

CASS 61511 Workshop

Overview of the CASS IEC 61511 Templates

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither The CASS Scheme Association nor its members will assume any liability for any use made thereof.



Contact us via T6A: https://61508.org / info@61508.org







IEC 61511 CASS Templates

- What are Targets of Evaluation (TOEs)?
- **CASS-511-FSM** Functional Safety Management.
- **CASS-511-LVL** Subsystem LVL software.
- CASS-511-FSA Functional Safety Assessments.
- **CASS-511-OP** Operations and Maintenance.



Why The CASS Templates Exist

- To support in the assessment of functional safety.
- Must be available before project start!
- To demonstrate compliance with IEC 61508 or related standard.
- Each functional safety standard has a lot of requirements (guide).
- Open to all and free-of-charge.
- Transparent methodology.
- Required by UKAS (accredited certification).

NOTE: Templates cover IEC, EN, and BS EN variants.



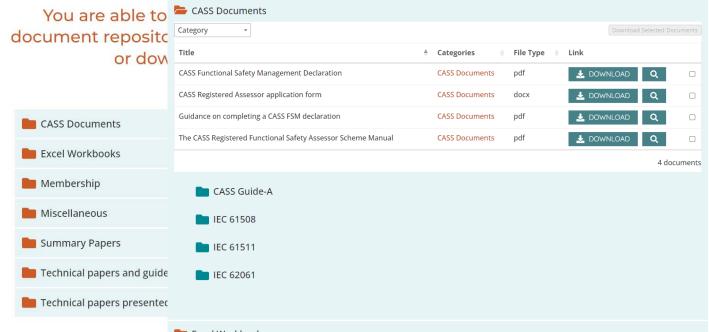


- CASS templates reliant on the competence of the assessor!
- CASS templates can be used for any level of rigor.
 - Full FSA's.
 - Full assessments of functional safety.
 - Gap analysis of requirements.
 - Simple checklist of requirements (buying an asset).
- The rigor of any assessment must increase commensurate with the SIL.
- CASS templates must be used with a copy of the standard.
- CASS templates must be used by competent persons.



Template Location

- Where are the templates (<u>https://61508.org/downloads/</u>)?
- How can I find them (search)?
- How do I know the templates have been updated?
- CASS membership.







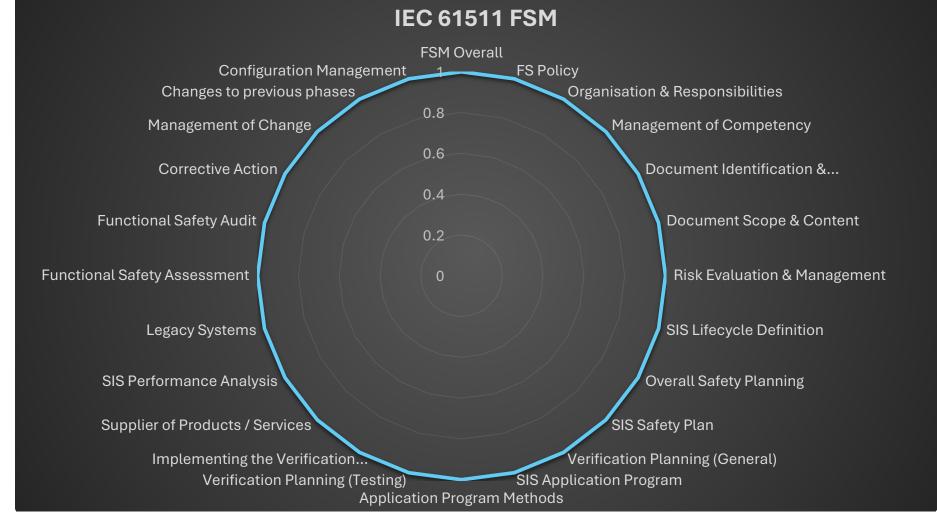
• We'll now cover **CASS-511-FSM** and some example TOE(s)



25 TOEs in total

TOEs Range from Documentation Control, & Competence through to Configuration Management

Question – What if you have an existing QMS against ISO 9001, can this be credited?



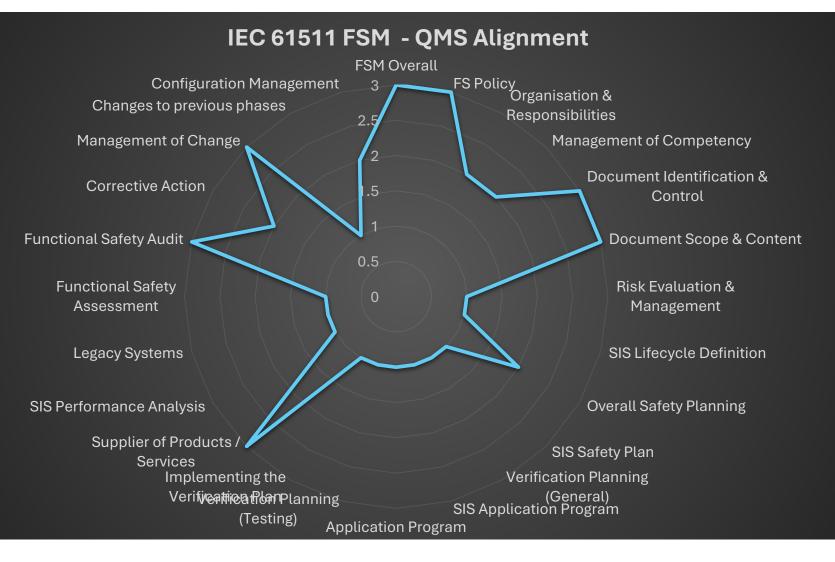


If we consider

1 – No commonality 3 – Commonality Between QMS and FSM

We now see our QMS **can** support in the development of an **Integrated Solution**

But this all looks a little scattered



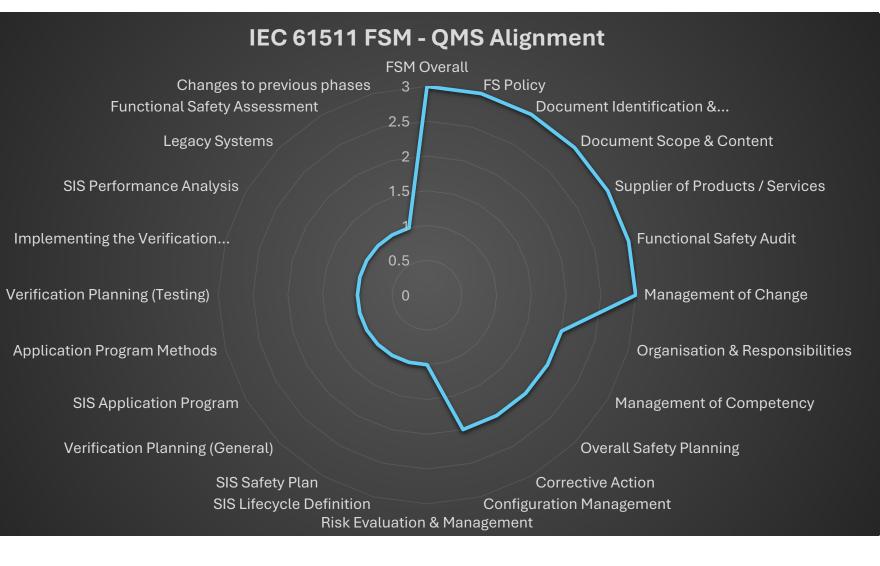


Now If we consider the same 1 – No commonality 3 – Commonality But in some form of Order

We can see where our QMS can support an **Integrated Solution** and where we need to focus our attention

