Certification for the IEC61508 group of standards put into perspective.

Clive de Salis, The 61508 Association

Keywords: IEC61508 certificate, Functional Safety Management, IEC61511 certificate, SIL

Safety instrumented systems designed to meet the specified Safety Integrity Level ("SIL") are now an established part of safety for process plants. These safety instrumented systems are covered by the IEC 61508 group of standards. IEC 61508 is the master standard and, for the process industries, IEC 61511 is the application standard. IEC61508 is now a European norm and so, in the UK, it is designated as BS EN 61508. The same adoption has occurred for IEC 61511.

Certification of products has become an established part of the safety instrumented systems industry. Now there is pressure for certified "experts". So if we use certified equipment, is the warm, comfortable feeling of having placed all the certificates in the project folder justified or is it worth taking a second look at the contents? The design, the analysis and decisions for all the conventional layers of protection for chemical plants and process plants are the "bread and butter" of chemical engineers. It is those layers of protection that form the basis of any decision to have a SIL rated safety instrumented system to complete the safety strategy. If chemical engineers are the lead figures in the decisions on layers of protection then why is it that some businesses are asking for "Certified Expert" Instrument loop designers to do this work? Current available courses for "Certified Experts" for safety instrument systems provide the expertise to design the safety loop to do the job. An "expert" on designing the instrument loop is not the same as a chemical engineer examining all the other layers of protection to see if a safety instrument loop is even needed.

Certification used properly can be a benefit but certification used wrongly can seriously impair safety. Would it surprise you to know that there is no requirement for certified devices, or for certified people, in the standard? For almost all serious process safety accidents the common cause is people and safety management. Functional Safety Management is mandatory under IEC61508 2nd edition whereas certified devices and experts don't appear anywhere in the standards. Are we putting our efforts into the right place?

Certification for the standard began in Germany and, in the case of the IEC61508 group of standards, has proved to be noticeably misleading. Some of the TUV certification bodies issued SIL certificates for transmitters, devices and other individual instruments. This was misleading because there has never, ever been a SIL rating for a component in the standards: The SIL rating is the SIL for the whole instrument loop, not for any individual part. The SIL number corresponds to the Probability of Failure on Demand (PFD) for the instrument loop. The "demand" is the moment when the safety loop has to act to keep you safe. If we assess the risk and decide that we need an additional risk reduction of more than a factor of 10 then we apply a SIL 1 safety loop. If the risk reduction required is more than a factor of 100, i.e. 10 to the power of 2, then a SIL 2 safety loop is required. If the risk reduction needed is more than 1000, i.e. 10 to the power of 3, then a SIL 3 safety loop is needed … and so on. The SIL number indicates the order of magnitude risk reduction required. Therefore, at the moment the safety instrumented loop has to act to keep you safe the probability of failure on demand ("PFD") needs to be the inverse of the required risk reduction. To put it in layman's terms: For SIL 1 the chance of failure has to be less than 10% (PFD=0.1). For SIL 2, the chance of failure must be less than 1% (PFD=0.01). For SIL 3 the chance of failure has to be less than 0.1% (PFD=0.001) … and so on. That probability of failure has to refer to the whole instrument loop. It is no use having an incredibly high reliability PLC connected to a valve that you know is going to be stuck open every time you need it to work and every time that you go and test it. The allegedly "SIL 3" PLC has misled people into thinking that the loop is SIL 3. That is not how it works and so giving SIL certificates to individual components was always misleading.

Certification of instruments was also misleading because it implies that if you put the ten instruments and devices together, each of which has a "SIL 2 certificate", to make your complete safety instrumented system, then the loop should be SIL 2 …. But it isn't. It's more likely to be SIL 1. Any one of the ten devices could fail and if each device PFD is 0.01 (i.e. allegedly "SIL 2"), and I have 10 of them, then the PFD for the whole loop is 0.1, i.e. SIL 1. I have written this in simplistic terms to explain the principle but please bear in mind that most instrument loops do have ten or more components. Thus the actual probability of failure on demand of the loop and its achieved SIL depends heavily upon the design and architecture of the loop and not just upon the reliability of each of the individual components.

