CASS 61511 Workshop

Overview of the CASS IEC 61511 Templates

Our Members


AFK Consultancy
ANALOX
arc AWE
NUCLEAR SECURITY TECHNOLOGIES
bp
CEPHA CONTROLS
cetix
CHARTER·TECH
CLEARLINE
cml Ex
CSA GROUP
DEKRA
DIAGEO
DNV
DOW CORNING
Dräger
EATON
Powering Business Worldwide
EDF
EMERSON
Process Management
ERM
evero
ExxonMobil
FICHTNER
Consulting Engineers Limited
FRAZER·NASH
CONSULTANCY
HAZCON
Haden Freeman Ltd
hitex
EMBEDDED TOOLS & SOLUTIONS
Honeywell
I&E SYSTEMS
IC&T
its
Invertek Drives
iti
Group
LR
=M
=Method
MOORE INDUSTRIES
MUTECH
national gas transmission
P & I Design Ltd
ProcessSafety
Solutions
procon
ProSalus
SAFETY CONSULTANTS
ROAKENGINEERING
ROSAS
rotork
Schneider Electric
SELLA CONTROLS
SENSIA
SGS
Baseefa
SIEMENS
SILMETRIC
sse
TAIT
UK Atomic Energy Authority
RACE
UL Solutions
uniper
VEOLIA
VAL-FSR
Virdee Advantage Limited
WITTENSTEIN
wsp
YOKOGAWA

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).

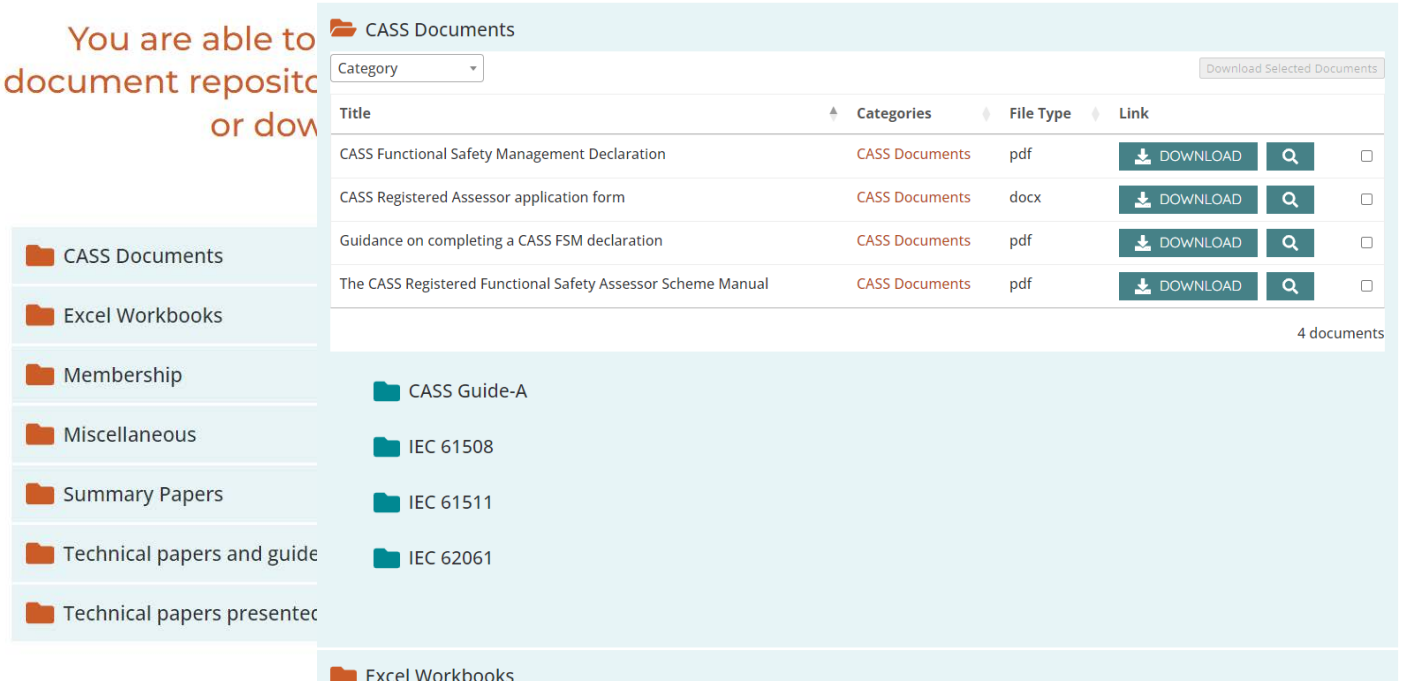
NOTE: Templates cover IEC, EN, and BS EN variants.

Rigor and Competence

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



TOE Walkthrough

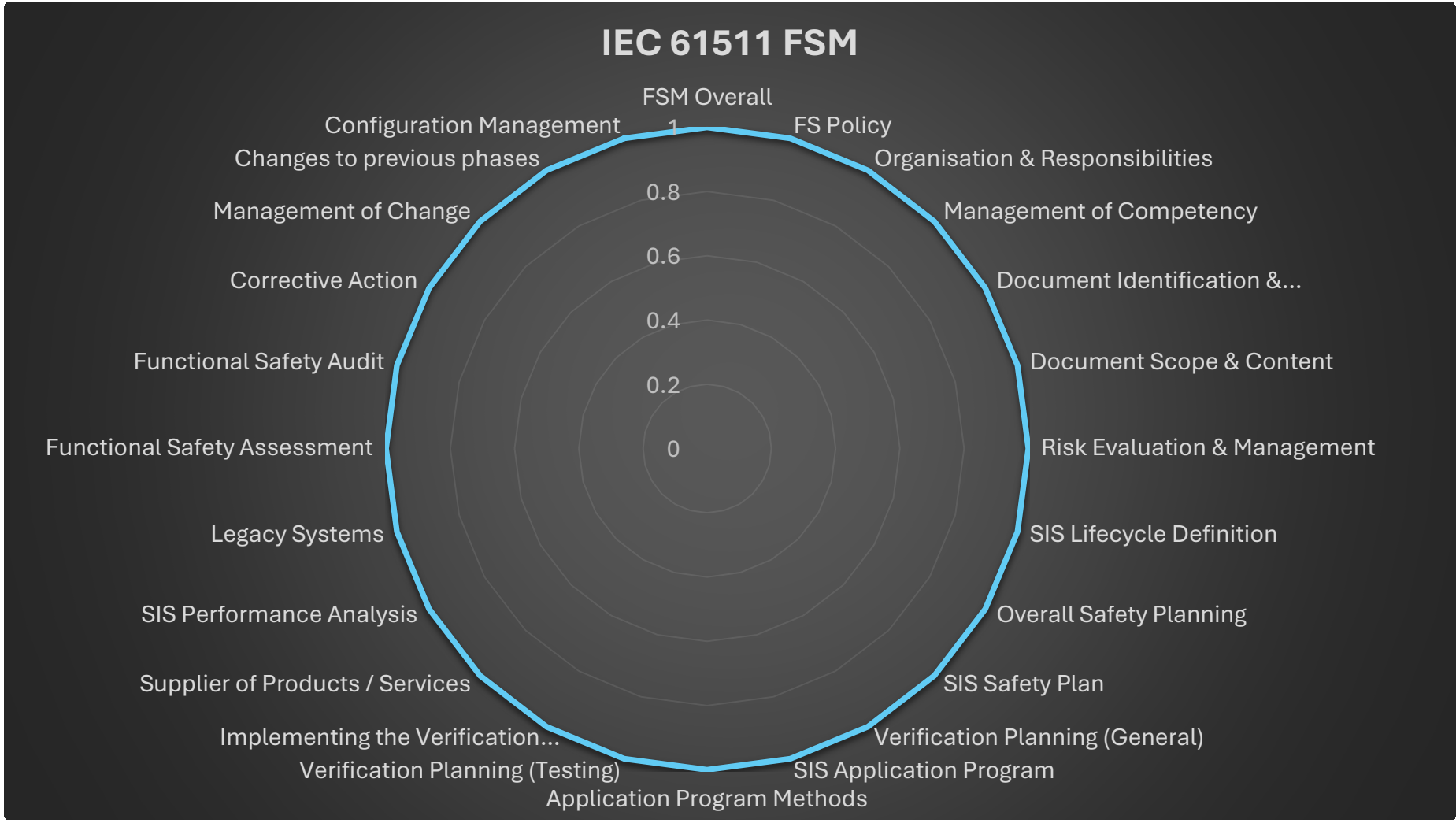
- We'll now cover **CASS-511-FSM** and some example TOE(s)

CASS-511-FSM Walkthrough

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?



