THE 61508 ASSOCIATION
Guidance in Compliance

The IEC61508 Project Manager's & Project Engineer's hymn sheet

A few key points for those project managers and project engineers undertaking a project using the IEC61508 group of standards

by the 61508 Association

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

Rev 4 20/12./017

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 1

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 a purchaser should ask for.

... interestingly, certificates for components 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
Guidance in Compliance

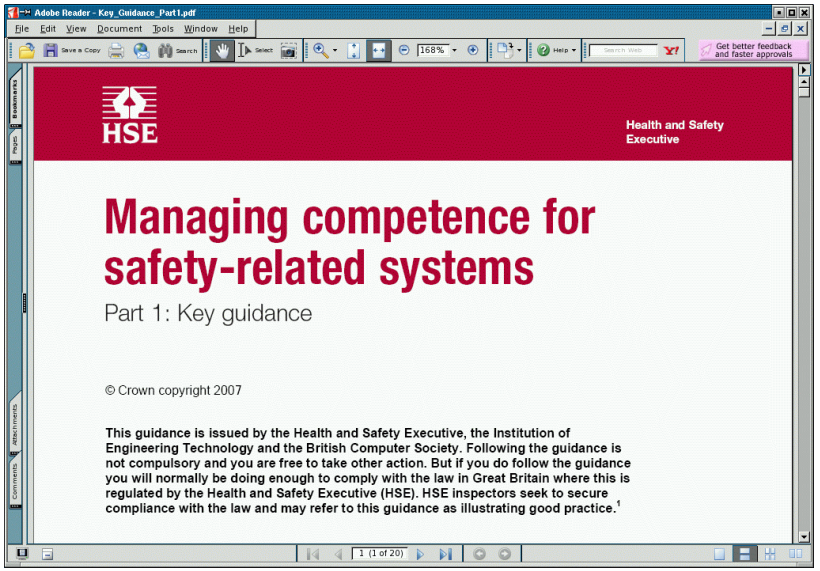
Important and surprising fact number 2

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 requiring 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
Guidance in Compliance

Important and surprising fact number 3

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

... The functional safety management will review the competencies of everyone involved and it identifies those who require particular expertise. Thus 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** Functional Safety Management

... Functional Safety Management covers EVERBODY involved

... not just the expert

... not just the technician

... it involves everybody involved with the safety system (including you, overseeing the project !)

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 4

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

A certificate alone is NOT proof of dependability 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
Guidance in Compliance

Important and surprising fact number 5

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 you don't have the report then you can't use the component

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 5 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 and limitations of use (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
Guidance in Compliance

Important and surprising fact number 6

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
Guidance in Compliance

Important and surprising fact number 7

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
Guidance in Compliance

Important and surprising fact number 8

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

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 functional safety management)*

You need to consider the whole list as equal in importance

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 9

"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 you "Proven in use" or "prior use" as evidence of a SIL rating claim

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

THE 61508 ASSOCIATION
Guidance in Compliance

Your guide for using and specifying

- Ask 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 buy 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 use product reliabilities based upon factory return data unless you can prove that the application is the same *(not just similar)* – See 61508 Association notes on Proven in use for further guidance
- The SIL applies to the whole loop – NOT just to the components – see fact 6