T6A033

"Functional Safety Certificates and Safety Manuals"

1 Contents

2 Revision History

Version	Date	Author	Comments
1.0	09/09/2022	PB / PR	First issue.

3 Scope

This document provides guidance for those who are:

- writing SIL compliance documents (whether they be certificates or safety manuals)
- referring to SIL compliance documents to select compliant elements for integration and use in a safety-related system (this includes interpreting the data, identifying any shortcomings in that data, and recommending actions should the data be inadequate)

This document does not aim to be a tutorial on general aspects of functional safety. It is assumed the reader has a reasonable understanding of functional safety principles. These principles include how an element's failure data is used in a specific safety function, system parameterisation (such as system architecture, PFD_{AVG} calculations, proof test intervals, etc), and the requirements for qualitative and quantitative safety integrity, adherence to stated conditions for safe use, and so on.

Please refer to the Glossary for a brief explanation of the main technical terms used in this document.

This guidance is aimed at the use of E/E/PE element / product functional safety certificates i.e., those making some form of SIL claim. This guidance does not cover non-E/E/PE elements / products as the issues for non-E/E/PE elements / products are similar but not the same. It is also possible to find functional safety management (FSM) company certificates and personal FS competence certificates, but these have different issues than those listed in this document.

SIL compliance documents may fall under other legislation or regulations that require additional information to be included. These other requirements are not covered within this guidance, but this guidance can still be applied in combination with this additional information.

3.1 Functional Safety Elements

Selecting an element for use in a safety function that is to meet the requirements of IEC 61508 (or related standards) requires knowledge of:

a) the element's failure data and associated information, with an assumed application context of the element;
b) the safety-related system, including where necessary other elements, subsystems, certain system parameters, the overall safety function(s) being performed and the SIL(s) involved;
c) the application context, including process parameters and environmental conditions; and
d) the facilities and resources available for inspection, testing and maintenance.

Typically, a) is provided by the element manufacturer who has no direct knowledge of b), c) or d) which is the domain of the system designer or integrator. Likewise, the system integrator typically has no intimate knowledge of the element design and is therefore relying on the relevant information provided by the element manufacturer. Therefore, the design and integration of a safety-related system requires the element failure data and associated information to be complete, fit for purpose for the intended applications and available to all those who require it.

IEC 61508 is clear that any element that is claimed to be compliant with the standard requires an accompanying safety manual to convey all the information required to enable the integration of the element into a safety-related system (see Annex D of IEC 61508-2 and IEC 61508-3). IEC 61508 requires an independent functional safety assessment, and it makes sense to have this done at the element level (separately from, and additional to, assessment at the integrated level) where access to the detailed processes, confidential design information and analysis must be made.

If the element manufacturer has appointed a conformity assessment body[1] to undertake this evaluation, some of the SIL capability data may be summarised in the certificate. In any case, the assessment should ensure that all the SIL capability data is available in the element safety manual, and that it is complete and correct for the application and conditions specified by the manufacturer.

Experience indicates that the current situation can be confusing with different forms of element data and information being produced, under conditions and assumptions that are not necessarily applicable to some applications. This paper aims to raise awareness of the issues involved, provide practical guidance, and improve the situation for all parties.

4 What is Certification?

Functional safety (FS) certification has now been around for many years. Like it or not, FS certification is here to stay and does have a role in the FS market. FS certification does not have the best reputation and considering there is no globally recognised approach for certification to IEC 61508 this is unlikely to be changed easily. This section explains some of the background to FS certification. The various functional safety standards (e.g., IEC 61508) do not detail any requirements for certificates or certification. If there are no requirements for certificates, there are therefore no requirements for a complete or correct certificate. They do however list documentation requirements to ensure that there is enough information to support the safe application and use of the safety-related element or system. In IEC 61508 this information is detailed via requirements for a safety manual.

In general terms, the term "certificate" is not protected in any way. Any party can create a certificate in any form that they please. A certificate can cover any topic not necessarily supported by assessment, evaluation, and / or testing to any level of rigor. It is incumbent on those wanting the certificate to check what is covered and any evidence that supports it. A certificate can cover only part of a standard, even down to a few clauses as agreed between the manufacturer and certification provider, the conformity assessment body (CAB). The principles of a "certificate" in this document can be applied to any declaration type document.