CASS-511-FSM Walkthrough

If we consider

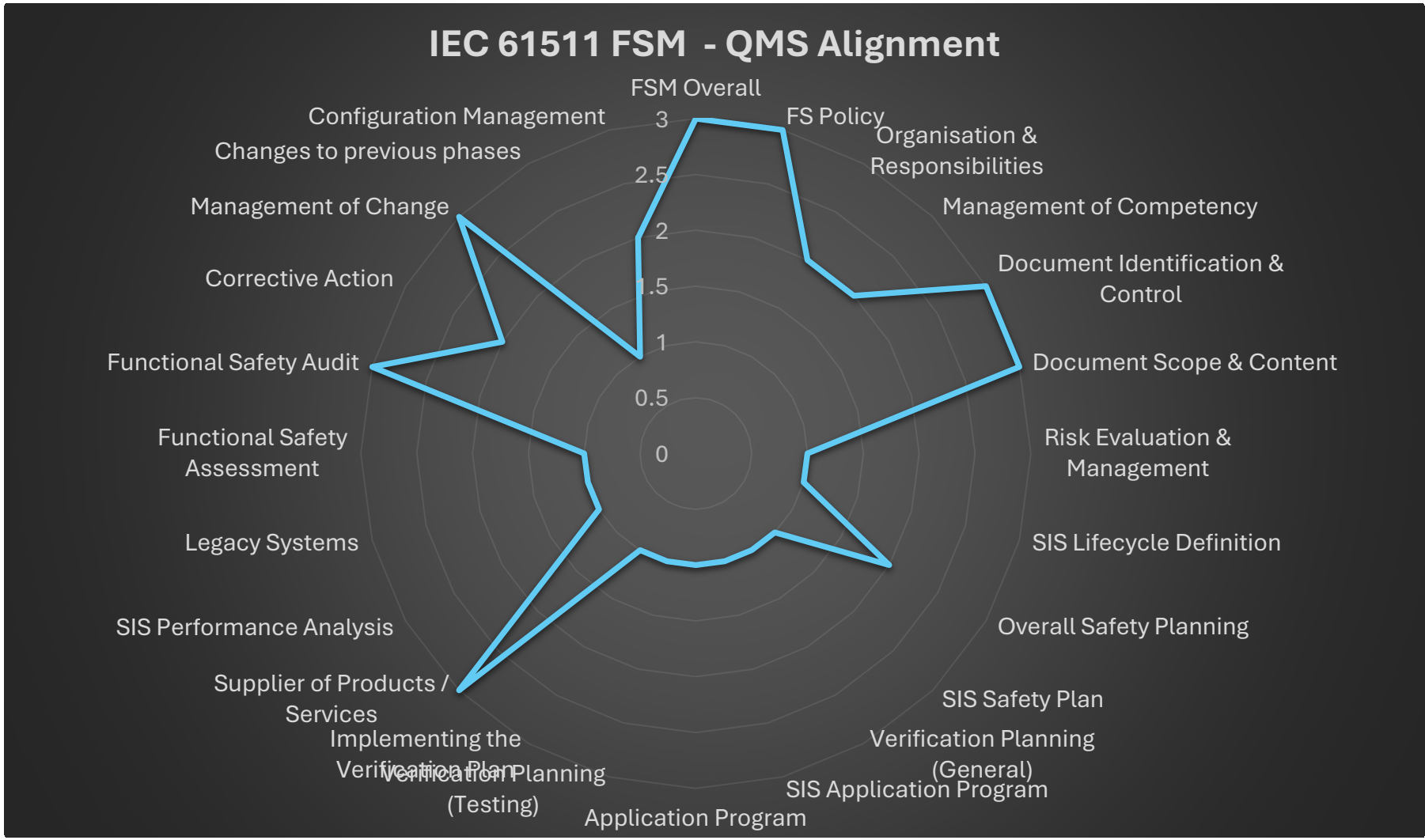
1 – No commonality

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



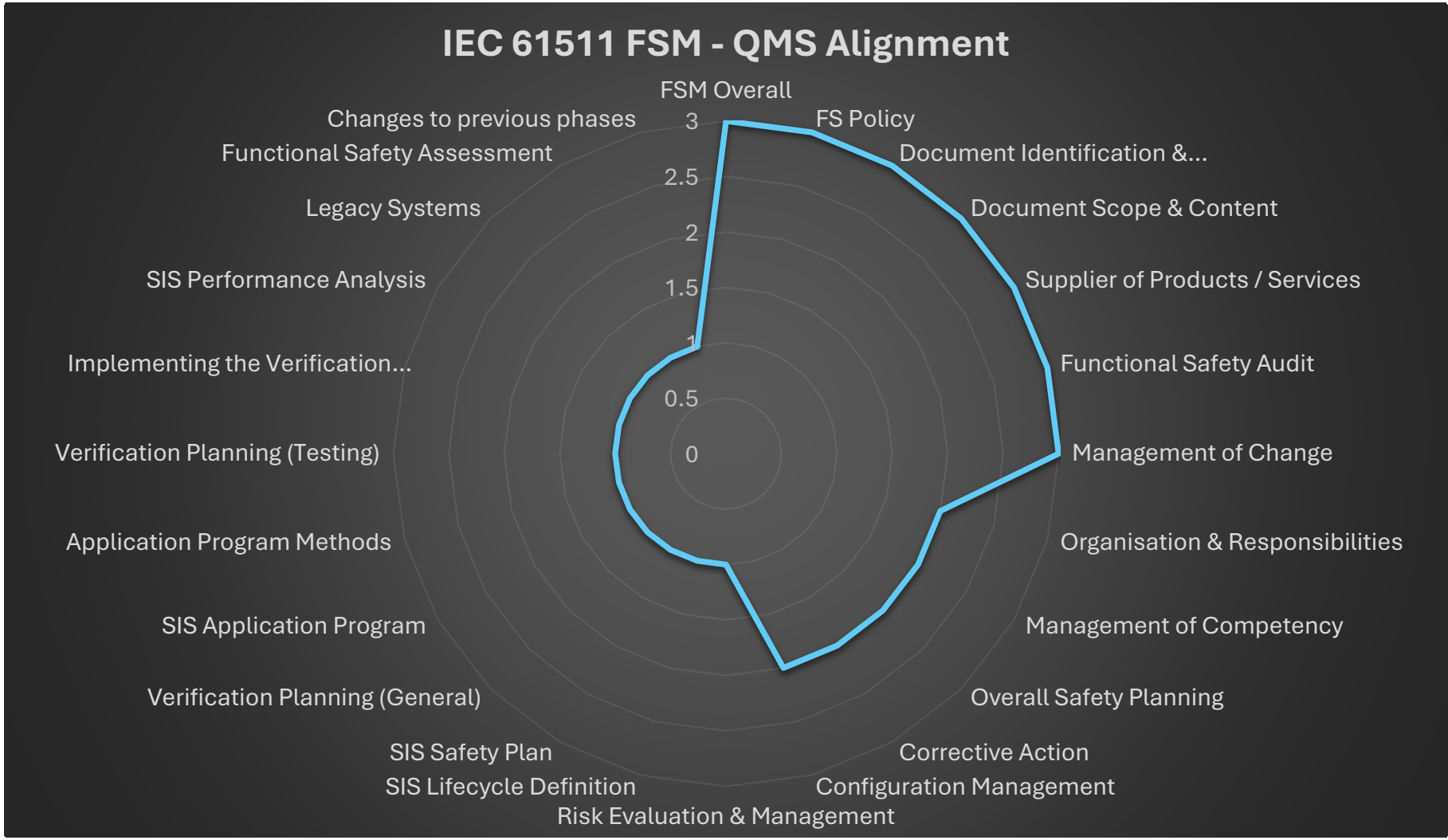
CASS-511-FSM Walkthrough

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



CASS-511-FSM Walkthrough

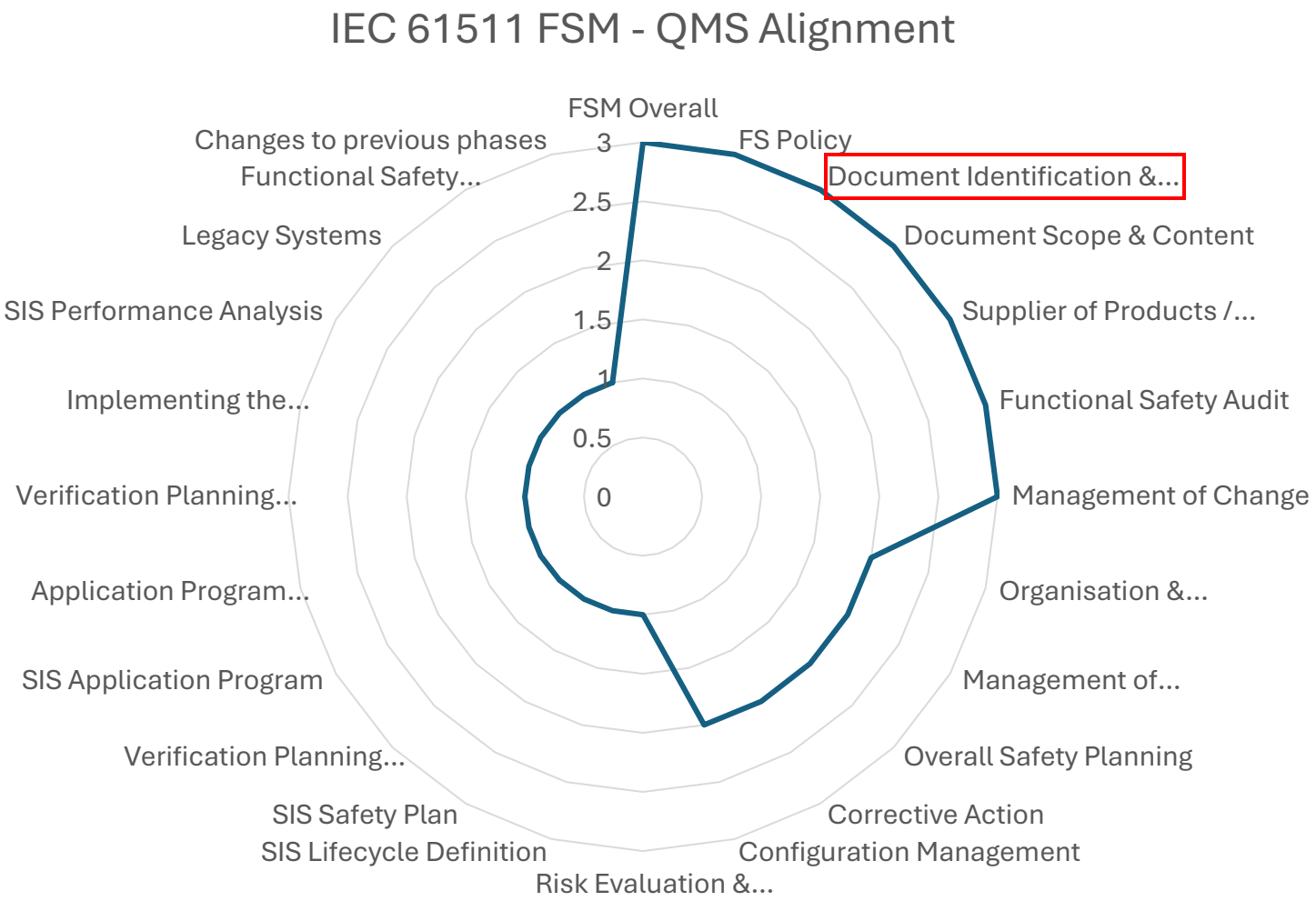
3 – Commonality

TOE 6
Document Identification and Revision Control

Purpose of the TOE
To ensure each document will be appropriately designated for its type, is uniquely identifiable, contains a revision index, is searchable and stored so as to allow location of the latest revision and is revised, reviewed, approved and under appropriate revision control

ISO 9001 Clause 7.5.3
Control of Documented Information

Functional Safety related information needs to be uniquely identifiable, but these can be within an existing Document Management System (DMS)



CASS-511-FSM Walkthrough

3 – Commonality

TOE 21
Functional Safety Audit

Purpose of the TOE
To ensure procedures exist for periodic and independent audits of the FSM system to monitor its effectiveness and facilitate its improvement. The procedures should define the frequency of the audits, degree of independence, recording and follow-up.

ISO 9001 Clause 9.2
Internal Audit

Functional Safety related audits can be scheduled within an existing internal audit program.

CASS-511-FSM Walkthrough

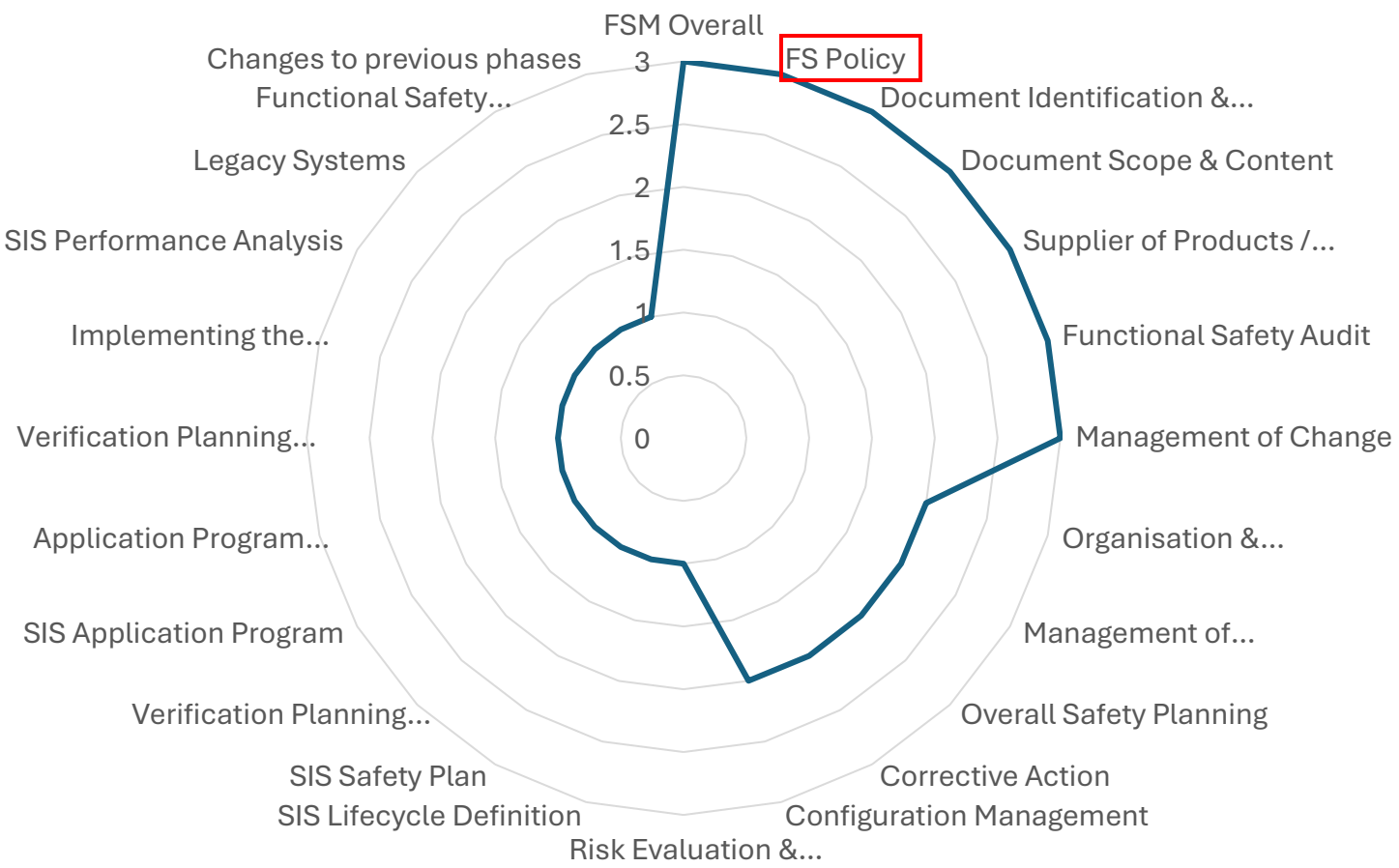
3 – Commonality

TOE 2
Functional Safety Policy

Purpose of the TOE
To ensure there is an appropriate policy and strategy for achieving functional safety, together with the means of evaluating its achievement, authorised by senior management and communicated within the organisation.

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



CASS-511-FSM Walkthrough

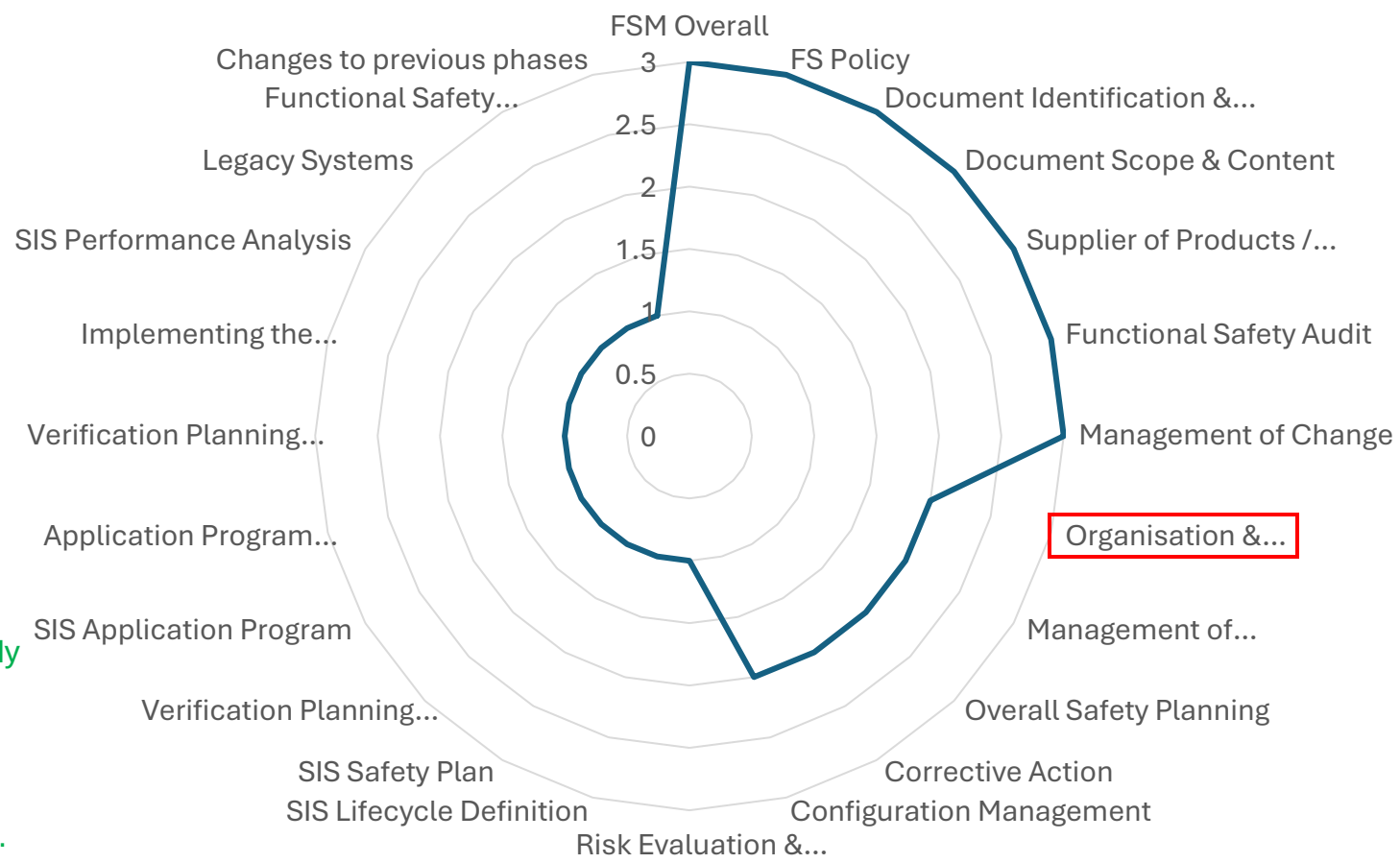
2 – Partial Commonality

TOE 3
Organisation and Responsibilities

Purpose of the TOE
To ensure that the persons, departments or organisations who perform, review, audit or assess SIS safety lifecycle activities are identified (documented) and informed of the responsibilities assigned to them.

ISO 9001 Clause 4
Organisational Context and Stakeholders

- Functional Safety related roles and responsibilities needs to be clearly defined, this can be internal or external roles within the lifecycle.
- This is applicable to all lifecycle phases and activities.
- Those assuming a particular role or responsibility need to be made aware of their duties.
- The person(s) performing such roles need to be suitably Competent.



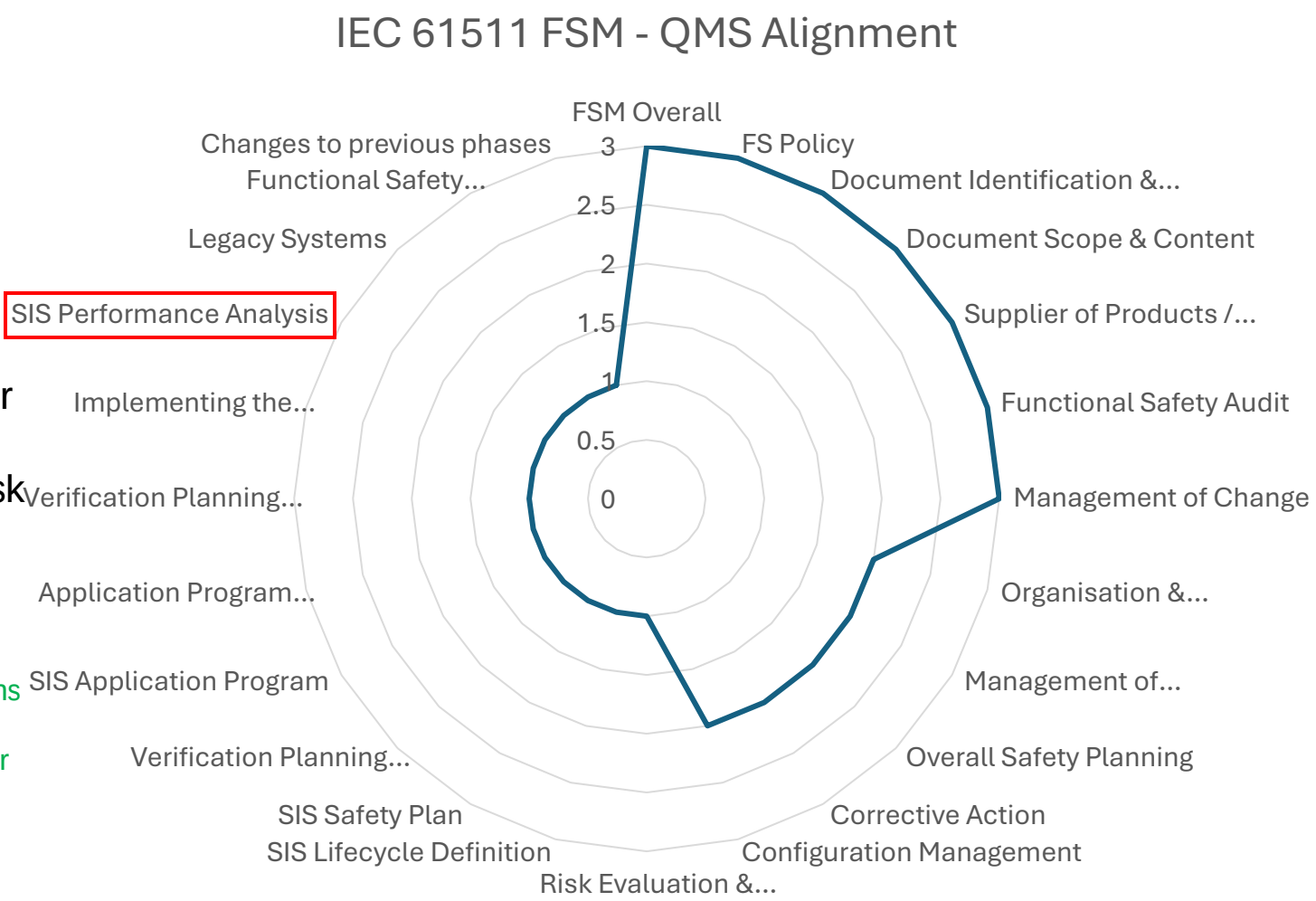
CASS-511-FSM Walkthrough

1 – No Commonality

TOE 18
SIS Performance Analysis

Purpose of the TOE
To ensure there are procedures in place to evaluate the SIS against its safety requirements, identify and prevent dangerous systematic failures, and to monitor and assess reliability parameters and demand mode assumptions of the SIS that were made during the risk assessment and design stages.

