

The concept of a safety life cycle (SLC) has been specified in various standards, such as ANSI/ISA-S84.01-1996 (replaced by ANSI/ISA-84.00.01-2004), IEC 61508, and IEC 61511. The safety life cycle is essentially an engineering process or method for specifying, designing, implementing and maintaining safety instrumented systems so as to achieve overall functional safety in a documented and verified way. This article discusses the benefits of SLC by providing low systematic failures, reduced risk, increased process up-time, decreased cost of engineering, and design consistency. Finally, the impact of the SLC on the safety instrumented function (SIF) loop components, in particular final control elements, will be thoroughly covered. The concept of frequent

safety life cycle starts with an initial concept, progresses through design, implementation, operation and maintenance to modification, and finally decommissioning. It does not end until decommissioning of the project when all the safety instrumented functions are no longer required for use.

A complete safety life cycle can be categorised into three major phases consisting of the listed tasks:

Analysis phase:

- Identify and estimate potential hazards and risks,
- Evaluate, if tolerable risk is within industry, corporate or regulatory standards,
- Check available layers of protection,
- If tolerable risk is still out of the limit then allow use of a safety instrumented system (SIS) with an assigned safety integrity level (SIL),
- Document the above into the safety requirement specifications (SRS).

Realisation phase:

- Develop a conceptual design (for technology, architecture, periodic test interval, reliability, safety evaluation),
- Develop a detailed design for installation planning, commissioning, start up acceptance testing, and design verification.

Operation Phase:

- Validation planning,
- Start up review, operation and maintenance planning,
- SIS start up, operation & maintenance, periodic functional test,
- Modification,
- Decommissioning.

Impact Of SLC On Field Devices

As shown in Figure 1, a recent study from OREDA reports (Offshore Reliability Data Handbook) that 92 percent of all SIS failures occur in field devices such as final control elements and sensors.

Following the SLC steps, a number of measures, listed below, can be used to minimise the number of dangerous failures in sensor component of SIF loop.

testing to improve the safety integrity level (SIL) and the mode and methods of testing will be discussed at length.

Safety Life Cycle

The safety life cycle is an engineering process intended to optimise design and increase safety. The safety life cycle approach applies to all design processes with the same fundamental steps: problems are identified and assessed; solutions are found and verified; and then the solutions are put into use to solve the identified problems. This is a closed-loop process approach as described in several functional safety standards, including IEC61508 and IEC61511. A

Safety Life Cycle: Implementation Benefits & Impact On Field Devices

The Safety life cycle approach offers significant benefits for increasing safety and up-time in process plants and considerably lowers operation and maintenance costs.

By AF Stanley and Dr Kung Hun Koy.

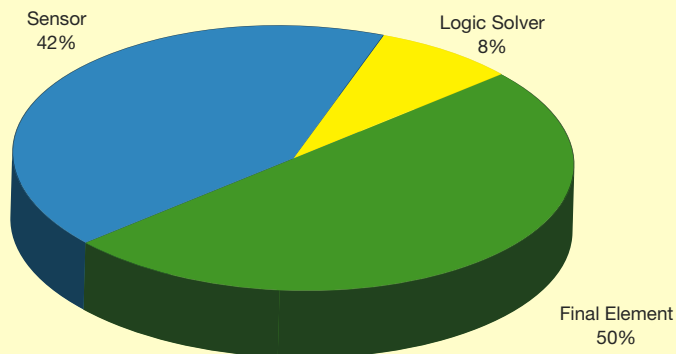


Figure 1: Where in the loop do SIS faults happen? – OREDA

- Use measurements that are as direct as possible. (Correct technology)
- Control isolation or bleed valves to prevent uncoupling from the process between proof tests. (Installation and maintenance)
- Use good engineering practice and well proven techniques for process connections and sample lines in order to prevent blockage, sensing delays, etc. (Correct specifications)
- Use analogue devices (transmitters) rather than digital (switches). (Better design equipment selection)
- Use appropriate measures to protect the process connections and sensors against effects of the process such as vibration, corrosion, and erosion. (Operation and maintenance)
- Monitor the protective system process variable measurement (PV) and compare it against the equivalent control system PV, either by the operator or the control system. (Design, specification and operation)
- Ensure integrity of process connections and sensors for containment, such as sample or impulse lines. Instrument pockets are often a weak link in process containment measures. (Better maintenance and modification plan)

