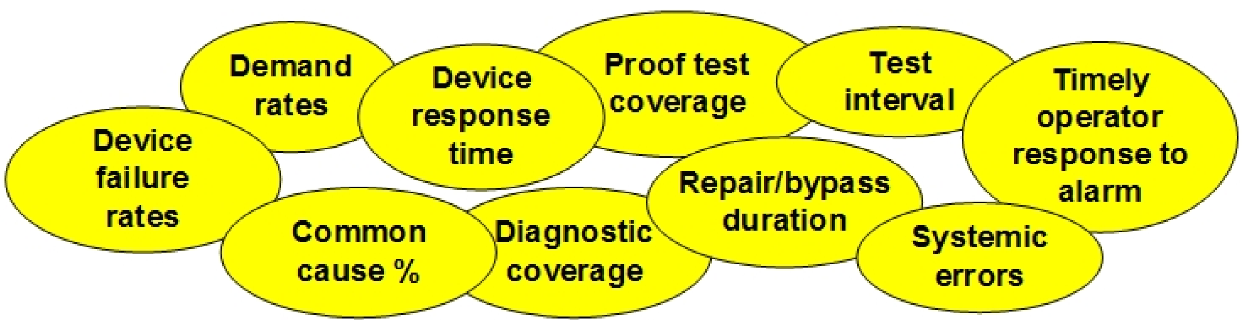
Part 3: Reliability Parameters

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

The new edition 2 has made great strides in addressing what needs to be done long-term at the site to demonstrate the claimed performance. During design and implementation, the reliability parameters for a new system or technology are estimated based on manufacturer information and any in-service information available. Once the equipment is approved for process start-up, the equipment transitions from being a new installation to an existing one that must be proven to be fit for purpose as an on-going activity.

There is plenty of data at most sites, but unfortunately much of it is often not in a form that can be easily accessed for tracking. A challenge for owner/operators will be to rationalize and prioritize data collection throughout different process operating modes and operating conditions. The concept of "store it all and sort it out later" is only good if your intent is to use the data for incident investigation where the need to understand how a specific event occurred serves as the data filter. "Store it all" is an ill advised plan, if your goal is to collect data so that you can proactively identify and resolve equipment deficiencies before an incident occurs. It is also ill advised given that the data could be sent on a millisecond resolution when the process moves in minutes, or worse yet the data is stored every 10 minutes on a process that deviates to disaster in seconds. Much like alarm floods result in a delayed operator response, data tsunamis do not help the process engineer anticipate and prevent process safety events. Data black holes where the event occurs between time stamps is also not helpful in resolving what went wrong. The challenge is to get just the right amount of data at an appropriate time resolution.



When estimating the SIS performance, IEC 61511 now requires that the reliability parameters "be credible, traceable, documented and justified" (clause 11.9.3). It acknowledges that industry often adopts processes that have been proven to work at sister or competitor sites. The standards states that the reliability parameters can be "based on the field feedback existing on similar devices used in a similar operating environment" (clause 11.9.3). The operating environment is related to conditions inherent to the installation of a device, which potentially affects its functionality and safety integrity. Examples of operating environment conditions include process composition and operating conditions, utility quality, and external environment factors such as winterization needs.

The standard also acknowledges that there is a lack of credible data for actual installations in many technologies deployed in SIS applications. The standard states that engineering judgement can be used to assess missing reliability data and to evaluate the impact of any differences in the operating environment on the selected reliability parameters (notes to clause 11.9.3).

Long-term procedures are required to collect performance data to support monitoring and assessment of the reliability parameters (clause 5.2.5.3). These procedures also need to ensure that human errors that impact the SIS performance can be tracked and that the verification and validations processes are challenged to quickly detect and eliminate these errors. Demonstrating the SIS's fitness for purpose means that the SIS achieves the intent and approach described in the safety requirements specification and exceeds the claimed performance in a sustainable manner. The standard now requires the following to be tracked (clause 16.2.9):

- Demands on the functions of the SIS
- Actions taken following a demand on the SIS
- Cause of demands
- Failures and failure modes of the SIS equipment, including safe, dangerous, incipient, and degraded.
- Failures of instrumentation and controls that are implemented as compensating measures

Deficiencies against expectations may be revealed as a result of routine maintenance and operations activities (16.2.9) or through the periodic performance assessment (functional safety assessment stage 4 – clause 5.2.6.1.10). Deficiency checks should be conducted annually to assure that any deficiencies in functional operation or performance are corrected in a timely fashion.