It is possible to get an accredited certificate. This is where another body monitors the CAB in relation to quality of work and quality of the certificate. This is mainly delivered via a national accreditation body, e.g., the United Kingdom Accreditation Service (UKAS) for the UK market. Impartiality is a key principle of both functional safety and certification. Impartiality can be referenced in other terms such as independence, freedom from conflicts of interest, freedom from bias, freedom from prejudice,

[1] This document does not discuss the requirements for functional safety conformity assessment bodies. Refer to IEC 61508-1 clause 8 for general aspects such as technical competence, procedural aspects and independence. See also the internationally recognised accreditation schemes for conformity assessment bodies operating conformity assessment services.

neutrality, fairness, open-mindedness, even-handedness, detachment and balance. Accreditation for functional safety certification follows the impartiality principles of ISO / IEC 17065.

Effectively, certification is the third-party confirmation via assessment and audit of a manufacturers management systems or elements / products, whilst accreditation is independent third-party recognition that a CAB organisation has the competence and impartiality to perform specific technical activities such as testing, inspection and certification. Just as a manufacturer must demonstrate their conformity with a set of criteria to a CAB in order to be certified, in turn conformity assessment bodies have to demonstrate their competence, impartiality and integrity to a national accreditation body in order to be accredited. In other words, if conformity assessment bodies are 'the checkers' then the government-appointed national accreditation bodies role is to 'check the checkers'.

It follows that only conformity assessment bodies can refer to themselves as 'accredited', whereas the organisations successfully audited by conformity assessment bodies hold 'certification'. If the conformity assessment body has been accredited by a national accreditation body to assess that particular activity, then organisations successfully audited by that conformity assessment body hold 'accredited certification'.

Accreditation for a CAB is not mandatory for functional safety. As stated above, any one or any party can issue a certificate. This is not to say that any non-accredited certificate is always of bad quality, there are many good quality non-accredited certificates. Likewise, this does not mean that every accredited certificate is of good quality, mistakes and poor culture can happen in any organisation plus audits are intermittent and sampling exercises. It is simply that there are more checks for accreditation when compared to a non-accredited certificate. In all cases it is very important to understand the scope of the certificate, does it cover all the parts of the standard(s) that are relevant for the equipment under certification?

4.1 Limitations of Certification

The main concern is that the elements used in safety functions are suitable for the intended application. Selecting elements that comply with IEC 61508 is one way of achieving an appropriate level of systematic safety integrity. It is important not to become too reliant on certification. Certification on its own is neither sufficient nor necessary to demonstrate systematic safety integrity.

Safety manuals for certified equipment include a summary of the failure modes and failure rates. The FMEDA, required for certification, carried out on a complex device is usually based on a database of standard components. We don't expect those components to be 'certified', yet a CAB can use that data in an FMEDA to predict a dangerous failure rate of a complex arrangement of those components. Certification is not a requirement for safety. At some point we always start where there is no certification.

A more modern trend is to find that sub-elements and software modules within a safety-related element also have their own certification. Common software tools such as compilers are also now being separately certified. A single safety-related element may have more than one certification to compare with the final application / install. There may therefore be more than a single CAB involved in the certification of a safety-related element.

It can be easier and safer to design and justify an element from components using the principles of the functional safety standards (i.e., without certification). For all element types, engineers need to monitor the performance of the installed system in any case. Thus, we should always be using data collected in situ to continually validate the original estimate and, if predictions were optimistic, these could be corrected over time. This data can be used to manage self-designed elements just as easily as commercially off the shelf elements. So, using self-designed elements is just as relevant as using commercially off the shelf elements.