During Design we assume a Demand, Failure and Spurious rate, based on published data.?
After a period of operating the SIS how can we be sure our assumptions were correct.?
- First, we must ensure we have an appropriate means of recording our data
- Secondly, we must ensure we have an appropriate means of measuring our data effectively
- Thirdly, we must ensure we take all appropriate action to ensure continued safe operation based on the data collected



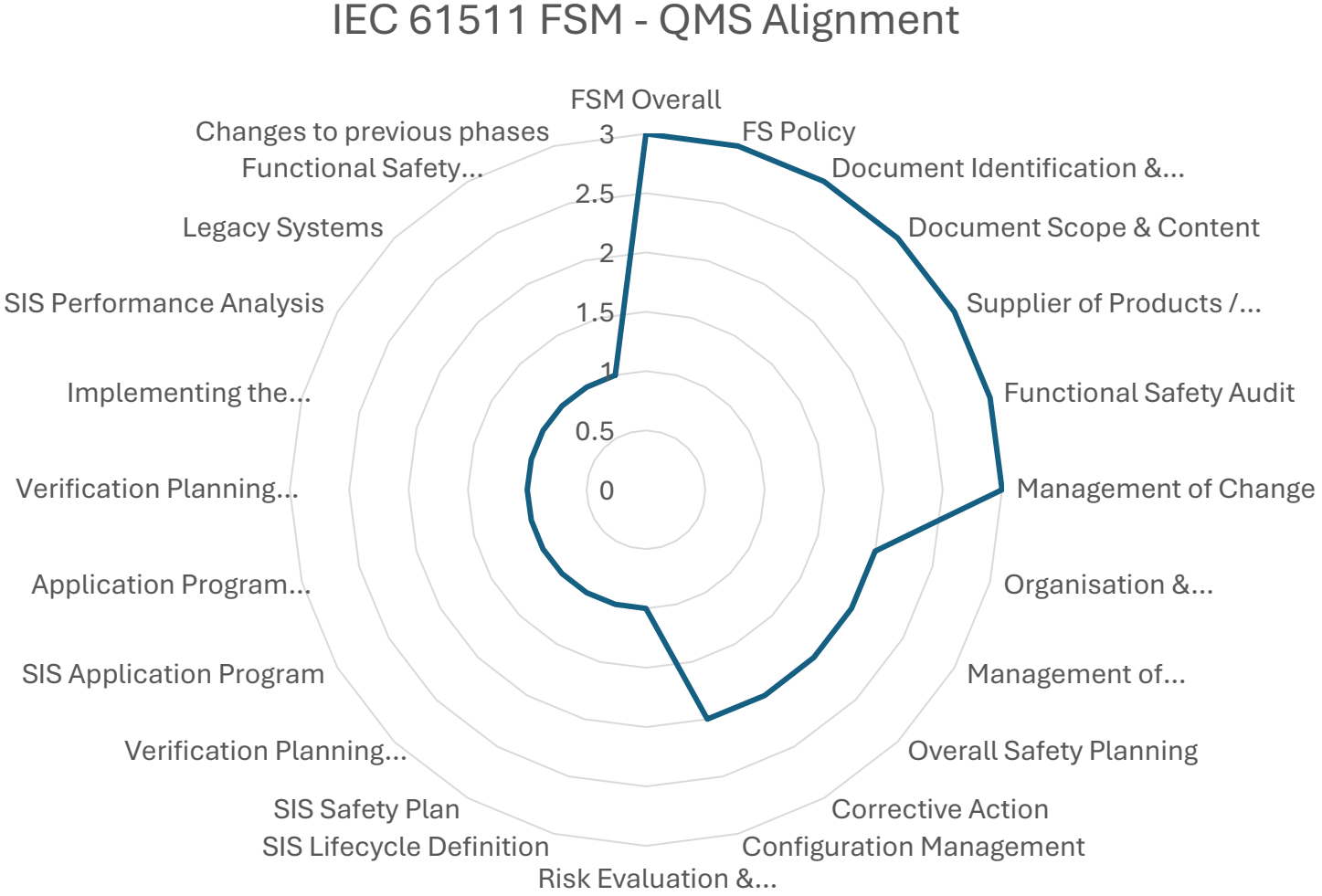
CASS-511-FSM Walkthrough

1 – No Commonality

TOE ??

Purpose of the TOE
??

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



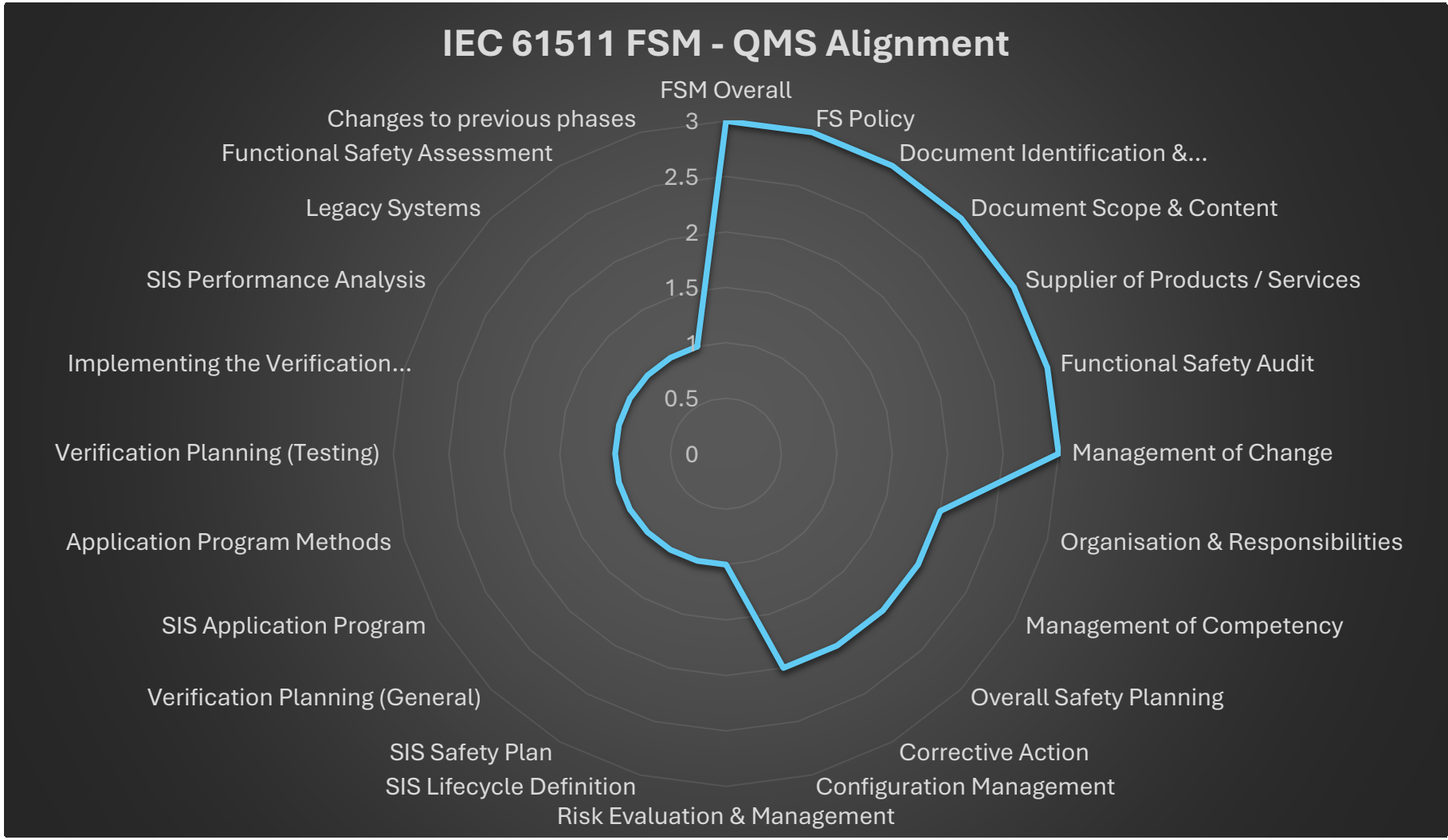
CASS-511-FSM Walkthrough

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.!



TOE Walkthrough

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

CASS-511-LVL Walkthrough

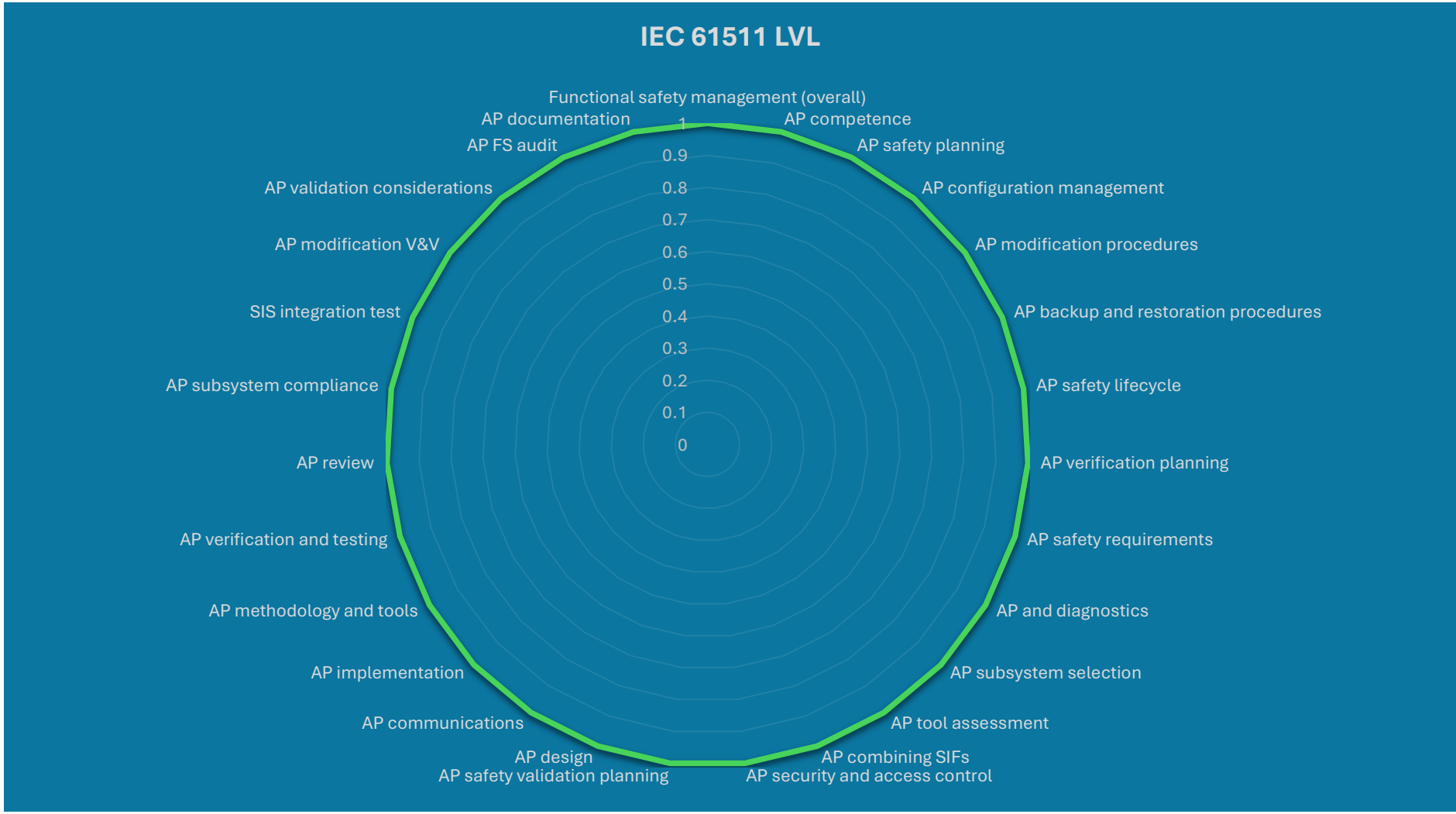
27 TOEs in total

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?



