The 61508 Association

The IEC61508 Inspection and QA Engineer's hymn sheet

A few key points for those inspectors and QA engineers involved with a project using the IEC61508 group of standards

by the 61508 Association

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither The 61508 Association nor its members will assume any liability for any use made thereof.

www.61508.org

The 61508 Association

Are you involved with functional safety?

Are you involved with “SIL”?

If you are involved with “SIL” then you are involved with Functional Safety and you should be using one of the IEC61508 group of standards.

The 61508 Association

Important and surprising fact number 1

The IEC61508 group of standards require that you have in place “Functional Safety Management” supporting all activities, claims and data.

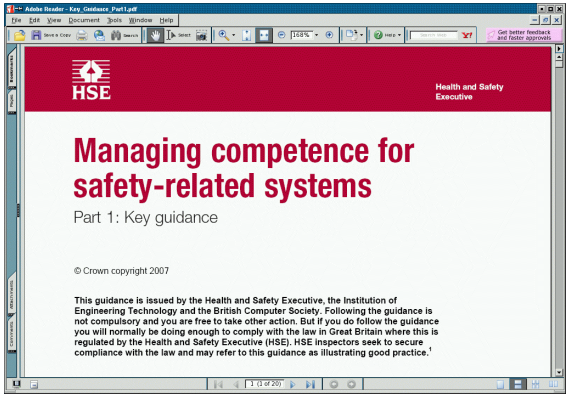
Safety is depending on that one SIL rated loop so EVERYONE involved has to be demonstrably competent –

... IEC61508 Part 1 Clause 6

... Matching requirements appear in the sector specific guidance standards (For example: IEC61511 Part 1 Clause 5)

... Regulators are increasingly demanding that safety management is properly covered (See the HSE guidance – “Managing Competence for Safety Related Systems” July 2007)

http://www.hse.gov.uk/consult/condocs/competence.htm



The 61508 Association

Important and surprising fact number 2

The IEC61508 group of standards require that your suppliers and sub-contractors demonstrate “Functional Safety Management”

... so certification of Functional Safety Management, or other appropriate proof, is the FIRST thing that inspection and QA should look for.

... interestingly, certificates for components (such as transmitters) are NOT required under the standard (but they might be appropriate for your project).

... so don't make the mistake of asking for certificates for equipment *(the bit that **isn't** demanded)* when you've forgotten to ask for proof of Functional Safety Management *(the bit that **IS** demanded)*.