5 Glossary

Item	Description
CAB	Conformity Assessment Body
Certification report	The report produced by the CAB that supports the FS certificate.
E/E/PE	Electrical / Electronic / Programmable Electronic.
Element	Part of a subsystem comprising a single component or any group of components that performs one or more element safety functions. (IEC 61508-4:2010, Cl. 3.4.5)
FS	Functional Safety.
FSA	Functional Safety Assessment.
FSM	Functional Safety Management.
HFT	Hardware Fault Tolerance.
Object of certification	The element, product or system that is or was certified.
PFD	Probability of dangerous failure on demand. (IEC 61508-4:2010, Cl. 3.6.17).
PFD_{avg}	Average probability of dangerous failure on demand. (IEC 61508-4:2010, Cl. 3.6.18)
PFH	Average frequency of a dangerous failure per hour. (IEC 61508-4:2010, Cl. 3.6.19)
Safety manual	See IEC 61508-2:2010 Annex D and IEC 61508-3:2010 Annex D.
SIL	Safety Integrity Level.
SIL compliance document	Document used for supporting or claiming compliance for SILs.

6 Executive Summary

1. Certificates should only be issued when the object of certification is compliant with ALL the relevant parts of IEC 61508, or related standard. All parties reliant on FS certificates need to be aware that impressive headline statements of conformity are meaningless or misleading if they are nullified by the small print.
2. It is essential to read both the FS certificate AND the safety manual very carefully. Do not just rely on the information shown in a FS certificate. A certificate should reference the safety manual (including its revision / version) and possibly a certification report.
3. If there is only a certificate (which is not required by IEC 61508) and no safety manual (which is required by IEC 61508 for compliant elements) then the element / product does not comply with IEC 61508.
4. Do not be over reliant of FS certification, it is compliance to the functional safety standards that is important (you are required to review the information).
5. Do not be over reliant on the information and data on the FS certificate, this may only be a best-case scenario (you are required to review the information).
6. It takes a reasonable amount of knowledge / competence to read and understand a functional safety certificate. Ensure staff with relevant responsibilities have the competence to perform their duties in relation to FS certificates.

7 Functional Safety Certificate(s)

The certificate is simply a declaration that the object of certification is compliant with the relevant parts of the applicable functional safety standard. Assuming the certificate covers the full scope of IEC 61508, the certificate does not need to hold all the technical detail for the object of certification. This technical detail needs to be detailed in the safety manual as per the requirements of IEC 61508. It can be detrimental or misleading to put too much technical information on a certificate.

Minimum information on a FS certificate includes:

- Identity of the conformity assessment body (CAB).
- Identity of the certificate / declaration holder.
- A unique identifier of the functional safety certificate / declaration.
- The functional safety standards applied in the functional safety certification, including specific clauses where relevant (e.g., those included or excluded if not the complete standard).
- A short description of the object of certification (for identification purposes), including relevant hardware and software versions.
- The safety functions / features which were the object of certification.
- The associated maximum achievable safety integrity level / systematic capability.
- Statement on certificate scope and limitations.
- A unique reference to the safety manual and certification report.
- The date and, if applicable, expiry date of the functional safety certificate.
- Name of the person taking the certification decision.
- A statement defining that all the relevant design / engineering information for the functionally safe use of the object of certification is covered in the safety manual (*e.g. the object of certification safety integrity is conditional upon compliance with the technical aspects detailed in the safety manual document xxxxxxxxxxx.pdf. The detail on this certificate is insufficient for the achievement of the safety integrity*).

NOTE: As the functional safety standards have no requirements for a certificate there are also no requirements on how the safety manual is referenced from the certificate. The reference could be direct or the certificate can reference to the certification report which in turn references the safety manual.

Other information can be added if the CAB and / or certificate holder wishes however confusion between the certificate and the safety manual should be avoided. This does mean limiting the amount of information contained on the certificate. A certificate should ideally be only one or two pages. If extra information is added to the certificate, then the guidance for the safety manual should also be considered for the certificate (see section 8). If the CAB is accredited, the accreditation body should also be detailed / referenced on the certificate.

If the certificate does detail safety-related or numerical data, this should only be used in conjunction with the detail in the safety manual. The data on the certificate may be for a single specific application (best case scenario). Over-reliance on certificate data should be avoided.

Key points for when reading / translating FS certificates:

1. The FS certificate is for the correct device / system from the correct manufacturer?
2. The FS certificate is current (not too old) and in date?
3. The FS certificate matches the hardware and software versions required for the application?

