Open IEC 61508 Certification of Products

Rainer Faller
exida GmbH
BirkensteinStrasse 53
83730 Fishbachau Germany
Rainer.Faller@exida.com

Dr. William M. Goble
exida L.L.C.
Sellersville, PA 18960, USA
wgoble@exida.com

Keywords: IEC 61508 Product Certification, Safety Case, Open certification

Abstract
IEC 61508 has been in use for several years since the final parts were released in 2000. Although written from the perspective of a bespoke system, it is more commonly used to certify products for a given SIL level. Valid product certification schemes must involve the assessment of specific product design details as well as an assessment of the safety management system of the product manufacturer and the personnel competency of those professionals involved in the product creation.

A proper assessment of a product must completely cover all the requirements of the IEC 61508 standard including the safety management system and build a safety case. The safety case must list each requirement, an argument as to how the product design or its creation process meets the requirement and the necessary evidence to provide reasonable credibility for the argument. This safety case must be available for inspection. Although the safety case typically contains manufacturer proprietary information, those who wish to review the full safety case should be able to do so, perhaps under confidentiality agreement. In addition, an open IEC 61508 certification must include a public certification report that provides an overview of the assessment and the product limitations, if any.

This paper describes an assessment technique for product designs and the product development process that produces a full safety case as well as additional public documentation. This “open certification” method has been used in dozens of instances on product design process. The assessment experiences to date show that most of the problems with conventional methods are solved or at least improved.

Introduction
The functional safety standard, IEC 61508, has existed for several years. This standard is written in the context of a bespoke (custom made, turnkey) system. Therefore it provides requirements for a full safety lifecycle including hazard and risk assessment as well as operations and maintenance. The IEC 61508 standard provides functional safety requirements, requirements to help a system either work properly or fail in a predictable manner. These requirements can be used for many different types of systems including those with mechanical, electrical, electronic and programmable electronic components. Requirements cover general safety management systems, specific product design requirements and design process requirements. The requirements provide coverage for both random hardware failures and systematic design faults.

A set of experience has been building on how to use this standard to design standard products that can be certified compliant to a particular SIL capability level [FAL03]. Product certification involves the assessment of specific product design details and also involves, even to a greater extent, an assessment of the safety management system of the product manufacturer and the personnel competency of those professionals involved in the product creation.

Product Certification
Functional safety product certification started with Logic Solvers (Safety PLCs) more than ten years ago. Originally product certifications were done to VDE0801 (VDE0801 A1), a German National Standard. Certifications were done on field instrumentation devices in the 1990’s when Moore Products Co. got a pressure transmitter (Model 345) certified. When IEC 61508 became ratified by the European Union, it replaced VDE0801 as the standard for product functional safety certification after a period of time.

Historically most certifications were done by one of the German companies collectively known as TÜV. The name TÜV is an abbreviation for “Technische Überwachungs Verein” which translates to “Technical Supervision Group.” Although it appears as if only one TÜV company exists, it must be understood that there is more than one privately held company in Germany called “TÜV.” At one time there were several different companies all using a variation of the TÜV name. Names that were once prominent in the market include TÜV Product Service, RWTÜV, TÜViT and others. Several mergers and name changes have taken place and there are now only three TÜV companies doing instrumentation product functional safety certification from Germany; TÜV Rheinland (www.tuv.com), TÜV Sud (www.tuvglobal.com) and TÜV Nord (www.tuevnord.de).

The conventional process for a functional safety assessment involves contracting an expert to review documentation and visit the manufacturer one or more times to interview product designers and run tests, primarily fault injection tests. The expert assessor will often follow a guideline (or other internal quality document) to help determine which questions to ask and what items to test. The quality of the assessment depends highly on the skill and knowledge of the assessor.

The Safety Case Methodology

The Safety Case methodology provides a systematic and complete way to show compliance to one or more standards. The methodology was established in industries which deal with functional safety of computerized automation in nuclear and avionics [DEF97, BIS98].

For each standard considered, all requirements from that standard are compiled. Each requirement is precisely documented along with the reasoning behind the requirement. This helps to make the requirement understandable. The safety case method structures the requirements (parent / child) and in some cases combines like requirements. “Arguments / Solutions” provide a description of how each requirement is met by listing design arguments, verification activities and test cases relevant to that requirement. For full traceability, each design argument and verification / test activity is linked with evidence documents showing the results of the work (Figure 1).

