THE 61508 ASSOCIATION
Guidance in Compliance

The IEC61508 Senior Manager's hymn sheet

A few key points for those Managers overseeing applications that use the IEC61508 group of standards

by The 61508 Association

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 1

The IEC61508 group of standards require that **your company** decides the level of tolerable risk. There is no set value in the standard.

... so the Management of the company might decide that the risk of fatality to an employee will be made to be less than 1×10^{-4} per year (*i.e. the risk of a fatal accident for each employee will be less than a 1 in 10,000 chance per year*). This is **NOT** decided by engineering but by management.

... If you have issued a COMAH report then the fatal accident rate is ALREADY written in the COMAH report and you should use that same value for your SIL assessments under the IEC61508 group of standards.

... Many industry bodies give recommended values. The Chemical Industries Association recommend members achieve better than 1×10^{-4} per year and suggest that anything below 1×10^{-3} per year would not be acceptable

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 2

If the SIL assessment says you need a SIL 1 safety loop then that means that without that one safety loop the actual risk of fatality* is more than 10 times the wrong side of your tolerable target

A SIL 2 loop means that without that one loop the actual risk of a fatal accident is more than 100 times the wrong side of your tolerable target

A SIL 3 ... actual risk is more than 1000 times the wrong side of tolerable without that safety loop being fully functional

A SIL 4 ... *it exists under the standard but does your company really want to admit that without that one safety loop you have a risk that large?*

*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
Guidance in Compliance

Important and surprising fact number 3

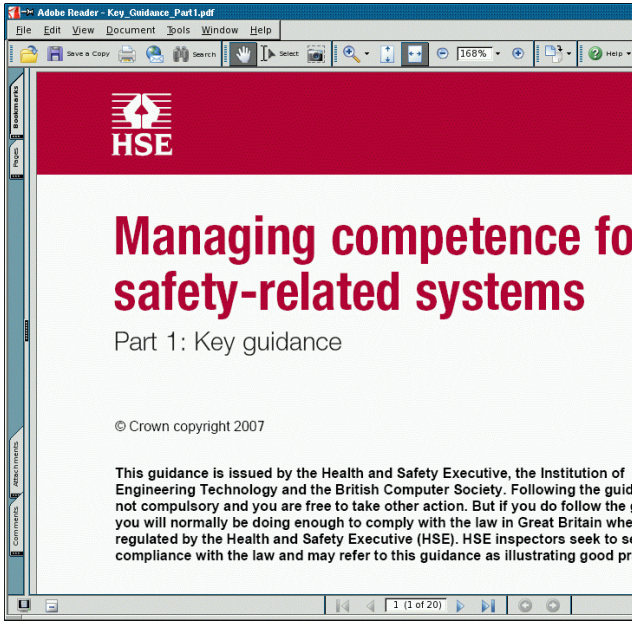
The IEC61508 group of standards require that you have in place “Functional Safety Management”

Safety is depending on that one SIL rated loop so EVERYONE involved has to be competent – *including your maintenance team*

... 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 4

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 your purchaser should ask for.

... interestingly, certificates for components are NOT required under the standard *(but they might sometimes be appropriate).*

... so don't make the mistake of having your staff ask 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

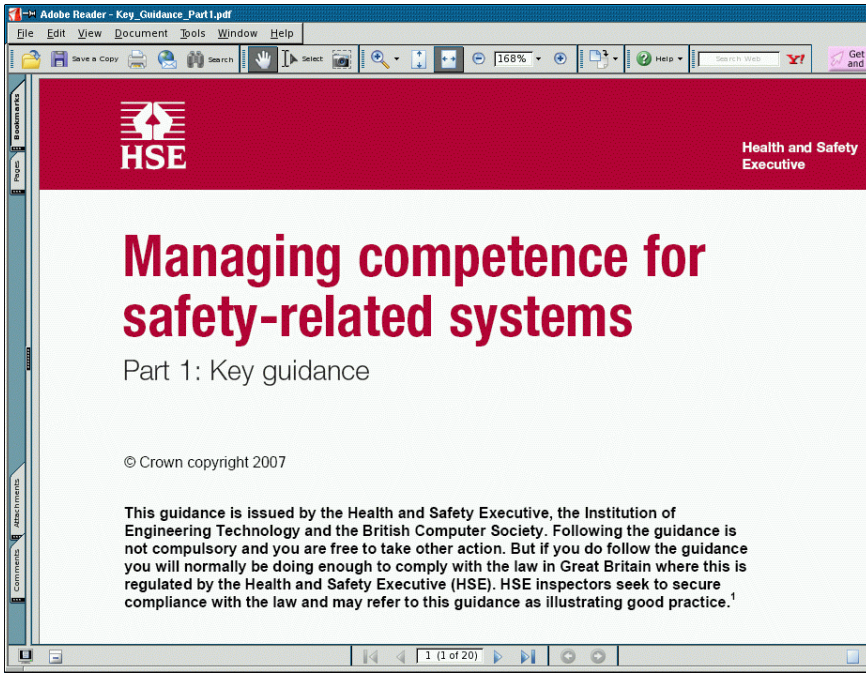
Important and surprising fact number 5

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 6

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, in the management !)

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 7

The part of a safety instrumented system that is most likely to fail is ... the people

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*** *)*

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 8

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.

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 normally proof of reliability and suitability for the actual application

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 8 *continued*

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

... 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

Let competent engineers decide which components to use and how to use them

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

... and one other point:

Safety-related systems designed and installed before the publication of IEC 61508 are not required to be replaced or upgraded just because the standard has been published. The organisation should be able to demonstrate that the measures in place to control the risks of hazardous events are adequate when seen in the light of the IEC61508 standard[1] and the requirements of the law.

Further guidance is available in "Legacy Systems: Basic Principles for Safety" published by the 61508 Association.

Note 1: Or other sector relevant standard within the IEC61508 group (such as IEC61511 for the process sector)

THE 61508 ASSOCIATION
Guidance in Compliance

Your guide for Management

- Decide as a company what level of risk is tolerable *(and if you have a COMAH report then make the fatality rate value agree with what you have already put in that report)*
- Assess and Manage the competencies of everyone involved in the safety loop's lifecycle.
- People's safety depends on that loop working so take your own Functional Safety Management seriously.
- Ask for evidence of Functional Safety Management from all suppliers and sub-contractors *(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” from your suppliers as proof of Functional Safety Management *(there are no certified experts mentioned in the standard)*
- Let competent engineers work out what reliabilities are needed from each part of the loop so that the reliability of the loop as a whole achieves the SIL rating *(Certificates can be misleading)*