

IEC 61511



Functional safety -
Safety instrumented systems for the
process sector

Blacksafe Consulting Ltd
Maidenhead , Berkshire SL6 3UT
Telephone 01628 823573
E-Mail - blackw@blacksafe.demon.co.uk

IEC 61511



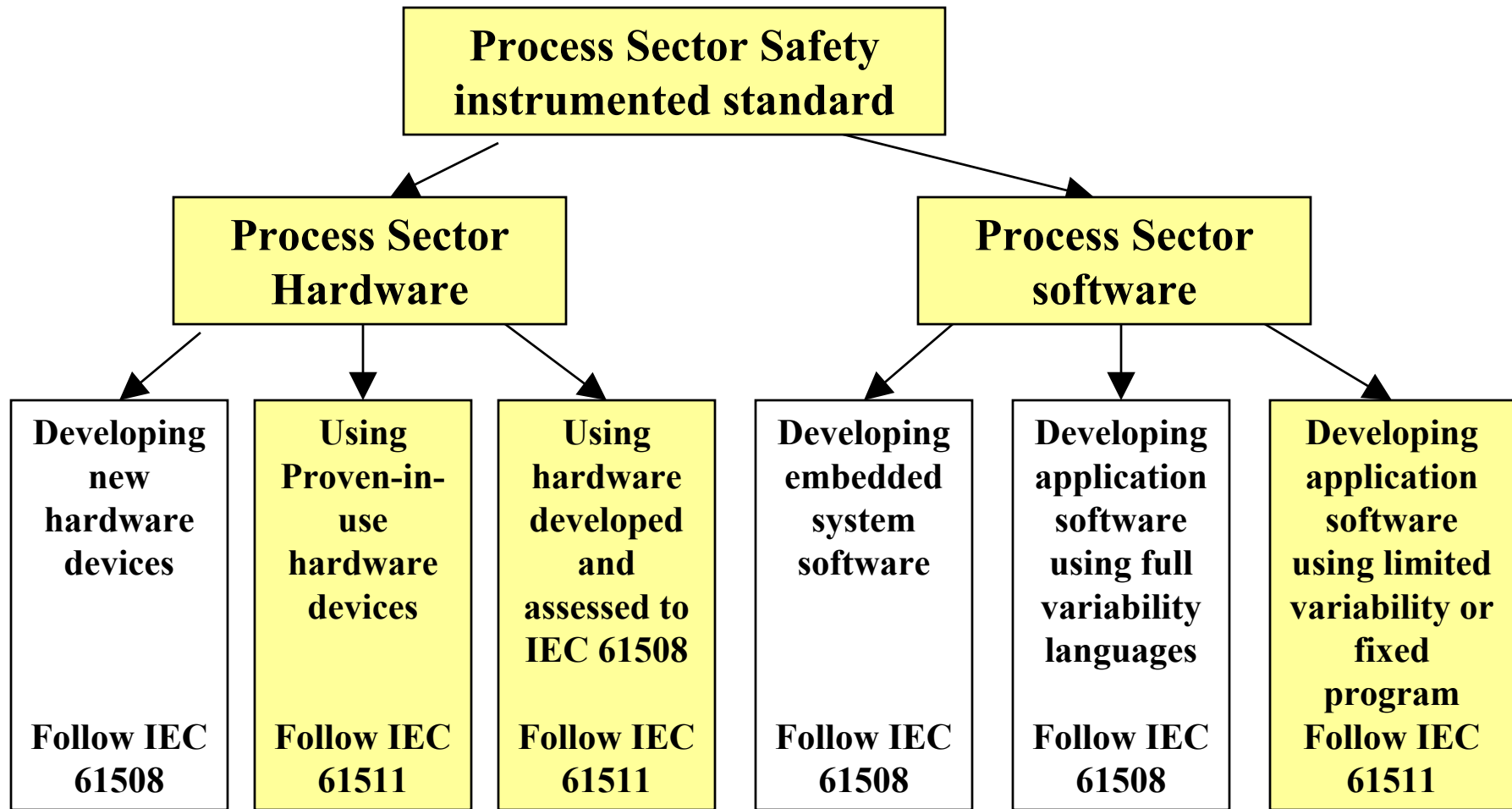
-
- Scope and structure
 - Differences to IEC 61508
 - Prior use
 - Differences to ANSI/ISA S84.01 - Application of Safety Instrumented Systems for the Process Industries
 - What else is new in process sector standards

