The CASS Guide

To functional safety conformity assessment

Document ID: CASS-Guide-A

REVISION HISTORY

Rev	Date	Comment
0.1	2017	Complete re-draft following review of original CASS Guide (ver. 2a, April 2000)
0.2	2017	Minor update (internal draft)
0.3	03-Nov-2023	Major update to contents and structure for review

Notes:
Revision numbers less than 1 indicate draft or preliminary versions; formal release begins at 1.0
Use of the revision format "X.Y" is to support major (X) and minor (Y) revision changes

This document is identified as **CASS-Guide-A** in the CASS documentation structure.

Issued by The CASS Scheme Association
c/o GAMBICA
Rotherwick House
3 Thomas More Street
London
E1W 1YZ

LIABILITY DISCLAIMER

While every care has been taken in developing and compiling the CASS scheme documentation, The CASS Scheme Association (TCSA) and its member organisations accept no liability for any loss, damage or injury caused, arising directly or indirectly in connection with reliance on the CASS documentation except to the extent that such liability may not lawfully be excluded under English Law.

This statement supersedes any disclaimer in any CASS documentation prior to this date.

The CASS Scheme Association
12th September 2023

Contents

Terms and abbreviations

The following abbreviations are used in this document

CASS	Conformity Assessment of Safety-related Systems
E/E/PE	Electrical/electronic/programmable-electronic
EUC	Equipment under control
FS	Functional safety
FSA	Functional safety assessment
FSM	Functional safety management
QMS	Quality management system
RFSA	Registered functional safety assessor (CASS)
SIL	Safety Integrity Level (1 to 4)
T6A	The 61508 Association (a cross-industry user's group, see www.61508.org)
TCSA	The CASS Scheme Association (formally The CASS Scheme Ltd)
TOE	Target of evaluation

1 Introduction and background

CASS (*Conformity Assessment of Safety-related Systems*) was introduced soon after the publication of the first edition of IEC 61508. It is intended to provide an industry-wide approach to the assessment of all aspects of safety-related systems.

The scheme has continued to develop (encompassing other functional safety standards) based on its original core principles, which are to provide an assessment process offering:

- **Integrity** by ensuring the requirements of the standard are all covered in a structured and comprehensive manner
- **Transparency** in the assessment process and results
- **Consistency** of the process used by different assessment providers who use it, thereby improving credibility in claims of conformity, and increasing stakeholder confidence (users and regulators)
- **Availability** to all and **free of charge** to those who use it

The CASS methodology can be used for informal reviews, gap analyses or for formal assessment including the basis for 3rd party certification. Thus, CASS is a conformity assessment "toolbox" that can assist a variety of organisations in their demonstration of compliance, such as:

- Product or sub-system suppliers
- Systems integrators
- Engineering-procurement-construction (EPC) companies
- Plant owners or operators (equipment end users)
- Consultancies offering assistance in preparing internal procedures or conducting independent assessments
- Certification bodies or conformity assessment bodies offering product or company certification (CASS may be stated by their accreditation body as the basis of the functional safety assessment process)

As the methodology (including its approach, scope, criteria and guidance) is open and freely available, those responsible for the safety-related product(s) and/or process(es) requiring assessment can prepare their evidence of conformity prior to the assessment.

Functional safety assessment also relies on assessor competence. To this end, the *CASS Registered Functional Safety Assessor (RFSA) scheme* is available for persons who perform conformity assessments using the CASS methodology. It is intended to provide an accessible and relatively non-bureaucratic process for experienced assessors who wish to be registered. (Note that use of the CASS methodology does not require the assessor to be registered through CASS, and other ways of demonstrating competence can be used). More information about the CASS RFSA scheme can be found in the CASS document *CASS-Guide-A1*.

The CASS scheme documentation is published on www.61508.org/cass under a memorandum of understanding with The 61508 Association (T6A), which provides public access to the CASS scheme.

2 CASS templates explained

At the heart of the CASS methodology is the use of the assessment 'templates' to cover different aspects of conformity. Initially, these were developed for conformity assessment with IEC 61508, and there are separate templates covering functional safety management (FSM), the overall safety lifecycle, the E/E/PE system safety lifecycle, subsystem elements, and software. Some related standards are not as broad in scope as IEC 61508 and they are covered with fewer templates (in some cases just a single template).