So the "SIL certified" claim is misleading the user. Those of us on the committees that writes IEC61508 and IEC61511, the author included, have responded to these uninvited SIL certificates by requiring a change of language to "Systematic Capability" or SC instead of the incorrectly used SIL language[1]. We are trying to get users to understand that the claim of a SIL certified component is meaningless. The user has to use the device in the correct configuration and within a suitable architecture to achieve the desired SIL. Even if this is done, the user must examine the claims made and see if their own application matches that for which the test data shown in the report is applicable.[2] The IEC61508 group of standards require that safety data is applicable to the user's actual application.

---

1 IEC 61508: 2010, Part 4, definitions:

Section 3.5.8 states:

Safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

Section 3.5.9 states:

Systematic capability measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

2 See IEC 61508: 2010, Part 2

The only way of checking that the equipment is suitable for use is to have the certified report. The report has value because it is certified by a third party. The report enables us to check that the claims made and the way in which the component is used are appropriate to the application. Without the report a SIL certificate is utterly useless. Any company that refuses to supply a copy of the report and only submits a certificate is putting the user in an impossible situation. Their equipment cannot be used.

A few years ago, with a previous employer, the author was involved in a project which was being undertaken by several contractors working together. The different parties were developing the design for an oil terminal. One of the parties wanted to use a particular "SIL 2 certified" PLC. The safety manual for the PLC shows that the basis of the claim and the basis of all the reliability data assumes that the PLC is being used for 16 hours per day, 5 days per week, 52 weeks per year. Of course the oil terminal needs to operate 24 hours per day, 7 days per week, 365 days per year. So there was no useable safety and reliability data for this product and yet the top management was angrily saying that the PLC has a SIL 2 certificate and the author should stop putting obstacles in the way of using it. To make matters worse the product claimed compliance with IEC 61511 and yet it was using assumptions based upon factory-returns. Factory returns are outside the scope of IEC 61511. The certificate was completely misleading the other contractors in the project. A device certified for 16 hours per day, 5 days per week is one designed for use in a machine-workshop, or similar duty, in which the user is expect to turn the lights out when they go home at the weekend. Therefore it does not follow that the same reliability is achieved when the device is used 24/7/365 in a refinery application. The SIL 2 claim might be valid for a machine-workshop but had no validity for an oil terminal.

IEC61508, and particularly the process industry application of it in IEC61511 has become the accepted standard for high integrity safety instrumented systems. However, the majority of industry is still naively asking for certification that the standard does not require, and has never needed, whilst ignoring its basic essentials. How long can this really go on for? Far too many companies specify in their enquiry that SIL certificates for the components are required and that certified experts should be employed. They fail to ask for either the safety manuals or reports that contain the data, and also fail to ask for proof of functional safety management. What is most deeply regrettable about this state of affairs is that neither of the former appear anywhere in the standard and both of the latter are basic fundamental requirements.

The standard never asked for certificates. PLCs are so complex that they are a good example of a device where third party certification is at its most useful, but let us get the emphasis right: we must have the report that goes with the certificate. A certificate without a report is a total waste of paper. The user needs the report. PLCs are so complex that a comprehensive report is a really important item to ask for and when it is backed by a third party then that is great. We don't actually need the certificate, what we need is the report. So why is it that many of the companies that get a certificate for their product then refuse to release the reports? They claim things like proprietary or commercially confidential information is in the report. This claim is heard for all sorts of products from valves and transmitters to PLCs. The report issued by the certification body is the property of the certification body's customer: The product manufacturer. Therefore the product manufacturers are able to release the report. Yet some withhold it. Is that reasonable? No. Let's be completely clear: The standards require evidence of the reliability of the loop for your application. If you don't have the safety and reliability data then you can't use the product because you don't have the evidence, and at that point it doesn't matter what the certificate says, or how many badges are on it, or how pretty the certificate looks. Without the safety and reliability data you cannot use the product. It is the data that is the absolutely essential part required by the standard. The designer is helpless without the reliability data and the evidence that the data is useable in their application. The promotion of certificates as being valuable and important has encouraged purchasers to ask for certification which is not required by the standard, whilst failing to ask for the safety and reliability data that is required by the standard.