IEC 61511 Scope



- Process sector version of IEC 61508
- Scope limited to users and system integrators
- Requires all sub-systems to be in compliance with IEC 61508 or proven by prior use
- Requires all free programmed software to be in compliance with IEC 61508
- Users and integrators also need to understand IEC 61508 as the basic requirement for equipment

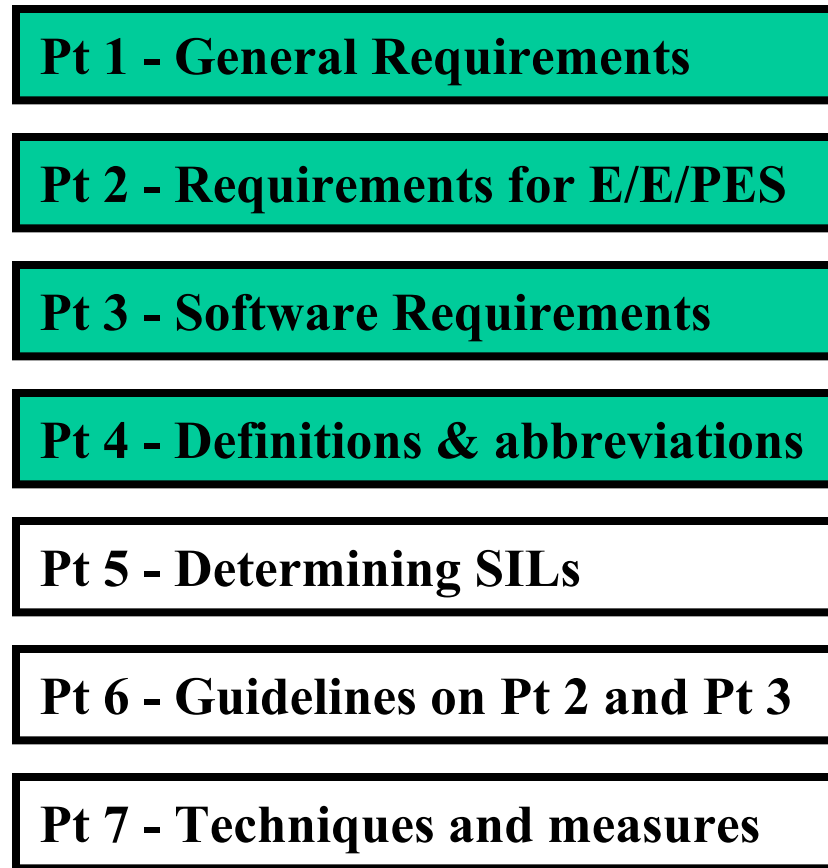
Safety lifecycle



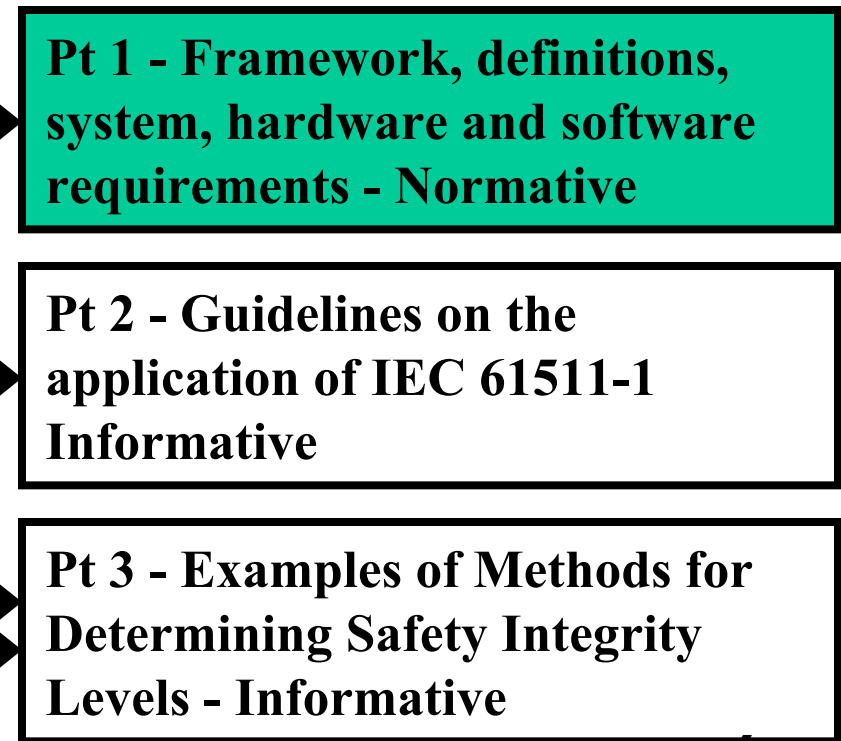
IEC 61511 Structure



IEC 61508



IEC 61511

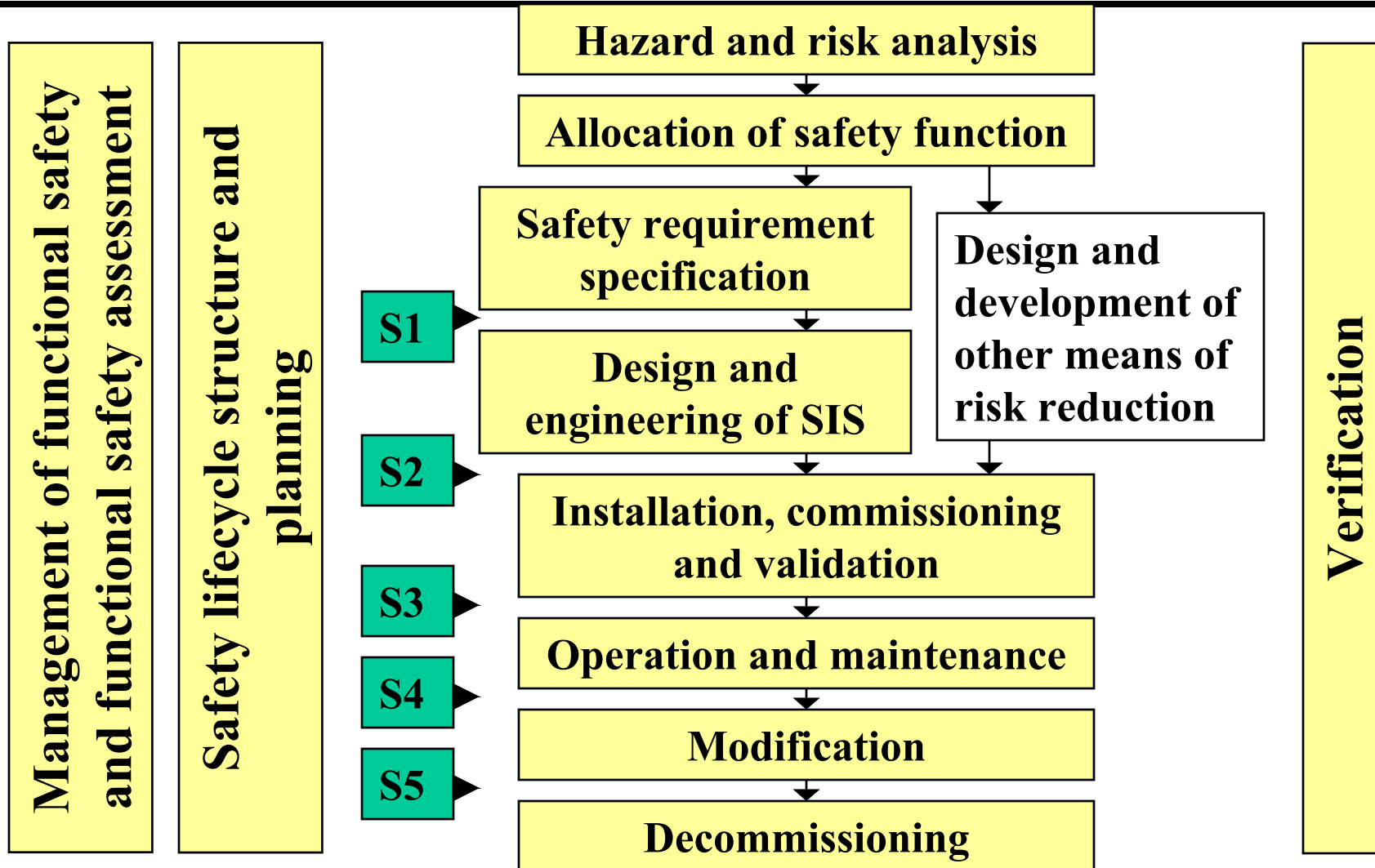


Part 1 differences to IEC 61508



- Process sector language used
- Safety lifecycle simplified
- Functional safety management normative
- Independent functional safety assessment integrated into functional safety management
- Independence limited to at least one senior competent person not involved in the project team
(Consider more if a large team is involved)

Safety Lifecycle



Part 1 differences to IEC 61508 - technical



- Mode definitions changed
- Type A and Type B not considered
- Fault tolerance tables simplified
- “proven in use” changed to “prior use”
- Sub-systems in accordance with IEC 61508 or prior use
- Technique tables deleted