Each assessment template:

- lists a number of 'Targets of Evaluation' (TOEs). Each TOE covers a discrete subject for the assessor and cross-refers to all the relevant clauses from the standard on that subject. A TOE does not necessarily group the clauses as they appear in the standard; for example, the subclauses within one section of the standard may be divided between different TOEs
- enables the assessee's documentation to be cross-referred to each TOE and hence to the requirements from the standard
- may include some prompts for the assessor under each TOE
- includes space to record the assessor's comments concerning the documentary evidence of conformity associated with each TOE

CASS templates do not replace any functional safety standard. They cannot be used for undertaking a conformity assessment on their own and a copy of the relevant standard(s) will be required when performing an assessment.

Appendix 1: The CASS scheme documentation shows the CASS scheme documentation structure and the templates currently available or planned at the time of writing this guide. Further templates are being developed to assist conformity assessment with other standards that deal with functional safety in specific industry sectors or applications. The CASS templates are available from www.61508.org/downloads/index.php (scroll to CASS Downloads and Conformity Assessment Templates).

Guidance on using some of the CASS templates is given in section on 5 below.

3 Assessment prerequisites

The following prerequisites are applicable to all functional safety assessments, and are therefore assumed when using the CASS methodology:

- The assessor should know which standard is applicable for the object/subject to be assessed. Typically, this is indicated by established practice in the specific industry or application, the type of EUC hazard (e.g., from a machine or process), stipulations in product standards, relevant regulations, or national regulator guidance, etc. Once the standard is known, refer to the diagram in Appendix 1: The CASS scheme documentation and select the relevant templates under that standard.

- The assessor should know what scope (within the standard) is applicable, for example, which lifecycle phases apply to the scope of the assessment, either directly, or indirectly (such as input or output information that involves other organisations). For some standards such as IEC 61508, it is unusual for one organisation to be directly responsible for meeting the requirements of all phases of the overall lifecycle, whereas for IEC 62061 it is quite common for one organisation to be responsible for meeting all aspects of the standard.
- The assessment should be planned. This is a key area and if in doubt further guidance should be sought from IEC 61508-1 clause 8. *CASS-Guide-A2* (the assessment process from IEC 61508-1) should prove useful, both for planning an individual assessment project and for a company-wide approach to performing assessments (if these are done routinely). The template can be used as a checklist to consider all aspects of the assessment process. See section 4 below for more information.
- The assessor (or assessment team) should be competent in the subject areas they are tasked with assessing. This is a matter for those appointing assessors and the assessors themselves. CASS provides an optional registration service for those who wish to be recognised as experienced assessors in their personal scope of functional safety using the CASS methodology. Further information is available in *CASS-Guide-A1* (the CASS Registered Functional Safety Assessor scheme manual).

4 Assessment planning and general principles

In the case when a formal independent assessment is being undertaken, whilst the CASS templates may be used as the technical basis for establishing conformity with the standard, the work should always be performed within a procedural framework that meets the general requirements of FSA in IEC 61508-1 clause 8.

The local procedures for conducting an independent FSA (typically part of the assessment provider's QMS) need to meet the general requirements from IEC 61508-1 clause 8, summarised below:

- Appointment of assessor(s) [8.2.1]
- Access to all relevant persons and information [8.2.2]
- Application to all lifecycle phases [8.2.3]
- Judgments of achieving functional safety based on compliance [8.2.4]
- Claims of compliance made by all suppliers and other relevant parties [8.2.5]
- Scheduling of the assessment [8.2.6]
- Evidence of that periodic audits have been performed [8.2.7]
- Coordination of actions from previous and for future assessments [8.2.8]
- Planning and resourcing [8.2.9]
- Approval of the assessment plan [8.2.10]
- Full documentation of the evaluations, recommendations and outcomes [8.2.11]
- Release of the assessment outputs to all those who need the information [8.2.12]
- Availability of safety manuals for compliant items [8.2.13]
- Competence of the assessor(s) [8.2.14]

- Independence of the assessor(s) [8.2.15, 8.2.16]

Where the assessment provider's internal procedures need to be checked against the requirements above, the CASS template *CASS-Guide-A2* can be used for this purpose.