CASS-511-LVL Walkthrough

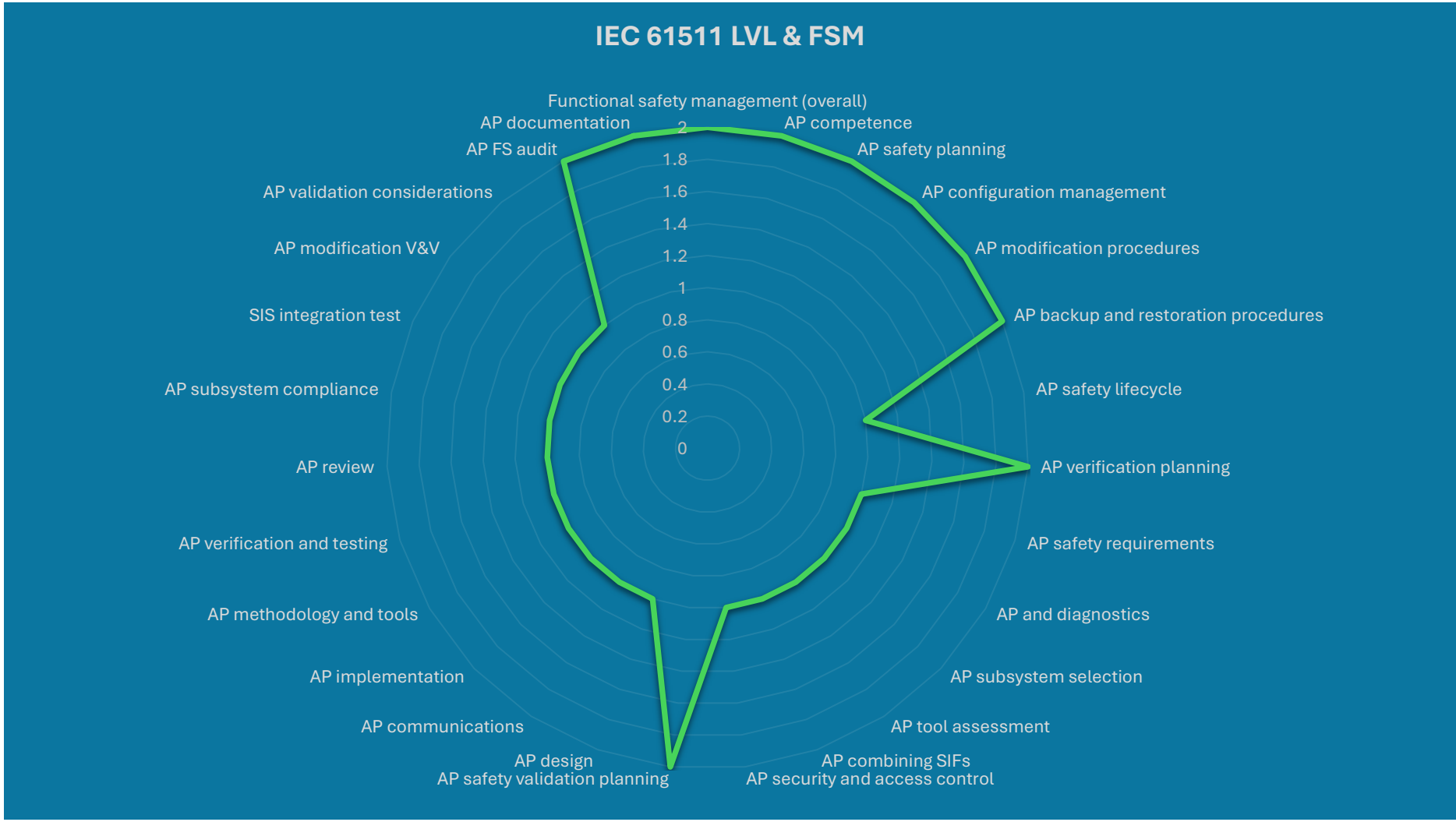
If we consider

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



CASS-511-LVL Walkthrough

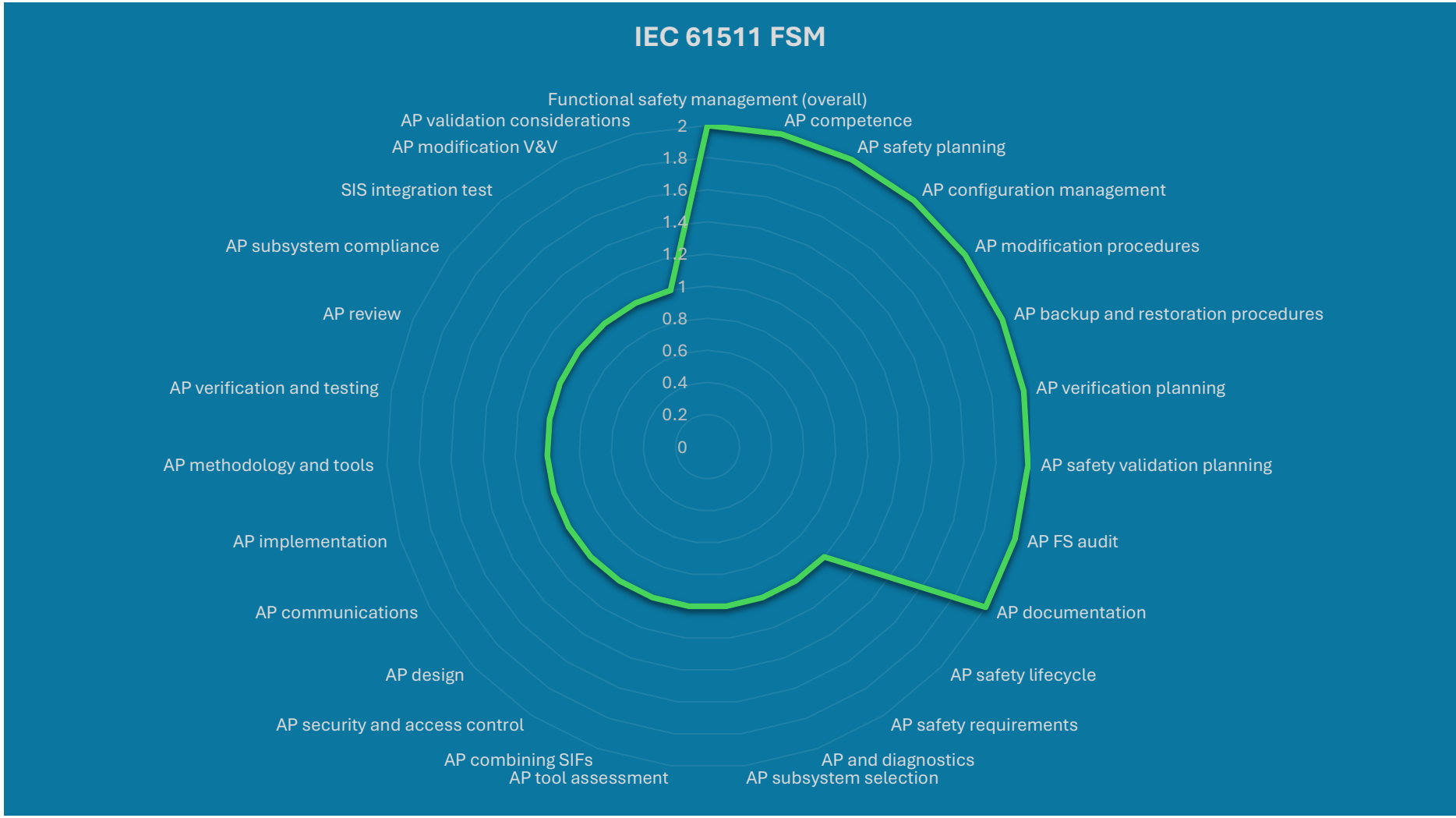
If we consider

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.



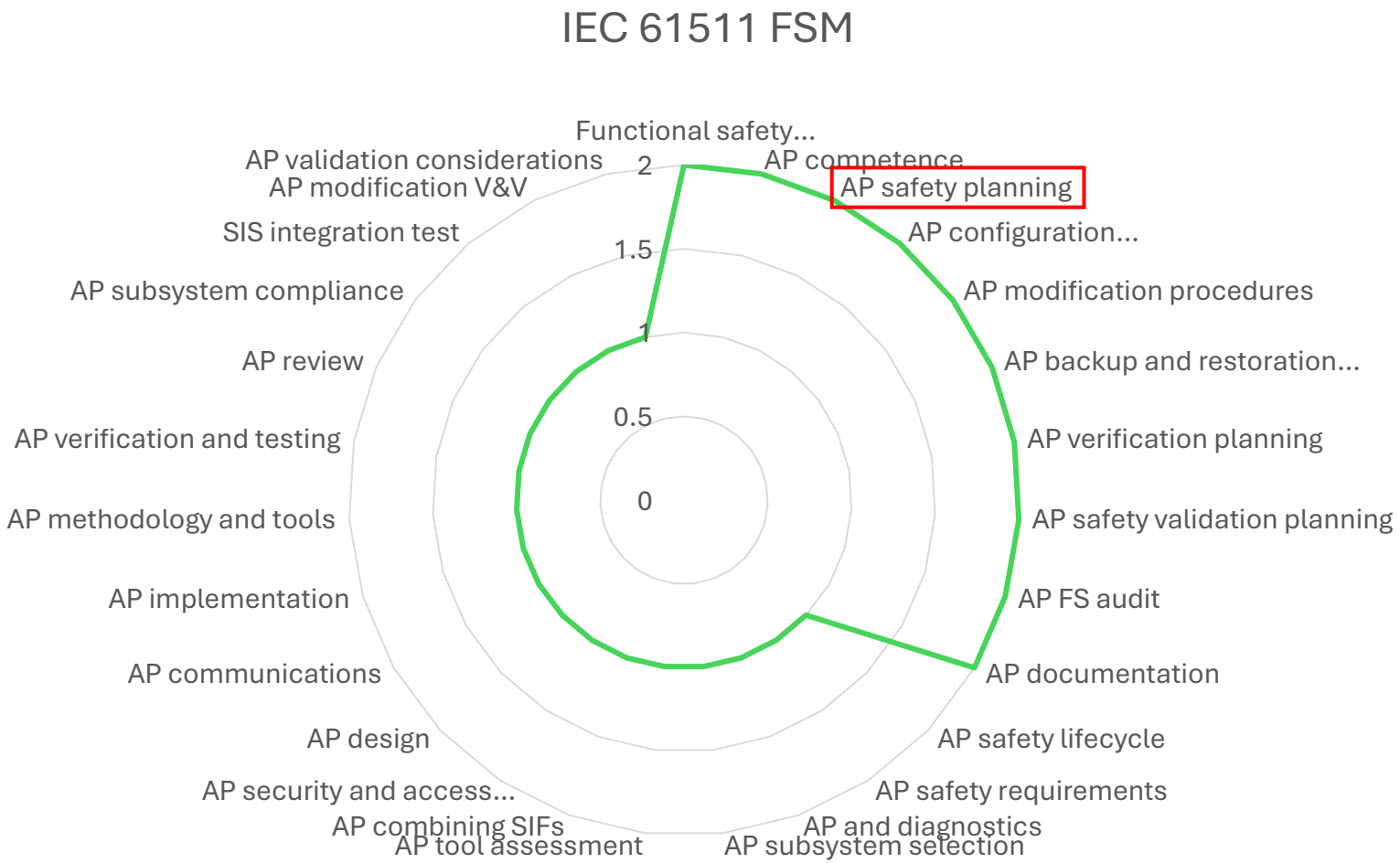
CASS-511-LVL Walkthrough

2 – FSM Requirement

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



CASS-511-LVL Walkthrough

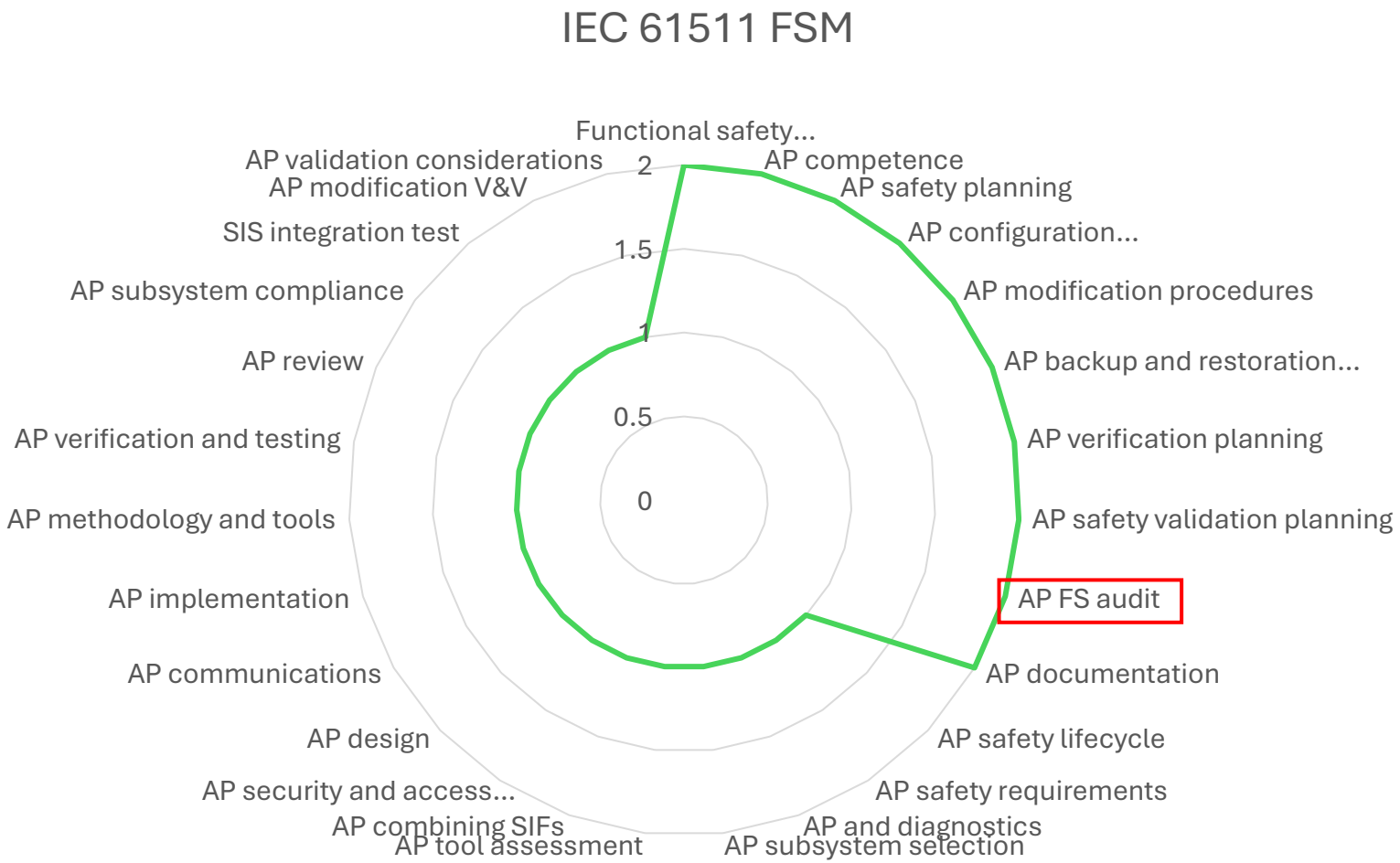
2 – FSM Requirement

TOE 26
AP FS Audit

Purpose of the TOE
For all SILs, ensure that relevant aspects of the software lifecycle and software development have been audited in relation to functional safety

The FSM or Integrated Management System should include an Audit Schedule.

For a company performing the AP design and development this Audit schedule should include periodic auditing of the AP design and development processes



CASS-511-LVL Walkthrough

1 – Project Requirement

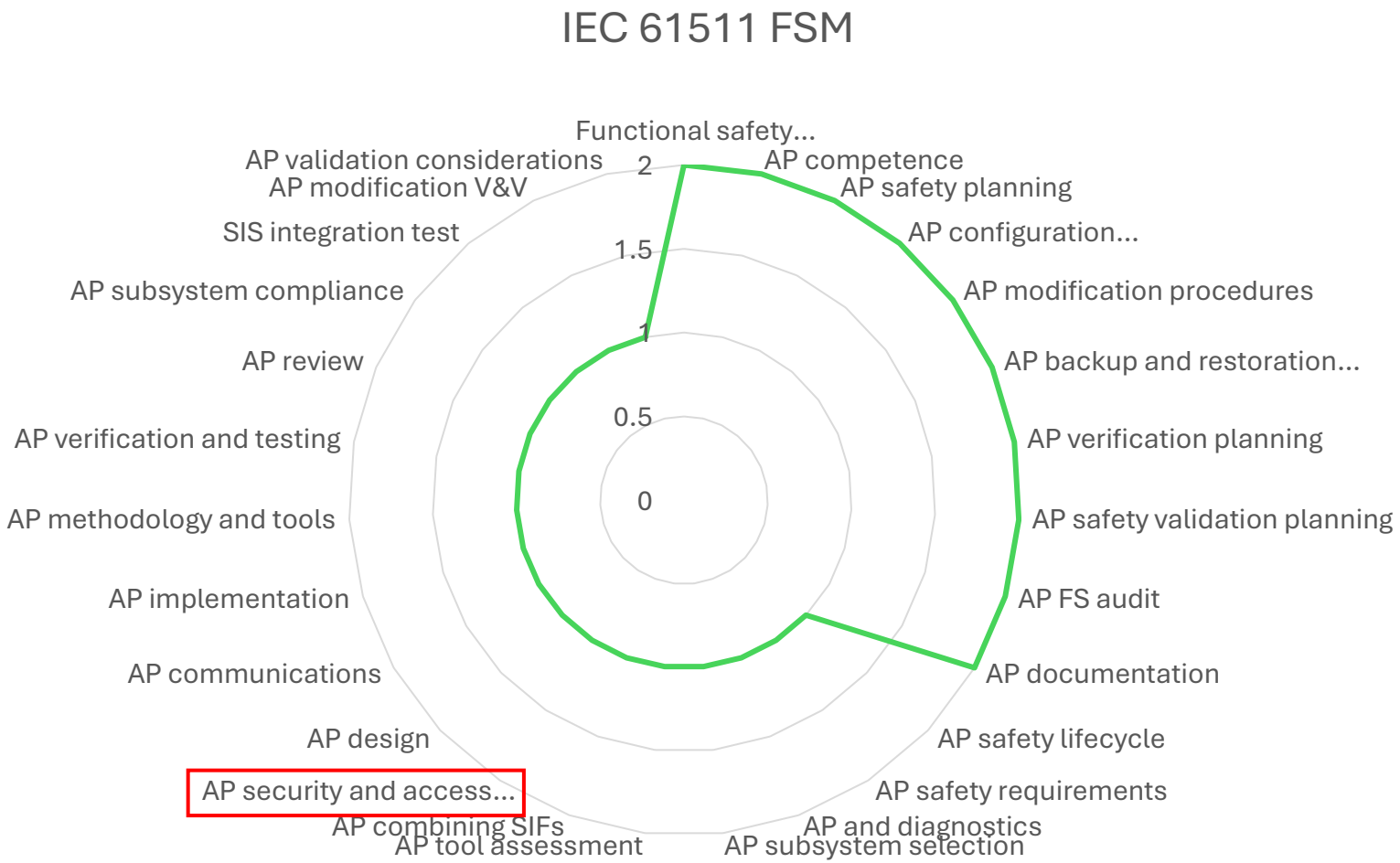
TOE 14
AP Security & Access Control

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.



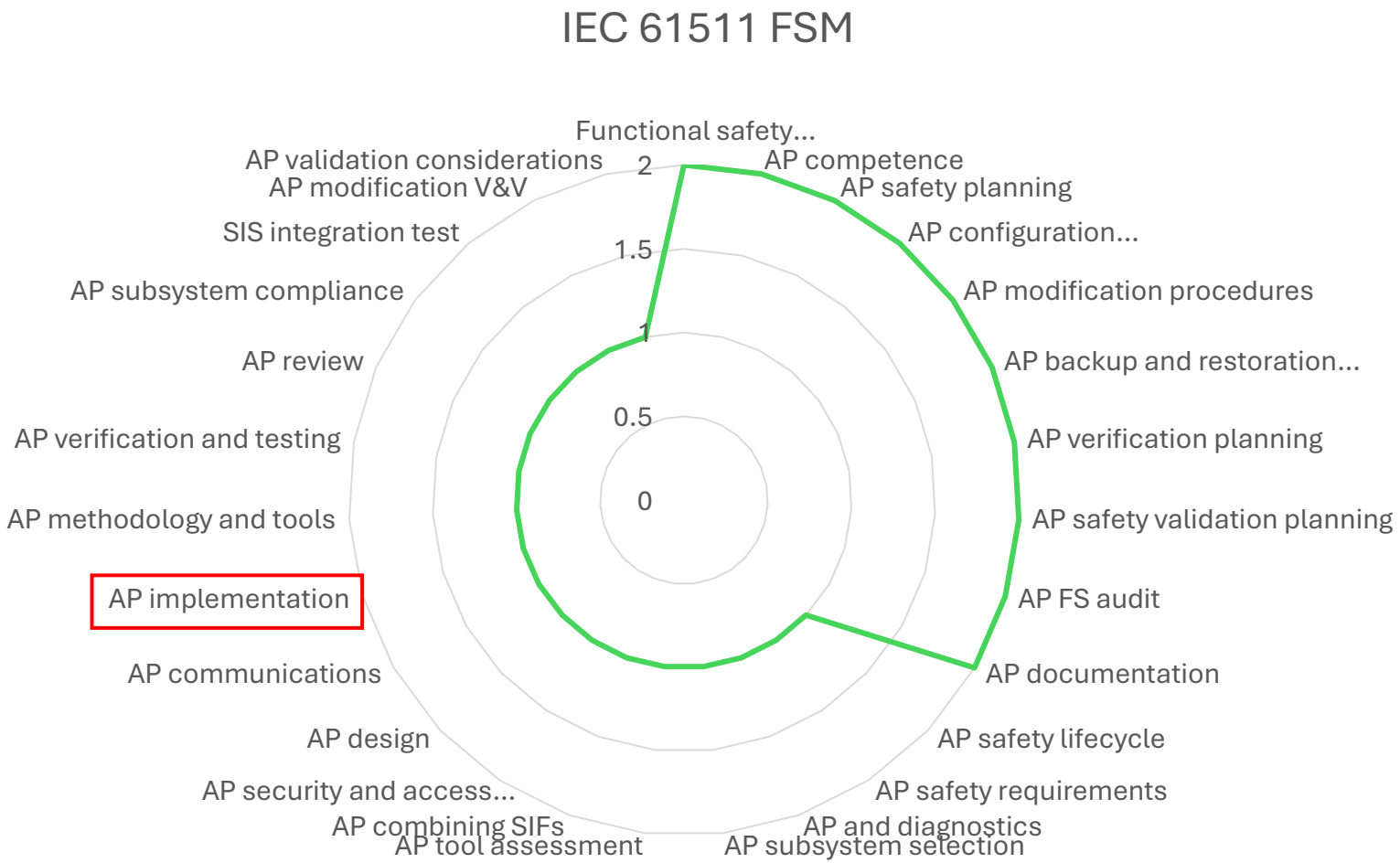
CASS-511-LVL Walkthrough

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.