The dangerous impact of this false requirement for certificates doesn't just stop there. A package plant

was supplied in the UK where certificates were delivered for the transmitters and the safety PLC, but no information was delivered showing the reliability of the total loop, its proof-testing requirements, use of diagnostics or any other important requirements of a safety loop. Nonetheless, at every level of the company they thought the certificates meant they had an approved safety system with the package. When the "SIL 2 certified" transmitter failed, the instrument engineer found another "SIL 2 certified" transmitter in stores from a different manufacturer. He replaced the failed unit and carried on until the visit of the safety inspector who asked the instrument engineer how he had adjusted the proof test interval to suit the change of transmitter. This was a completely new and baffling question for the instrument engineer, who thought he had simply done the sensible thing of swapping one "approved" transmitter for another. Of course reliability is a function of testing and maintenance as well as design. Therefore, the testing and maintenance plan for a safety loop is an essential. In this case the certificates had completely misled everyone involved into thinking that what they had was safe. And, sadly, it is not an isolated example.

The latest fashionable trend is to ask for a certified expert; yet again the standard never mentions certified experts anywhere, but it does demand functional safety management. This is dragging us gently by the nose towards the idea that if the project uses a certified expert then everything is OK. The standard requires functional safety management of everyone: not just the expert, not just the technician, but everyone (even including purchasing department). To have a certified expert and to fail to have functional safety management is to absolutely fail to comply with the standard. It is no use having a system designed by an expert based upon a SIL determination exercise undertaken by 'the misguided', and installed in a panel assembled by 'the foolish' that was tested and commissioned by 'the idiotic'. The "Safety Expert" Certificate of the one person in the chain is never proof that the rest of the people involved were also competent. Functional Safety Management is required to confirm that all people involved are competent at their tasks.

Section 7.4.10.2 states:

The documentary evidence required by 7.4.10.1 shall demonstrate that:

a) the previous conditions of use (see Note 1) of the specific element are the same as, or sufficiently close to, those that will be experienced by the element in the E/E/PE safety related system;

NOTE 1 The conditions of use (operational profile) include all the factors that may trigger systematic faults in the hardware and software of the element. For example environment, modes of use, functions performed, configuration, interfaces to other systems, operating system, translator, human factors. Rigorous conditions for similarity of operational profile may be found in IEC 61784-3.

Of course, it may well be right, having put the functional safety management in place, to find that the use of one of the certified expert courses is appropriate to meet the training needs of one of the people in the team ... but that decision arises out of functional safety management, it is not a replacement or substitute for functional safety management. The emphasis must be right: the standard requires functional safety management; the standard does NOT require a certified safety expert (see IEC61508 Part 1 clause 6 and the matching requirement exists in all the sector guidance standards – e.g. IEC61511 Part 1 clause 5).

The current certified safety expert exams concentrate on the design of safety instrumented systems and so they do not produce expertise on other areas such as SIL assessment (although the courses do partially cover the subject). However course titles like "certified safety expert" make far too many contractors and end-users assume that they are expert at everything. So, yet again, this approach is presently undermining safety and it just further reveals that the contractors and end-users have failed to put in place functional safety management.

The design, the analysis and decisions for all the conventional layers of protection for chemical plants and process plants are the "bread and butter" of chemical engineers. It is those layers of protection that form the basis of any decision to have a SIL rated safety instrumented system with which to complete the safety strategy. If chemical engineers are the lead figures in the decisions on layers of protection then why is it that some businesses are asking for "Certified Expert" Instrument loop designers to do this work?