It is often beneficial if those who are appointed to perform assessments are identified and involved early in the project / lifecycle to avoid any wasted effort and associated costs later.

5 Assessments to functional safety standards

5.1 IEC 61508

As this standard is generic to all industries and covers a wide scope, some context and explanation is provided below in relation to using the CASS templates. (IEC 61508 should only be used in the absence of a more suitable sector-specific standard).

5.1.1 Functional safety management assessments

IEC 61508 (and most of its related standards come to that) require that organisations dealing with one or more phases of the overall, E/E/PE system or software safety lifecycles need to have functional safety management (FSM). The requirements are detailed in IEC 61508-1 clause 6 and these necessitate procedures for the specific safety lifecycle phases and activities the organisation is responsible for. Furthermore, persons responsible for these safety lifecycle activities need to be competent for the role(s) they are undertaking.

For equipment suppliers, some of the requirements of FSM may already be covered by their ISO 9001 quality management system. It is not the intention to re-assess those areas where they are already shown to be working effectively, however, several aspects of FSM applicable to equipment suppliers are not covered in ISO 9001.

The CASS FSM template *CASS-508-A* is used to assess the procedures that define and govern the organisation's approach to its safety-related activities. It is typically the case that not all TOEs in the template apply to a single organisation. The scope of the assessment may therefore be tailored accordingly, e.g., by entering "Not applicable" to any TOEs that do not apply. As FSM only covers the overall management aspects, one or more additional CASS templates would also be used in an assessment depending on the organisation's scope of activities.

Some examples of types of organisations and FSM assessments are:

- **Systems integrators**. The assumption is that systems integrators are informed about the requirements for the safety system and its safety function(s). The CASS FSM template would normally be used together with procedures that define and govern the safety-related *system design* and *integration* activities. Some systems integrators also deal with overall safety lifecycle activities (for example, writing the safety requirements specification, installation or commissioning, etc) in which case the CASS Overall Safety Lifecycle template *CASS-508-C* should be used, and the assessment tailored by using the applicable TOEs.
- **Engineering-procurement-construction (EPC) companies.** Generally, these companies are only involved with the safety lifecycle phases that lead into the specification and then oversight delivery of safety-related systems (which might include installation, commissioning

and validation). The *CASS-508-A* (FSM) and *CASS-508-C* (overall safety lifecycle) templates should therefore be used and the assessment tailored by using the applicable TOEs.

- **End-users**. Owner/operators of safety-related systems will need to demonstrate they have appropriate procedures and personnel competence for the operation and maintenance of the safety-related systems they are responsible for. The *CASS-508-A* (FSM) and *CASS-508-C* (overall safety lifecycle) templates should therefore be used and the assessment tailored by using the applicable TOEs.

Depending on the industry sector and lifecycle phases, other CASS templates might be more applicable to use, for example, FSM and operations and maintenance in accordance with IEC 61511 phase 6.

5.1.2 Product assessments

Field devices, logic solvers and any other components of safety-related systems need to be assessed as 'compliant items' if they are to be qualified for use in these systems.

The purpose of a product assessment is to establish all the information pertaining to the hardware reliability and systematic integrity with respect to the specified *element safety function* (IEC 61508-4, 3.5.3). The focus of the assessment is therefore the:

- Analysis of the effects of random hardware failures and the properties that determine the architectural constraints
- Development method, design features and various techniques and measures, used to avoid and control systematic faults, in order to determine the systematic capability (SC 1, 2, 3 or 4)

The functional safety information for an element that should be confirmed by the assessment is listed in IEC 61508-2 clause 7.4.9. The assessment should also verify the safety manual meets the requirements of IEC 61508-2 Annex D for compliant items.

For subsystem elements, *CASS-508-E* can be used together with *CASS-508-A* for FSM of safety-related product realisation. (The latter should be tailored according to the applicable TOEs and the scope and depth considering the quality management system in place). If software (firmware) is used in performing the element safety function(s), *CASS-508-F* should additionally be used.

