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 MIInstMC
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)
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)

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’)

---

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.

<table>
<thead>
<tr>
<th>SC &lt;no.&gt;</th>
<th>is related to</th>
<th>SIL &lt;no.&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC 1 ...</td>
<td>meets the</td>
<td>... of SIL 1</td>
</tr>
<tr>
<td>SC 2 ...</td>
<td>systematic</td>
<td>... of SIL 2</td>
</tr>
<tr>
<td>SC 3 ...</td>
<td>safety integrity requirements</td>
<td>... of SIL 3</td>
</tr>
<tr>
<td>SC 4 ...</td>
<td></td>
<td>... of SIL 4</td>
</tr>
</tbody>
</table>

**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.

*Safety Manual gives:*
- *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 1₅: by a realisation lifecycle with ‘techniques and measures’ and documentation
- Route 2₅: by a ‘proven-in-use’ justification of the element safety function reliability performance
- Route 3₅: (pre-existing software), compliance with 61508-3, 7.4.2.12

The rest of this talk will be considering Route 1₅

Achieving SC: Route 1₅

- Following the full \textit{realisation lifecycle} (see 61508 Parts 2 & 3)
  - including software
  - including the right user documentation (safety manual)
- Using the correct \textit{techniques and measures} throughout the \textit{lifecycle(s)} to avoid introducing systematic failures (see Part 2, Annex B and Part 3 Annexes A & B)
- Using the correct \textit{techniques and measures} in the design to control systematic failures (see Part 2, Annex A, A.15-A.18)
- Don’t forget the \textit{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 realisation lifecycle (IEC 61508 Parts 2 & 3)

Overall installation & commissioning

**PART 3**
Note: All software lifecycle aspects not shown for simplicity.

Each lifecycle phase is divided into elementary activities, with the scope, inputs and outputs specified for each phase.

The lifecycle above needs to be applied appropriately for suppliers of E/E/PE subsystems and elements.

---

**VERIFICATION PLANS**

- **Design**
  - Requirements — verification plan
  - Validation Planning — verification plan
  - Design & development — verification plan
  - Integration — verification plan
  - User documents — verification plan

**E/E/PE SYSTEM LIFECYCLE MODEL**

- **Design**
  - Requirements
  - Validation Planning
  - Design & development
  - Integration
  - User documents

**VERIFICATION REPORTS**

- **Design**
  - Requirements — verification report
  - Validation Planning — verification report
  - Design & development — verification report
  - Integration — verification report
  - User documents — verification report
  - User documents — verification report

Could be:
- Completion of a standard design review form
- Emails?
- Report documents?
- Test results?

- **Verification form/checklist:**
  - Doc reviews
  - Des reviews

- **Completed Verification forms:**
  - Verif.
  - Des reviews
  - User documents
  - User documents

- **Validation — verification report**
  - Validation — verification report
  - Validation — verification report

- **Review validation results and sign off (approved)**
### Techniques and measures - Table B.5

<table>
<thead>
<tr>
<th>Technique/measure</th>
<th>SIL1</th>
<th>SIL2</th>
<th>SIL3</th>
<th>SIL4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional testing</td>
<td>B.1.1</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Individual testing under environmental conditions</td>
<td>B.8.1</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.8.2</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Expanded functional testing (when required diag coverage &lt; 100%)</td>
<td>B.6.10</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Project management</td>
<td>B.1.1</td>
<td>B.1.2</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.1</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Functional testing under environmental conditions</td>
<td>B.6.1</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.2</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Functional testing</td>
<td>B.6.3</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.4</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.5</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.6</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.7</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Interference surge immunity testing</td>
<td>B.6.8</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

### Effectiveness of techniques & measures to avoid systematic failures

<table>
<thead>
<tr>
<th>Technique/measure</th>
<th>See IEC 61508-7</th>
<th>Low effectiveness</th>
<th>High effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project management</td>
<td>B.1.1</td>
<td>Definition of actions and responsibilities; scheduling and resource allocation; training of relevant personnel; consistency checks after modifications</td>
<td>Validation independent from design; project monitoring; standardised validation procedure; configuration management; failure statistics; computer aided engineering; computer-aided software engineering</td>
</tr>
<tr>
<td>Documentation</td>
<td>B.1.2</td>
<td>Graphical and natural language descriptions, for example block diagrams, flow-diagrams</td>
<td>Guidelines for consistent content and layout across organization; contents checklists; computer-aided documentation management, formal change control</td>
</tr>
<tr>
<td>Expanded functional testing</td>
<td>B.6.3</td>
<td>Test that all safety functions are maintained in the case of static input states caused by faulty process or operating conditions</td>
<td>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)</td>
</tr>
<tr>
<td>Fault insertion testing</td>
<td>B.6.10</td>
<td>At subunit level including boundary data or the peripheral units</td>
<td>At component level including boundary data</td>
</tr>
<tr>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>
Techniques and measures – Table A.16

