IEC 61511-2016 Changes: Treatment of Existing Systems

This is one of a continuing series on the major technical changes in IEC 61511 ed 2

When ISA voted to accept the 1st edition of IEC 61511 as the US national standard, what was colloquially called the "grandfather clause" in ANSI/ISA 84.01-1996 was added to its scope:

> ANSI/ISA 84.00.01-2004 Clause 1 y) For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the user shall determine that the equipment is designed, maintained, inspected, tested and operating in a safe manner.

This clause was intended to emphasize that the existing equipment could be maintained as is, as long as it met the performance specification. Compliance requires collection of sufficient information and records that a reasonable person would believe that the functions of the SIS will operate as required when demanded.

The US delegation made repeated requests that an existing system clause be placed in IEC 61511 edition 1 to ensure that all stakeholders understood that the installed SIS could remain as is, as long as the SIS was providing the necessary protection. However, most other national delegations did not understand why such a clause was needed. The safety lifecycle and the functional safety management system cover the collection of prior use information concerning the installed SIS and the use of this information to judge the fitness for purpose of the SIS. The effort by the US delegation to introduce a clause addressing existing systems was not successful in edition 1.

The application of new or evolving standards to existing SIS has been a cultural undercurrent for the IEC 61511 committee for as long as this committee has existed. The driver of the undercurrent is predominately the regulatory and certification community who want standards and practices that are absolute, since the determination of acceptability is easier if everything can be reduced to a checklist. This desire is unrealistic when a standard applies to something as broad as the *process industry*.

The generation of instrumentation and controls applied at any site in safety applications will be representative of the site's adoption of control system technology in general. Many combinations of manual and automated approaches can be used to achieve the same level of safety. IEC 61511 is deliberately not absolute and instead mandates the application of a functional safety management system across the SIS lifecycle and the periodic examination of site records to determine that the equipment is fulfilling its functional and integrity requirements. As with OSHA PSM, IEC 61511 is performance-based, so acceptability is determined by historical performance, or prior use as it is called in IEC 61511.

In developing the 2nd edition, the US again pursued the inclusion of the *existing system clause*, so that the US and international versions would match exactly. Now, all delegations were in the same position as

the US during 1st edition. Are the SIS designed per the 1st edition unsafe? For edition 2, all delegations were on-board with the need to explicitly address existing SIS.

Initially, the *existing system clause* was placed in the scope as in ANSI/ISA 84.00.01-2004. However, comments were received by IEC that inclusion of the clause in the scope could lead to the potential misinterpretation that IEC 61511 only applies to new systems and not to existing. It was a common sense choice for the committee to address existing systems at the end of the monitoring clause as 5.2.5.4. Fundamentally, the proof needed to satisfy the *existing system clause* is as follows:

- Does the demand rate during actual operation agree with the assumptions made during the risk assessment when the SIL was determined?
- Is there an active program to identify and prevent systematic errors, whether associated with equipment failure or human error in multiple applications?
- Is there an active program to monitor and assess whether reliability parameters of the SIS are in accordance with those assumed during the design?
- Is there an active program to troubleshoot and correct performance gaps?

The new edition went a bit further in tying up related loose ends. The stage 4 functional safety assessment (FSA) is now required to be conducted periodically during the operation and maintenance phase. The 1st edition only required the stage 3 FSA, which is performed prior to start-up. Another new clause - 5.2.6.1.9 - states that any FSA conducted after change should confirm that the modification work performed is in compliance with IEC 61511 requirements. Other clauses have been updated to state that documentation must be maintained up-to-date and written so that the documentation is understandable to plant personnel assigned SIS responsibility.

The editorial process that produced IEC 61511 edition 2 put a lot of effort into better defining the requirements for long-term operating and maintenance and for performance monitoring. The edits may appear subtle to some but the practical impact can be significant, depending on your company's culture and its position on the applicability of standards and practices to existing systems.