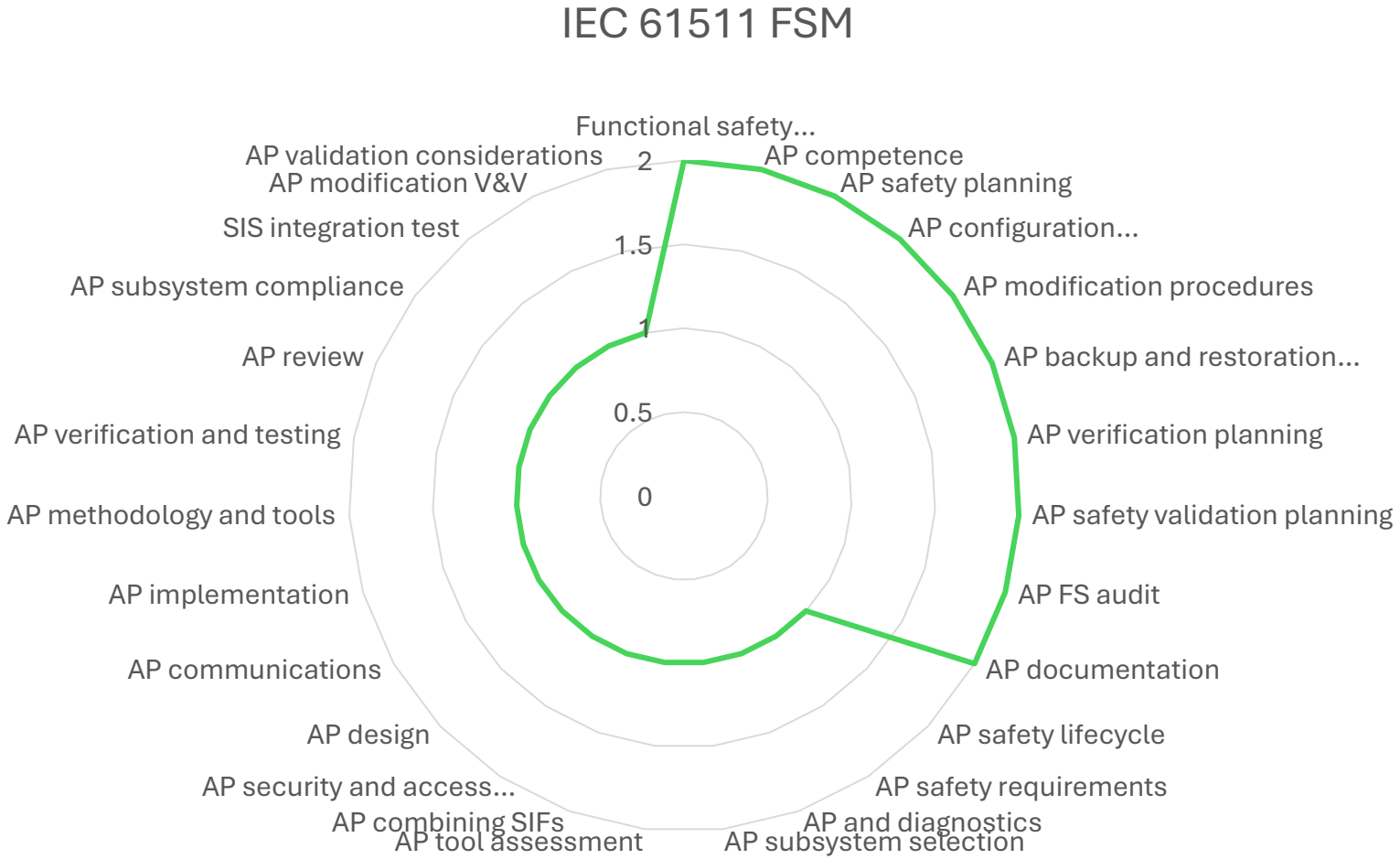
CASS-511-LVL Walkthrough

1 – Project Requirement

TOE ??

Purpose of the TOE
??