IEC 61508 - Modes of Operation



- Low demand mode
Demand frequency:
 - less or equal to 1 per year and
 - less or equal to twice the proof test frequency
- High / Continuous Demand mode
Demand frequency:
 - greater than 1 per year or
 - more than twice the proof test frequency

Modes of Operation (IEC 61511)



- Demand mode use Table 3 (PFD) or Table 4 (λ_d)
if Table 4 is used then neither the proof test interval or the demand rate shall be used in the determination
(formula Hazard rate = PFD x demand rate and $\lambda_d = 2 \times \text{PFD} / T$ not to be used to determine SIL)
- Continuous mode use Table 4 (λ_d)

NOTE - For demand rates higher than 1 per year SIL will be lower if Table 4 is used as a basis

Demand mode Table 3



Safety integrity level (SIL)	Target average probability of failure on demand	Target risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	10,000 – 100,000
3	$\geq 10^{-4}$ to $< 10^{-3}$	1000 – 10,000
2	$\geq 10^{-3}$ to $< 10^{-2}$	100 - 1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	10 - 100

Continuous mode (Table 4)



Safety integrity level	Target frequency of dangerous failure to perform the safety instrumented function (per hour)
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 $< 10^{-5}$

Prior use (general)



-
- Appropriate evidence shall be available in either safety or non safety applications
 - Evidence of suitability shall include:
 - consideration of manufacturers quality and configuration management
 - adequate specification and identification of components
 - performance in similar operating profiles and physical environments
 - the volume of the operating experience (user list of approved equipment may support claims provided ...)

User list



User list can be used provided

- The list is updated and monitored regularly
- Field devices are only added after sufficient operating experience
- Field devices are removed if not performing in a satisfactory manner
- The process application is included in the list where appropriate

Prior use (fixed program devices) additional requirements



- Unused features identified and unlikely to jeopardise required safety functions
- Evidence of suitability includes:
 - characteristics of input and output signals
 - modes of use
 - functions and configurations used
 - previous use in similar applications and environment
- For SIL 3 a formal assessment shall be carried out
- For SIL 3 a safety manual shall be available

Prior use (Limited variability) additional requirements



- Applies to SIL 1 and SIL 2 only
- Differences between operating profiles and physical environments identified and assessment made to show likelihood of systematic faults is low
- Operating experience necessary takes account of SIL, complexity and functionality
- Safety configured PLC can be used subject to:
- Formal assessment (functional safety assessment) if PE logic solver is used in a SIL 2 application

Prior use (full variability)



-
- Applications programmed using a full variability language shall be in accordance with IEC 61508-2 and IEC 61508-3

IEC 61508 - Type B

Fault tolerance



Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	N/A	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Minimum hardware fault tolerance of PE logic solvers



Table 5

SIL	Minimum hardware fault tolerance		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply see IEC 61508		

IEC 61508 - Type A Fault tolerance



Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

Hardware fault tolerance of sensors, final elements, and non PE logic



Table 6

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	special requirements apply (see IEC 61508)

Table 6 conditions



-
- Conditional on dominant failure mode is to the safe state or dangerous failure are detected otherwise fault tolerance is increased by one
 - May be reduced by 1 if all the following apply:
 - hardware is selected on the basis of prior use
 - configuration is of process parameters only
 - adjustment of parameters is protected
 - function has a $SIL < 4$
 - IEC 61508 fault tolerance an alternative

Part 2 Guidance



-
- More guidance on audit
 - Guidance on typical process lifecycle where allocation may be prior to risk assessment
 - Allows for relief valves to be considered adequate without risk assessments
 - Allows shared equipment with BPCS with further risk assessments
 - Limits on claims if diagnostics are in BPCS
 - Guidance on wiring, interfaces, maintenance etc taken from ISA S84.01

Part 3 Guidance



-
- More examples included
 - Safety matrix method modified, definition of IPL is changed from ISA SP84.01
 - Calibrated risk graph included as semi-qualitative method, example from industry
 - DIN 19250 risk graph included
 - Layer of protection analysis included (LOPA)
 - Techniques directory included
 - Common mode a concern for high risk reduction

Other process sector standards



- ISO 10418 - Analysis, design, installation and testing of surface protection systems
New standard published in October, previous edition was based on API 14 C. New version references IEC 61511 for secondary
- prEN 50402 - Functional safety requirements for fixed gas detection systems
References IEC 61511 and EN 954-1