The 61508 Association

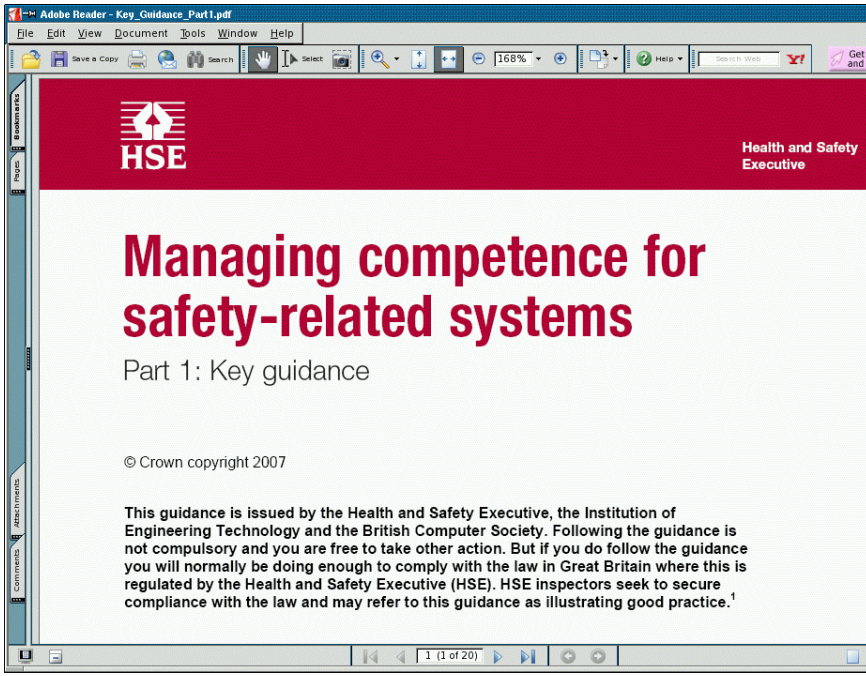
Important and surprising fact number 3

The IEC61508 group of standards require that your suppliers and sub-contractors demonstrate "Functional Safety Management"

... IEC61508 Part 1 Clause 6

... matching requirements appear in the sector specific guidance standards (For example: IEC61511 Part 1 Clause 5)

... Regulators are increasingly demanding that safety management is properly covered (See the HSE guidance - "Managing Competence for Safety Related Systems" July 2007)



http://www.hse.gov.uk/consult/condocs/competence.htm

The 61508 Association

Important and surprising fact number 4

The presence of a certified expert is NOT proof of "Functional Safety Management"

... The use of a functional safety expert may sometimes be appropriate as a decision that comes out of a contractor's or supplier's Functional Safety Management, but **it is NOT a substitute for** a Functional Safety Management system

... Functional Safety Management covers EVERBODY involved

... not just the expert

... not just the technician

... it involves everybody involved in the safety system (including you, the Inspection and QA engineer, the Project Manager, the Engineering Manager...everyone!)

The 61508 Association

Important and surprising fact number 5

A SIL 3 safety loop means that without that one loop functioning correctly the risk of fatality* is more than 1000 times the wrong side of tolerable.

A SIL 2 safety loop means that without that one loop functioning the risk of fatality* is more than 100 times the wrong side of tolerable.

A SIL 1 safety loop means that without that one loop functioning the risk of fatality* is more than 10 times the wrong side of tolerable.

We suggest that you don't even think about SIL 4 !

*That is if the SIL loop has been provided for protection of people.
The SIL loop may have been provided for environmental or asset protection.

The 61508 Association

Important and surprising fact number 5 continued ....

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

Maintenance and proof testing of safety instrumented systems are not just important they are ESSENTIAL

The proof testing is to reassure EVERYONE that the loop works correctly and will save lives*

Audit your maintenance departments records of testing and maintenance – make sure they are up to date and that all failures – particularly dangerous failures are fully documented and the loop designer informed so that continuing compliance (or not) with the required SIL is confirmed.

Note that if the recorded dangerous failures are worse than predicted then it is possible that the loop will no longer achieve the required risk reduction and consequently some 'urgent' redesign will be required to maintain safety.

*That is if the SIL loop has been provided for protection of people.
The SIL loop may have been provided for environmental or asset protection.

The 61508 Association

Important and surprising fact number 6

You can't replace one certified component with another certified component from a different manufacturer even if they are both certified to the same “level”

You can't even replace a component with one of a different version or model

The reliability required to perform correctly in the safety loop is a combination of factors that include the maintenance and proof testing of the component.

The component from a different manufacturer will be expected to achieve reliabilities in the same range but with DIFFERENT maintenance and proof-testing requirements.

If you substitute a component with one from a different manufacturer then you are affecting the maintenance and proof-testing requirements for the entire loop and the whole loop design must be referred back to the designer.

The 61508 Association

Important and surprising fact number 7

IEC 61508 group of standards does NOT require certification for components. It does require proof of reliability and suitability for the application

A certificate alone is NOT proof of reliability and suitability for the application

... The report behind the certificate gives the designer of the safety loop the reliability data needed to design the loop

... The report needs to show how the data was generated

... The report needs to show the limits of applicability for the data

... The report needs to show restrictions and conditions of use

The 61508 Association

Important and surprising fact number 8

The report that gives the reliability data for the component is the ESSENTIAL information that the designer needs to design the safety loop

The safety loop designer CANNOT design the safety loop without the reliability data

... A certificate without the report giving the data is useless to the loop designer

... A certificate without the reliability data and the basis of the assessment is a waste of paper

... If your safety loop designer doesn't have the report then they can't use the component – When auditing – make sure the right information is available!