4. The FS certificate covers the appropriate functional safety standards for the object of certification? For example, it is highly recommended that IEC 61508-1 is always covered plus IEC 61508-2 if the object includes safety-related hardware aspects and IEC 61508-3 if the object includes safety-related software aspects.
5. The FS certificate covers the safety functions or safety features required for the application?
6. The FS certificate scope and limitations align with the application requirements?
7. The FS certificate has a clear link to the element safety manual / documents?
8. Caution for when the FS certificate states compliance via proven-in-use (see below).

FS certificates should not be issued if an applicable part of IEC 61508 has not been applied or has failed a conformity assessment. As an example, if an intelligent level sensor contains safety-related software to perform its function then IEC 61508-1 (FSM), IEC 61508-2 (hardware) and IEC 61508-3 (software) shall be assessed during a certification. If, however the level sensor manufacturer requests that IEC 61508-3 is not in scope or if the CAB assessment finds compliance issues in relation to IEC 61508-3 a FS certificate should not be issue by the CAB. The overall compliance of the level sensor to IEC 61508 has not been established and therefore any FS certificate will be without value and possibly just misleading. A detailed CAB report only can be issued instead explaining the status of compliance.

According to the relevant functional safety standards the overall SIL rating is applied to the safety function, so the whole function (loop) not just the individual elements within the function (loop). The FS certificate may claim a maximum achievable SIL and / or systematic capability (SC) for the element but this does not mean that this SIL is possible in every safety function. The actual achievable SIL in a specific application is defined by many factors and this level of detail is intended to be found in the safety manual.

The hardware version but more specifically the software version can obviously change / increase over time. Always ensure that the current version being sold or supplied by the manufacturer is covered by the FS certificate. Documentation and / or compliance information that is out of date is an indication of a poor functional safety management system.

Always put some consideration into the date of issue for the FS certificate. If the date of issue is several years old, make enquiries about the surveillance activities between the manufacturer and the CAB that issued the certificate. If there has been no surveillance or recertification, then there is no assurance for if the management and lifecycle aspects for functional safety have been maintained.

There are FS certificates on the market that list the scope as IEC 61508-1, IEC 61508-2 and IEC 61508-3. There are then others that listed all seven parts of IEC 61508 as their scope. This does not matter. The important parts are the first 3, the normative parts, and the remaining four parts (including the 5th, part 0) are there to support these first 3 parts. The most important thing is to ensure the scope for the object of certification includes all the relevant parts from IEC 61508-1, IEC 61508-2 and IEC 61508-3. If in doubt, challenge the manufacturer and ask them to justify the standards used.

There are many products on the market that can be made up from multiple components with varying configurations or architectures, for example safety PLC's and SIS controllers. The overall product line may have an FS certification but that doesn't mean that all the modules, components, configurations or architectures are compliant to the same SIL / SC. The FS certificate will state a claim, often seen to be the best possible case, but typically cannot detail all the possible options. This level of detail is usually

found only in the safety manual. It is very possible that the use of the certain components, architecture or software can result in the same product achieving no SIL / SC.

For elements that can be highly configurable (see section 8), this also means that any functional safety criteria detailed on the FS certificate is only relevant for a single combination / architecture. It is essential that final system designer understands and compares the combination / architecture for the FS certificate compared to the final system combination / architecture. It is highly recommended to detail the FS certificate with the functional safety criteria for a HFT = 0 and proof test interval of one year (if relevant), anything else can be considered misleading for the final system designer. It is best to keep certificate data to the most basic level for the element / product, so that it is most universally applicable (within the boundary of the stated applications).

IEC 61508-2 allows for a route to compliance via "proven-in-use" for functional safety elements (Cl. 7.4.10). This compliance route allows for element historical performance data to be used to justify a defined level of safety integrity. This proven-in-use approach is intended to be used by those with close access to elements in their end application as the element is required to have clearly restricted and specified functionality plus adequate documented evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough for the required safety integrity. This justification is based on analysis of operational experience of a specific configuration of the element together with suitable analysis and testing. There are both unaccredited and accredited certificates available on the market that rely on a proven in use approach. These proven in use certificates must be treated carefully, if you intend to use an element like this, it is highly recommended that you challenge the manufacturer and CAB to check the approach was appropriate. This requires a very detailed check of the safety manual.