Implementing FSM is not difficult if developed correctly

Let's look at some of these in more detail





Contact us via T6A: https://61508.org / info@61508.org

3 – Commonality

TOE 6

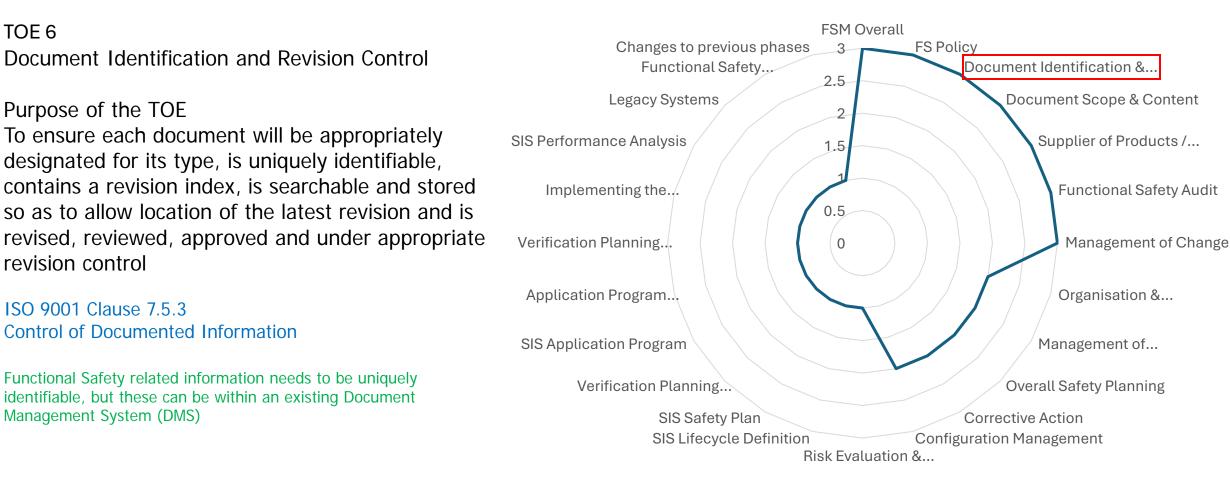
Purpose of the TOE

revision control

ISO 9001 Clause 7.5.3

Control of Documented Information

IEC 61511 FSM - QMS Alignment





Management System (DMS)

Contact us via T6A: https://61508.org / info@61508.org

3 – Commonality

Functional Safety Audit

Purpose of the TOE

ISO 9001 Clause 9.2

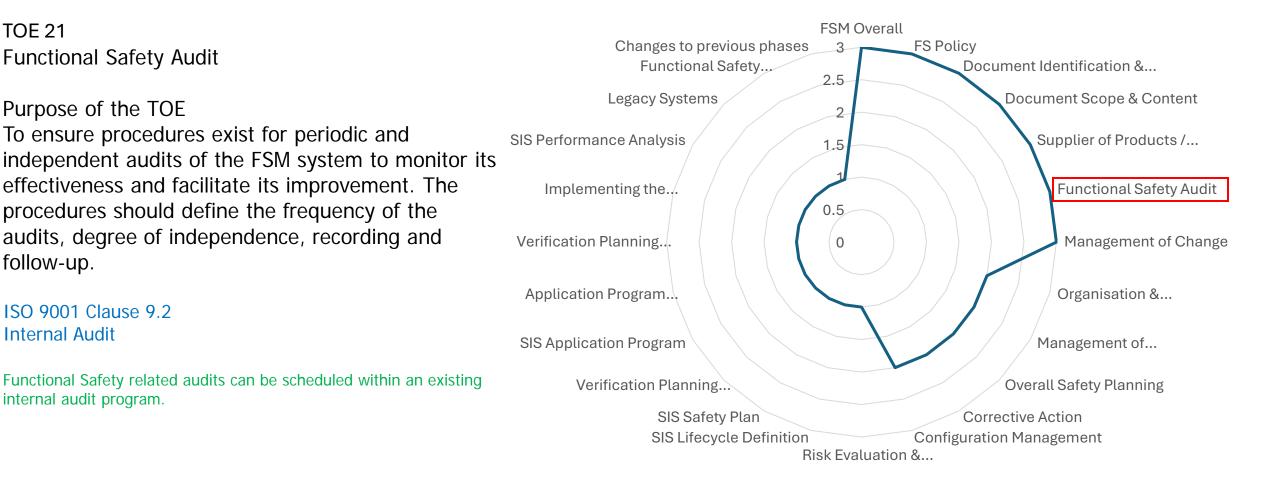
internal audit program.

TOE 21

follow-up.

Internal Audit

IEC 61511 FSM - QMS Alignment

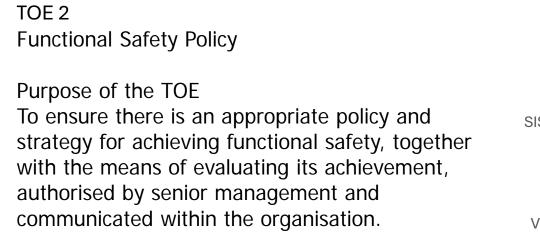




Contact us via T6A: https://61508.org / info@61508.org

<u>3 – Commonality</u>

IEC 61511 FSM - QMS Alignment



ISO 9001 Clause 5.2 Quality Policy

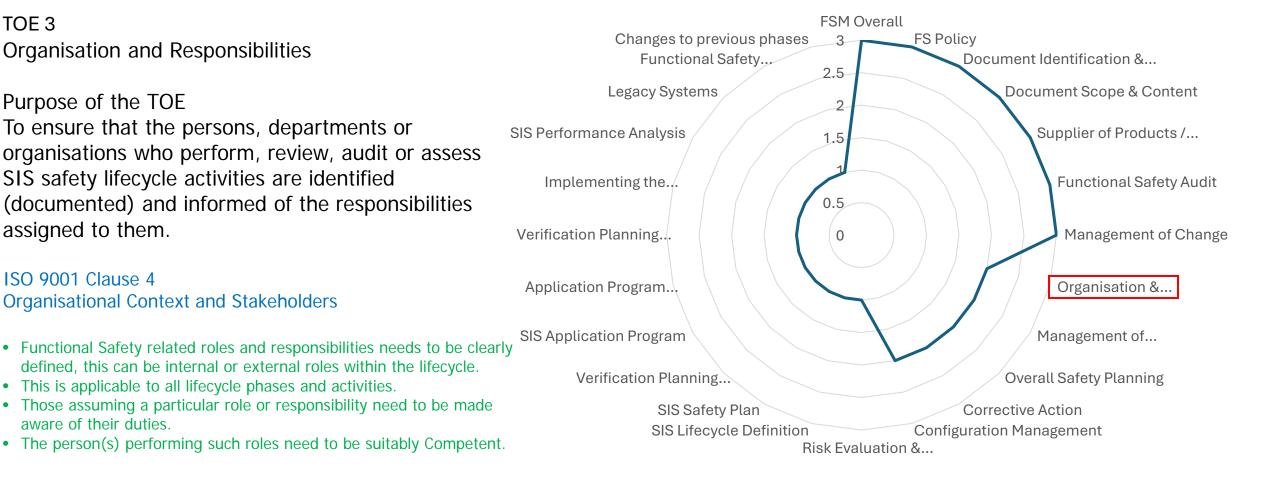
- Appropriate to the Organisation & Activities
- Aligned with the company strategic direction
- Commitment to meeting standards
- Framework for establishing and reviewing objectives (KPI)
- Communicated and Understood





