IEC 61508 PRODUCT APPROVALS – VEERING OFF COURSE

Angela E. Summers, P.E., PhD, President, SIS-TECH Solutions, LP

Published on-line: "IEC 61508 Product Approvals–Veering off Course," ControlGlobal.com, July 2008.
http://www.controlglobal.com/articles/2008/187.html

Upon close examination it appears that the product approval process of IEC 61508 (1) has veered seriously off-course, possibly rendering many Safety Instrumented System (SIS) applications less reliable than expected or required.

Following a careful review of a significant variety of product safety manuals, it appears that many field devices are achieving higher safety integrity level (SIL) claims than can be supported by process industry data. Appendix F.1.3 of CCPS Guidelines for Safe and Reliable Instrumented Protective Systems (2) states that 'a sampling of data for pressure transmitters from various manufacturers report theoretical mean time to failure dangerous ($MTTF^D$) values that are three to ten times better than owner/operator prior use data.' – a claim that some manufacturers (3) have openly validated.

Unfortunately, changes now being considered by the IEC 61508 committee will not likely improve the situation. It appears that the committee is intent on piling on additional requirements, instead of addressing serious structural weaknesses. The only sensible option is for users to take control of this situation by refusing to install any field device in a safety application that has not demonstrated its required integrity and reliability in a similar non-safety operating environment. Users should demand that manufacturers stop making exaggerated performance claims, manipulating the safe failure fraction (SFF), and shifting responsibility for safe operation to the production operator when products behave unreliably. Users must also demand that safety manuals provide complete proof test procedures that achieve compliance with IEC 61511 (5) and OSHA process safety management (PSM, 6) requirements.

The following sections highlight a few of the issues associated with safety manuals and their performance claims.

Exaggerated performance claims

Prior to the release of IEC 61508, many manufacturers provided in-service and accelerated test failure data. Following the approval of IEC 61508, manufacturers increasingly began claiming compliance based on a shelf-state analysis with seemingly perfect operating environment conditions. IEC 61508 allows manufacturers to make SIL claims based on predictive analysis without any burden of later substantiating the claims using actual field data, so technically manufacturers are not doing anything wrong. However, the theoretical dangerous failure rate, safe failure rate, and probability of failure on demand (PFD) values declared in analysis reports are much better than can be achieved in actual field applications. The gap between the theoretical analysis and real world performance is egregious and pervasive.

With rare exception, these analysis reports do not provide enough information to fully illuminate the disparity between manufacturer's claims and user experience – exactly the point being made by Thomas et al. (4) in stating 'quality and consistency in safety manuals is lacking.' The analysis reports do not provide a boundary description, installation and configuration assumptions, or a failure modes and distribution listing. Instead the reports provide a summary table of the failure class distribution. The issue this raises is that while failure modes and effects are product-related and can be independently evaluated by the manufacturer, the failure classification is application-dependent.

There are many ways that a field device can be installed and configured, making the failure classification difficult for manufacturers, especially for commodity products. A manufacturer cannot properly assess whether a failure should be classified as safe or dangerous without first acquiring knowledge of the intended application.

For example, in a typical demand mode operation where a solenoid operated valve controls the pneumatic supply to a valve actuator, solenoid coil burn-out is safe in a de-energize-to-trip application and is dangerous in an energize-to-trip application. All failures of the solenoid operated valve are likely dangerous in a continuous mode application.

Users should be provided with the failure modes and effects results, not just a failure classification summary. Armed with this information, the user can then classify the failures according to their intended application and calculate an application-specific PFD and spurious trip rate.

Most reports do not clearly define the analysis boundary or describe what is included or excluded from the analysis. For a variety of reasons, many in-service failures are excluded from the product analysis reports. Some failures are deemed to occur due to product 'wear out' and excluded from the useful life analysis. Operating environment impacts, such as plugging, corrosion, and electrical interference, are considered application issues that are the user's responsibility to analyze and estimate. The restricted view of the product and its environment is a significant source of disparity between the theoretical analysis and real-world performance, but it is not the only problem.

Excessive diagnostic coverage claims are routinely made on programmable electronic field devices. Claims in excess of 90% are very common even with the restricted boundary and operating environment assumptions. A high diagnostic coverage translates directly into a high SIL Claim Limit and low reported PFD. That makes sense when the credited diagnostic actually yields safer operation and is periodically proven to work – the same rule applied to any safety device. Diagnostics must be verifiable and auditable.

Unfortunately, many manufacturer- supplied diagnostics are not capable of being tested in compliance with IEC 61511 Clauses 11.3 – Requirements for system behavior on detection of a fault – and 16.3.1.1 – periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the safety requirements specification. Additionally, analysis reports do not include information on the product's integrity, if the diagnostics are not configured per the safety manual or fail during operation.

The safety manual should clearly describe the analysis boundary and the assumptions with regard to installation, commissioning, configuration, diagnostics, maintenance, and testing that support the SIL claim. Without such information, it is very difficult for users to comply with IEC 61511 Clause 5.2.5.3 –

Procedures shall be implemented to evaluate the performance of the safety instrumented system against its safety requirements – which requires a comparison of equipment reliability assumptions with field operating performance. Identified failure modes and effects should be included in the maintenance troubleshooting guide in order for in-service failures to be tracked using the same modes, thereby allowing users to periodically compare their actual operating results against manufacturer's claims.