Requirement – IEC 61508, Part 3: (S/W) Safety requirements verification shall check for incompatibility between: - System safety requirements; - S/W safety requirements; - (S/W) safety validation planning.
Argument: The SIRS is peer reviewed where incompatibility is checked. This is specified in DOP 416, 4.2.3.2, item 15.
Evidence: DOP416 SIS Product Design and Development Process
Assessment: DOP 416 was examined. Developers were interviewed and they stated this was done. Minutes of the peer review meeting were stored in the project archives with version number.

Figure 1: Requirement-Argument-Evidence and Assessment relationship.

When a safety case for IEC 61508 compliance of a product is completed it must show all requirements along with an argument for each requirement as to how the product meets the requirement. A link to the evidence document that supports the argument (Figure 2) is also provided. An additional field is provided for the independent assessor to record the results of the assessment.

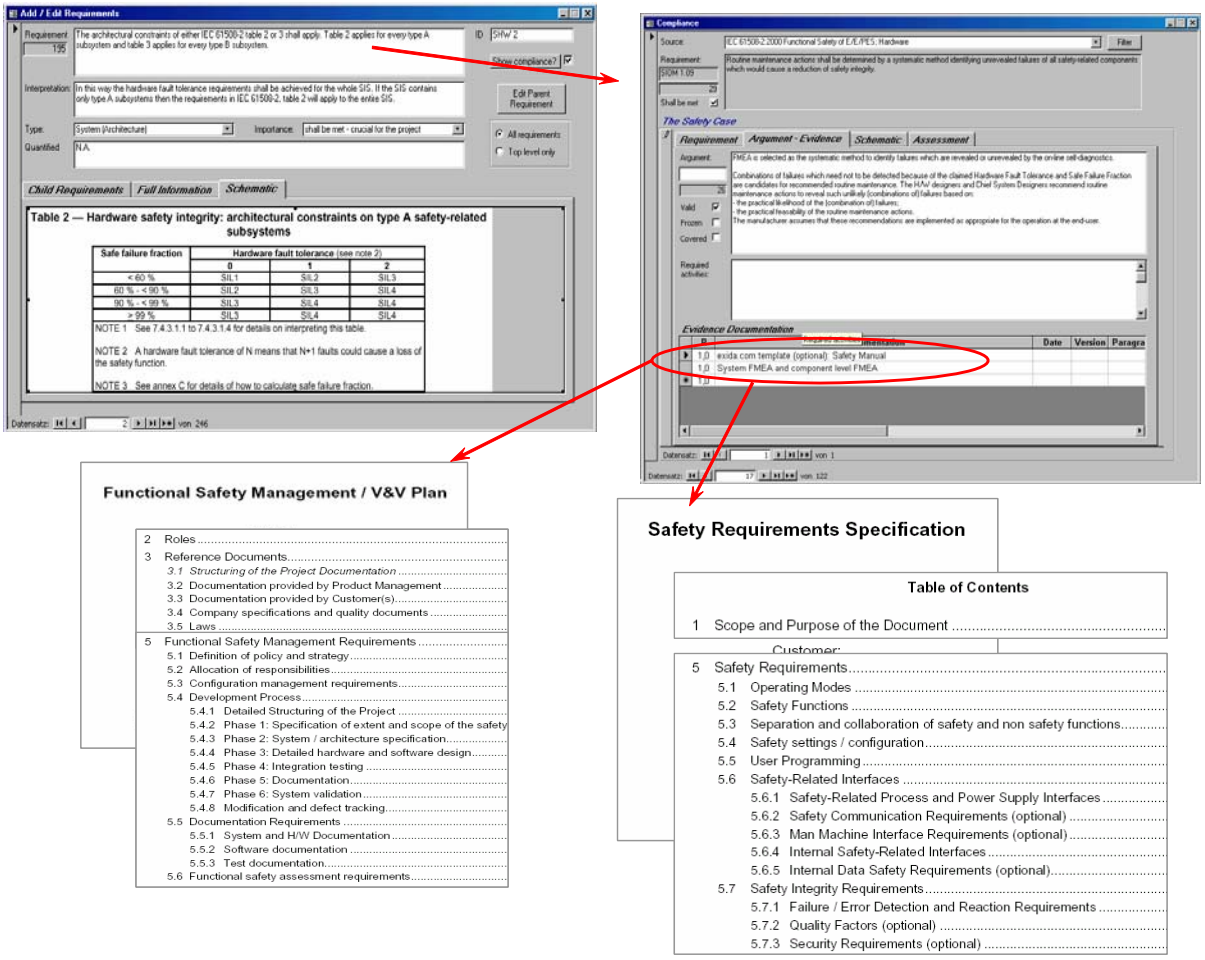

Figure 2: Linkage between argument and supporting evidence documents.