2 – Partial Commonality

IEC 61511 FSM - QMS Alignment

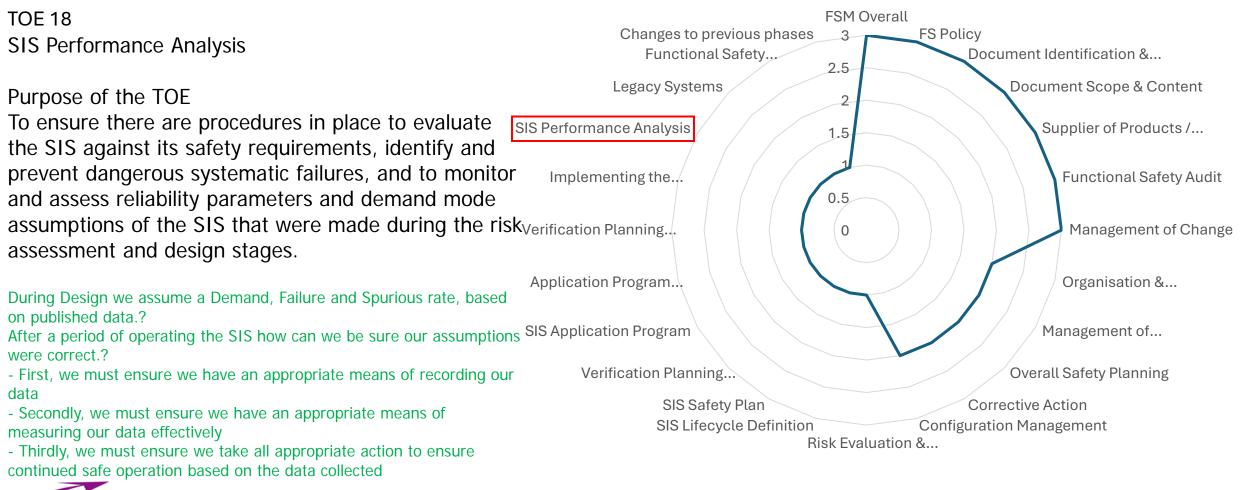




TOE 3

<u>1 – No Commonality</u>

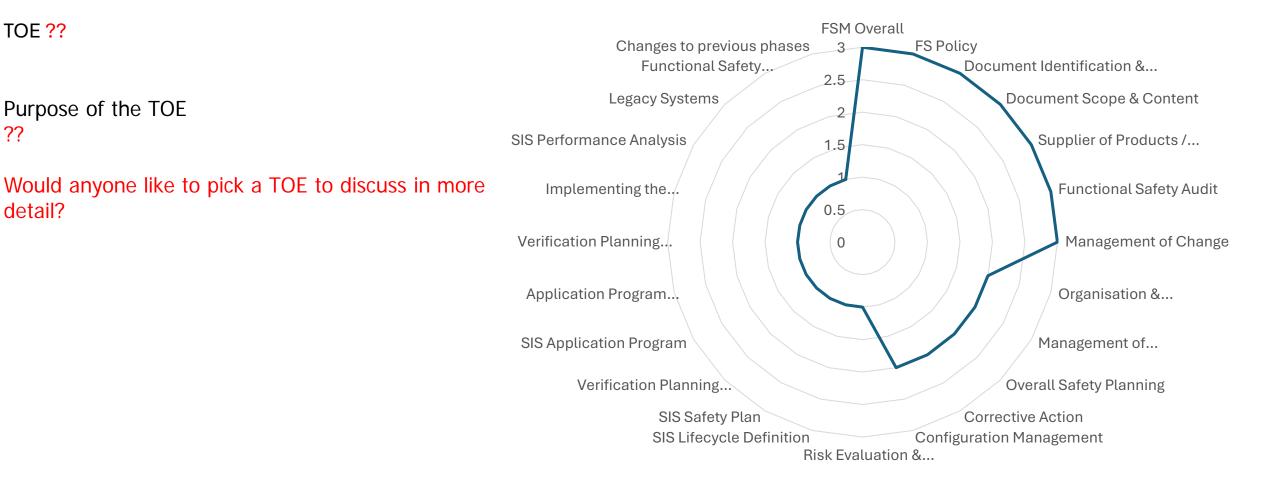
IEC 61511 FSM - QMS Alignment





<u>1 – No Commonality</u>

IEC 61511 FSM - QMS Alignment





??

Contact us via T6A: https://61508.org / info@61508.org

FSM Conclusion

FSM is MANDATORY for all involved in the lifecycle.

We can demonstrate FSM through an **Integrated Solution** which reduces over burden, ensures alignment of procedures, and prevents conflicting processes.

Implementing FSM is not difficult if developed correctly.!

IEC 61511 FSM - QMS Alignment FSM Overall Changes to previous phases FS Policy **Functional Safety Assessment Document Identification &...** 2.5 Legacy Systems Document Scope & Content 2 SIS Performance Analysis Supplier of Products / Services 1.5 Implementing the Verification... Functional Safety Audit 0.5 Verification Planning (Testing) Management of Change **Organisation & Responsibilities** Application Program Methods SIS Application Program Management of Competency Verification Planning (General) **Overall Safety Planning Corrective Action** SIS Safety Plan SIS Lifecycle Definition **Configuration Management Risk Evaluation & Management**



Contact us via T6A: https://61508.org / info@61508.org



• We'll now cover **CASS-511-LVL** and some example TOE(s)



27 TOEs in total

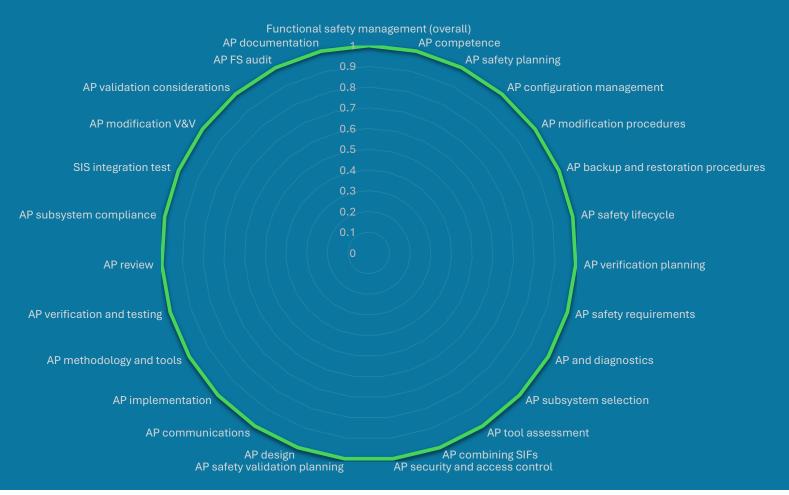
TOEs Range from FSM, & AP Competence through to AP Testing and Verification

IEC 61508 Part 3 TOEs total 46 – but this is for FVL, Embedded, LVL – all software types

IEC 61511 only considers LVL, Application Specific software development.

Question – What does my FSM need to include as a developer of LVL?

IEC 61511 LVL



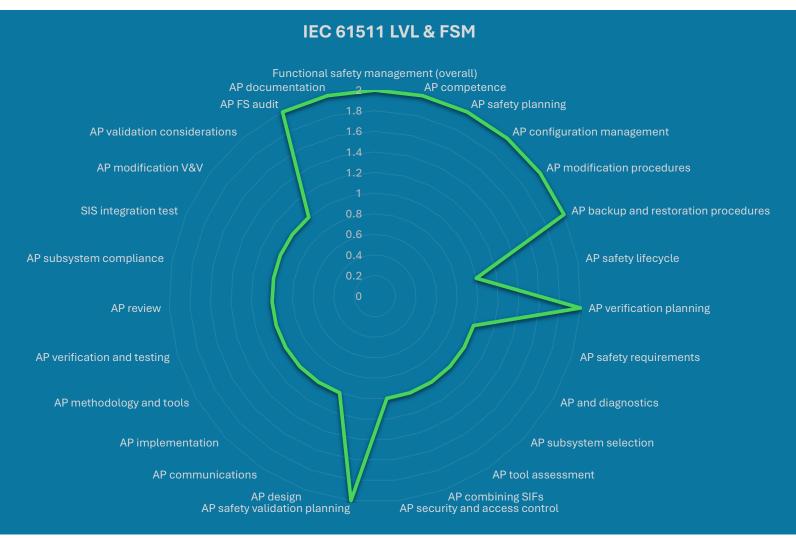


If we consider

2 – FSM Requirement 1 – Project Requirement

We now see which TOEs are in regard to FSM and which are Project Specific

But again, this all looks a little scattered



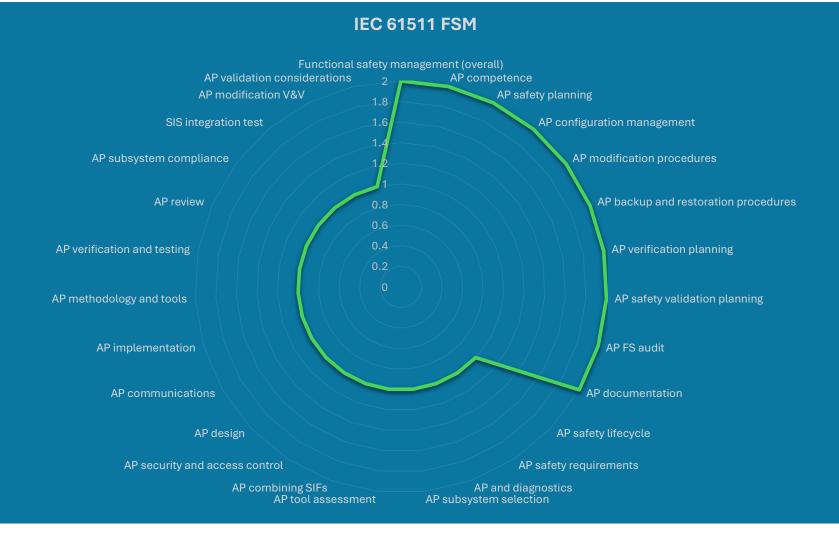


If we consider

2 – FSM Requirement 1 – Project Requirement

Now with some order we can see 10 of the TOEs (40%) relate to our FSM

The remaining TOEs are Project specific however it should be noted these can be linked to specific templates or schemes of work to ensure consistency across multiple projects.