Chemical engineers are competent to design process plant with appropriate layers of safety such as relief valves, safety trips, quench systems, inert atmospheres, bursting discs, bunds, flares etc. There is no requirement in either IEC61508 or in IEC61511 for certification. We do not need certified experts as much as we need competence for all people involved in the design from SIL assessment through to design, build and implementation. The I.Chem.E Safety & Loss Prevention group has been working on a core-curriculum to decide what an engineer undertaking a SIL determination exercise on a process plant needs to know. Training is available through a wide variety of companies for each of the competencies needed for good SIL assessment and the I.Chem.E is happy to provide supporting information to guide people through course selection.

Of course, one of the profound ironies of all the certification industry is that the same companies that promote the certificates they produce and the experts they certify also claim to be the leading experts in IEC61508 and its sector guidance standards. That claim will only gain genuine integrity when the report is promoted by those companies as being the essential requirement for the customer and the certificate as optional, and when they promote functional safety management as being the essential requirement of the standard and the certified experts as optional. In other words, the claim that such certification companies are the leading centre of expertise in IEC61508 is a hollow claim as long as their foremost promotions are certificates and experts when neither are required by the standard.

If safety is to be real then we must promote functional safety management. This must be top of the certification companies' agenda and not simply some lesser known offering. Contractors and end-users must require functional safety management from their suppliers and of themselves.

In August the HSE published their new guidance "Managing Competence for safety-related systems" that has significant implications for all process plant with safety critical trips and shutdown systems. The guidance is available from the HSE website and can be freely downloaded (http://www.hse.gov.uk/humanfactors/comah/competence.htm)

If you have a critical safety trip you surely want to know that the people who designed it, those who installed it, those who are doing the maintenance and testing of it are all competent to do so. Your safety depends on it so you'd want to know that wouldn't you?

IEC61508 and the process industry guidance standard IEC61511 have titles that make them sound like its the instrument engineers' problem but it is actually us chemical engineers. We have responsibility for defining what is safety related for four out of the seven layers of protection so it is us chemical engineers who take the lead role in the assessment of the safety integrity level (SIL) for each safety related trip.

The seven layers of protection can be summarised as: 1) The process itself, 2) the design operating parameters (i.e. chemical inventory, design pressures and temperatures etc), 3) the mechanical design of vessels and pipework for containment, 4) the process control, 5) the passive protection systems and devices (equipment that will operate irrespective of power or air, e.g. relief valves) and 6) the powered safety systems (this layer includes the safety instrumented systems). The seventh layer is the emergency responses that work to minimise the impact of the unwanted event. Chemical engineers are involved heavily with layers 1, 2, 4, 5 and 6. They are also involved with layer 3. Therefore this subject of getting all the layers of protection right and avoiding unnecessary reliance upon SIL rated safety loops is of key importance to chemical engineers.

Since we have the lead role in the SIL assessment process, the HSE's new guidance for managing competency applies to us. The guidelines require us to assess the competency of our suppliers, contractors and sub-contractors. As a director of the first chemical engineering business in the UK to gain certification under the UKAS accredited scheme that covers competency management for safety systems, the author had a real insight into what is involved.

IEC61508 allows you to assess the risk of an unwanted event and evaluate the gap between that risk and your corporate tolerable target. The reliability demanded of the safety trip is proportional to that gap. The larger the gap, the more reliable the safety trip is required to be. If the gap is less than a factor of 10 then no SIL (Safety Integrity Level) is required but the HSE competency guidelines still apply as it has been carefully written to apply to everything safety-related. After all, it naturally follows that the existence of that gap means your safety depends on that trip. So it would become indefensible if you should have such trips designed, built, installed and maintained by people who are not properly competent to do so. Proper competency management is a completely reasonable requirement.