NOTE: A FS certificate covering just IEC 61508-1 can be described as a Company FSM certificate. This is a valid approach that is not covered or discussed in this guidance.

8 IEC 61508 Safety Manual(s)

The safety manual is the descriptive term for all the information that enables the functionally safe application and use of the object of certification. The safety manual does not need to be available as a single document or even as a document with that specific title, but the information must be available to all parties that may wish to use the element within a safety function, that is freely available. IEC 61508-2 and IEC 61508-3 both have an Annex D which details the relevant information required for compliant elements. It is worth reading some of the specific safety manuals clauses from IEC 61508 including IEC 61508-2 clauses 7.4.9.3, 7.4.9.4, 7.4.9.6, 7.4.9.7 and IEC 61508-3 7.4.2.12 to fully understand the overall requirements.

As IEC 61508-2 and IEC 61508-3 both have an Annex D that covers the detail there is no need for this document to repeat the information, however it is worth spending a little time considering some of the important points. The first, and possibly most important, requirement to be aware of is that the claims made in the safety manual must be supported by justification (e.g., IEC 61508-2, Cl. 7.4.9.7), for example claimed safety performance is supported by evidence. This justification is typically not found on a certificate meaning a certificate without the safety manual is not compliant with IEC 61508 series of standards. Some manufacturers or CAB's may claim the FS certificate is the justification, but this can only be the case with a good quality certification report backing the certificate.

For any safety-related hardware element, in terms of the behaviour of its outputs, the safety manual must provide information on the failure modes due to random hardware failures including if these are detected by diagnostics and estimated failure rates. Similar information must also be provided for the diagnostics themselves and how these can impact the safety. Failure modes can only be classified as being safe or dangerous when the application of the compliant element is known in relation to the hazards of the final application. Due to all this it is therefore also important for the element manufacturer to make the final system designer aware of any specific proof testing and / or maintenance requirements relevant for maintaining the safety integrity of the element. The manufacturer of the element cannot be aware of every possible safety function application so must provide enough detail to allow the final system designer to engineer the safety function. Hardware Fault Tolerance (HFT) is an important concept within functional safety standards. It sets requirements on the level of redundancy in the safety function. The HFT options available for the element are important aspects of the safety manual. This level of hardware detail cannot be easily summarised on a FS certificate, hence the IEC 61508 approach for requiring the safety manual.

It is worth noting that equipment failure rates can only be predicted to within an order of magnitude. It is inappropriate or even misleading to quote estimated failure rates to two or three decimal places. The safety manual is the location for all the key detail for reliability data. High reliability is a key requirement for any element within a safety function. Part of the assessment of functional safety is to consider reliability data and associated failure modes for the components or elements someone may wish to use in their safety product or safety function. This data can come from numerous sources such as industry databases, end-user reliability monitoring or manufacturer accelerated life testing. Before anyone accepts and uses any reliability data, it is important they understand the relevance of that data for their product or application. Read the small print associated with the data and ensure you understand any limitations and constraints such as the environmental conditions (e.g., temperature) and functionality (e.g., similar application). It is also recommended to keep in mind the derating principles of IEC 61508.

As software is very different from hardware then as you would expect the requirements of Annex D of IEC 61508-3 are very different from those in Annex D of IEC 61508-2. It is possible that the safety manual covers a pure software element or a combined software and hardware element. The focus for software is not on failure modes or failure rates but on systematic aspects such as specification, interfaces, run-time environments, resources, installation and compatibility. Fundamentally providing as much information as possible to support either further development or integration into other elements. It is important to detail the software safe state which the software will revert to in the case of certain application failures to allow the final system designer to engineer the safety function they need. Again, the manufacturer of the element cannot be aware of every possible safety function plus they cannot design their software element to consider endless states or possibilities, so software design uses assumptions as part of the design. It is essential these assumptions are detailed in the safety manual so that the final system designer can consider them for the safety function.