2 – FSM Requirement

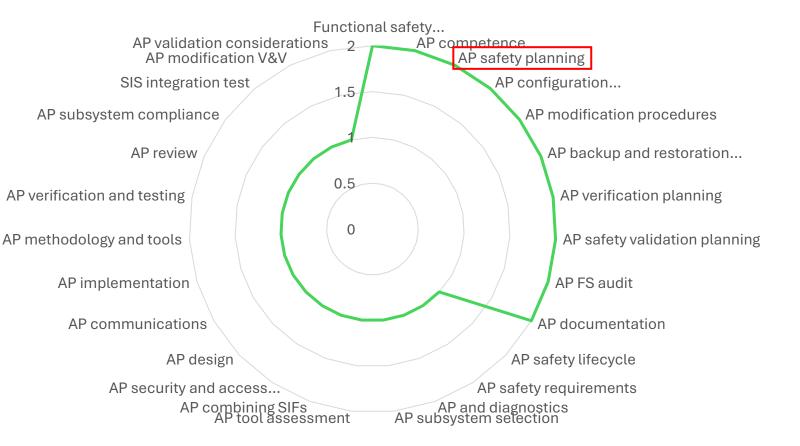
IEC 61511 FSM

TOE 6 AP Safety Planning

Purpose of the TOE For all SILs, ensure there is general evidence of safety planning for the software lifecycle and development

The FSM should define AP Safety Planning;

- When planning is to be performed for AP Development
- Who drafts the AP Safety Plan
- What the AP Safety Plan should contain
- Ensuring the AP Safety Plan details all of the requirements





2 – FSM Requirement

the software lifecycle and software

AP design and development processes

IEC 61511 FSM

Functional safety... AP validation considerations AP competence 2 AP modification V&V AP safety planning SIS integration test AP configuration... 1.5 For all SILs, ensure that relevant aspects of AP subsystem compliance AP modification procedures **AP** review AP backup and restoration... development have been audited in relation 0.5 AP verification and testing AP verification planning 0 The FSM or Integrated Management System should include AP methodology and tools AP safety validation planning AP implementation AP FS audit For a company performing the AP design and development this Audit schedule should include periodic auditing of the **AP** communications AP documentation AP design AP safety lifecycle AP security and access... AP safety requirements AP combining SIFs AP tool assessment AP and diagnostics AP subsystem selection



TOE 26

AP FS Audit

Purpose of the TOE

to functional safety

an Audit Schedule.

1 – Project Requirement

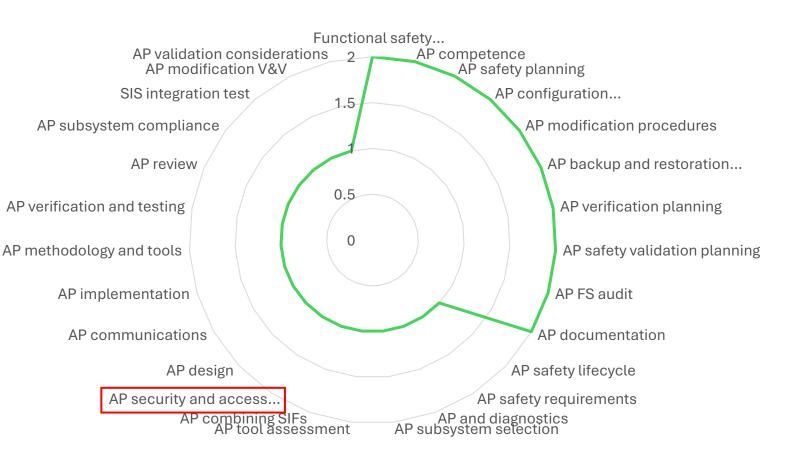
TOE 14 AP Security & Access Control

Purpose of the TOE For all SILs, ensure that the AP design and coding has considered the relevant security risk and access control requirements

The design and development of the AP should consider any security risk assessment requirements.

The security risk assessment will define any identified threats and mitigations which need to be considered during design.

IEC 62443 is the common standard which is used when conducting the security risk assessment during earlier phases.



IEC 61511 FSM



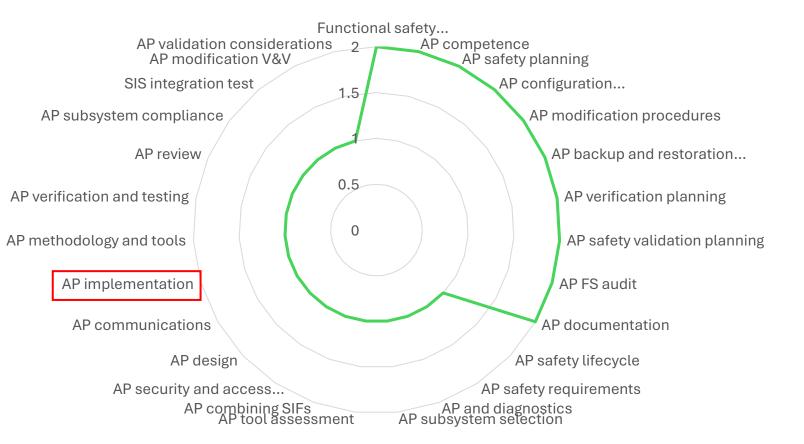
1 – Project Requirement

TOE 18 AP Implementation

Purpose of the TOE For all SILs, ensure that the application program development methodology complies with the development tools and restrictions of the SIS PE subsystem, is produced in a structured manner (e.g., modularity), justifies the use of previously developed libraries, and details clear ownership / identification. To also ensure AP implementation is traceable to the AP safety requirements

Usually for LVL applications standard configurable and modular coding is used from a pre-approved library. All of this needs to be defined, justified and verifiable.







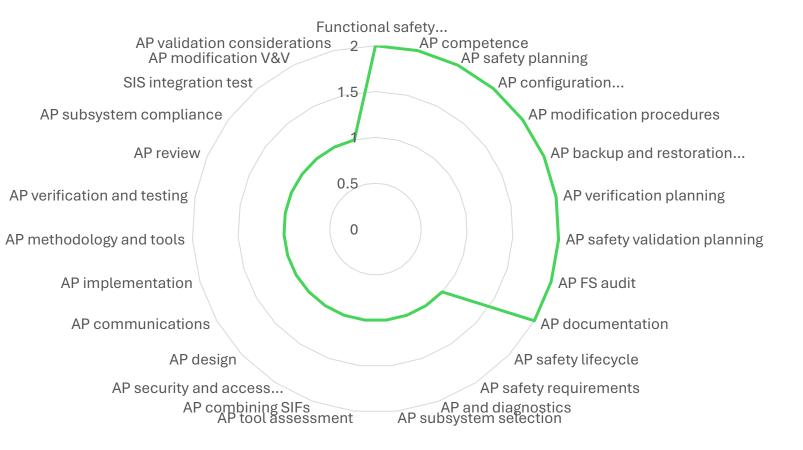
1 – Project Requirement

IEC 61511 FSM

TOE ??

Purpose of the TOE ??

Would anyone like to pick a TOE to discuss in more detail?