The real problems start to arise when you consider what the management of competency for safety critical systems actually requires. The HSE guidance for example does require that you assess the competency of all your suppliers and subcontractors. It even goes so far as to say that you should assess the competence of your suppliers' and subcontractors' suppliers and subcontractors. Further it says

that if any of your suppliers and subcontractors come under new ownership or new management you should reassess their competency management. It starts to get potentially onerous doesn't it?

There is a natural connection between the HSE guidance and the international master standard IEC61508 and its sector guidance standards such as IEC61511. The funny thing is that elsewhere in Europe we have this peculiar market that has been created for certificates. The IEC61508 group of standards do not require, and have never required, certificates and yet that phoney market in certificates has been very successful. This market in certificates has created the completely bizarre situation that purchasers are often asking for certificates without asking for the reports. It is amazing how often people ask for a certified PLC (probably the most reliable part of the loop), overlooking the proper questions about the reliability of the transmitter or the valve (the least reliable end of the loop) and completely overlooking certification, auditing and proper competence of the people who are by far the most likely source of error and failure. We have got ourselves into a situation where all too often we ask for certification for the most reliable part and completely ignore the least reliable part: The people and management. You can, as mentioned above, now get a "certified expert" and they are popular in the USA. The expert has passed an exam but this only leads us to the ridiculous scenario that you can have a misguided team specifying SIL, and, consequently, a loop designed by a "certified expert", built by an idiot, installed by a fool and maintained by a moron. What is clearly lacking is the managing of competence for the whole team of people involved and it is this that the HSE guidance is aiming to tackle. Competency management is for <u>everyone</u> involved in the safety loop, not just one or two individuals.

Competency is by no means just the requirement for the loop designer. The whole process begins with a team assessment for what safety integrity is required (this is usually referred to as the SIL assessment). The methodology applied should properly assess the risk and the team should be competent to make the assessment. Then there is the writing of the specification for the safety loop – you need competent people for that. Only then do we arrive at the competency of the loop designer. With the design in place you need competent people to build it, to test it, to document both the design and all the procedures and create the design file for the user. But competency hasn't stopped there. You now require competent people to install it on site, to do the system test and initiate the proof testing. You need competent people to maintain it, to manage any non-conformances and you actually also need competent people to operate it. Competency is a holistic requirement that covers everyone and not just an individual.

The existence of a "certified expert" does NOT prove that you comply with the requirement for competency management. Indeed for your purchasing department to ask for a certified expert and think that is enough is a serious mistake. Your specification must ask for proof of "Functional Safety Management" to IEC61508 Part 1 Clause 6. That is what the standard requires. The certified expert doesn't even exist in the standard. If certified expert is needed as a qualification for your loop designer then that will have been identified by the competency management scheme that IS required by the standard and is covered under IEC61508 Part 1 clause 6 (IEC61511 has the matching requirement under Part 1 clause 5).

For businesses, the disconcerting side to competency management, will be managing suppliers and sub-contractors and their supply chain. This is where management systems that have third party accreditation have their place. Here in the UK, there is a free UKAS-accredited scheme for functional safety management such that whatever you negotiate with the certification body for its costs is up to you. It is called CASS which stands for Conformity Assessment of Safety Systems. There is a free downloadable functional safety management declaration. It is downloadable in standard office-software formats. At Murco, we use it to ask our suppliers and those involved in a project to document their functional safety management. We are happy to accept third party certification appropriate for the scope of work, but the standard doesn't require certification and so we are equally happy for a company to use the free downloadable form to make a declaration of their functional safety management. Thus we avoid unnecessary and unjustifiable barriers.

Since the CASS declaration form is free to use there is no barrier to good functional safety management. Therefore, let's not put up false claims about cost as an obstacle to functional safety management. Too many companies have been fooled into spending large sums of money on things that the standard does NOT require, like certificates and experts, whilst they have failed to invest in what the standard DOES require: functional safety management - IEC61508 Part 1 clause 6 / IEC61511 Part 1 clause 5.