Functional Safety Management

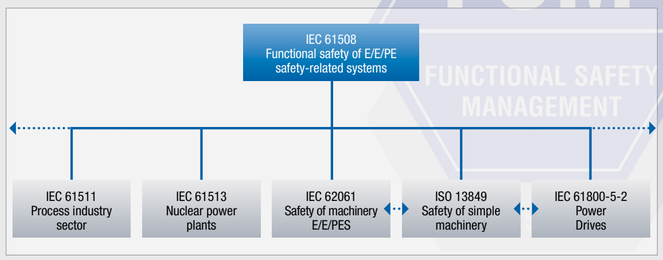
Eaton's MTL FSM poster

CROUSE-HINDS SERIES

IEC 61508 & SAFETY LIFECYCLE

WHAT IS FUNCTIONAL SAFETY?

In the process industries, safety can be defined as being protected from unacceptable risk of injury or damage to people, property or the environment. **Functional Safety** relates to the part of overall safety that depends upon the correct operation of an electrical/electronic/programmable electronic safety instrumented system, SIS. The requirements for such a SIS are defined in the IEC 61508 group of standards.



IEC 61508 aims to:

- release the potential of E/E/PE technology to improve both safety and economic performance;
- enable technological developments to take place within an overall safety framework;
- provide a technically sound, system based approach, with sufficient flexibility for the future;
- provide a risk-based approach for determining the required performance of safety-related systems;
- provide requirements based on common underlying principles to facilitate:
  - improved efficiencies in the supply chain for suppliers of subsystems and components to various sectors
  - improvements in communication and requirements (i.e. to increase clarity of what needs to be specified),
  - the development of techniques and measures that could be used across all sectors, increasing available resources,
  - the development of conformity assessment services if required.

Functional Safety Management

A basic requirement of the standards is that all aspects of the safety lifecycle activities demonstrate Functional Safety Management. As well as concerns for equipment, this includes management of personnel competency, covering the end-user, contractors, suppliers and sub-contractors.

(In the UK see also guidance from HSE' "Managing competence for safety-related systems".)

The **MTL Application Note AN9025** provides an introduction to the subject.

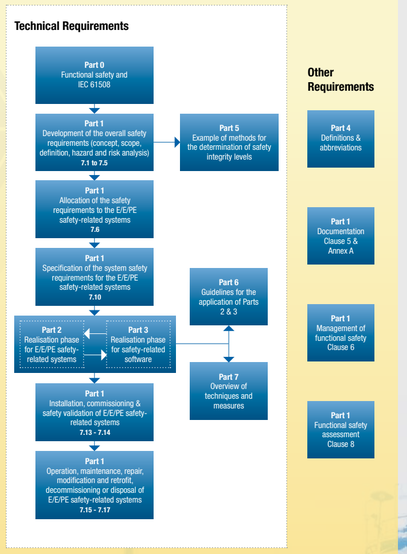
MTL Instruments are members of 'The 61508 Association'

The 61508 Association

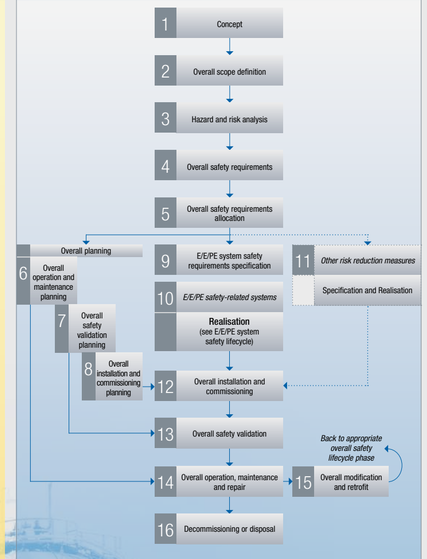
Baseefa (2001) Ltd
QUALITY ASSURANCE NOTIFICATION