A full E/E/PE system (developed or integrated from pre-compliant subsystems/elements) can be assessed using *CASS-508-D*. In certain circumstances, *CASS-508-D* may also be more suitable for large scale, significant or complex E/E/PE subsystems where the specific target application is known. Ultimately this decision is something the assessor should make considering all factors on a case-by-case basis. As for elements, *CASS-508-A* (for FSM) and *CASS-508-F* (for firmware/software) should additionally be used.

Only the relevant tables of techniques and measures (e.g., from IEC 61508-2 Annex A or B) are referenced in the relevant templates, not each individual technique or measure. Therefore, the assessor should conduct a more detailed evaluation of the techniques and measures used, together with their 'effectiveness', as required in the standard according to the DC, SFF or SIL being targeted. This evaluation should be included with the completed CASS template(s) in the assessment documentation (report(s)).

It should be realised that IEC 61508-2 does not attribute a SIL number to an element (see IEC 61508-4, 3.5.8, and related Notes which explicitly state this). Rather, 'SIL capability' of an element is better understood as a set of properties, all of which need to be available to the safety function designer to determine suitability of the element for its contribution to the safety function at the specified SIL (1, 2, 3 or 4).

Although not defined in the standard, there is a common tendency to take the element properties that have a limiting effect on the SIL of the safety function the element is used in, and attribute the element with a 'SIL *n* capability' (n = 1, 2, 3 or 4) dictated by the property that imposes the lowest limit. However, this so called 'SIL *n* capability' must make certain assumptions about the safety function in which the element is used, such as how certain failure modes of the element will affect the safety function, e.g., whether it is rendered unavailable, causes a spurious trip, no effect, etc.

If 'SIL *n* capability' is claimed for a product (and many certificates state this as a headline), it should only be understood as a *provisional indicator* (e.g., for marketing purposes) and the safety function design team should always verify suitability of the element in the specific application based on all the functional safety properties which should be documented in the safety manual.

The considerations above show that care needs to be taken when forming compliance statements about an element's suitability for use in SIL applications.

5.1.3 Software assessments

Software assessments for IEC 61508-3 is a challenging topic. To support this CASS has created a detailed guide, the Guide to CASS-508-F, which explains the approach and TOEs in detail. This guide needs to be studied in significant detail before the use of the template. The actual template, CASS-508-F, is a more simplified form (when compared to the guide) to allow the assessor to focus on the actual assessment. For an IEC 61508-3 focused software assessment the assessor will need a copy of the standard, a copy of the CASS guide and the assessment template to hand.

5.2 IEC 61511

There are a number of templates associated with IEC 61511 assessments as explained below.

5.2.1 IEC 61511 FSM assessment

In cases when assessing an organisation's generic FSM procedures in accordance with IEC 61511-1 clause 5, *CASS-511-A* may be used. This is typically used in conjunction with *CASS-511-C*.

5.2.2 IEC 61511 FSA stages 1 to 5

CASS-511-B is an excel workbook with structured worksheets and links for undertaking stages 1 to 5 FSAs in IEC 61511.

5.2.3 IEC 61511 SIS safety lifecycle procedures

In cases when assessing an organisation's generic procedures for a SIS project in accordance with IEC 61511-1 clause 6, *CASS-511-C* may be used, typically used in conjunction with *CASS-511-A*.

5.3 IEC 62061

Functional safety assessments for machinery can use the CASS-061 assessment template which is for IEC 62061. This is a single complete template that covers all aspects of machinery safety control

systems including an informative annex on mechanical, pneumatic and hydraulic aspects. The CASS-061 template can also be used to sanity check / challenge an ISO 13849-1 based machine design by following the TOEs and ignoring the clauses.

5.4 EN 50495

EN 50495 covers the concept of "safety devices" under the EU ATEX Directive. This standard acknowledges that in some applications a safety device may be specified, designed and realised in accordance with the functional safety principles of IEC 61508.