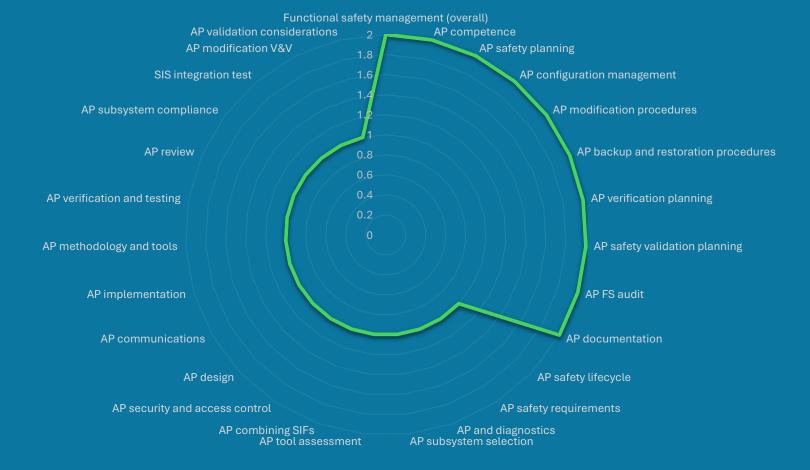
LVL Conclusion

LVL development leans on the **FSM** in at least **40%** of TOEs.

LVL Scheme was developed to reflect IEC 61511 requirements for Application Program development and to eliminate the need to follow the IEC 61508 Part 3 TOEs

- Planning
- Specifying
- Verifying &
- Validating

Are all still crucial and fundamental requirements of LVL development



IEC 61511 FSM





• We'll now cover **CASS-511-FSA** and some example TOE(s)



Functional Safety Assessment scheme developed for IEC 61511

The Scheme is broken down into the FSA stages defined in IEC61511

- Stage 1 During H&RA
- Stage 2 During Detailed Design
- Stage 3 Prior to Introducing Hazards
- Stage 4 Periodically in Operations
- Stage 5 During Modifications

The Scheme is in Excel format

×	AutoSave	Off [] り、 マ マ CASS-511-FSA-Functional-Safety-Assessment-v2 (1).	xlsx 🌘 G	General* •	Saved to	o this PC 丶	✓ Search	- e						
File	e Hom	e Insert	Page Layout Formulas Data Review View Automate	Help					Comments 🖻 Shar						
A1		-	$f_x \sim$ Project:												
4		в			E	F	G	н	1						
Project Title:		='Planning '!B1 ='Planning '!B2													
Client: Asset:		='Planning '!B3 ='Planning '!B4													
Issue: The fol		='Planning '!B5 ted when using this as	sessment checklist:												
- Not a - Postil Stage			id manifest to complete an assessment, the second charde and the fracted as a field han exercise, in a the SIS synthet is arisen as quienesses of the tradeoff ECS SUS and shall not be treated as an addit against this checklist, competent person(c) and use of this checklist shall not negate the competence requirements, completing the checklist.		Oute			Assessment Team Comments	Recommendations / Acti						
Phase 1	1 - Həzərd ənd Risk	Assessment		Yes	No	Partial	N/A								
	FSA-1: 1-1	8.2.1	Is there a description of the hazardous event and the factors that could contribute to it? (Including Human factors)												
	FSA-1: 1-2	8.2.1	Is there a description of the consequences and the likelihood of the event occurring?												
	FSA-1: 1-3	8.2.1	Have all conditions of operation been considered such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown?												
-	FSA-1: 1-4 FSA-1: 1-5	8.2.1	Have any additional risk reduction methods been identified to achieve the required safety? Have measures to reduce or remove hazards and risk been considered fidentified?												
	FSA-1: 1-6	8.2.1	There means use or round we remove neares, and round contractive nearest of the second												
	FSA-1: 1-7	8.2.1	Have safety functions been allocated to layers of protection, taking into account common cause failures between the safety layers and between safety layers and BPCS?												
	FSA-1: 1-8	8.2.1	Have safety functions applied as safety instrumented functions been clearly identified and are they deemed effective against all initiating events?			1									
	FSA-1: 1-9	8.2.2	Has the dangerous failure rate of the BPCS as an initiating source (i.e. placing a demand on a protection layer) not assumed to be less than 10 ⁴ per hour?												
	FSA-1: 1-10	8.2.3	Ib the lowest and right possesment recorded such that it is: - decimant and such and the second such that it is: - seconds and such and second such that it is: - seconds and second such and second such form; - sequitable distribution of second such and second seco												
	FSA-1: 1-11	8.2.4	Has a security risk assessment been carried out to identify the security vulnerabilities of the SIS (including BPCS or any other device connected to the SIS)?												
	FSA-1: 1-12	8.2.4	Deep the rewrity risk sectormat contain a description of identificat theorem that could supplit-inducebilities and scott is a security events (including intentional attacks on the hordware, applications programs and robated contrars, as well as unintended events resulting from human error)?												
	FSA-1: 1-13	8.2.4	Are various phases considered in the Security Risk Assessment such as design, implementation, commissioning, operation, and maintenance?												
	FSA-1: 1-14	8.2.4	Have additional requirements for risk reduction been identified in the Security Flick Assessment?						1						
1	FSA-1: 1-15	8.2.4	Does the security risk assessment include descriptions of, or references to information on, the measures taken to reduce or remove the threats?												
Phase 2	2 - Allocation of sa	fety functions to prote	ctive layers		I			1 	1						
4	CASS TOE	IEC 61511 Clause	Assessment Prompt	Yes	Out	ome Partial	N/A	Assessment Team Comments	Recommendations / Act						
[FSA-1: 2-1	9.2.1	Have allocation of safety functions to specific protection layers been documented for the purpose of prevention, control or mitigation?												
<		Plannin	G FSA Stage 1 Requirements FSA Stage 1 Checklist	A Stage 2	Reauire	ements	FSA S	Stage 2 Checklist FSA Stage 3 Requiremer	nts FSA Sta ··· + :						



Functional Safety Assessment scheme developed for IEC 61511

FSA Planning is a mandatory requirement of IEC 61511

The Scheme template has a Tab which can be used to complete the planning portion

A oject:	∽] : [× ∿	$/ f_x \sim $ Project:						
A								
	в	C C		E	F	G	н	1
e:	='Planning '!B1 ='Planning '!B2							
at:	='Planning "!B3							
iet: Ie:	='Planning '!B4 ='Planning ''B5							
ot all checklist entries ostitive reporting show age 1FSA	maybe relevant for every Id be considered when o	id menoire to complete an assessment, the assessment should not be treated as a trick how exercise, tere of the IR against the relevant reprimensates of the standard RC 6011 and shall not be treated as an andit against this checklist, present and a standard shall not acquire the computance requirements, completing the checklist.		Ostcos	na ana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny			
CASS TOE	IEC 61511 Clause	Assessment Prompt	Yes		Partial	N/A	Assessment Team Comments	Recommendations
FSA-1: 1-1	8.2.1	is there a description of the hazardous event and the factors that could contribute to it? (Including Human factors)						
FSA-1: 1-2	8.2.1	Is there a description of the consequences and the likelihood of the event occurring?					_	
FSA-1: 1-3	8.2.1	Have all conditions of operation been considered such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown?						
FSA-1: 1-4	8.2.1	Have any additional risk reduction methods been identified to achieve the required safety?						
FSA-1: 1-5	8.2.1	Have measures to reduce or remove hazards and risk been considered lidentified?						
FSA-1: 1-6	8.2.1	Does the assessment contain a detailed description of the assumptions made during analysis of the risks, including probable dumand rates and equipment failure rates, and of any credit taken for operational constraints or huma intervention?			1			
FSA-1: 1-7	8.2.1	Have safety functions been allocated to layers of protection, taking into account common cause failures between the safety layers and between safety layers and BPCS?						
FSA-1: 1-8	8.2.1	Have safety functions applied as safety instrumented functions been clearly identified and are they deemed effective against all initiating events?						
FSA-1: 1-9	8.2.2	Has the dangerous failure rate of the BPCS as an initiating source (i.e. placing a demand on a protection layer) not assumed to be less than 10 ⁻⁴ per hour?						
FSA-1: 1-10	8.2.3	Ie he haard and rik soezimaat recorded spek that it is: - electra and tractical spek of date; - saccurata da glo to date; - sacapto understand; - swalikhin in a accessibili, minitabable date defable form; - swalikhin in a accessibili, minitabable date defable form; - swalikhin in a accessibili, minitabable date defable form;						
FSA-1: 1-11	8.2.4	Has a security risk assessment been carried out to identify the security vulnerabilities of the SIS (including BPCS or any other device connected to the SIS)?						
FSA-1: 1-12	8.2.4	Does the security risk assessment contain a description of identified threats that could apploit wherehilds and earth in security events (including intentional attacks on the hardware, application programs and related software, as well as winiteded events resulting from human error)?	on .					
NSA-1: 1-13	8.2.4	Are various phases considered in the Security Risk Assessment such as design, implementation, commissioning, operation, and maintenance?						
	8.2.4	Have additional requirements for risk reduction been identified in the Security Risk Assessment?						
FSA-1:1-1			-					
FSA-1: 1-1 FSA-1: 1-15	82.4	Does the security risk assessment include descriptions of, or references to information on, the measures taken to reduce or remove the threats?						
FSA-1: 1-15	8.2.4 fear functions to prote							