Final Control Elements

The 'final control elements' are frequently the most unreliable part of the SIF loop. The reason is that final control elements have moving parts and are the mechanical portion of the SIF loop. Also, the final control element is downstream of the logic solver and receives commands from it. If it does not operate on 'demand', it can cause a

hazardous situation to occur. Sensors, on the other hand, are on the upstream side of the SIF loop and, when the analogue type is used, they allow easy read back by the logic solver to detect system faults.

Final control elements consisting of valves (shutdown, isolation, block and bleed), pilot valves, valve actuators, positioners, accessories, power supplies and utilities which are required for the actuator to perform its safety function, should all be adequately reliable. A measure of their reliability is used in confirming the integrity level of the protective system. This measure should take into account the proportion of failures of the final control element under the relevant process conditions leading to dangerous failures.

Fail Safely

Dangerous failures of final control elements of SIF loop can be minimised by a number of measures such as:

- Use of 'fail-safe' principles so that the actuator takes up the Safe state on loss of signal or power (electricity, air etc); eg: use of a spring return actuator; (De-energise to trip) [Proper Specifications during SRS]
- Provision for uninterruptible power or reservoir supplies of sufficient capacity for essential power; (Energise to Trip) [Proper Specifications during SRS]
- Failure detection and performance monitoring (valve travel diagnostics, limit switches, time to operate, torque, etc) during operation; (Online Testing & Diagnostics) [Operation and Maintenance]
- Exercising actuators or performing partial stroke shutoff simulation

during normal operation in order to reveal undetected failures or degradation in performance. Note that this is not proof testing but it may reduce the probability of failure by improved diagnostic coverage; (Partial Stroke Test) [Testing and inspection]

- Overrating of equipment; (Safety factor) [Design and Specification]

In recent times, tough competitive pressures have not allowed industries to make normal plant turnarounds. Process Industries are extending their plant shutdowns from the usual two years to a 5-year period. This puts pressure on final control elements to remain untested for an extended period of time. Digital valve controllers (smart positioners) have come to the rescue to allow testing of the valves on line and in service, as well as to provide diagnostics information.

Online Testing

Per the SLC steps, testing of the final control element is required at each stage, whether it is validation, commissioning, plant start up, operation, maintenance, modifications, etc. Digital valve controllers are communicating, microprocessor-based devices and have the capability to perform online partial stroke testing of final control elements in the SIF loop. The test can be done locally at the device or remotely, either directly from the logic solver or by companion software.

Because the digital valve controller provides diagnostic (output pressure) as well as positioning (travel) information, the valve status and response time can be monitored during the test (See Figure 2).

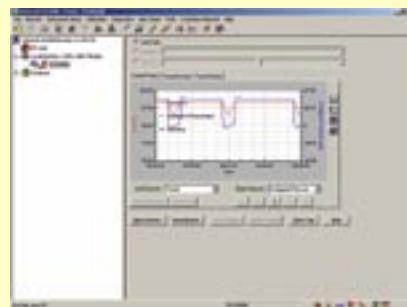


Figure 2: Valve trending status

Valve Performance

Valve performance trends are monitored and automatically analysed after each partial-stroke test so that potentially failing valves can be identified long before they become inoperable. This procedure is in line with the operations phase of the safety life cycle as defined in IEC61511. A cycle counter and travel accumulator will show the extent of valve movement.

The results of a valve signature test (See Figure 3) can be used to easily determine packing problems (through friction data), leakage in the pressurised pneumatic path to the actuator, valve sticking, actuator spring rate, and bench set. The digital valve controller can save the results of this data for printout or later use. Overlaying the results of the current signature test with those of previous tests can determine if valve response has degraded over time. This information increases valve availability and ensures that the valve responds upon demand. It also reduces the amount of scheduled maintenance on the valve, because the tests can be used to predict when the valve needs maintenance.