Manipulation of safe failure fraction

The IEC 61508 committee included the safe failure fraction (SFF) and associated hardware fault tolerance requirements as a way of preventing manufacturers from claiming high SILs for non-redundant devices simply based on the PFD calculation. The SFF tables were intended to ensure fault tolerance (through required redundancy) in an environment of optimistic theoretical data. However, because the SFF is calculated from the same potentially 'bad' data, the SFF is susceptible to the same error.

In practice, there is no correlation between SFF and product safety. The inverse is being demonstrated in the product approval process where it has become easier to certify a high total failure device with a high diagnostic coverage claim to SIL 3 than it is to certify one with a low total failure rate but no diagnostics.

While reviewing the various safety manuals, it became obvious that manipulation of the SFF is quite common. Many analysis reports, in direct disregard of the original intent of SFF, have included failure classifications that are not even acknowledged in IEC 61508 or IEC 61511. Contrary to what these reports frequently state, 'no effect,' 'residual,' 'don't care,' and 'annunciation undetected' are not discussed in IEC 61508 and are not included in any failure definition.

Within some analysis reports, failure classes, such as 'no effect,' 'don't care,' and 'residual' are being loosely defined as a failure that is neither safe nor dangerous. IEC 61508 defines a failure as the termination of the ability of a functional unit to perform a required function. Similar definitions can be found in IEC 61511 and the CCPS book, Guidelines for Safe and Reliable Instrumented Protective Systems. If the device has not failed in a deterministic state - safe or dangerous – it is still functional. It has not terminated its ability to function as specified. However, the analysts have counted these non-failures as safe in the SFF calculation, thereby artificially inflating the calculated SFF value.

IEC 61508 only acknowledges two types of failure, safe and dangerous, so it must be that analysts believe that any degraded, not safe, or not dangerous failure can be assumed to be a safe failure. Ironically, though these non-failures are generally included in the SFF calculation, the analysis reports actually recommend not including them in any spurious trip rate calculation.

Some reports are defining 'annunciation undetected' as the failure of a diagnostic circuit such that it will not annunciate a future fault occurrence. The simple truth is that, if the user is not notified of the diagnostic failure, the user can not be in compliance with IEC 61511 Clause 11.3.1 which addresses the requirement of using diagnostic tests, proof tests or other means to detect dangerous faults. Dangerous diagnostic failures should not be classified as safe, but again, analysts are consistently reporting 'annunciation undetected' failures as safe and astonishingly cite IEC 61508 as a basis for their claim.

When analysts count these 'new' failure classes as safe, the product achieves a higher SFF without any measurable safety benefit. Products with mechanical components are often assumed to have a substantial percentage of 'no effect' failures thus achieving SFF values greater than the 60% or 90% values

required to reduce the hardware fault tolerance requirements in accordance with IEC 61508 Tables 5 and 6. A higher SFF frequently leads to SIL 2 or 3 Claim Limits without any redundancy requirement.

For example, a diaphragm-actuated globe valve manufacturer has claimed failure rates of 9.356e-03/yr 'no effect' on a product with only 8.226e-03/yr of real safe and dangerous failures. More non-failures are included than real failures. The SFF calculated without the 'no effect' failure is 59.2%, which is below the SIL 2 claim for a type A component. With the 'no effect" failures included, the SFF is increased to 80.9%, sufficient for an SIL 2 claim.

All this to say, these "new" failure classes appear to have been created since IEC 61508 was approved solely for the purpose of inflating the SFF; thus these "new" failure classes are unsubstantiated theoretical constructs – the very phlogiston of safety engineering. Users should reject hardware fault tolerance claims based on such failure classes and should demand that manufacturers substantiate their claims following accepted reliability engineering principles.

A tendency to shift responsibility for safe operation to the operator

Many reports are issued with SIL claims assuming detected failures are configured to alarm rather than forcing the failed product to its specified safe state. This assumption allows manufacturers to report a low spurious trip rate and a low dangerous undetected failure rate, even when the product is inherently unreliable. Under IEC 61508 requirements, a product with a high total failure rate can achieve a high SIL Claim Limit as long as its failure is detected and annunciated. The SFF is not penalized by the choice to alarm rather than achieving the safe state. Therefore, the more failures that are detected, the higher the SFF becomes, regardless of the number of times, or the total amount of time, that the device is in the failed state, essentially dumping responsibility for process protection back on the operator.

Fault detection simply informs the user that the device is no longer capable of operating as required; it does not achieve or maintain process safety. Continuing to operate the process with a degraded or disabled SIS is a serious decision, requiring planned compensating measures that ensure safe operation and provide equivalent risk reduction. Many safety instrumented systems (SISs) are installed because the operator does not have sufficient time, is not continuously present, or is not capable of achieving a consistent, reliable protective response in the time required. If the hazard and risk analysis has already taken credit for an operator appropriately acknowledging an alarm, the operator's contribution to process hazards management has already been considered. An operator acknowledging a diagnostic alarm does not reduce the risk or make the operator stronger, faster, or smarter. Only the user, through careful consideration of many application-specific factors, including the process hazard, process safety time, operator attendance, required safe state actions, and operator work load, can determine if the operator is capable of providing equivalent risk reduction while the detected failure is corrected.