The 61508 Association

Important and surprising fact number 8 continued ...

The report that gives the reliability data for the component is the ESSENTIAL information that the designer needs to design the safety loop

The safety loop designer CANNOT design the safety loop without the reliability data

... The report should show the assumptions made and the basis of the reliability assessment as well as the scope (it is not unusual to find that the component's reliability assessment only covers electronic hardware and not the process interface!)

... The report should show the techniques of assessment and not just a bland statement that “it was assessed”. The techniques used are a real part of what demonstrates that the reliability evidence is appropriate for the application

The 61508 Association

Important and surprising fact number 9

A certified claim that a component is “SIL 2” *(or any other SIL number)* does NOT mean that it is suitable for use in your “SIL 2” safety loop.

... The SIL number does not apply to the components in isolation

... The SIL rating applies to the whole loop and NOT just the individual components in the loop

... The loop architecture also plays a part in the reliability required of an individual component

... It is NOT at all unusual to find that a collection of “SIL 3” parts put together in a loop only achieve SIL 1 or SIL 2 ... and the SIL rating is a safety LOOP value not a component value

The 61508 Association

Important and surprising fact number 10

Every component in the loop needs to provide sufficient reliability so that the loop achieves the SIL rated integrity

... This means that the valve, pump or end device that takes the ultimate action to maintain safety is INCLUDED.

... It is NOT enough to simply use a SIL certified PLC and connect all the loops into that.

... It is NOT enough to get a SIL certified PLC and a certified transmitter and ignore the other parts of the safety loop

The 61508 Association

Important and surprising fact number 11

The part of a safety instrumented system that is most likely to fail is ... the people (see fact numbers 1, 2 & 3)

- Almost everyone will choose a certified PLC
  - ***usually the MOST reliable part of the loop even without a certificate***
- A lot of people will ask for a certified transmitter
  - ***less reliable than the PLC but usually robust***
- Some people will ask for a certificate with the valve
  - ***... an unreliable part of the loop***
- Too many people fail to ask for the safety report
  - **... the bit that is ESSENTIAL for the design** *(they went away surprisingly happy with a certificate!)*
- Hardly anyone asks about the people
  - **... the LEAST reliable part** *(the part covered by functional safety management)*

You need to consider the whole list as equal in importance

The 61508 Association

Important and surprising fact number 12

"Proven in use" or "Prior use" claims require substantial evidence and cannot easily be used

... ONLY the end user can offer a "Proven in use" or "Prior use" claim as evidence of suitability in a safety instrumented system (and they need substantial valid evidence of previous use in the same application complete with failure records and safety management amongst other requirements)

... A salesperson or supplier cannot offer "Proven in use" or "prior use" as evidence of a SIL rating claim – As Auditor ensure that your engineers are not required to engineer safety loops with invalid equipment

... See the 61508 Association statement on "Proven in use" and "Prior use" claims

The 61508 Association

Your guide for inspection and QA

- Ask suppliers for evidence of Functional Safety Management (meeting the requirements of IEC61508 part 1 clause 6 or its matching requirements under the sector standards)
- Don't accept the presence of an “expert” as proof of Functional Safety Management (there are no certified experts mentioned in the standard)
- Don't approve components without the report (or equivalent) giving the evidence of reliability and all the associated conditions even if it does have a certificate
- Don't approve product reliabilities based upon factory return data unless you have proof that the application is the same *(not just similar)*
- The SIL applies to the whole loop – NOT just to the components
- Make sure that all parties are involved in safety – don’t forget the operations, maintenance and service departments!