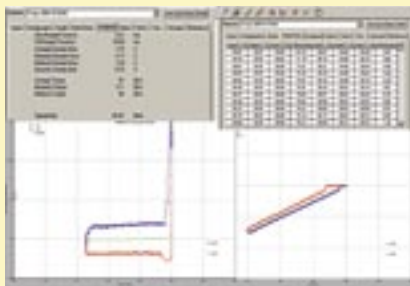


Figure 3: Valve signature test

Digital Valve Controllers

Digital valve controllers have the capability to alert the operator if a valve is stuck. As the valve begins the partial stroke, it continually checks the valve travel to see if it is responding properly. If it is not, it will abort the test and alert the operator that the valve is stuck. This will prevent the valve from slamming shut if the valve does eventually break loose. This will avoid spurious trips of the plant. Spurious trips are not only strenuous on the

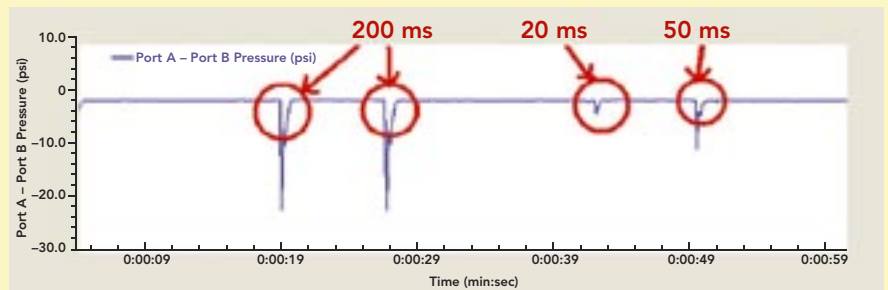


Figure 4: Plot of the pressure drop across the solenoid valve.

plant, but also affect equipment and interruption to production.


A digital valve controller can provide complete diagnostic health information on the final control element, as well as itself. In addition, the digital valve controller can provide complete documentation of any emergency event as well as documentation of all testing. Insurance companies will accept this documentation for proof of testing. Best of all, this documentation can be completely automated so that expensive operator time is not required. The safety life cycle process requires documentation of validation and verification of each phase. A digital valve controller provides system audit documentation for comparison and future reference. This provides relief to the maintenance staff by making documentation available automatically and it provides the capability to cross check with past performance by comparing previous test results.

Users who like to retain their solenoid valve while adding the digital positioner for the additional diagnostics can use the digital positioner to verify that the solenoid valve vents actuator pressure during on-line testing without disturbing the process. This gives users the ability to now document that

the solenoid valve vented actuator pressure, as shown in Figure 4, when tested online in addition to checking for coil integrity.

A Safer Plant

Safety life cycle implementation provides a safer plant with low systematic errors. It decreases the cost of engineering and increases process up-time. It considerably lowers operation and maintenance cost by selecting the right technology equipment with correct implementation, as well as providing proper guidelines for operation, maintenance, modifications and decommissioning. This will not only reduce plant risk, but it will also provide overall design consistency.

The SLC process impacts components of the SIF loop. Following SLC guidelines, selecting a digital valve controller for the 'final control element' of the SIF loop can reduce dangerous undetected failures of the field devices. A digital valve controller allows online partial stroke testing while the process is running. It also provides remote testing capability allowing for fewer maintenance field trips. In addition, it allows establishment of an automated test routine that can produce great savings in time. 



Stanley Amirthasamy is the Marketing Manager for Instruments and Software with the Fisher division of Emerson Process Management Asia Pacific Pte Ltd. He has been in the valve industry, with a focus on the Fisher digital positioner offering for over seven years.



Dr Kung Hun Koy is a Plant-Web and Diagnostics Specialist for Emerson Process Management Asia Pacific Pte Ltd, Fisher Division. He has been a marketing and support engineer for digital positioners for six years.

References were made to the paper 'Safety life cycle - Implementation benefits and impact on field devices', ISA 2005, by Riyaz Ali.