Certificate No. CASS 00015/01

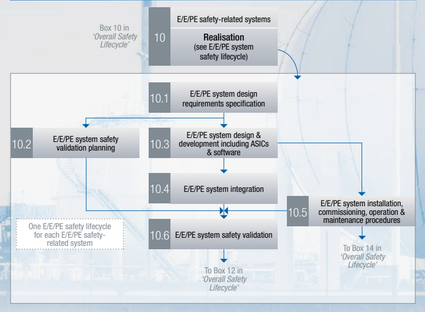
Overall framework of the IEC 61508 series



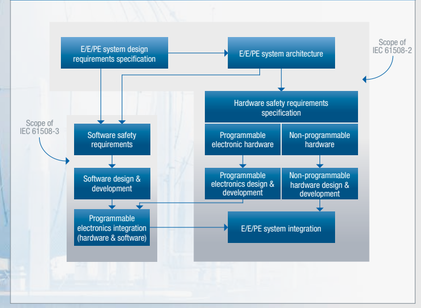
Overall safety lifecycle



E/E/PE system safety lifecycle (in realisation phase)



Relationship between & scope of IEC 61508-2 & IEC 61508-3



SAFETY INTEGRITY LEVELS

DEFINITION

Safety integrity is the ability of the SIS to perform the required safety function **as and when required**. Four levels of safety integrity are defined, each corresponding to a range of target likelihood of failures of a safety function. Safety integrity level 4 (SIL4) is the highest level of safety integrity and safety integrity level 1 (SIL1) is the lowest level.

Note that a safety integrity level is a property of a safety function rather than of a system or any part of a system.

Safety integrity is considered to be composed of the following two elements:

- **Hardware safety integrity**; that part of safety integrity relating to random hardware failures in a dangerous mode of failure. It may be necessary to use redundant architectures to achieve adequate hardware safety integrity.
- **Systematic safety integrity**; that part of safety integrity relating to systematic failures in a dangerous mode of failure. Techniques such as redundant channels of identical hardware, which are very effective at controlling random hardware failures, are of little use in reducing systematic failures such as software errors.

Devices, elements and systems may be Type A or Type B.

Type A is when the components required to perform a specified function meet all of the following:

a) The failure modes of all components are well defined; and
b) The behaviour of the device under fault conditions can be completely determined; and
c) There is sufficient dependable failure data to show that the claimed failure rates for detected and undetected dangerous failures are met.

Type B is simply when one or more of the components required to perform a specified function is not Type A.

SIL for High Demand Mode

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

SIL for Low Demand Mode

Safety Integrity Level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Type A Safety System

Safe failure fraction of an element	Hardware fault tolerance 0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Type B Safety System

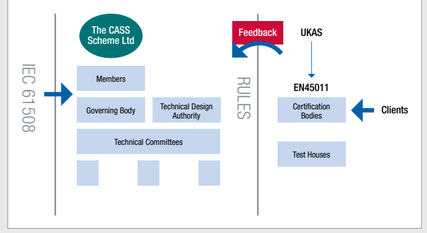
Safe failure fraction of an element	Hardware fault tolerance 0	1	2
< 60 %	Not Allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

www.61508.org
www.iec.ch/functionalsafety www.cass.uk.net
www.hse.gov.uk

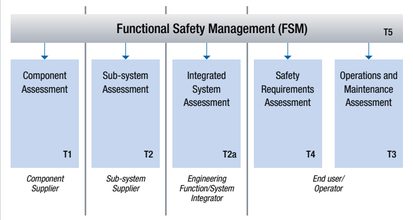
CASS SCHEME

CASS is a scheme for assessing the compliance of safety related systems with the requirements of IEC 61508 and associated standards. It provides a systematic approach to be used by certification bodies and others when assessing compliance at all stages from the specification of safety requirements through the design, development and manufacture of system components to integration, commissioning, operation and maintenance.

