Upcoming Changes in IEC 61511 2nd Edition

Paul Gruhn, P.E., CFSE
Global Functional Safety Consultant
Paul.Gruhn@aesolns.com
aeSolutions, Houston, Texas, USA

This paper summarizes the differences between the first and second editions of IEC 61511.

Historical Background

The ISA (International Society of Automation) 84 standard ("Application of Safety Instrumented Systems for the Process Industries") was first published in 1996. During the time of its development, the IEC (International Electrotechnical Commission) was working on the 61511 standard ("Functional Safety: Safety Instrumented Systems for the Process Industry Sector"). Some members of the ISA 84 committee were also members of the IEC 61511 committee. In essence, the ISA 84 committee had direct involvement (along with all the other national committees) in the creation of the IEC 61511 standard. IEC 61511 was published in 2003.

ISA and IEC, like many standards development organizations, try and put their standards through a 5 year review and development cycle. In the early 2000's the ISA 84 committee felt that the more recent 61511 standard was a considerable improvement compared to its original work, and the committee agreed to adopt 61511 as the 2nd edition of ISA 84. The only change was the addition of the "grandfather clause" (1.y) which comes from a US regulation. ISA 84 (IEC 61511 mod) 2nd edition was released in 2004.

It has been over 10 years since the first release of IEC 61511. That committee has worked diligently to create a 2nd edition. A CD (Committee Draft) went out for review and comment by the national committees in 2012. The FDIS (Final Draft International Standard) went out to the committee in November 2015. The standard is expected to be released in 2016. Note that there may still be editorial changes to the standard, but no further technical changes will be accepted for this edition. The ISA 84 committee will then decide whether to accept the 2nd edition of IEC 61511 as the 3rd edition of ISA 84, or whether they may wish to make any changes. Considering the desire for international design practices and standards, changes would be unlikely.

For copyright reasons, this paper will paraphrase the changes without directly quoting or copying any particular sub-clauses.

Clause 1: Scope

One sub-clause defines the process industry. In addition to chemicals, oil and gas, pulp and paper, and non-nuclear power generation which were listed in the 1st edition, pharmaceuticals and food and beverage have been added.

The “grandfather clause” – that only appeared in ISA 84 and not IEC 61511 – has been accepted by the IEC committee, although it was moved to clause 5 (on Management).

Figure 4 in the 1st edition had a decision tree showing how a demand mode safety function could be further split into prevention or mitigation functions. (This is what prompted many people to believe that fire & gas systems fell under the scope of this standard.) The second edition removes this distinction and simply shows continuous mode or demand mode functions.

Clause 2: Normative References

There are minor editorial changes, such as referencing the 2010 version of IEC 61508, a 2010 IEC standard on communication networks, and no longer listing several other older IEC standards.

Clause 3: Definitions

There are definitions for new terms such as “bypass”, “compensating measure”, “mean repair time”, “mean time to restoration”, “maximum permitted repair time”, “process safety time”, “systematic capability”, and a few other terms. There are many new notes for the definitions of common cause and common mode failures. The definitions for safe and dangerous failures (and many other terms) have been improved. In addition to demand mode and continuous mode, high demand mode has been added. The previous term of “proven-in-use” has been replaced with “prior use”. The term and concept of safe failure fraction (SFF) has been removed. Interestingly, the term “hardware fault tolerance” is still not defined (although the term is obviously used in the standard).

There are a number of other minor editorial changes.

Clause 4: Conformance

This one sentence clause has not changed.

Clause 5: Management of Functional Safety

A sub-clause still lists requirements for personnel competency, but new sub-clauses require that procedures shall be in place to manage the competence of individuals, and that periodic assessments

shall be carried out to document that competence against the activities they are performing, and on change of an individual within a role.

New requirements have been added for suppliers. One new paragraph states that if a supplier makes any functional safety claims for a product or service which are used to demonstrate compliance with the standard, then the supplier shall have a functional safety management system. The supplier must also have procedures in place to demonstrate the adequacy of their functional safety management system.

The “grandfather clause”, previously a sentence only in the ISA 84 standard, has now been added to 61511.

There are a few other minor editorial changes.

Clause 6: Safety Lifecycle Requirements

The first edition of the standard had software lifecycle requirements listed in clause 12. Most of those requirements, along with the software lifecycle diagram and overview table, have now been moved to clause 6.

There are no other significant changes.

Clause 7: Verification

There are a few new bullet points regarding verification planning. A new sub-clause states that when verification includes testing, the verification planning shall also address a dozen bullet points listing details.

There are a few other minor editorial additions and clarifications.

Clause 8: Process Hazard and Risk Assessment

A new sub-clause states that a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS, and that it shall result in items called out in six bullet points and four notes.

Clause 9: Allocation of safety functions to protection layers

There is considerably more detail and cautionary warnings on the requirements for SIL 4 applications.

There are still clauses stating the risk reduction for a BPCS protection layer shall be ≤ 10, and if greater than 10 is claimed, the BPCS shall be designed and managed according to this standard. The words “and managed” are new. It further states that if the BPCS is not going to conform to the standard, it sets limits on how many protection layer credits may be claimed for the control system. If the BPCS is the source of the initiating event, then no more than one BPCS protection layer may be claimed. If the BPCS

is not the initiating source, then no more than two protection layers may be claimed. When these concepts apply, it must be shown that each BPCS protection layer is independent and separate from the initiating source and from each other. A note explains that a hot backup controller is not considered to be independent of the primary controller.

There are a few other minor editorial changes and explanatory notes.

