety manual is mandatory – see IEC 61508-2 Annex D

- Provide all functional safety related information [7.4.9.3, 7.4.9.4]
  - Including all hardware and systematic failure measures
  - Any restrictions /conditions in use
  - Maintenance requirements
- Could include a recapitulation of the manufacturer's declaration / certificate
- Review (verify) the document before release

How is the SC assessed?

- Some qualitative judgements are required!
- SC needs to be the subject of a functional safety assessment (FSA) to IEC 61508-1, clause 8
- Remember what "independence" means!

Instructor (not independent!)

Independent assessor

- Objective examination of the evidence
- SC is one of the functional safety attributes of an element (together with failure modes, failure rates, element safety function, etc) - see next slide…

Example of an element FS data sheet showing SC

FUNCTIONAL SAFETY DATA	
Product identification:	Position Sensor, part no. XXX-YYYY-ZZ
Element safety function (1):	To provide a 4-20mA signal corresponding to position measured
Architectural parameters:	Type B; HFT=0; SFF = 74%; category 2 [ISO 13849]
Random hardware failures:	λ_{DD} = 3.2E-06; λ_{DU} = 2.1E-06; λ_{SD} = 2.2E-08; λ_{SU} = 2.8E-06
PFD_{AVG}:	9.4E-03
MTTFd:	53 years [ISO 13849]
Performance Level:	PL c [ISO 13849]
Diagnostic coverage:	60%
Diagnostic test interval:	<1 second
Restrictions in use:	Digital communications are not assessed for safety related use
Hardware safety integrity compliance:	Route 1_H
Systematic safety integrity compliance:	Route 1_S
Systematic Capability:	SC 2
Environment limits:	Operational temp: -20 to +70^{o}C
Lifetime/replacement limits:	10 years
Proof Test requirements:	Refer to safety manual, document no. xyz, rev 1.3
Maintenance requirements:	Refer to I, O & M manual, document no. xyz, rev 1.1
Repair constraints:	Refer to I, O & M manual, document no. xyz, rev 1.1

Systematic capability and redundancy

There are limits to what SIL capability can be claimed for a combination of multiple (redundant) elements *in respect of systematic capability*.

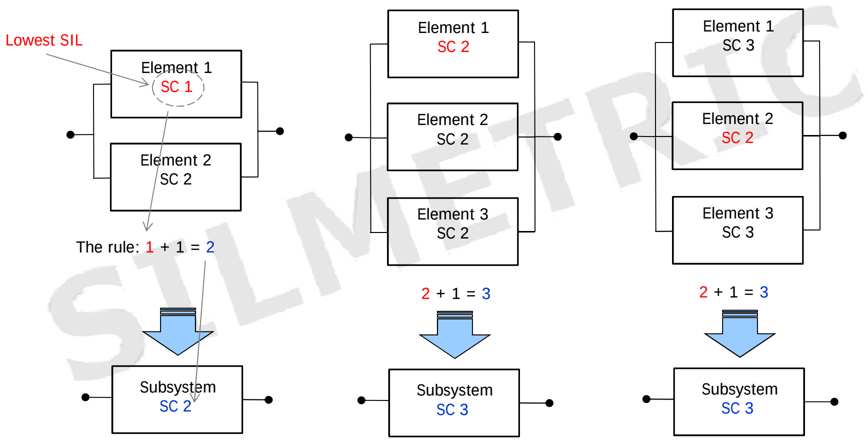
Rule: The SC of a combination of elements (arranged in redundancy) is limited to the lowest SC (1, 2, 3) of the elements +1, *providing there is sufficient independence between the multiple elements* [7.4.3.2]

The SC claimed for the combination can only be SC N+1 at most, regardless of how many elements are used in the combination [7.4.3.3]

Note that 'sufficient independence' should be justified by common cause failure analysis and be commensurate with SIL involved [7.4.3.4]

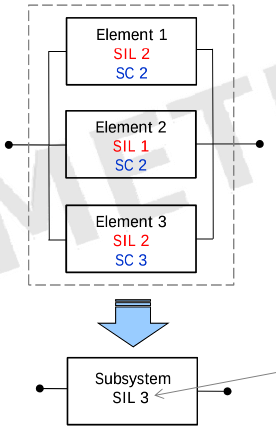
SC and redundancy (cont.)

Examples of systematic capability using a combination of elements...



SC and hardware architectural constraints

The SIL-capability needs to take account of systematic capability and hardware architectural constraints and is determined by the lowest of the two, for example:



Hardware architectural constraints

Highest SIL = 2
Subsystem HFT = 2

Rule: 2 + 2 = 4

Systematic Capability

Lowest SC = 2
>1 elements are used

Rule: 2 + 1 = 3

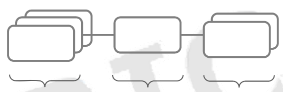
SC is lower than hardware architectural constraints so this determines final SIL capability

SILMETRIC **Functional Safety** TRAINING • CONSULTANCY • ASSESSMENT © SILMETRIC Ltd 2014 **slide 23**

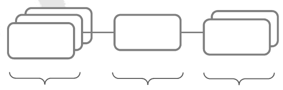
When to assess the SC and hardware architecture?

A suggested sequence…

1. Select and arrange the elements in each subsystem to meet the hardware **architectural constraints** for the SIL



2. Ensure each subsystem meets the **systematic capability** (SC) of the SIL



3. Then calculate **PFD**$_{AVG}$ or **PFH** for each subsystem and ensure the sum meets (or is <) that required to meet the SIL

$PFD_S + PFD_L + PFD_{FE} = PFD_{SIF}$

Refer to simplified PFD equations in BS EN 61508-6

SILMETRIC **Functional Safety** TRAINING • CONSULTANCY • ASSESSMENT © SILMETRIC Ltd 2014 **slide 24**

In summary...

- SC is about the integrity against systematic failures of the element:
  - during product realisation (to avoiding introducing them)
  - during operation (with specific design features)
- SC should always be assessed and stated by the manufacturer (it's part of the functional safety data!)
- The element should have followed an appropriate realisation lifecycle (Route 1_S) or else a 'proven-in-use' justification (Route 2_S)
- Check documentation (e.g., the safety manual) for indications of the SC, the Route used and any restrictions in use
- Follow IEC 61508-2, 7.4.3, when multiple elements are involved

That's the end of this talk...

ARE THERE ANY QUESTIONS?

You might be interested in some of the author's other papers, e.g., on tank overfill, HIPPS, etc, see www.miinet.com/WhitePapersandArticles/TechnicalWhitePapers.aspx

SILMETRIC

Thanks for listening

Functional Safety

TRAINING • CONSULTANCY • ASSESSMENT

www.silmetric.com