THE 61508 ASSOCIATION
Guidance in Compliance

The IEC61508 Operators' hymn sheet

A few key points for those Operators of plant or equipment that involve SIL rated safety functions, trips or interlocks*

by The 61508 Association

SAFETY INSTRUMENTED SYSTEMS
are too important to leave to chance!

*SIL rated safety functions are safety trips or loops using the international safety standards within the IEC61508 group of standards

Rev 3 19.12.2017

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 1

Your company will have compared each risk to your company's tolerable target value and assigned a Safety Integrity Level (“SIL”) for each risk that is too great. The SIL defines the reliability demanded of the safety loop needed to keep you safe.* These SIL safety loops should be CLEARLY IDENTIFIED.

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 the 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 the 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 2

Your safety is depending on that SIL rated loop functioning correctly

…… So you CANNOT operate the process plant with any part of the SIL rated safety loop bypassed or knowingly faulty.*

…… If you see a fault occur then you MUST report that the loop is faulty so that the plant or equipment you are using can be put into a safe state* (that usually means stopping the process).

KEEP A RECORD of all equipment failures.

* *Other operational measures would need to be specified, applied and managed*

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 3

Your safety and the safety of others is depending on that SIL rated loop functioning correctly

…… You need to have a record of every time the safety loop operates and makes the plant safe and every time the saftey loop was required to operate but failed to make the plant safe.*.

Usually the design of the safety loop has to initially estimate how often the safety loop is going to have to act as part of the planning for testing and maintenance and for the design of the loop.

The data showing how often it ACTUALLY operates is needed under the standard to check and revise the reliability calculations and to KEEP YOU AND OTHERS SAFE.

You MUST report every time the SIL rated safety loop operates.

* *We call this "a demand" on the SIL rated system, so the designer needs to know each time there is a demand on the system whether or not the SIL rated loop acted successfully.*

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 4

Safety critical ALARMS don't just demand a response ... that response must be on time.

…… ALL safety critical alarms must have a clear response action and/or procedure.

Safety critical FAULTS don't just demand a response ... that response must be on time.

…… ALL safety critical faults must have a clear response action and/or procedure.

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 5

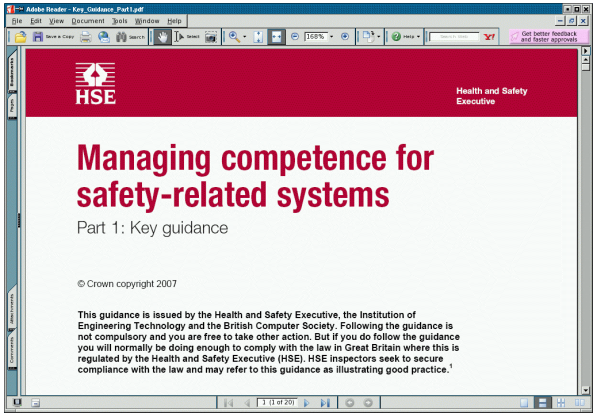
The IEC61508 group of standards require that you, the operator, have a place in “Functional Safety Management”

If you have a SIL rated loop then Safety is depending on that one SIL rated loop so EVERYONE involved has to be competent – *from those specifying what is needed right through to the operations and 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


HSE
Health and Safety Executive

Managing competence for safety-related systems

Part 1: Key guidance

© Crown copyright 2007

This guidance is issued by the Health and Safety Executive, the Institution of Engineering Technology and the British Computer Society. Following the guidance is not compulsory and you are free to take other action. But if you do follow the guidance you will normally be doing enough to comply with the law in Great Britain where this is regulated by the Health and Safety Executive (HSE). HSE inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.[1]

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.

... Functional Safety Management covers EVERYBODY involved

... not just the expert

... not just the technician

... it involves everybody involved with the safety system (including you, the OPERATOR)

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 7

Management of change

Safety critical loops should not normally be changed.

ANY change to the safety critical loop MUST go through a management of change procedure and you should be informed and re-trained on the functionality of the safety loop.

YOUR SAFETY AND OTHERS DEPENDS ON THIS SAFETY LOOP

THE 61508 ASSOCIATION
Guidance in Compliance

Important and surprising fact number 8

Testing a safety loop

YOUR SAFETY AND THE SAFETY OF OTHERS DEPENDS ON THE SAFETY LOOP

Testing of the loop MUST follow the proper procedure written down for the safety loop
AND
Operation of the plant whilst the loop is being tested MUST ALSO follow the safety measures for operation of the plant whilst the safety loop is unavailable.

The SIL of a safety related system that isn't tested for functionality will over time be reduced to zero, meaning it stops being dependable.
An increased test interval will result in an increased Probability of Failure at the moment when you need it to keep you safe
(this is referred to as the Probability of Failure on Demand or PFD_{avg}).

THE 61508 ASSOCIATION
Guidance in Compliance

Your guide for Safe Operation

IEC61508 is considered good engineering practice.

- You CANNOT operate the process plant or machinery with any part of the SIL rated safety loop bypassed or knowingly faulty.
- SIL rated safety loops should be clearly identified.
- You need to have a record of every time there is a demand on the Safety loop – i.e. a record of every time the loop is needed to operate and make the plant safe
- Safety critical alarms and faults don't just demand a response … that response must be on time and have a clear action and/or procedure.
- Everyone involved with a safety related system has to be competent in their role.
- ANY change to the safety critical loop MUST go through a management of change procedure and you should be informed and re-trained on the functionality of the safety loop.
- Testing of the loop MUST follow the proper procedure written down for the safety loop and operation of the plant must also follow the correct procedures during testing of the safety loop.