Clause 10: SIS Safety Requirements Specification (SRS)

What was approximately two dozen bullet points is now a longer and lettered list making items easier to reference. Items such as requirements relating to proof test implementation are now clearly stated. Portions of the old clause 12 on software have now been added to clause 10. There are many new excellent details to consider such as action to be taken on a sensor value out of range, excessive range of change, open and short circuit, etc. One should consider functions enabling proof testing and automated diagnostics tests of field devices performed in the application program.

The changes could be described as new details that many did in the past, but are now clearly stated.

Clause 11: SIS Design and Engineering

There are new sub clauses stating the system shall be resilient against identified security risks, that devices' safety manuals shall be available and followed, and communications shall use techniques appropriate to meet the required SIL.

Since safe failure fraction is no longer used, the old Table 5 covering the minimum hardware fault tolerance requirements for programmable electronic logic solvers no longer appears. One of the most significant changes to the standard is the single fault tolerance table that does appear. SIL 1 still requires a minimum hardware fault tolerance of 0. SIL 2 low demand also has a minimum hardware fault tolerance of 0. SIL 3 requires a fault tolerance of 1. In essence, the fault tolerance requirements for SIL 2 and 3 have been lowered by one compared to the first edition of the standard.

There are three options to meet the fault tolerance requirements for subsystems; follow the table and five clauses in the standard, or base the claim on either route 1H or 2H from IEC 61508. Route 1H is based on safe failure fraction concepts, route 2H is based on prior use. The "H" is intended to signify hardware safety integrity, in order to distinguish it from systematic safety integrity. The five clauses in 61511 are derived from route 2H in 61508. There are still exceptions allowing the numbers in the table to be reduced further. However, such cases must be justified and documented showing evidence of suitability, systematic failures must be considered, diagnostic coverage of programmable devices cannot be less than 60%, and reliability data must have a confidence limit no less than 70%.

The table should not be interpreted as a "get out of jail free" card allowing everyone to claim SIL 2 while using a single (non-redundant) dumb (without any diagnostics) switch and valve. Probability of failure on

demand (PFD) calculations must still be done to justify a design. Published failure rates would show such a claim to be a difficult justify.

There are a number of useful clarification statements. The standard acknowledges that devices may exhibit different failure rates depending upon the operating environment and mode of operation. It acknowledges that failure rate data from manufacturers may not be valid in all applications. For example, failure rate and mode distributions may be different for a valve that is frequently exercised versus one that remains still for long periods of time. There are additional details on prior use such as identifying devices by revision number and controlling the devices under a management of change procedure.

The old sub-clause on field devices stating that each device shall have its own dedicated wiring has been removed.

There are now sub-clauses stating the maximum time a function is allowed to be in bypass shall be defined, and that compensating measures shall be provided while in bypass.

Sub-clauses still lists items that need to be included in the performance calculation. Failures that are undetected by diagnostic tests and undetected by proof tests are now acknowledged and listed.

There are new sub-clauses clarifying that reliability data shall be credible, traceable, documented, justified, based on devices used in a similar environment, and account for data uncertainties.

There are a number of other minor technical and editorial changes, all adding useful clarification.

Clause 12: SIS Application Program Development

Clause 12 in the first edition was 17 pages; it is now 3 and a half pages. This clause has obviously been significantly rewritten. As stated above, what was previously in clause 12 covering lifecycle steps and requirements specification has essentially been moved. This new clause actually reads better, has much more useful information, and provides longer lists of specific items that need to be addressed. What were considered good and common practices by some are now clearly spelled out. For example, the application program and its documentation shall be reviewed by a competent person not involved in the original development. The approach used for such a review and the review results shall be documented. This clause still states that 61511 does not address the use of full variability languages or SIL 4 application; it still refers readers to 61508 in such cases. The old V-model diagram of software development and testing no longer appears.

Clause 13: Factory Acceptance Test (FAT)

Other than this clause now being normative (it was informative before), there are no significant changes.

Clause 14: SIS Installation and Commissioning

No significant changes.

Clause 15: SIS Safety Validation

No significant changes.

Clause 16: SIS Operation and Maintenance

There is now a requirement to record the status of all bypasses in a log. Demand rates on functions shall be tracked. There are a number of other minor changes that could simply be described as cleanup and clarification. For example, there is still a clause stating that deficiencies found during testing shall be repaired, but now there is a second sentence stating that the proof test shall be repeated after the repair is completed. There is a new clause stating that management procedures shall be applied to review deferrals and prevent significant delays to proof testing. This was something that was always understood, but is now spelled out.

Clauses 17-19

There are no significant changes to clause 17 on SIS modification, 18 on SIS decommissioning, or 19 on information and documentation requirements.

Summary

The majority of changes can be classified as clarifications and improvements. Many items that were previously understood and commonly practiced are now spelled out. However, the lowering of the fault tolerance requirements by one compared to the earlier edition is cause for concern and potential abuse.

Author Bio

Paul Gruhn is a Global Functional Safety Consultant with aeSolutions in Houston, Texas. Paul is an ISA Fellow, a member of the ISA 84 standard committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, the author of two ISA textbooks, two chapters in other books, and over two dozen published articles, and the developer of the first commercial safety system software modeling program. Paul has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (PE) in Texas, and both a Certified Functional Safety Expert (CFSE) and an ISA 84 Safety Instrumented Systems Expert.

Disclaimer

The following paper is provided for educational purposes. While the authors have made reasonable efforts in the preparation of this document, aeSolutions makes no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of this document.