The 61508 Association

The IEC61508 Installer's hymn sheet

A few key points for those Companies undertaking installation and commissioning work under the IEC61508 group of standards

by the 61508 Association

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

www.61508.org

The 61508 Association

Important and surprising fact number 1

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 1 continued ....

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

Thorough commissioning of safety instrumented systems is not just important it is ESSENTIAL

*Thorough testing reassures EVERYONE that each and every safety loop works correctly and will save lives**

Keep thorough records of project drawings that show the installation, the commissioning, the testing and modifications and keep them up to date, documenting everything

*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 2

Each SIL rated safety loop should have a “design file”. You must be in possession of some key items of information from this design file before you start.

You need the following from the design file:

The project drawings for the loop.
The installation requirements.
The installation and set-up procedure.
The commissioning plan
The pre-commissioning checks.
The commissioning checks.

... and if you are doing the first proof test then you need the proof test procedure

ANY change to the above MUST go through the project change control procedures to be fully assessed

The 61508 Association

Important and surprising fact number 3

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 from the same manufacturer 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 4

A certified claim that a component is “SIL 2” *(or any other SIL number)* does NOT mean that it is suitable for use in a “SIL 2” safety loop. Has the design that you are installing been adequately assessed?

... 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 5

You need to see the reports or safety manuals for the components:

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

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

The report or safety manual provides the installer with installation instructions that will ensure that the safety performance is not compromised by poor or incorrect installation.

... The report will show restrictions and conditions of use – these must be reviewed by the commissioning team to ensure that there are no unrevealed problems.

REMEMBER: People's safety depend on this loop

The 61508 Association

Important and surprising fact number 6

The IEC61508 group of standards require that <u>everyone</u> involved in the implementation of the safety system, including 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 when selecting safety loop installation and/or commissioning teams. So make sure your Company has such certification or similar proof.

The 61508 Association

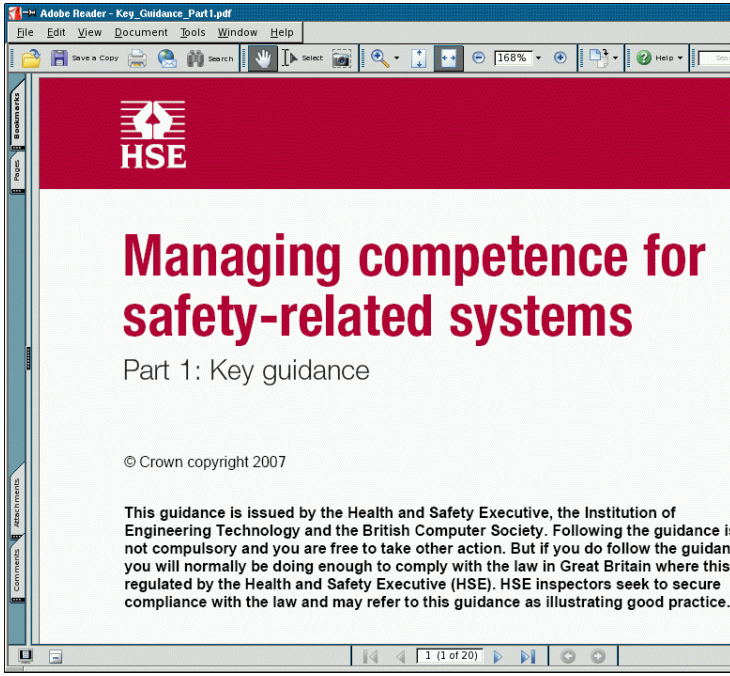
Important and surprising fact number 7

The IEC61508 group of standards require that everyone involved, including 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 8

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** Functional Safety Management

... 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 installation and commissioning engineer!)

The 61508 Association

Important and surprising fact number 9

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)*

www.61508.org

You need to consider the whole list as equal in importance

The 61508 Association

Your guide for installing safety loops

- Thorough and correct installation in accordance with ALL the manufacturer's and design file's recommendations is ESSENTIAL (keep your records up to date and document everything)
- The SIL applies to the whole loop – NOT just to the components
- Don't replace a component in the loop with a different model even if it seems to be compatible (you will be messing up the proof-testing and maintenance requirements designed into the loop)
- Make sure you, the Installer and the commissioning team, have proof of Functional Safety Management (meeting the requirements of IEC61508 part 1 clause 6 or its matching requirements under the sector standards)