Some elements covered by a FS certificate and safety manual can be highly configurable, that is they can be arranged in various combinations and / or various architectures. Examples are safety PLC's, SIS controllers, other devices with input / output boards and multi axis drives systems. The safety manual must detail all these options to ensure the final system designer uses the element safely, in a manner required to meet the target performance, (e.g., which combinations of components, configurations and architectures can be used to achieve which SIL / SC). Possibly even which combinations cannot be used

for safety-related applications. This can mean that the relevant functional safety criteria (e.g. PFD, PFH, HFT) can vary greatly depending on these combinations / architectures and these must also be detailed in the safety manual. Many element manufacturers will support these options with extra application examples that detail relevant combinations. This detail should be very clear and specify any additional aspects required to achieve the SIL / SC such as programming, feedback signal and diagnostic signal wiring. The overall diagnostics approach (inherent and additional) should also be covered including its relationship to testing, maintenance, and modification, stating any timing constraints or limitations. An elements SIL / SC can be affected by missing, not applied or incorrectly applied diagnostics, it can also be affected during system maintenance and modification. The safety manual should clearly document these impacts and what is needed to manage them (e.g., scan time increases, effecting the safety response time, forced or disabled signals during online maintenance activities, that may impact SIF coverage). Greater details for use are required for elements with greater flexibility and complexity.

The safety manual is the best place to show typical (hypothetical) examples of how the reliability data can be used (at system level), and/or how the data can be improved upon to achieve various SIL capabilities (e.g., by adding diagnostics, redundancy, or simply showing how data for different failure modes leads to different SIL capabilities depending on the application). The safety manual has the space / time to allow the element / product manufacturers to clearly present their elements / products in the best light, without misleading or confusing the system integrator or end-user. The element / product manufacturers should do this in a way that leaves flexibility for the integrators / end-user engineers to apply their engineering judgment!

The security of functional safety elements and systems is becoming more and more important as the majority of systems are now networked and many devices are becoming "smart". A final system cannot be considered safe if security aspects have not been considered. Likewise, there is literally no value in a system that is secure but fundamentally unsafe. Safety and security must therefore work hand in hand. The safety manual therefore must cover the approach for security, both the design related elements to support security performed by the manufacturer as well as the security issues and requirements that the final system designer must consider.

Key points for when reading safety manuals:

1. The safety manual contains sufficient and appropriate justification for information?
2. The safety manual contains all the relevant information (see IEC 61508-2 / 61508-3 Annex D)?
3. The safety manual identifies function failure modes (in terms of the behaviour of its outputs) for the element / device.
4. The safety manual and/or certificate lists the expected failure rate for each failure mode and the range over which the failure rate should be expected to vary.
5. The listed range of variation in failure rates allows for operation across the entire range of environmental conditions specified for the device in the safety manual, preferably based on the worst-case scenario.
6. The listed estimated range of variation for electronic devices takes into account all of the stress factors considered in IEC 61709, *Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion*, or the approach from IEC TR 62380, *Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment*.
7. The listed range of variation in failure rates allows for the age and wear related deterioration that can be expected over the useful operating life or mission time recommended for the device.

8. The safety manual specifies the preventive maintenance, inspection, testing and condition monitoring practices that are required to achieve the failure rate performance that has been claimed.
9. The safety manual details the software safe state, if relevant.
10. The safety manual sufficiently details the software design and any safety relevant assumptions made during the software development.
11. The safety manual details the various element combinations and / or various element architectures that can be supported for safety-related applications including the relevant achievable SIL / SC.
12. The safety manual details the approach for security especially the aspects to be undertaken by the final safety function designer.
13. The safety manual details the route to compliance as Route 1_H. If Route 2_H was selected instead, investigate the approach in much greater detail to ensure the information is there to support Route 2_H.