Overall, the safety case concept provides a single place to store compliance information in an organized manner. The use of a safety case provides a systematic means to ensure completeness of any assessment. The Safety Case method supports company learning over multiple projects by establishing a knowledge base consisting of patterns of fundamental requirements and related design arguments. Templates and previous examples of evidence documents provide the ability to reduce effort on subsequent projects.

Note: The term “Safety Case” is being used beyond its original definition [DEF97] in the context of product certification to IEC 61508 and is based on concepts presented and developed earlier [BIS98, WEA03].

The Open Certification Assessment Process

A typical assessment (Figure 3) begins with a complete review of the written functional safety management system (SMS). The SMS should consist of a document or set of documents that describe the process by which a new safety product is to be developed or modified. The information contained should include all design steps (inputs required, processes to be performed and outputs required), all verification activities, personnel responsibilities and all project documentation generated.

Product design documents are reviewed next. The documents supplied should match those required in the functional safety management plan. Evidence that the required verification activities have been done should also be included. Competency records must be in place and show that those assigned to the project were competent to perform their specific tasks. When the initial paper review is complete, the assessment continues with detailed on-site meetings.

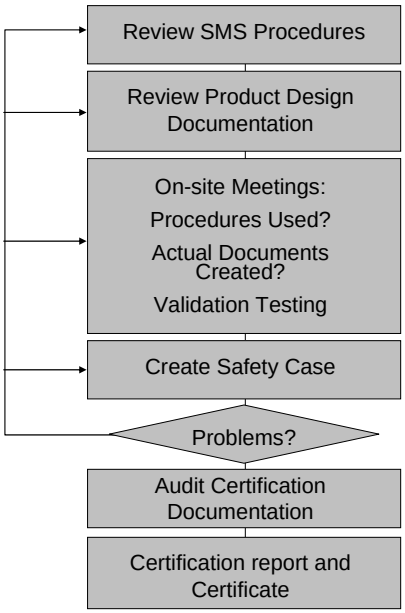

Figure 3: Assessment procedure.

When all relevant documents are reviewed, interviews with the responsible personnel must take place. This is done by visiting the development and manufacturing control site(s). One of the key interview questions is "What process was followed in the design of this project?" It is surprising how often the answer varies from the process described in the 'official" procedures. Any discrepancies must be justified and documented. This is often done in a "project work plan" or "project specific functional safety management plan". The site visit must also include witnessed validation testing often including specific fault injection tests.

If all documentation for both the process and the product are complete and seem fit, a safety case document is created. This step provides a systematic method to ensure that no requirements of the standard(s) are missed. Often missing requirements are identified and the assessment must return to a previous step to correct the problem. When the safety case is judged to be accurate and complete, the certification report describing all assessment activities and their results is written. The documentation is given to an independent auditor to verify. When the audit is complete, the certificate is issued.

Problems

Problems - assessors

In spite of the fact that IEC 61508 is one of the most detailed and useful standards in the functional safety field, there are always issues of different interpretation between assessors. A significant number of additional issues exist when using the IEC 61508 standard to certify standard products meant for multiple applications. Some of the most significant of these issues include:

- the interpretation of which requirements apply to standard products versus bespoke systems,
- the interpretation of which requirements apply to complex logic solvers with multiple computer communications networks versus a simple programmable device or simple electronic device without any programming,
- the interpretation of which requirements apply to mechanical products (if the standard applies at all) and
- the interpretation of which methods and solution combinations apply to which SIL level.

In the first few years of experience with IEC 61508, it is clear from reading existing product certification reports that different assessors have made those interpretations quite differently.

The IEC 61508 standard was appropriately written from the perspective of a bespoke system. As such there are requirements for a full safety lifecycle compliment of activities including hazard and risk analysis through on-going operations and maintenance. Some of these requirements do not apply to a standard product designed to be used as a component in a bespoke system. When performing a certification assessment for a product the question must be answered “Which requirements do not apply”?

The safety management system required for a complex computer based device must be quite comprehensive and rigorous given the risk of systematic design faults in such products. However since this risk is considered lower in simple devices, do the same requirements apply? The safety management system should match the risk of a design fault. What are the requirements of a safety management system for a simple mechanical device like a solenoid valve? Simple mechanical products have apparently been certified only on the basis of “cycle test”. Is this sufficient?

Problems – product manufacturers

Experience in product certification projects has shown that the safety management system of a product manufacturer is likely to be the biggest area of non-compliance in an assessment to IEC 61508. The main problems are:

- Lack of sufficient detail in product design (functional safety management) procedures,
- Missing steps in product design procedures,
- Designers not following procedures,
- Personnel competency records and
- Lack of documented verification activities.