Accredited Certification for Safety Systems... to IEC 61508 and related standards



Relationship between CASS assessment types



TERMINOLOGIES & ABBREVIATIONS

Definitions and abbreviations

Abbreviation	Full expression	Abbreviation	Full expression
AC/DC	Alternating current/direct current	LVL	Limited variability language
AIChE	American institute of chemical engineers	MooN	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)
ALARP	As Low As Reasonably Practicable	MooND	M out of N channel architecture with Diagnostics
ANSI	American National Standards Institute	MTBF	Mean Time Between Failures
ASIC	Application Specific Integrated Circuit	MTTR	Mean Time To Repair
BPCS	Basic process control system	MRT	Mean Repair Time
CCF	Common Cause Failure	NP	Non-programmable
CPLD	Complex Programmable Logic Device	PAL	Programmable Array Logic
CCPS	Center for chemical process safety	PE	Programmable Electronic
DC	Diagnostic Coverage	PES	Programmable electronic system
(E)EPLD	(Electrically) Erasable Programmable Logic Device	PFD	Probability of Dangerous Failure on Demand
E/E/PE	Electrical/Electronic/Programmable Electronic	PFDavg	Average Probability of dangerous Failure on Demand
E/E/PE (system)	Electrical/Electronic/Programmable Electronic System	PFH	Average frequency of dangerous failure [h^{-1}]
EEPROM	Electrically Erasable Programmable Read-Only Memory	PLA	Programmable Logic Array
EPROM	Erasable Programmable Read-Only Memory	PLC	Programmable logic controller
EMC	Electro-magnetic compatibility	SAT	Site acceptance test
EUC	Equipment Under Control	SC	Systematic capability
FAT	Factory acceptance testing	SFF	Safe failure fraction
FPGA	Field Programmable Gate Array	SIF	Safety instrumented function
FPL	Fixed program language	SIL	Safety integrity level
FSA	Functional safety assessment	SIS	Safety instrumented system
FTA	Fault tree analysis	SRS	Safety requirement specification
FVL	Full variability language	UON	Unless otherwise noted
GAL	Generic Array Logic	λs or λsafe	Failure rate of all safe failures
H&RA	Hazard & risk assessment	λd or λdangerous	Failure rate of all dangerous failures
HFT	Hardware Fault Tolerance	λdd	Failure rate of all dangerous detected failures
IEC	International Electrotechnical Commission	λdu	Failure rate of all dangerous undetected failures
IEV	International Electrotechnical Vocabulary	λsu	Failure rate of all safe undetected failures
ISA	Instrumentation, Systems & Automation Society	λsd	Failure rate of all safe detected failures
ISO	International Organization for Standardization		

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton, Beds, LU2 8DL, UK.
Tel: +44 (0)1582 723633
Fax: +44 (0)1582 422283

AUSTRALIA
Tel: +61 1300 308 374
Fax: +61 1300 308 463

BeNeLux
Tel: +31 (0)418 570290
Fax: +31 (0)418 541044

CHINA
Tel: + 86 21 2899 3817
Fax: + 86 21 2899 3992

FRANCE
Tel: +33 (0)4 37 46 16 53
Fax: +33 (0)4 37 46 17 20

GERMANY
Tel: +49 (0)22 73 98 12 - 0
Fax: +49 (0)22 73 98 12 - 2 00

INDIA
Tel: +91 (0)44 24501660/24501857
Fax: +91 (0)44 24501463

ITALY
Tel: +39 02 959501
Fax: +39 02 95950759

JAPAN
Tel: +81 (0)3 6430 3128
Fax: +81 (0)3 6430 3129

NORWAY
Tel: +47 66 77 43 80
Fax: +47 66 84 55 33

RUSSIA
Tel: +7 (495) 981 3770
Fax: +7 (495) 981 3771

SINGAPORE
Tel: +65 6 645 9888
Fax: +65 6 487 7997

SOUTH KOREA
Tel: +82 6380 4805
Fax: +82 6380 4839

UNITED ARAB EMIRATES
Tel: +971 2 44 66 840
Fax: +971 2 44 66 841

UNITED KINGDOM
Tel: +44 (0)1582 723633
Fax: +44 (0)1582 422283

AMERICAS
Tel: +1 281-571-8065
Fax: +1 281-571-8069

www.mtl-inst.com mtlenquiry@eaton.com

For technical advice or further information call:

+44 (0)1582 723633

ZL-P-FSM-EN-0916