Functional Safety Assessment scheme developed for IEC 61511

Each FSA stage has a Requirements and Checklist Tab

The Stage 3 & 4 also have an additional Visual Inspection Tab

Note – An FSA should be performed by an independent Competent Person(s) and should NOT be treated as a Tick Box exercise, the Scheme is to aid engineering judgement and ensure thoroughness of the assessment

] ∽ ∼ ∼ CASS-511-FSA-Functional-Safety-Assessment-v2 (1).:						
ile Hor	ne Insert	Page Layout Formulas Data Review View Automate H	Help					Comments
		$f_x \sim f_x \sim f_x$						
ict:	"Planning '!B1							
A:	='Planning '!B2 ='Planning '!B3							
t: :	='Planning '!B4 ='Planning '!B5							
	noted when using this as							
checklist is only fo assessment is a jud	or guidance to act as an a dgement based on the rev a parformed by cuitable	id memoire to complete an assessmeat, the assessmeat should not be treated as a fick box exercise, riew of the SIS against the relevant requirements of the standard IEC 61511 and shall not be treated as an andit against this checklist, completent person(s) and use of this checklist shall not agained the completence requirements,						
all checklist entrie	s maybe relevant for ever ould be considered when	re assessment.						
ge 1 FSA								
CASS TOE	IEC 61511 Clause	Assessment Prompt	Yes	Outco	ne Partial	N/A	Assessment Team Comments	Recommendations
e 1 - Hazard and Ri:								
FSA-1: 1-1 FSA-1: 1-2	8.2.1	Is there a description of the hazardous event and the factors that could contribute to it? (Including Human factors) Is there a description of the consequences and the likelihood of the event occurring?	-					
FSA-1: 1-3	8.2.1	s use a description of the consequences and the memory of the event occurring: Have all conditions of operation been considered such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown?						
FSA-1: 1-4	8.2.1	Have any additional risk reduction methods been identified to achieve the required safety?						
FSA-1: 1-5	8.2.1	Have measures to reduce or remove hazards and risk been considered /identified?						
FSA-1: 1-6	8.2.1	Does the assessment contain a detailed description of the assumptions made during analysis of the risks, including probable demand rokes and equipment failure rates, and of any credit taken for operational constraints or human intervention?						
FSA-1: 1-7	8.2.1	Have safety functions been allocated to layers of protection, taking into account common cause failures between the safety layers and between safety layers and BPCS?						
FSA-1: 1-8	8.2.1	Have safety functions applied as safety instrumented functions been clearly identified and are they deemed effective against all initiating events?			1			
FSA-1: 1-9	8.2.2	Has the dangerous failure rate of the BPCS as an initiating source (i.e. placing a demand on a protection layer) not assumed to be less than 10 ⁻⁵ per hour?						
FSA-1: 1-10	82.3	Is the located and risk assessment recorded such that it is: • vorwards and ph doug: • vorwards and ph doug: • couple is and ph doug: • couple is and ph doug and editable form; • vorwards in an accessible, maintainable and editable form; • vorwards in an accessible, maintainable and editable form; • vorwards and and vorwards exact rolled;						
FSA-1: 1-11	8.2.4	Has a security risk experiment been carried out to identify the security vulnerabilities of the SIS (including BPCS or any other device connected to the SIS)?						
FSA-1: 1-12	8.2.4	Over the receiving risk successment exaction bettergings of identified threads that could applied vulnerabilities and scale in exactly events (including intensional attacks on the hardware, application programs and related Decompose, or well as unintended events resulting from human error)?						
FSA-1: 1-13	8.2.4	Are various phases considered in the Security Risk Assessment such solarign, implementation, commissioning, operation, and maintenance?						
FSA-1: 1-14	8.2.4	Have additional requirements for risk reduction been identified in the Security Risk Assessment?						
FSA-1: 1-15	8.2.4	Does the security risk assessment include descriptions of, or references to information on, the measures come to reduce or remove the threats?						
	safety functions to prote	ective layers				1	1	
e 2 - Allocation of	IEC 61511 Clause	Assessment Prompt	Yes	Outco	me Partial	N/A	Assessment Team Comments	Recommendations
CASS TOE								
	9.2.1	Have allocation of safety functions to specific protection layers been documented for the purpose of prevention, control or mitigation?						



	-					_							
Project: Title:	-'Planning '!B1												
Client:	-'Planning '!B2 -'Planning '!B3			1									
Arrot:	-'Plenning 'B4												
lerve:	-'Pleasing 'B5												
		sir arrorrmont chocklirt:											
 The arrorsmont is a The arrorsmontshal Hat all checklist on Partitive reporting 	judgement bared un tl 11 be performed by zuit triez maybe relevant 1	ably compotent person(s) and use of this checklist shall a	the standard IEC 61511 and shall not be treated as an audit against t	hir checklirt,									
Stage 1 FSA													
CASS TOE	IEC 61511 Claura	. Ar	rorrmont Prampt			Partial			arrmont Toom Commonts	Røcar	amondations / Actions	By dd/mm/tr	Statur
Phare 1 - Hexard and	Rick Assessment						- 						
FSA-1:1-1	8.2.1	ir there a description of the hazardow event and the factors that coul-	d contribute to it? (Including Human Factors)										Not Arrorrod
FSA-1:1-2	8.2.1	Ir there a description of the consequences and the likelihood of the eve	ont accurring?										Not Arrorrod
FSA-1:1-3	8.2.1	Have all conditions of operation been considered such as normal opera	tion,start-up,shutdown,maintenance,processupret,andemergencyshutdown?										Not Arrorrod
FSA-1: 1-4	8.2.1	Havo any additional rick roduction mothods boon idontified to achieve	the required safety?										Not Arrorrod
FSA-1:1-5	8.2.1	Have measures to reduce or remove hazards and risk been considered	fidentified?								1		Not Arrorred
~ · ~ ~ =	~ -				·								
CASS T	OE		Outo	come							Date of Asses	sment	
Unique nur			Yes – E	vidence	e provi	ded					Date Assessment co	mpleted	
for each TC	DE		No – N	o evideı	nce pr	ovided							
				– Partia	•				1				
	6161					-	A a a a	oomont To	eam Comme	nto		Sta	tuo
IEC 61511 Clause			N/A – 0	outside	the sc	оре	A226	SSILLEIL IE		iiis		Sla	เนร
Refe	erence to tl	ne IEC 61511					Field fo	or the assessme	ent team to provide			- Ass	essed
مامير	se for the	portioulor							nclude positive				npliance
									netude positive				•
asse	essment pi	rompt					reportii	ng			•	- Part	tial
Assessment Prompt										Recommenda	tions / Actions		pliance
		Provides a prom	nt. like the							Field to detail any nor	-conformances	- Not	Assessed
		other scheme TO	-							Observations, Opport			
		an understandir	ng of the							Improvement			
		requirement											



FSA Common Pitfalls

Stage 4 - Is periodically required and it not completed once only.

A Stage 5 - should be performed on *any* Modification to the SIS.

A Stage 3 – needs to be performed before the hazards are introduced.

If an earlier FSA is performed, evidence of this and action status needs to be provided.

A Project should not conduct their own Assessment.