<table>
<thead>
<tr>
<th>Technique/measure</th>
<th>See IEC 61508-7</th>
<th>SIL1</th>
<th>SIL2</th>
<th>SIL3</th>
<th>SIL4</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>A.8</td>
<td>low</td>
<td>M</td>
<td>medium</td>
<td>M</td>
</tr>
<tr>
<td>Separation of electrical energy lines from information lines</td>
<td>A.11.1</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Increase of interference immunity</td>
<td>A.11.3</td>
<td>low</td>
<td>M</td>
<td>medium</td>
<td>M</td>
</tr>
<tr>
<td>Measures against physical environment (e.g. temperature, humidity, water, vibration, dust, corrosive substances)</td>
<td>A.14</td>
<td>M</td>
<td>low</td>
<td>M</td>
<td>high</td>
</tr>
<tr>
<td>Program sequence monitoring</td>
<td>A.9</td>
<td>medium</td>
<td>M</td>
<td>low</td>
<td>medium</td>
</tr>
<tr>
<td>Measures against temperature increase</td>
<td>A.10</td>
<td>M</td>
<td>medium</td>
<td>M</td>
<td>high</td>
</tr>
<tr>
<td>Spatial separation of multiple lines</td>
<td>A.11.2</td>
<td>M</td>
<td>M</td>
<td>low</td>
<td>medium</td>
</tr>
<tr>
<td>Failure detection by on-line monitoring</td>
<td>A.1.1</td>
<td>medium</td>
<td>R</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>Tests by redundant hardware</td>
<td>A.2.1</td>
<td>low</td>
<td>R</td>
<td>low</td>
<td></td>
</tr>
<tr>
<td>Code protection</td>
<td>A.6.2</td>
<td>low</td>
<td>low</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>Antivalent signal transmission</td>
<td>A.11.4</td>
<td>high</td>
<td>M</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>Diverse hardware</td>
<td>B.1.4</td>
<td>M</td>
<td>low</td>
<td>M</td>
<td>high</td>
</tr>
<tr>
<td>Software architecture</td>
<td>7.4.3 of 61508-3</td>
<td>See Tables A.2 and C.2 of IEC 61508-3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Techniques and measures – A.18

Effectiveness of techniques & measures to control systematic failures

<table>
<thead>
<tr>
<th>Technique/measure</th>
<th>See IEC 61508-7</th>
<th>Low effectiveness</th>
<th>High effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure detection by on-line monitoring</td>
<td>A.1.1</td>
<td>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); this hardware is retriggered by temporal and logical signals of the E/E/PE safety-related systems (time window for temporal watchdog function)</td>
<td></td>
</tr>
<tr>
<td>Tests by redundant hardware</td>
<td>A.2.1</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Standard test access port and boundary-scan architecture</td>
<td>A.2.3</td>
<td>Testing the used with state logic, during the proof test, through defined boundary scan tests</td>
<td></td>
</tr>
<tr>
<td>etc</td>
<td>etc</td>
<td>etc</td>
<td></td>
</tr>
</tbody>
</table>

© Silmetric Ltd, 2014
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!
- 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

<table>
<thead>
<tr>
<th>FUNCTIONAL SAFETY DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Identification:</strong></td>
</tr>
<tr>
<td><strong>Element safety function (1):</strong></td>
</tr>
<tr>
<td><strong>Architectural parameters:</strong></td>
</tr>
<tr>
<td><strong>Random hardware failures:</strong></td>
</tr>
<tr>
<td><strong>PFDAVG:</strong></td>
</tr>
<tr>
<td><strong>MTTFd:</strong></td>
</tr>
<tr>
<td><strong>Performance Level:</strong></td>
</tr>
<tr>
<td><strong>Diagnostic coverage:</strong></td>
</tr>
<tr>
<td><strong>Diagnostic test interval:</strong></td>
</tr>
<tr>
<td><strong>Restrictions in use:</strong></td>
</tr>
<tr>
<td><strong>Hardware safety integrity compliance:</strong></td>
</tr>
<tr>
<td><strong>Systematic safety integrity compliance:</strong></td>
</tr>
<tr>
<td><strong>Systematic Capability:</strong></td>
</tr>
<tr>
<td><strong>Environment limits:</strong></td>
</tr>
<tr>
<td><strong>Lifetime/replacement limits:</strong></td>
</tr>
<tr>
<td><strong>Proof Test requirements:</strong></td>
</tr>
<tr>
<td><strong>Maintenance requirements:</strong></td>
</tr>
<tr>
<td><strong>Repair constraints:</strong></td>
</tr>
</tbody>
</table>
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...

Lowest SIL

- Element 1 SC 3
- Element 2 SC 2
- Subsystem SC 2

The rule: 1 + 1 = 2

- Element 1 SC 2
- Element 2 SC 2
- Subsystem SC 3

2 + 1 = 3

- Element 1 SC 3
- Element 2 SC 2
- Subsystem SC 3

2 + 1 = 3

- Element 1 SC 3
- Element 3 SC 2
- Subsystem SC 3

2 + 1 = 3
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

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

Refer to simplified PFD equations in BS EN 61508-6
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) or else a ‘proven-in-use’ justification (Route 2)
- 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
Thanks for listening

Functional Safety
TRAINING • CONSULTANCY • ASSESSMENT
www.silmetric.com