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



CASS-511-LVL Walkthrough

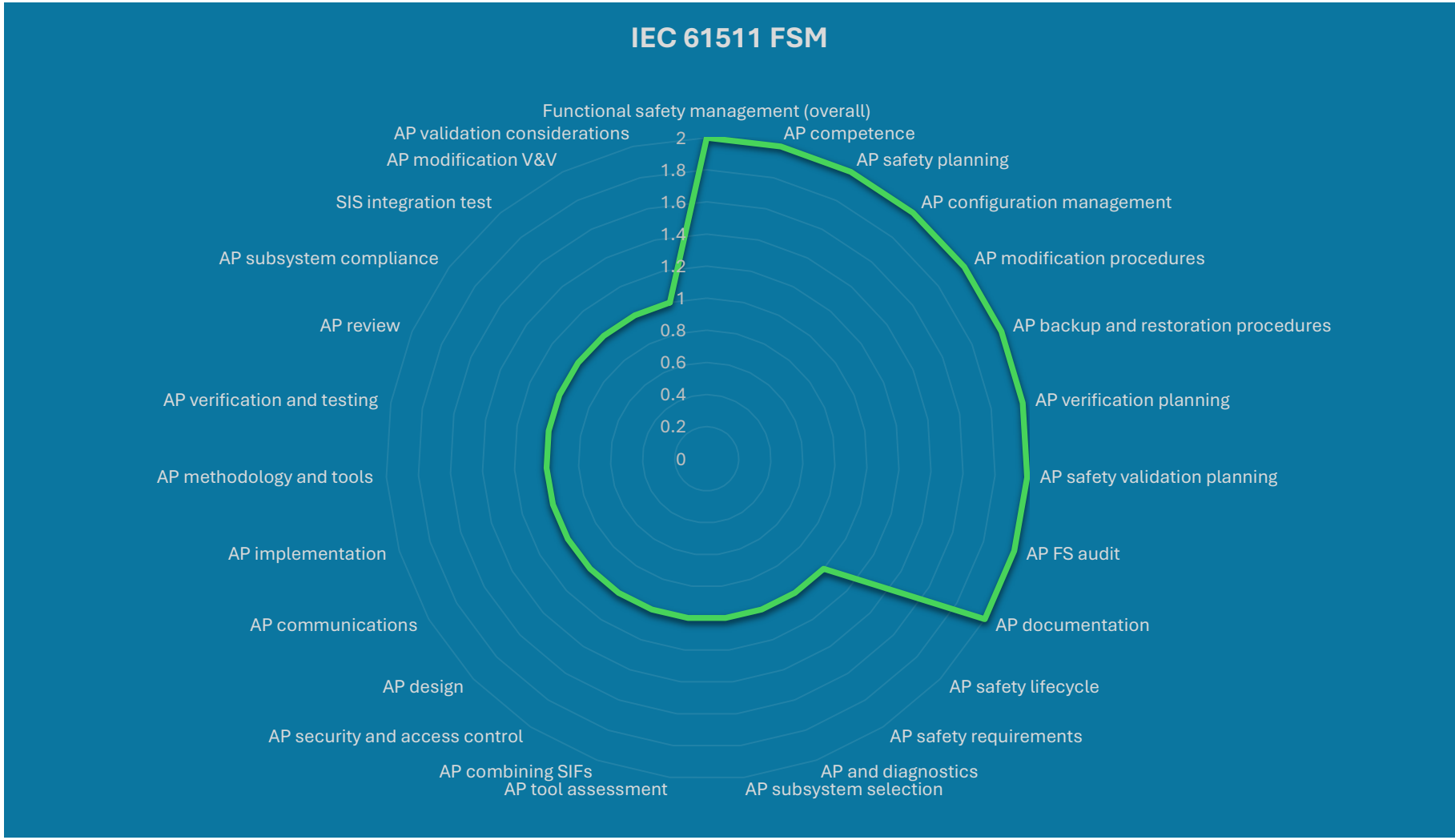
LVL Conclusion

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



TOE Walkthrough

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

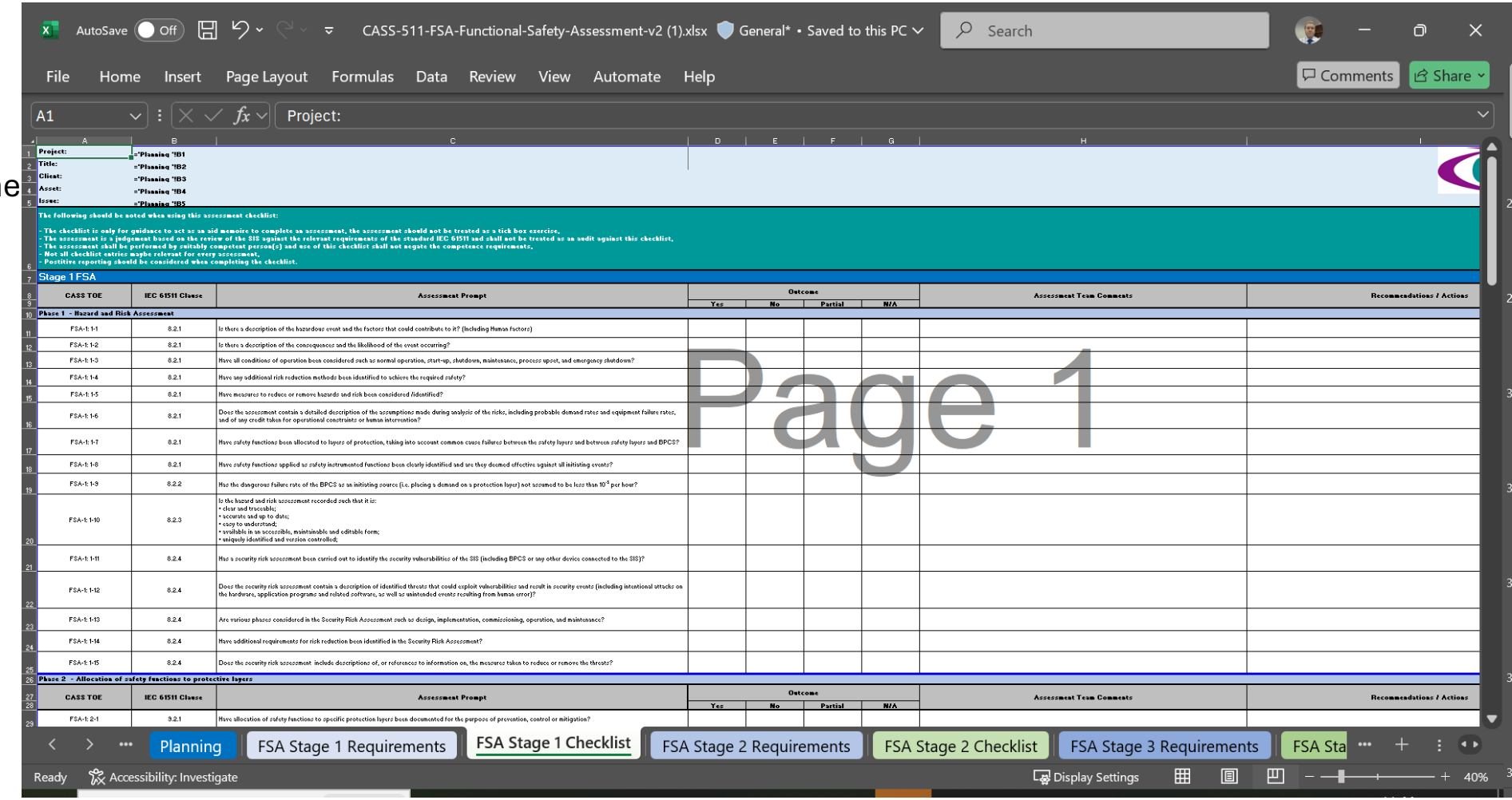
CASS-511-FSA Walkthrough

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

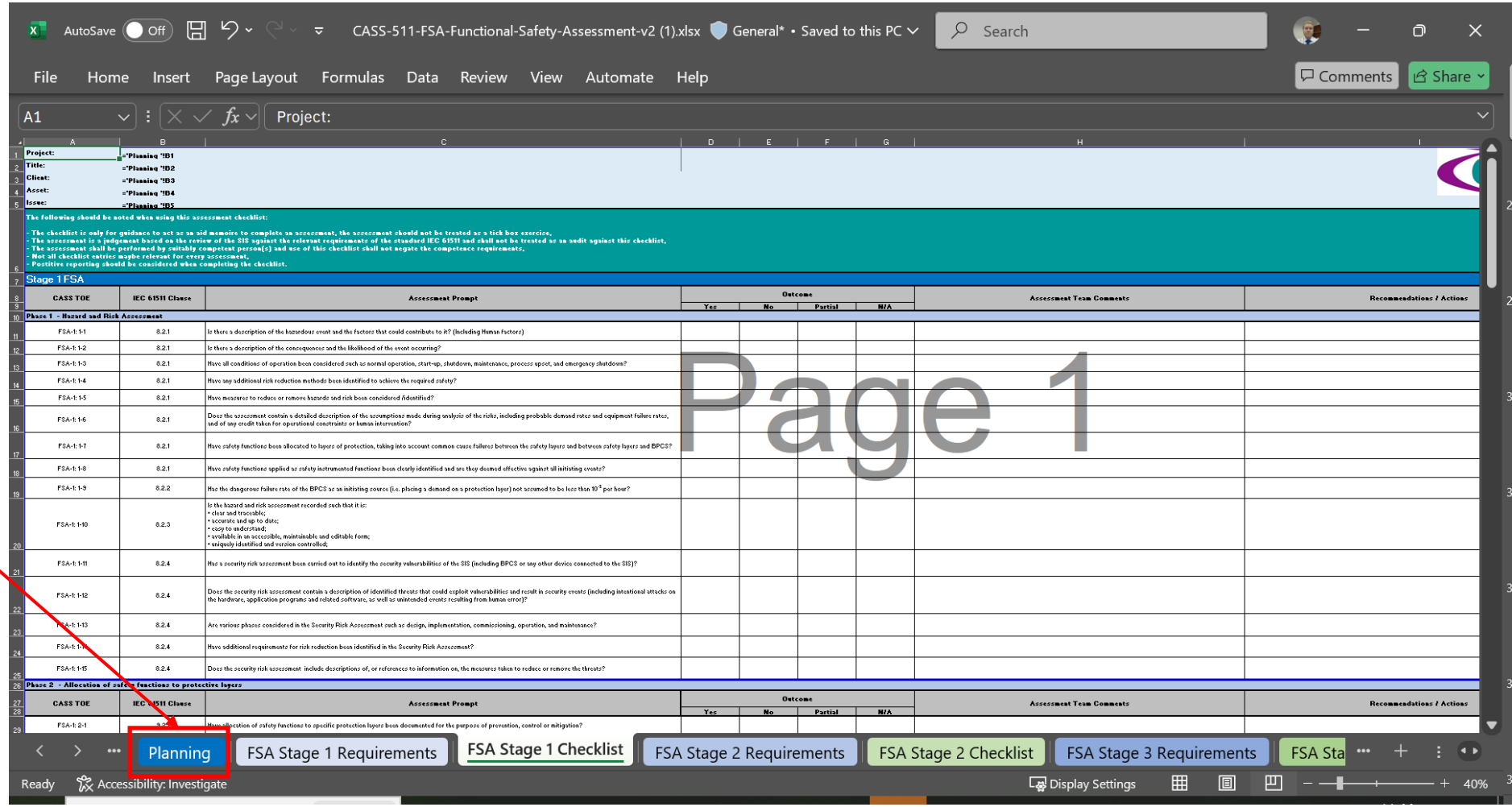


CASS-511-FSA Walkthrough

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



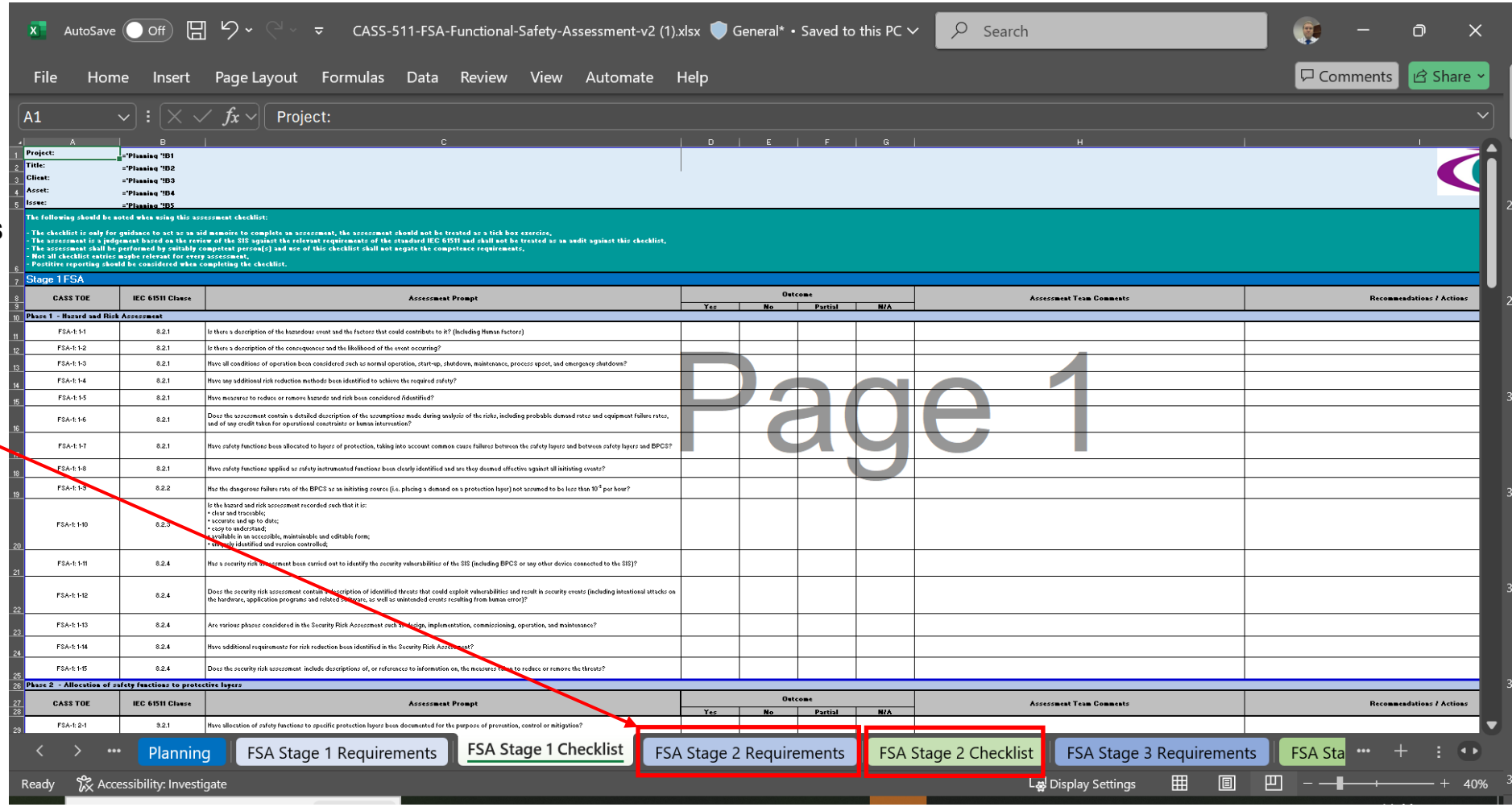
CASS-511-FSA Walkthrough

Functional Safety Assessment scheme developed for IEC 61511

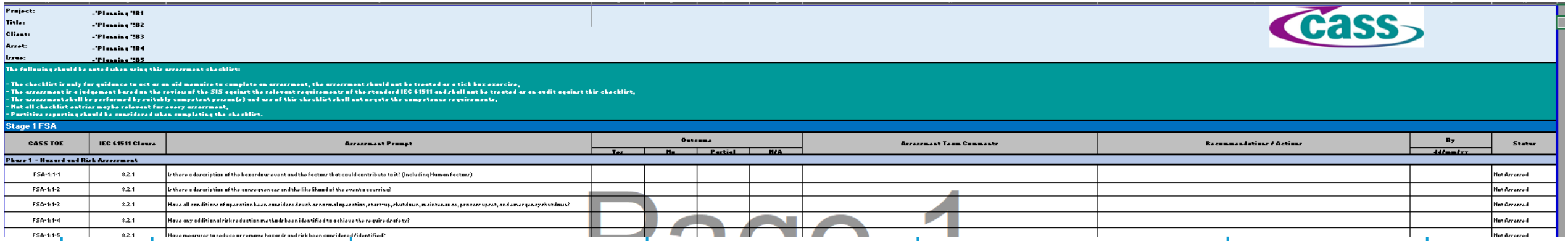
Each FSA stage has a Requirements and Checklist Tab

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 Walkthrough



Project:	-'Planning '!B1
Title:	-'Planning '!B2
Client:	-'Planning '!B3
Asset:	-'Planning '!B4
Issue:	-'Planning '!B5

The following should be noted when using this assessment checklist:

- The checklist is only for guidance to act as an aid memoire to complete an assessment, the assessment should not be treated as a tick box exercise.
- The assessment is a judgement based on the review of the SIS against the relevant requirements of the standard IEC 61511 and shall not be treated as an audit against this checklist.
- The assessment shall be performed by suitably competent person(s) and use of this checklist shall not negate the competence requirements.
- Not all checklist entries maybe relevant for every assessment.
- Partitive reporting should be considered when completing the checklist.

Stage 1 FSA

CASS TOE	IEC 61511 Clause	Assessment Prompt	Outcome				Assessment Team Comments	Recommendations / Actions	By	Status
			Yes	No	Partial	N/A			dd/mm/yy	
Phase 1 - Hazard and Risk Assessment										
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)								Not Assessed
FSA-1:1-2	8.2.1	Is there a description of the consequences and the likelihood of the event occurring?								Not Assessed
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?								Not Assessed
FSA-1:1-4	8.2.1	Have any additional risk reduction methods been identified to achieve the required safety?								Not Assessed
FSA-1:1-5	8.2.1	Have measures to reduce or remove hazards and risk been considered/identified?								Not Assessed

CASS TOE

Unique number for each TOE

IEC 61511 Clause

Reference to the IEC 61511 clause for the particular assessment prompt

Assessment Prompt

Provides a prompt, like the other scheme TOEs, to provide an understanding of the requirement

Outcome

Yes – Evidence provided
No – No evidence provided
Partial – Partial compliance
N/A – outside the scope

Assessment Team Comments

Field for the assessment team to provide comment, which can include positive reporting

Recommendations / Actions

Field to detail any non-conformances, Observations, Opportunities for Improvement

Date of Assessment

Date Assessment completed

Status

- Assessed
-Compliance
- Partial Compliance
- Not Assessed

CASS-511-FSA Walkthrough

FSA Common Pitfalls

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

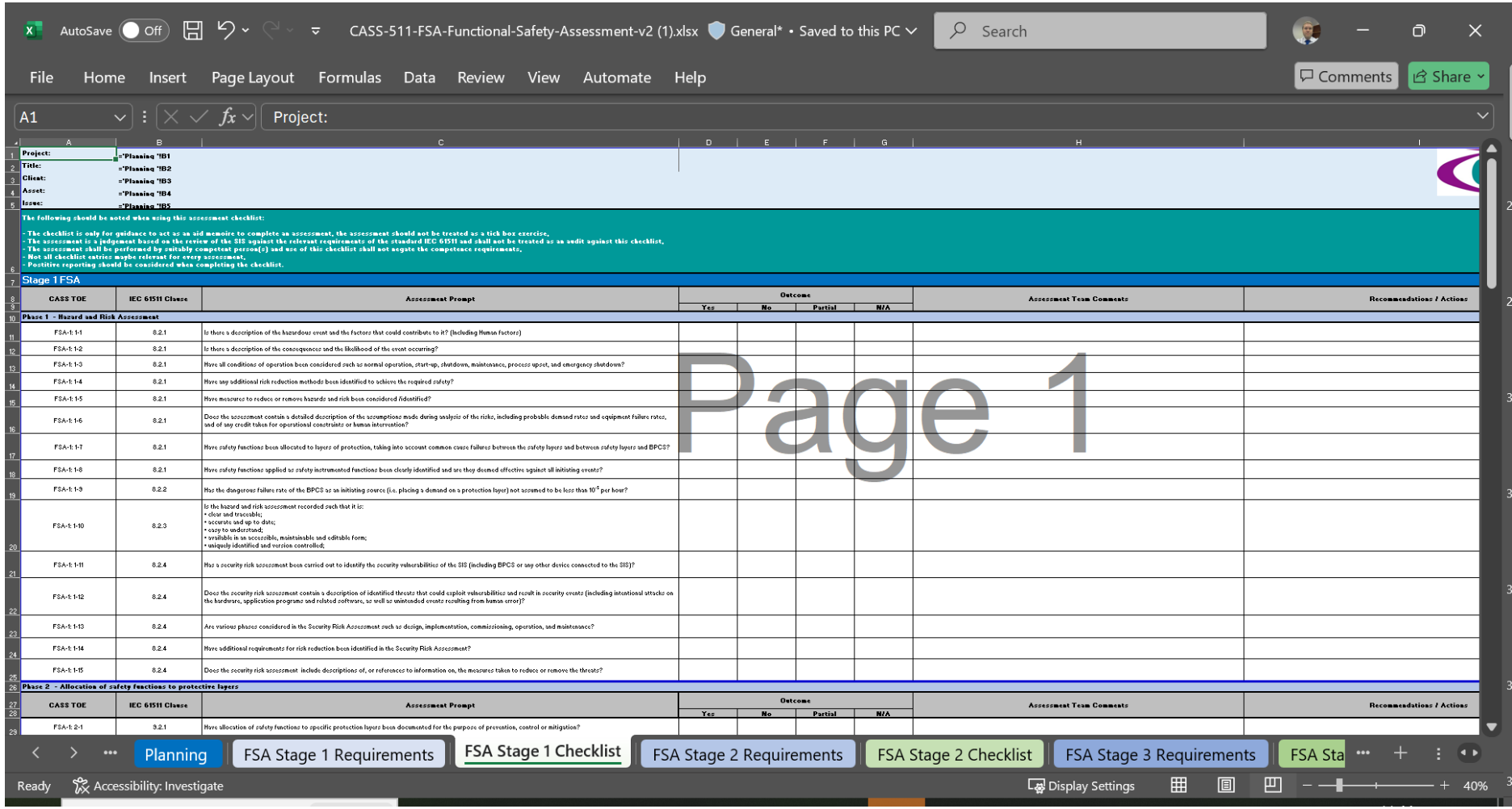
A Stage 5 - should be performed on *any* Modification to the SIS.

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.?