Anyone can do an FSA.?



X AutoSave	Off [] り、 マー・マー CASS-511-FSA-Functional-Safety-Assessment-v2 (1).	xlsx 🛡 (General* • S	Saved to	o this PC ∖	Search			- 0
File Horr	ne Insert	Page Layout Formulas Data Review View Automate	Help						Comm	nents 🖻 Share
A1	✓): (× ∨	$f_x \sim f_x$ Project:								
	 в		0							
Project: Title: Client: Asset: Issue:	"Planning '!B1 "Planning '!B2 "Planning '!B3 "Planning '!B4 "Planning '!B5									<
The following should be n - The checklist is only for - The assessment is a judy - The assessment shall be - Not all checklist entries - Positive reporting show Stage 1FSA	guidance to act as an ai rement based on the revi performed by suitably c maybe relevant for ever	d memoire to complete an assessment, the assessment should not be treated as a tick how exercise, we of the 2B against the relevant requirements of the standard RCs BSH and shill have be treated as an andit against this checklist, assessments								
CASS TOE	IEC 61511 Clause	Assessment Prompt	Yes	Outco	Partial	N/A	Asses	sment Team Comments		Recommendations / Actions
Phase 1 - Hazard and Risk										
FSA-1: 1-1	8.2.1	Is there a description of the hazardous event and the factors that could contribute to it? (Including Human factors)	L							
FSA-1: 1-2	8.2.1	Is there a description of the consequences and the likelihood of the event occurring?								
FSA-1: 1-3	8.2.1	Have all conditions of operation been considered such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown?								
FSA-1: 1-4	8.2.1	Have any additional risk reduction methods been identified to achieve the required safety?								
FSA-1: 1-5	8.2.1	Have measures to reduce or remove hazards and risk been considered /identified?								
FSA-1: 1-6	8.2.1	Does the assessment contain a detailed description of the assumptions made during analysis of the risks, including probable demand rates and equipment failure rates, and of any credit taken for operational constraints or human intervention?								
FSA-1: 1-7	8.2.1	Have safety functions been allocated to layers of protection, taking into account common cause failures between the safety layers and between safety layers and BPCS?								
FSA-1: 1-8	8.2.1	Have safety functions applied as safety instrumented functions been clearly identified and are they deemed effective against all initiating events?								
FSA-1: 1-9	8.2.2	Has the dangerous failure rate of the BPCS as an initiating source (i.e. placing a demand on a protection layer) not assumed to be less than 10 ⁴ per hour?		1 1						
FSA-1: 1-10	8.2.3	Eth hard and rich storssonent recorded such that it is: + exicute and spot date; + scorts and spot date; + svalbeh in as accessible, maintainable and editable form; + svalbeh in as accessible, maintainable and editable form; + svalbeh of available date variable exact rolled;								
FSA-1: 1-11	8.2.4	Has a security risk assessment been carried out to identify the security vulnerabilities of the SIS (including BPCS or any other device connected to the SIS)?								
FSA-1: 1-12	8.2.4	Does the security risk sessement contain a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the bardware, application programs and robacd software, as well as miniteded events resulting from human error)?								
FSA-1: 1-13	8.2.4	Are various phases considered in the Security Risk Assessment such as design, implementation, commissioning, operation, and maintenance?								
FSA-1: 1-14	8.2.4	Have additional requirements for risk reduction been identified in the Security Risk Assessment?								
FSA-1: 1-15	8.2.4	Does the security risk assessment include descriptions of, or references to information on, the measures taken to reduce or remove the threats?								
hase 2 - Allocation of s	afety functions to prote	ctive layers				·				
CASS TOE	IEC 61511 Clause	Assessment Prompt		Outco			Asses	sment Team Comments		Recommendations / Actions
FSA-1: 2-1	32.1	Have allocation of safety functions to specific protection layers been documented for the purpose of prevention, control or mitigation?	Yes	No	Partial	N/A				
< > ••	Plannin		A Stage 2	2 Require	ments	FSA S	Stage 2 Checklist	FSA Stage 3 Requirements	s FSA Sta	• + : •
andy St. Acc	essibility: Investi							Display Settings III 🗐	四	+ ,



• We'll now cover **CASS-511-OP** and some example TOE(s)





43 TOEs in total

Developed before the FSA scheme was created

Now integrated into the FSA scheme

OPS Scheme still considered useful for FSM development in Operations and for performing Gap analysis

OPS scheme against IEC 61511 aligned with the CDOIF Guide

Record – Results from test / inspection Planning - Proof Testing Planning - Operational Response to faults Record – Name of person(s) who Planning - Verification activities 0.9 Record – Dates and Times of Test/Inspection Planning – Schedule of Proof Testing 0.8 Record - Test/Inspection carried out Planning - Operation and maintenance... 0.7 Record – Audits and Tests of the SIS. 0.6 Record - Data on demand rates for SIS. 0.5 Inspection – Periodic Inspection of the SIS 0.4 0.3 Review - Hazard and Risk analysis 0.2 Review - Operational and maintenance. 0.1 Analyse - Discrepancies between expected. Analyse - Test frequency for the system. Analyse – Failure of equipment forming part. Analyse – Expected and actual cause and. Analyse – Failure modes of equipment. Analyse – Expected and actual actions. Analyse – Discrepancies between expected.

IEC 61511 OPS

Planning - Routine and Abnormal...

Training – Maintenance crews Training – Operational crews. Log – Authorisation of all by passes.

Planning - Responsible Person(s) /... Planning – SIS Spare Parts Procedures - Maintain the SIS in an 'as... Procedures – Quality and consistency of... Procedures - Validation after replacement... Procedures – Minimise the unwanted... Procedures - To test the diagnostic part of ... Procedures – Fault diagnosis and Repair of... Procedures - Identification and correct use... **Procedures - Proof Test Procedures** Procedure - Application Software update Procedure – Deferral of Proof Test Procedures - Compensating measures with... Procedures – Applying and removing of a... Procedures – Maring Halan Band temoving of a...



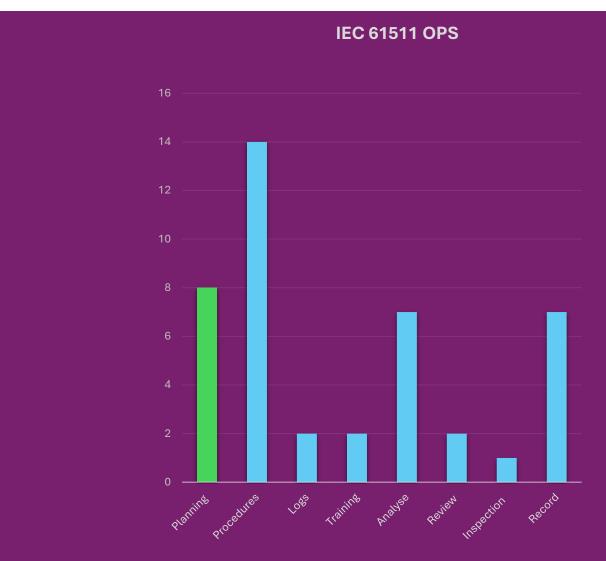
Contact us via T6A: https://61508.org / info@61508.org

8 TOEs Associated with Planning

- Routine and Abnormal operational activities
- Proof Testing
- Operational Response to faults
- Verification activities
- Schedule of Proof Testing
- Operation and maintenance scheduling
- Responsible Person(s) / Department(s)
- SIS Spare Parts

Note - The planning requirements should be defined in the FSM and the audit Schedule include a review of adherence to those requirements.

Note - Planning for Spare Parts is essential for any claims of MTTR which forms part of the PFD Calculations.



Cass Integrity Transparency Consistency

Contact us via T6A: https://61508.org / info@61508.org

14 TOEs Associated with Procedures

- Maintain the SIS in an 'as designed' condition.
- Quality and consistency of proof tests.
- Validation after replacement of any device.
- Minimise the unwanted hazardous event from occurring during maintenance/SIS is unavailable.
- To test the diagnostic part of the SIS.
- Fault diagnosis and Repair of the Safety Instrumented System.
- Identification and correct use of calibrated test equipment.
- **Proof Test Procedures**
- Application Software update
- Deferral of Proof Test
- Compensating measures with operational limits due to disabled or degraded SIS
- Applying and removing of a by-pass
- Maximum length of time a by-pass can be in place for.
- Performing a Hazard analysis to determine compensating measures provide adequate risk reduction.