5.5 Gas detection standards

The standard EN 50271 covers gas detection at SIL 1 for functionality detailed within EN 50271. The standard EN 50402 covers gas detection (systems) when not covered by EN 50271 and for higher SILs. Please note the ATEX Directive harmonisation status for EN 50402. CASS assessment templates for EN 50271 and EN 50402 do not exist at this time but as these standards follow the principles of IEC 61508 the CASS-508-XXX series of templates can be used instead. The CASS Association is considering the development of templates for these standards.

5.6 IEC 61513

Details may follow in later revisions of this guide.

5.7 ISO 26262

Details may follow in later revisions of this guide.

6 Rules for use of the CASS logo

6.1 Situations when the CASS logo may be used

There are only two situations when the CASS logo may be used:

- By a nationally accredited certification body that uses the CASS methodology in accordance with the conditions in section 6.2 below
- By a CASS registered functional safety assessor (RFSA) in accordance with the conditions in section 6.3 below

When it is used under the stated conditions, it may appear only on a document that contains functional safety statements that have been (or can be) substantiated by the conformity assessment that used the CASS method. In this context, such a "substantiated document" would be the assessment report, certificate, declaration, datasheet, or product safety manual (in their verified and approved version).

When the CASS logo is applied to a substantiated document that is released externally to the organisation concerned (e.g., a certificate or safety manual), it shall only appear when all relevant CASS templates were used in the conformity assessment. An example of not meeting this condition would be applying the CASS logo to a certificate for a smart instrument when only the hardware has been assessed using CASS.

6.2 Conditions for accredited certification bodies

A nationally accredited certification body may use the CASS logo on its conformity assessment related documentation (e.g., reports, certificates) only where the assessment has complied with latest (at the time of assessment) CASS methodologies and in relation to standards which are listed in the scope of the certification body's accreditation.

A certification body may use the CASS logo and/or reference the CASS methodology in publicity material but shall not do so in a way that it misrepresents the scheme or could be misleading. Use of the logo and any references that are made to the CASS methodology shall agree with this document and related scheme documents.

A certification body shall take appropriate action to deal with any holders of its certificates (that bear the CASS logo) if it becomes aware that the holder makes incorrect statements about or references to the CASS methodology. Examples would be statements that could imply that CASS takes responsibility or liability for any assessments. (See the Liability Disclaimer at the beginning of this guide).

6.3 Use of the CASS logo by a registered CASS assessor (RFSA)

CASS RFSAs have strict requirements about how and when they may use their CASS logo on assessment related documents. These are detailed in the RFSA scheme manual, and they are also conveyed to each assessor on their certificate of registration. In summary, the CASS logo may only be used when CASS has been used as the assessment method, appearing on certain documents, and when the assessor is either the primary author or verifier of the report. The assessor takes sole responsibility for the use of their personal CASS logo and for recording each time it is used, which is audited periodically by the RFSA scheme administrators.

A key condition is that the CASS logo is only used within the assessor's personal scope which is stated on the public register (www.61508.org/cass/assessors.php).

The CASS logo may not be used if the assessor's registration has expired.

6.4 Conditions for organisations whose products/systems have been assessed

Organisations that have products, safety systems, or functional safety management systems that have been successfully assessed by a CASS RFSA or an accredited certification body may make reference to the CASS scheme but shall not use the CASS logo on its documentation (other than what has been supplied to it by the assessor/certifier).

An organisation that has its functional safety management (FSM) system successfully assessed by an RFSA or accredited certification body shall not use the CASS logo on a safety related product or E/E/PE system, or in a way that may be interpreted as denoting product or system conformity (unless the product/system is additionally assessed).