TOE Walkthrough

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

CASS-511-OP Walkthrough

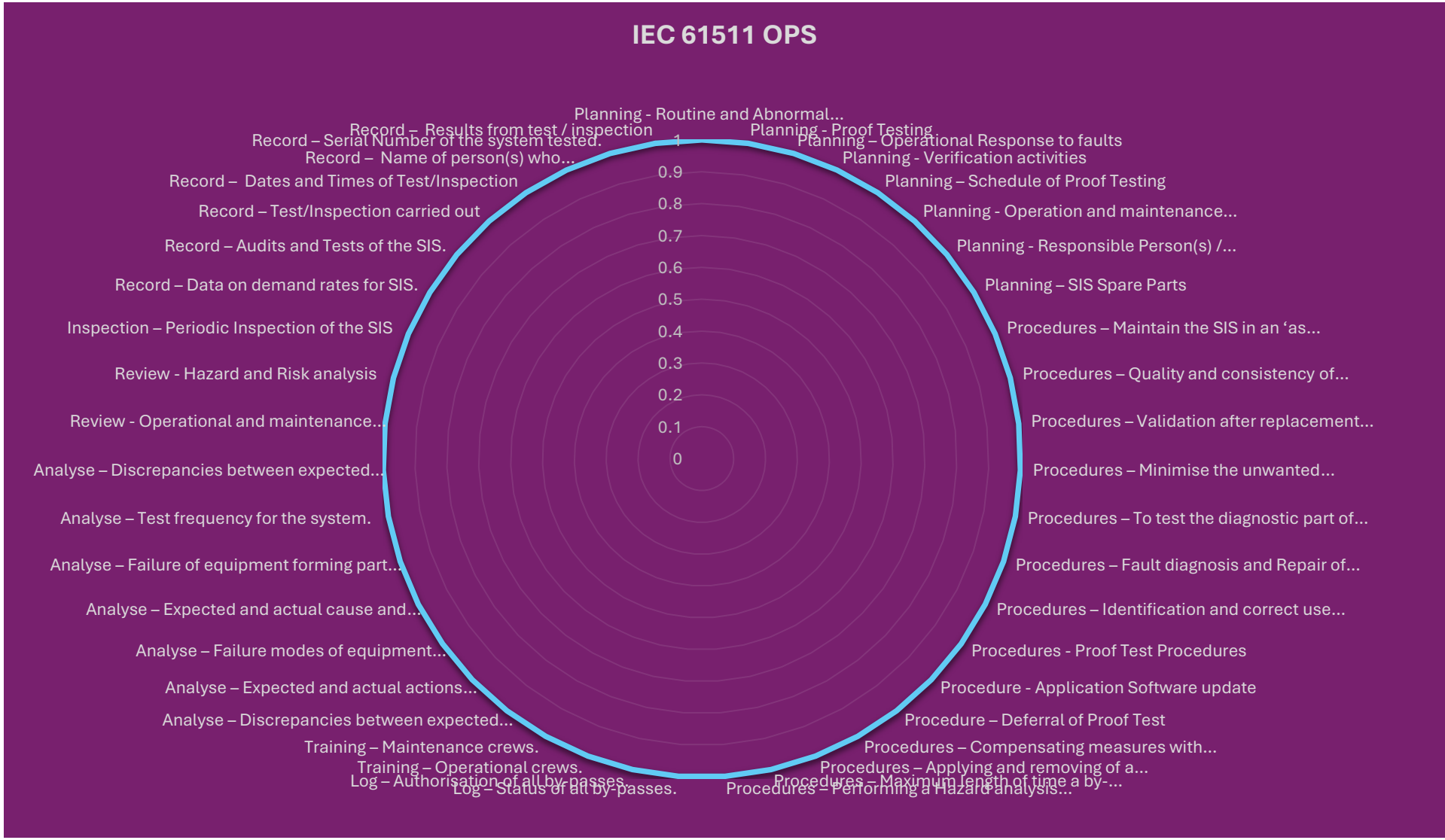
43 TOEs in total

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



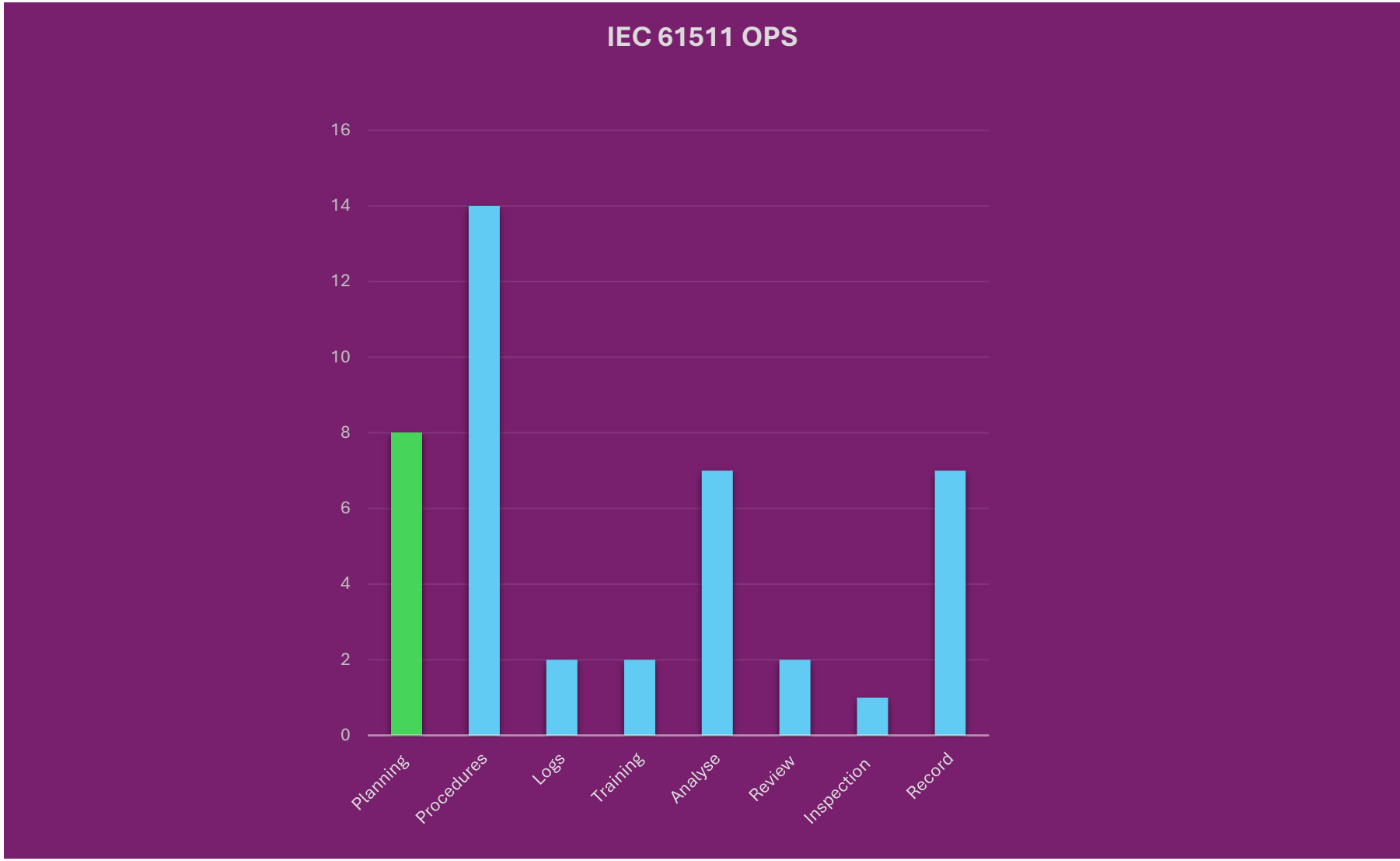
CASS-511-OP Walkthrough

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.

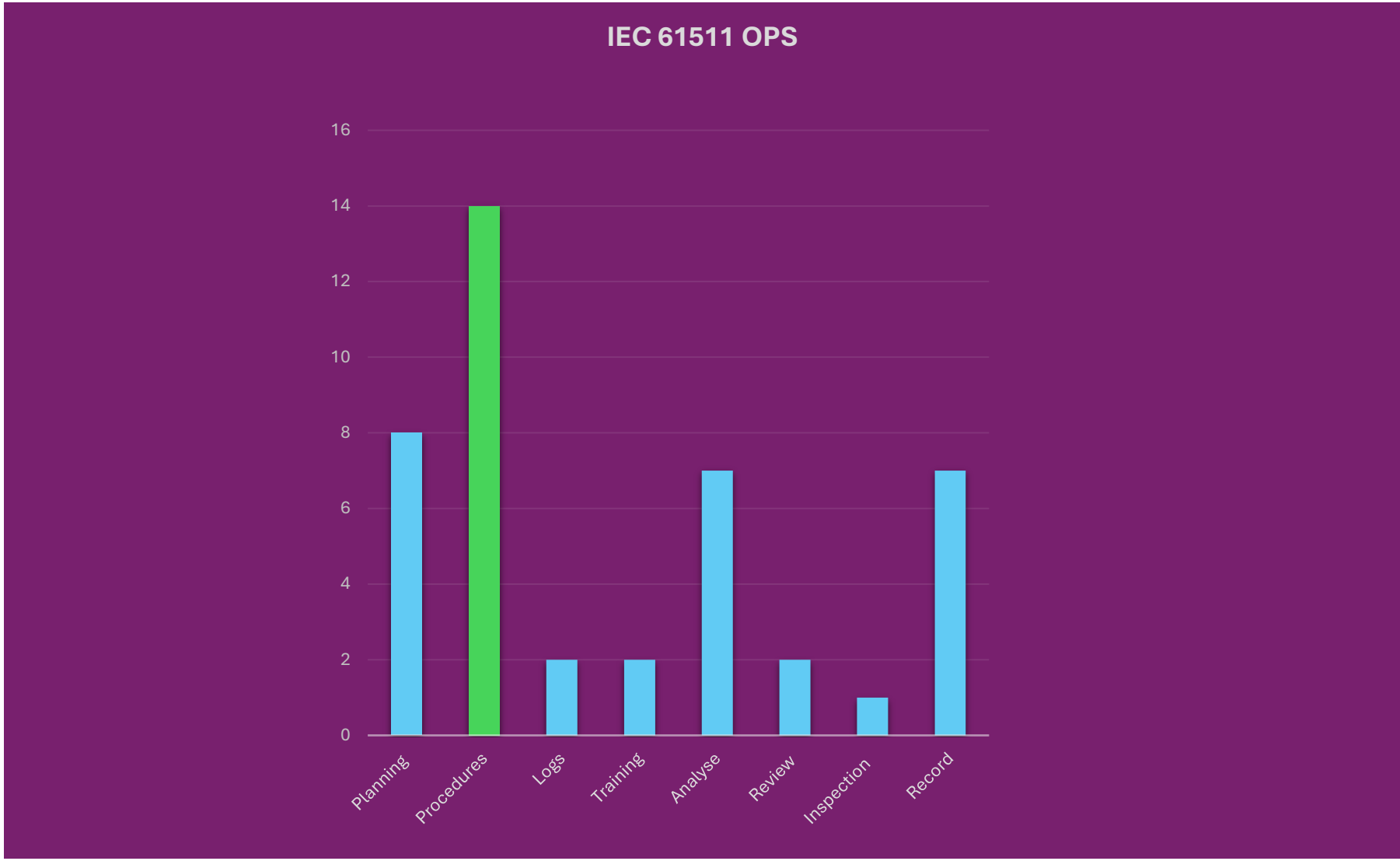
Note - Planning for Spare Parts is essential for any claims of MTTR which forms part of the PFD Calculations.



CASS-511-OP Walkthrough

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.

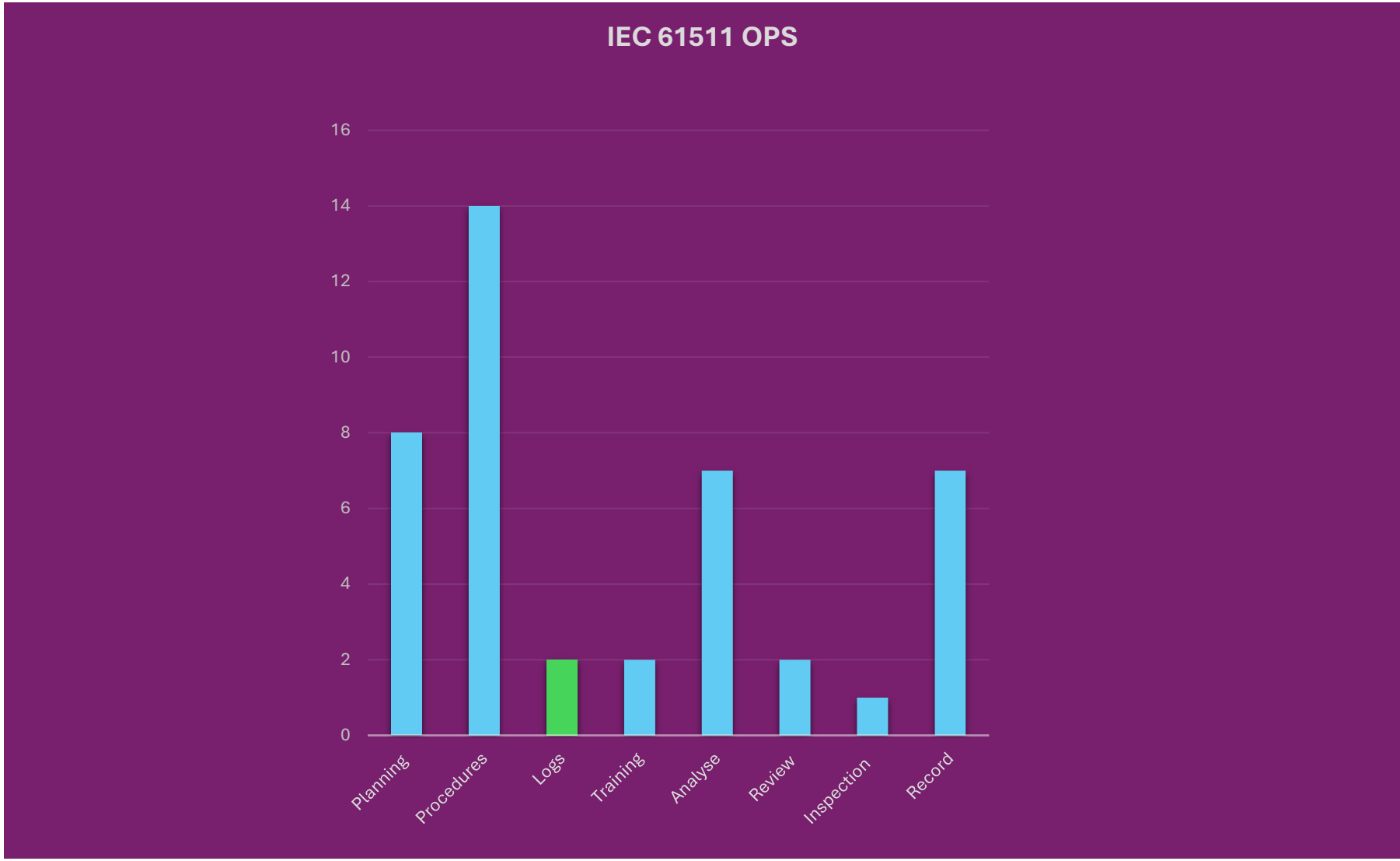


CASS-511-OP Walkthrough

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.

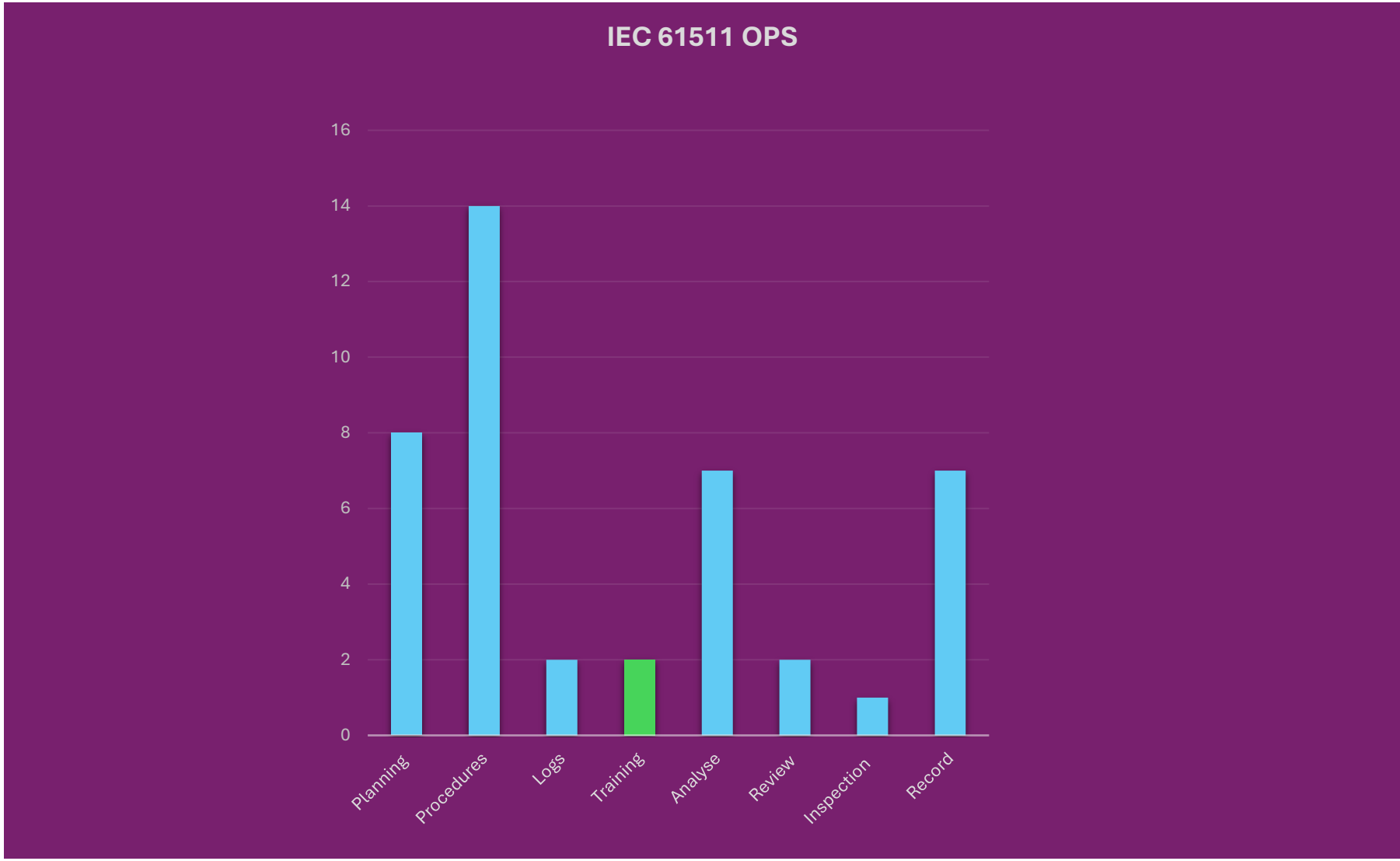


CASS-511-OP Walkthrough

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.

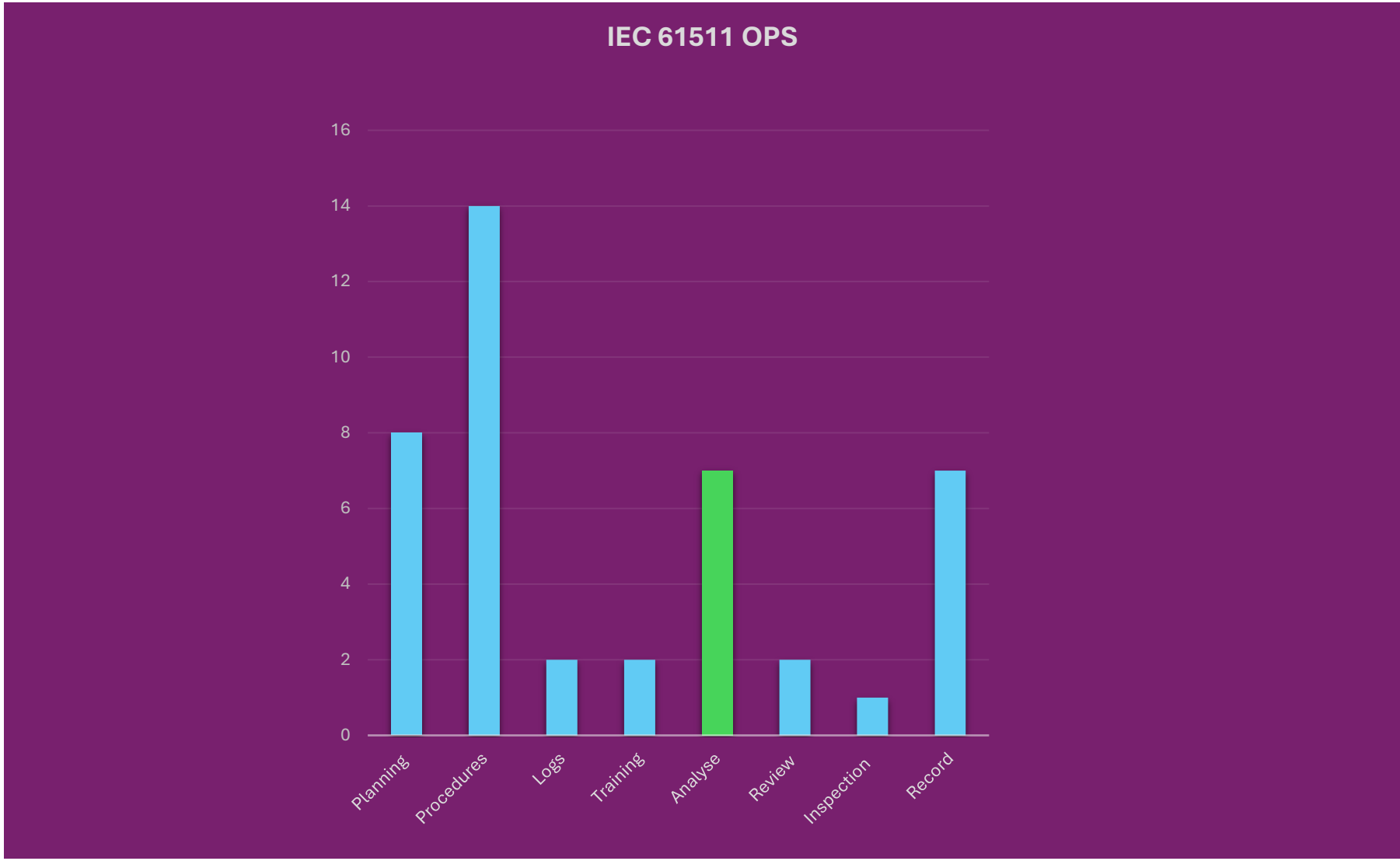


CASS-511-OP Walkthrough

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.