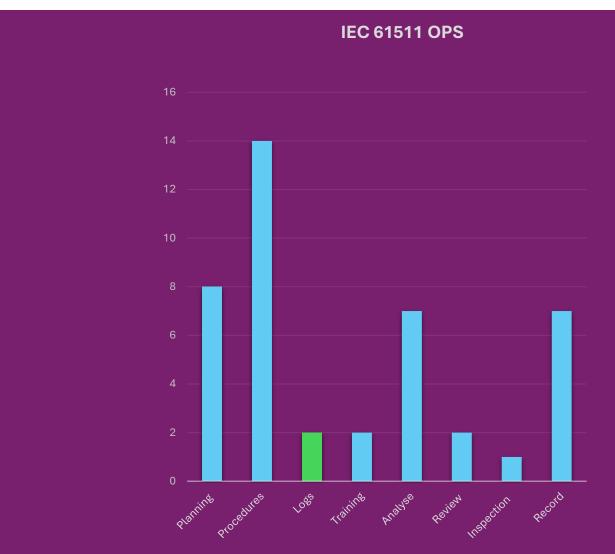
Contact us via T6A: https://61508.org / info@61508.org



2 TOEs Associated with Logs

- Status of all by-passes.
- Authorisation of all by-passes.

Note - There may be other Logs (Electronic or Paper based) in the Control Room, which should also be clearly defined and controlled.



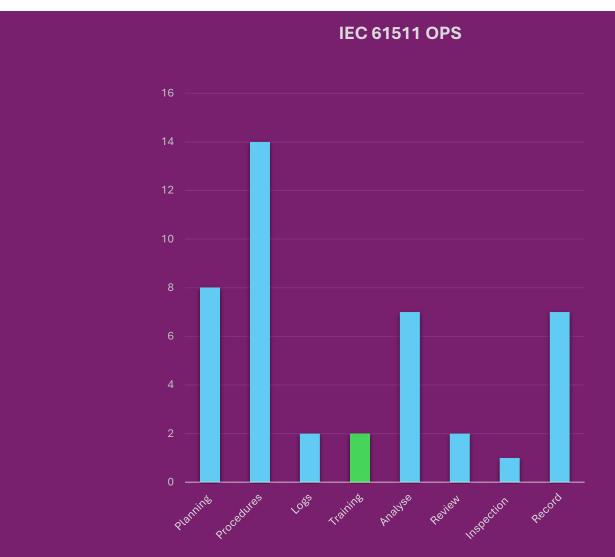
Contact us via T6A: https://61508.org / info@61508.org



2 TOEs Associated with Training

- Operational crews.
- Maintenance crews.

Note – This is only in relation to the specific SIS and is not the same as a Competency Management System (CMS) which is for all activities and persons engaged in the lifecycle.



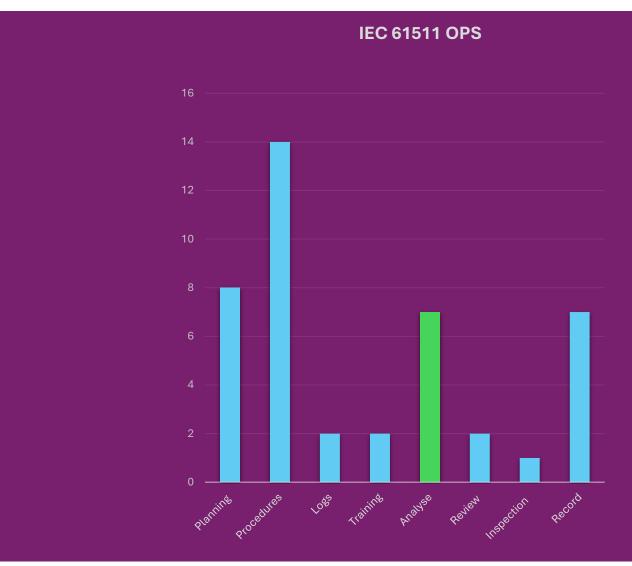
Contact us via T6A: https://61508.org / info@61508.org



7 TOEs Associated with Analyse

- Discrepancies between expected and actual demand rate of the SIF.
- Expected and actual actions following a demand on the system.
- Failure modes of equipment forming part of the system.
- Expected and actual cause and frequency of spurious trips on the system.
- Failure of equipment forming part of the compensating measures.
- Test frequency for the system.
- Discrepancies between expected and actual demand rate of the SIF.

Note – These are new requirements in IEC 61511 and expect greater emphasis in the future on analysis of actual against predicted rates.





2 TOEs Associated with Review

- Operational and maintenance procedures.
- Hazard and Risk analysis.

IEC 61511 OPS 1anning es Loss Training Angues Review Dection Record



Contact us via T6A: https://61508.org / info@61508.org

1 TOE Associated with **Inspection**

• Periodic Inspection of the SIS

Note – When developing the FSA scheme, the inspection requirement was developed into a more comprehensive checklist containing 51 TOEs.

Note – The vendors of SIS equipment may require specific inspection routines as defined in the Safety Manual which should not be ignored.

IEC 61511 OPS usine have being being

Contact us via T6A: https://61508.org / info@61508.org



7 TOEs Associated with **Records**

- Data on demand rates for SIS.
- Audits and Tests of the SIS.
- Test/Inspection carried out
- Dates and Times of Test/Inspection
- Name of person(s) who performed the Test/Inspection
- Serial Number of the system tested.
- Results from test / inspection.

Note – Maintaining traceable and accurate records is important and this should be linked to the Document Management System as part of the FSM.





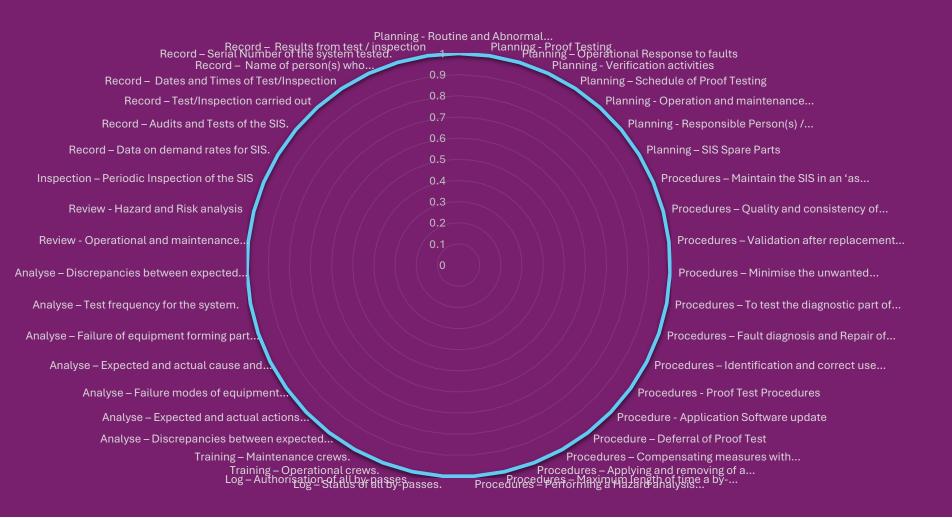
^{te}grity Transparency Consisten



TOE **??**

Purpose of the TOE ??

Would anyone like to pick a TOE to discuss in more detail?



IEC 61511 OPS



Contact us via T6A: https://61508.org / info@61508.org

Any Questions?

Presenter:Andy Derbyshire, Deepti ChauhanContact Details:info@61508.orgWhat's next....

Start Time Slot Paper **Finish Time** Workshop Slot A-9: Machinery Functional Slot B-9: Functional Safety Tool 15:05 9 14:35 Safety with IEC 62061 and ISO Qualification 13849 15:05 Short Comfort Break 15:25 10 15:25 Slot A-10: The Importance of Slot B-10: SIL Calculations and 15:55 use of IEC 61508 Part 6 Alarms for Functional Safety

We would be more than happy to discuss membership with you (https://61508.org/cass/)