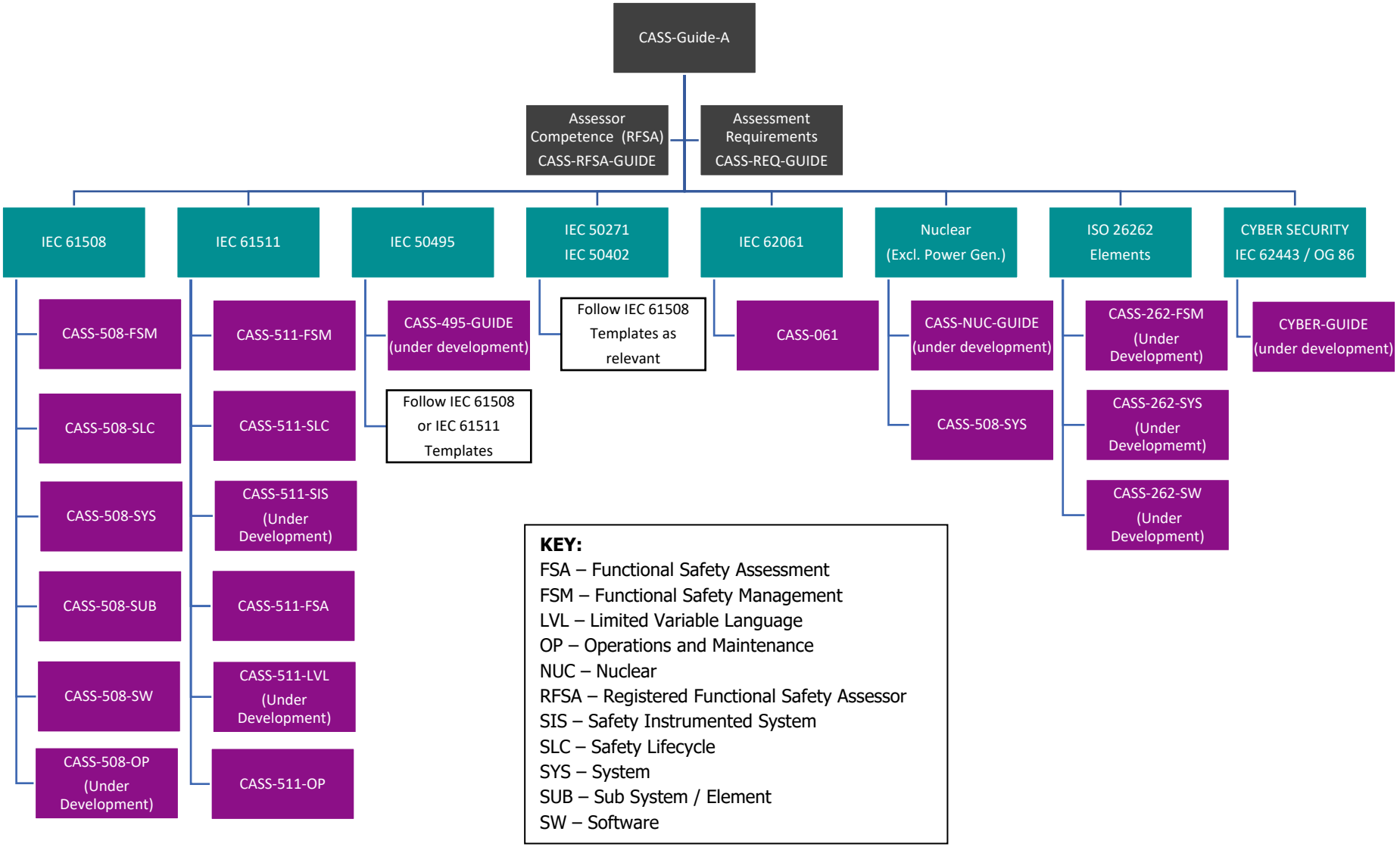
Appendix 1: The CASS scheme documentation

The structure of the CASS scheme documentation is shown in the diagram below. Overall guidance (e.g., this document), supporting guides, and the registered competence scheme is shown at the top in black. Below that, the blue coloured boxes correspond to the relevant standard being used for conformity assessment. Under each standard, the conformity assessment templates are arranged. The meaning of the colour coding for the CASS templates is given in the key below the diagram.

The template ID reference system uses:

- 3 letters (following the text 'CASS') that correspond to the related standard, e.g., "508" for IEC 61508
- 2 or 3 letters in the suffix that correspond to the scope of the template, e.g., "-FSM" for functional safety management, "-SYS" for system (there are some exceptions where no suffix is used because the template covers the entire scope of the standard, e.g., IEC 62061)

The choice of which standard to follow (and hence which templates to use) is a matter for the assessment team as it depends on factors beyond the scope of this document.



This page intentionally left blank