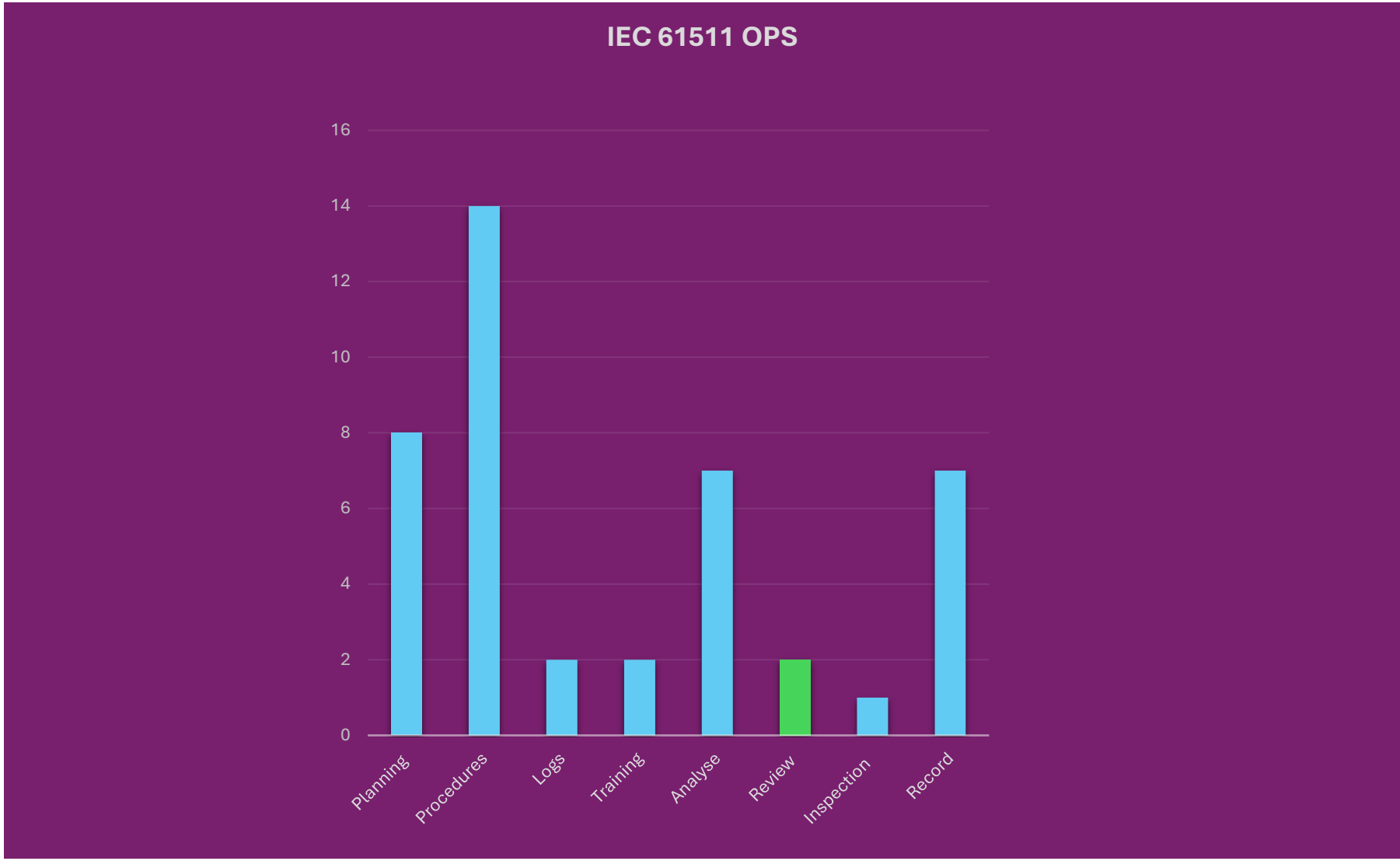
Note – These are new requirements in IEC 61511 and expect greater emphasis in the future on analysis of actual against predicted rates.



CASS-511-OP Walkthrough

2 TOEs Associated with **Review**

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



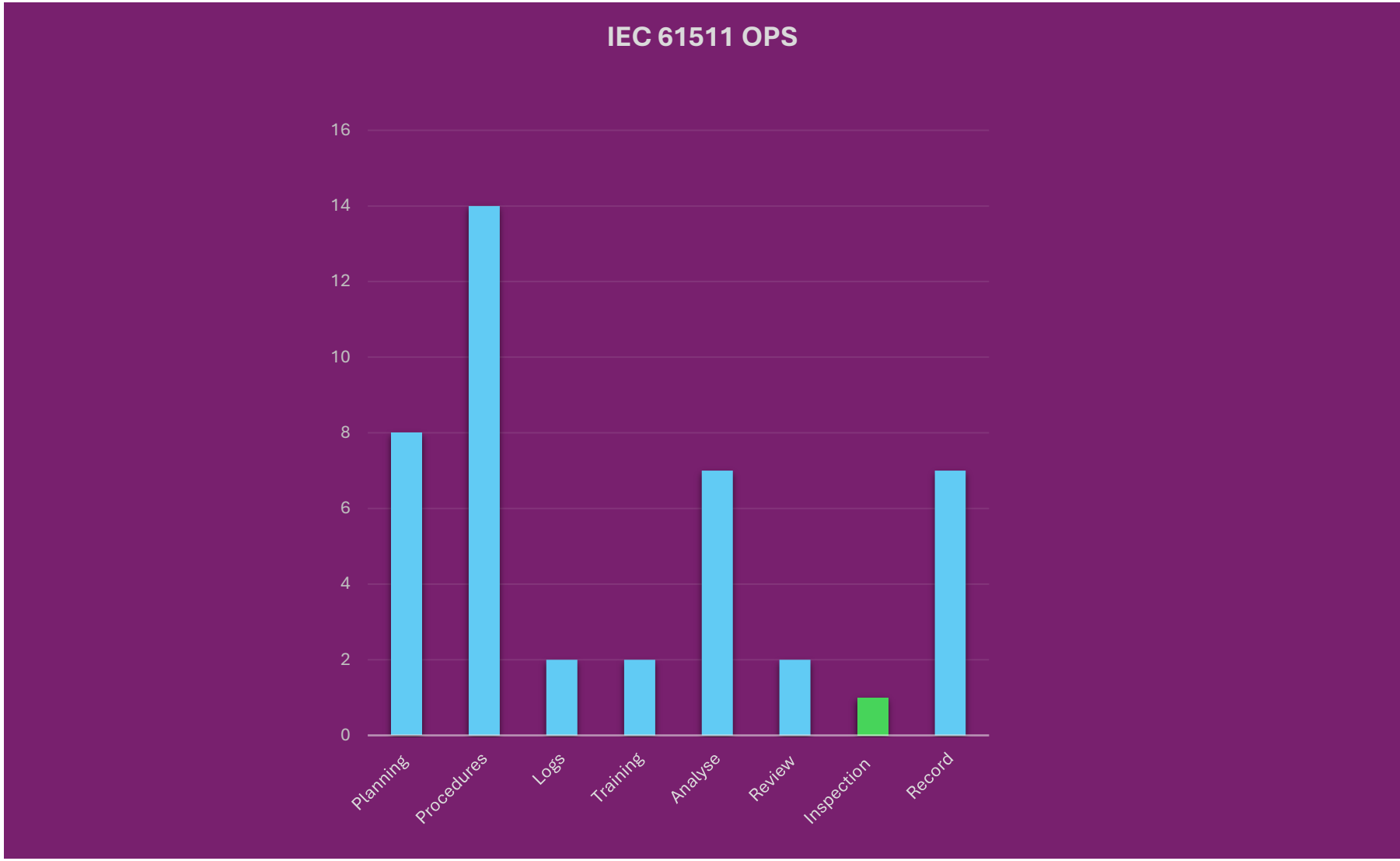
CASS-511-OP Walkthrough

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.

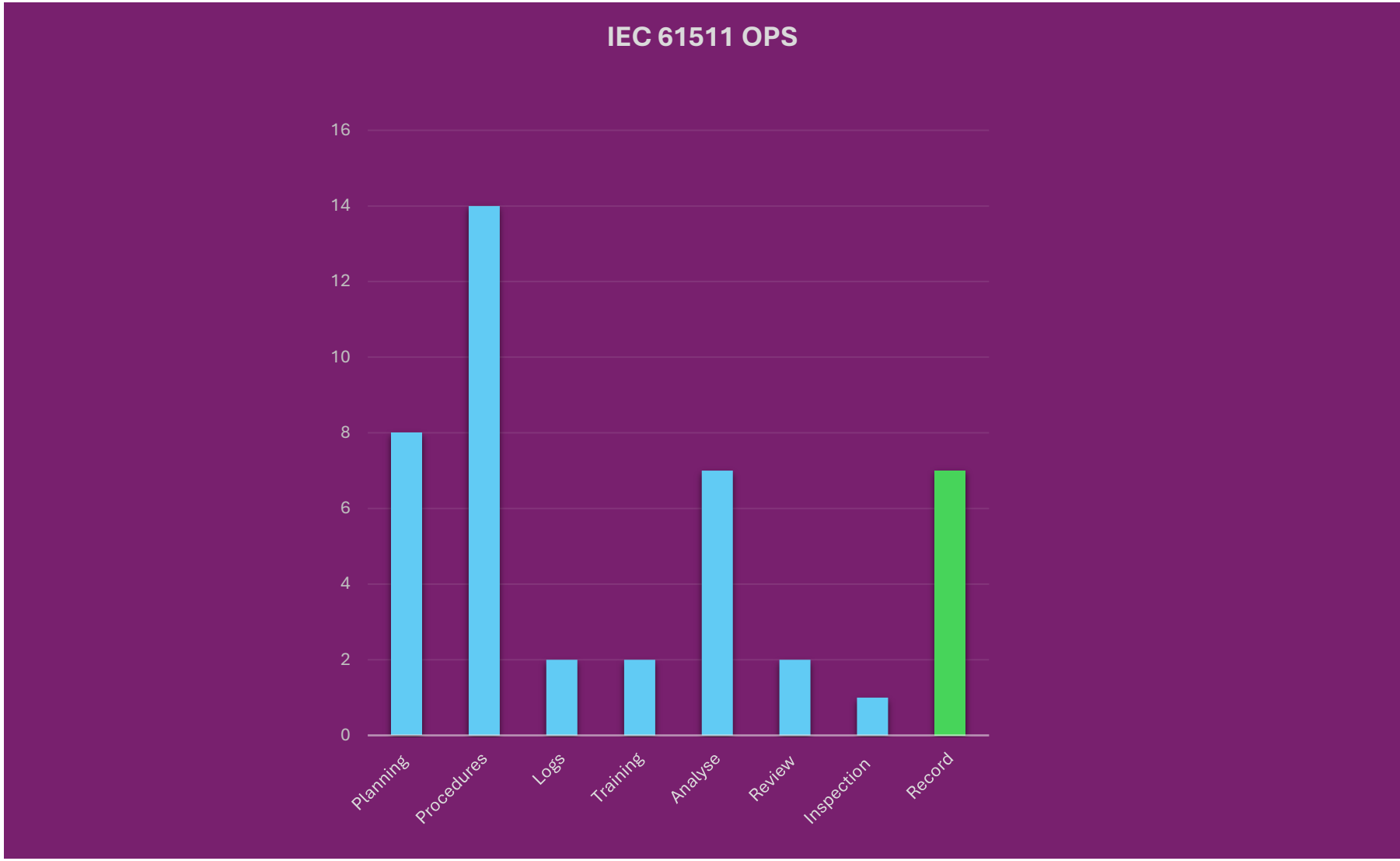


CASS-511-OP Walkthrough

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.

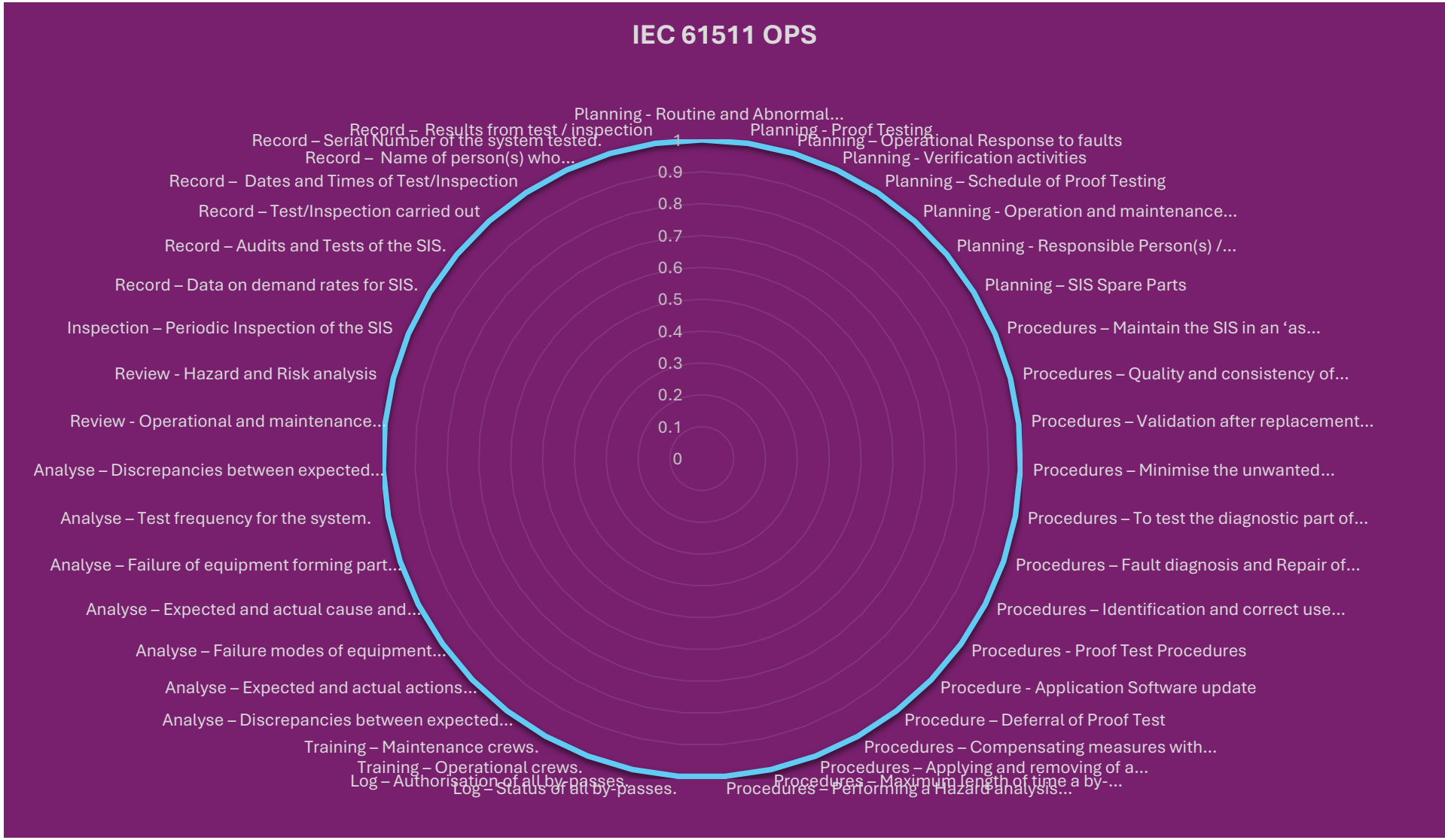


CASS-511-OP Walkthrough

TOE ??

Purpose of the TOE
??

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



Any Questions?

Presenter: Andy Derbyshire, Deepti Chauhan

Contact Details: info@61508.org

What's next....

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

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