Manufacturers recommending that failures be alarmed rather than taking the appropriate safety action are potentially accepting significant liability. They simply do not have sufficient information about the intended operation or process risk to make such recommendations. Unfortunately, nearly every analysis report reviewed assumes that an operator is on-hand to step in and substitute for the basic process control system (BPCS) and/or SIS immediately upon receiving a diagnostic alarm and that they will remain available to monitor the process equipment until the failed device is returned to service. Such assumptions are unrealistic and manufacturers would be better advised to provide a detailed failure modes and effects analysis, so users armed with an understanding of what is necessary for safe operation can calculate an application-specific PFD and spurious trip rate.

Lack of complete proof test procedure

The user must validate and periodically demonstrate that the equipment operates according to the safety requirements specification. This demonstration includes diagnostics, alarms, manual operation, and safety functionality as required by IEC 61511 Clauses 11.3, 16.2.2, and 16.3. Unfortunately, very few of proof test procedures reviewed actually satisfy OSHA PSM requirements for a witnessed test of the equipment's ability to operate as required.

Most safety manuals provide limited scope proof tests with estimated test coverage. Product operation is not fully proven by these partial tests. Since failure modes and distributions are not provided, it is not possible to determine whether the claimed proof test coverage is reasonably conservative, or what failures the suggested test covers or does not cover. As already discussed, the proof test procedures do not address testing product diagnostics. Many devices have achieved a high SIL claim limit via large diagnostic coverage factors; yet, means and procedures for testing the diagnostics are not provided or discussed in the majority of safety manuals reviewed.

Safety manuals should provide proof test procedures that demonstrate equipment operation, including diagnostic, alarm and trip functions. Partial testing and diagnostics are tools for allowing more frequent validation of a subset of the failure modes, but the use of partial testing does not eliminate the need for full functional testing. Fundamentally, all protection layers must be auditable, therefore periodic proof testing is necessary in order to prove that random and systematic errors have not degraded equipment performance. Incomplete testing cannot be accepted solely based on probabilistic techniques. Any failure that is not covered by test is a latent condition that can manifest itself anytime in the device's life. No user should approve a device for a safety application that cannot be fully proof tested in order to ensure proper operation according to the safety requirements specification.

Path Forward

Processes operate in a safe manner when installed equipment meets the owner's operability, reliability, and maintainability requirements. Safety is not sustainable when unreliable equipment is used. Low reliability equipment increases maintenance costs, reduces operation's trust in the equipment and those that specified it, and increases overall risk due to process upset, shutdown, and start-up. Users must assess how well a device works in the intended application. Prior use information is essential to ensure proper installation, commissioning, testing, and maintenance in process industry applications.

The root of the safety manual problem is an inadequate understanding by manufacturers of what is really needed by users. The manuals reviewed do not contain sufficient information to ensure compliance with IEC 61511 or OSHA PSM requirements. To better support users, manufacturers must perform reasonable and conservative analysis of their products and provide better documentation of assumptions. Users require more than a table of numbers in order to verify that analysis assumptions match their device's application. Manufacturers are responsible for providing the 'fundamental information for that which they have control, thereby enabling users to efficiently and consistently do their job (4).' Instead, most devices are making exaggerated claims based on rather flimsy and in some cases suspect evidence.

Unfortunately, it appears that many of these issues will not be addressed by an upcoming release of IEC 61508. Committee members are encouraged to seriously consider changes to IEC 61508 that steer

manufacturers in a direction that yields safe and reliable products. Manufacturers should be required to supply a failure modes and effects analysis with failure distributions so users can track their failures against the defined modes. They should also be required to report in-service data, ensuring that product claims can be met by field performance. Manufacturers should not assume that it is safe to alarm a fault rather than forcing the product to its safe state condition. They should report the failure modes that can be detected and allow users to determine whether it is appropriate to alarm or trip based on a hazards and risk analysis of the process equipment. Finally, manufacturers should provide proof test procedures that fully test all required product functionality in order for users to achieve and remain in compliance with IEC 61511 and OSHA PSM.

References

IEC 61508, *Functional Safety of Electrical /Electronic/Programmable Electronic Safety Related Systems,* Parts 1-7, Geneva, Switzerland (1999-2001).

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, NY, (2007).

http://www.emersonprocess.com/rosemount/solution/faq61508.html

Thomas, Harold, David Deibert, David C. Arner, and David Weir, Air Products & Chemicals, Inc., *"Safety Instrumented System Manuals-A Need to Balance Reliability and Safety,"* Process Safety Progress, Vol 27, No 1 (March 2008)

IEC 61511, Functional Safety: *Safety Instrumented Systems for the Process Industry Sector*, Geneva, Switzerland (2003).

OSHA, *"Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents,* 29 CFR Part 1910." Federal Register 57, 36, Washington, DC (1992).