9 Existing and Emerging Standards

- IEC 61508-1:2010, *Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 1: General requirements*
- IEC 61508-2:2010, *Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 2: Requirements for electrical / electronic / programmable electronic safety-related systems*
- IEC 61508-3:2010, *Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 3: Software requirements*
- IEC 61511:2017, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*
- IEC 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*

10 The 61508 Association Recommended Practices

This document sets out to describe current best practices in functional safety certificates and IEC 61508 safety manuals for functional safety systems, but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the installation.

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither *The 61508 Association* nor its members will assume any liability for any use made thereof.

11 ANNEX A – Certificate Checklist

If a certificate is being referred to (not mandated by IEC 61508), the following checklist is offered to check for completeness of the information on the certificate.

No.	Item of information	Y/N/NA
1	CAB identity (name and address) plus accreditation details, if any (relevant to scope of certificate)	
2	Name and address of certificate holder (manufacturer) - the legal entity responsible for compliance with the certification scheme requirements	
3	Unique certificate identifier including revision	
4	Standard(s), parts, and year(s) of publication that the element / product conforms with – this should include all relevant aspects that affect the functional safety of the element such as hardware, software and functional safety management	
5	Element (or subsystem) identifier, including any variants and/or configuration (short description for identification)	
6	The type of certification, e.g., type-examination only, type-examination plus inspection of samples from production, type-examination plus QA surveillance and re-assessment, etc	
7	Typically, the element safety function(s), a brief product description and further details of the failure data and associated information may be added, or the safety manual referred to where these must be contained in full	
8	The unique document reference (including revision) of the element safety manual that contains all the relevant information required to design the element into a safety-related system and which has been ratified by the conformity assessment body	
9	Dates of issue and, if applicable, expiry (a type-examination certificate might not require an expiry date)	
10	The signature, name and role of the person taking the certification decision (some conformity assessment bodies have more than one signatory, in which case the same information should be provided for each signatory)	
11	Statement defining that all the relevant design / engineering information to meet the safety integrity is covered in the "safety manual"	
12	The reference number, date, revision and title of the report(s) in which the conduct of the conformity assessment and the evidence of conformity are recorded for traceability (the report is generally confidential)	
13	Conditions / limitations for the certificate holder to adhere to (e.g., modifications) may be included	
14	Conditions / limitations for the user to be aware of on which the certification validity depends may be included (in addition to the safety manual)	
15	A list of the element / product documents (such as specifications, drawings, etc) may be given in a schedule or annex to the certificate	

12 ANNEX B – Safety Manual Checklist

The following checklist is offered to check for completeness of the information in the safety manual required by Annex D of IEC 61508-2 Parts 2 and 3.

No.	Item of information	Y/N/NA
1	Unique document identifier including revision	
2	Element (or subsystem) identifier, including any variants and/or configuration	
3	The element safety function(s) including relevant timing constraints or limitations	
4	A description of the safety applications for which the element is intended	
5	Element / product description and/or technical specification	
6	For each element safety function or application context, a description of each failure mode, the effect (if known, or not self-evident) and failure rate for each failure mode	
7	The diagnostic coverage and safe failure fraction (including the extent of coverage)	
8	The diagnostic test interval, where appropriate	
9	The diagnostics failure modes, and failure rates, where applicable	
10	The hardware fault tolerance (either internal, or any requirement to use more than one element) and associated common cause aspects.	
11	The element or subsystem type: A or B	
12	The service lifetime of the element (with any conditions regarding maintenance)	
13	The systematic capability (SC 1, 2, 3 or 4) of the element that will determine the highest SIL in which the element / product may be used based on the measures used to avoid and control failures	
14	Whether Route 1H or Route 2H has been used. If the former, the database used for the analysis of failure rates (e.g., IEC TR 62380, SN 29500, HRD5)	
15	Conditions regarding any functionality that is not to be used for safety applications (e.g., certain interfaces, auxiliary functions, displays, etc)	
16	Definition of the output state(s) that should be used to produce the EUC safe state (if not self-evident)	
17	Any specific diagnostic measures that should be provided by external equipment and how these relate to the quantitative data provided	
18	Conditions and/or restrictions in use when used in safety applications (e.g., environmental, EMC, mechanical, etc)	
19	Specific maintenance requirements if necessary to maintain functional safety	
20	Proof test / mission time requirements (equipment required, procedure, maximum intervals)	
21	Instructions for installation, operation and maintenance, or reference(s) to the document(s) where these can be found	
22	Details of how to report issues or element / product failures that may affect functional safety that the manufacturer should be notified about	