Even in the case of a simple mechanical product, assessment experience has shown that design omissions (systematic errors) exist. Some examples include cases where the product functional specifications were written from the perspective of continuous control and the constant cycling of discrete manufacturing. When the same product was used in a low demand safety related system, the design weaknesses surfaced. This example also points out the importance of personnel competency. Those designing products to be used in safety related systems must have an understanding of the application and its environment.

Problems – end users

Those who purchase IEC 61508 products are also having problems with the methods in use today. The most common problem is lack of visibility into the certification process. Some end users want higher visibility so that they can determine the scope of the certification effort and make sure it applies to their specific application. End users also want to completely understand any restrictions and limitations. In one case, the certification depended heavily on end user programming and that was not made clear in the certification report.

Experiences with Open Certification using a Safety Case

An open certification scheme has been proposed and is being used to help solve many of the problems listed above. Overall, experiences to date indicate that this approach is preferred over existing methods.

Which requirements apply?

One potential solution to the issue of assessor interpretation is an open certification scheme based on a detailed safety case. Consider a simple mechanical device. Given that a manufacturer would like to have this product certified to applicable requirements of IEC 61508, a full safety case showing all requirements of the standard can be produced. For any requirement not applicable to a mechanical product, the argument is simply “not applicable” with a justification for that statement. The value in this is the statement is the justification. It is clear what requirements were considered and which requirements were not considered. These declarations provide clear examples of interpretation and allow for open debate if anyone disagrees with an interpretation.

A complete SMS

It is almost impossible for an assessor to remember all requirements of IEC 61508. The use of the safety case in effect provides a checklist of all requirements that must be met and assures a more thorough assessment. This is important because it forces the assessor to review the product design procedures in sufficient detail. The safety case provides all requirements and rational behind each requirement. When the assessor finds something missing, it is easier to explain what is missing and why it is needed. When an explanation is made clear, it is more likely the product manufacturer will upgrade the procedures and that the designers will actually follow the procedures.

Documentation

The documentation produced by an open certification scheme using a safety case consists of the safety case report, a certification report which summarizes the effort and a certificate. The safety case report is quite detailed and actually provides all information listed above. Some end users want to review this and some manufacturers provide the report on a confidential basis. This provides full visibility into the certification effort. The certification report is a summary of that effort and usually provides enough information for most end users.

As part of the certification effort, the manufacturer is required to produce a “safety manual” which lists all restrictions and limitations of the certification. While the need to produce a safety manual is not new, the items in that manual now come from the safety case and include:
Failure rate data or an alternative means to perform probabilistic SIL calculations,
Proof test recommendations,
Proof test effectiveness,
Maintenance procedures,
And other items rarely addressed by manufacturers.
This more comprehensive document has been welcomed by many end users.

Conclusions

An open certification scheme based on a safety case will help manufacturers design products with better safety integrity because important requirements of the standard are less likely to be missed in an assessment. The safety case explanations have been used to more rapidly convince manufacturers of the need and value of IEC 61508 requirements. Personnel are more likely to get proper training and competency records are more likely to be kept and audited. The open scheme will help resolve issues of interpretation by providing clear examples that can be debated if disagreement exists. An open scheme based on the use of a safety case will ensure that all needed documents are prepared.

An open certification scheme will help end users by providing clear visabililty into the certification effort. A prospective customer can read the certification and see what level of assessment has been done. Those that wish may dig further and upon permission of the vendor review the entire safety case document.

The primary disadvantage of the safety case approach is a higher initial cost for a manufacturer for the first project. Subsequent projects will benefit from any existing work and the overall cost for several projects should be lower when compared to conventional assessment techniques.

References

[DEF97] Defence Standard 00 – 55, Parts 1 and 2, Issue 2, August 1997, U.K. Ministry of Defence.

[BIS98] Peter G. Bishop and Robin E. Bloomfield, "A Methodology for Safety Case Development", in Safety-Critical Systems Symposium, Birmingham, UK, February 1998. http://citeseer.ist.psu.edu/bishop98methodology.html

[WEA03] Robert Andrew Weaver, “The Safety of Software – Constructing and Assuring Arguments”, Department of Computer Science, University of York, U.K., September 2003. http://www.cs.york.ac.uk/ftpdir/reports/YCST-2004-01.pdf

[FAL03] Rainer Faller, “Project Experience with IEC 61508 and its Consequences,” Proceedings of SALFECOMP 2003, available on www.exida.com/company/articles.asp