13 ANNEX C – Guidance for CAB's

Impartiality is essential for any certification program (think independence, freedom from conflicts of interest, freedom from bias, freedom from prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment and balance). It is accepted that FS certification is a commercial relationship between a manufacturer and a CAB, but that relationship needs balance between commercial and safety aspects. It is recommended that the CAB adds mechanisms for safeguarding impartiality to their quality, FSM or safety culture programs. Safety culture is important for all parties involved with functional safety including the CAB, please see ISO 26262-2 Annex B.

IEC 61508 and IEC 61511 have requirements for formal Functional Safety Assessments (FSA's) which need to be undertaken by person(s) or organisation(s) that provide a certain level of independence (see the relevant standard for details). The same standards also have requirements for the definition and communication of clear roles and responsibilities. Certification of an element / product or system may or may not be a formal FSA. In most cases this is the free choice of the parties involved but as per the requirements of the standards this needs to be defined and communicated in the commercial relationship between the parties. It is not unusual to find a CAB that thinks they just provided a simple certification service when the device manufacturer believes they have provided a formal FSA. The CAB should be prepared to distinguish between any FSA and non-FSA service offerings, and we recommend that the CAB has material available to clearly communicate their different service offerings.

NOTE: IEC 61508 uses both functional safety assessment and functional safety audit. Confusions can easily arise when discussing an assessment of functional safety compared to a formal FSA.

For manufacturers that have safety-related software within a device, please be aware that the party providing the FSA must be involved very early in the development lifecycle (see IEC 61508-3). The CAB should be aware that if they are delivering formal FSA's then, according to IEC 61508, they may require their own small formal FSM (coordinating FSA's) or quality system.

Some functional safety standards have detailed competence requirements. These competence requirements apply to all parties involved in functional safety including the CAB. The CAB should consider both the competence of individual staff and the collective competence of the overall CAB. Having minimal competent staff mentoring significant numbers of unqualified staff is not conducive to impartial and quality certification (safety culture). It could be argued that the personal competence of the person conducting the certification is more important that the organisation competence of the CAB. It is accepted that the CAB will have a mix of competent staff and developing staff but the best approach is a balanced mix of significant experience and enthusiastic beginners. The Association actively encourages the transfer of functional safety knowledge to all.

NOTE: Competence has a big impact on the quality for the assessment of functional safety and the quality of any certification.

It is becoming more common for a CAB to perform an assessment or certification for a product that uses a previously certified element. For example, the functional safety of a power drive system is being assessed for certification, but the software compiler used by the manufacturer has already been certified by another CAB (on a previous occasion). The first CAB will need to decide how much trust they will place in the second CAB's work (this will typically involve at least sampling some of relevant requirements). In this situation, the guidance in this document can also be used by the first CAB but

then the final product safety manual must detail and reference the supporting certificate, supporting safety manual and supporting certification report.

14 ANNEX D – Selecting a CAB

Challenging questions to ask CAB's when you are trying to select from numerous service providers.

- Are you accredited, and if so by whom and for how long?
- How are you audited by the accreditation body and how often does this happen?
- Please can you overview your functional safety experience for us, especially those aspects relevant for our element / application?
- Please can you overview your functional safety competence process with us (if accredited, they may state the national accreditation body has covered this; insist anyway)?
- How many functional safety competent staff do you have, and which standards can they cover?
- Please can you overview your impartiality process with us? How do you ensure you are not unduly influenced during the assessment of functional safety / functional safety assessment?
- How do you synchronise your functional safety sector / field knowledge to ensure you are inline with the accepted state-of-the-art?
- Please can you overview your staff continuous personal development process in relation to functional safety?
- Please can you outline your approach to support for staff delivering functional safety-related assessments?
- Typically, by standard in scope, how many functional safety-related assessments do you perform per year?

*** END OF DOCUMENT ***