AS SEEN IN THE SUMMER 2007 ISSUE OF...
Valve MAGAZINE

HOW TO IMPLEMENT A SAFETY LIFE-CYCLE

A SAFER PLANT, DECREASED ENGINEERING, OPERATION AND MAINTENANCE COSTS, AND INCREASED PROCESS UP-TIME ARE ALL ACHIEVABLE WITH THE IMPLEMENTATION OF A SAFETY LIFE-CYCLE. IN THIS ARTICLE, THE AUTHOR FOCUSES ON THE AREA IN WHICH MOST ERRORS OCCUR—THE 'FINAL CONTROL ELEMENT.' **BY RIYAZ ALI**

The purpose of a safety instrumented system (SIS) is to reduce risk from a hazardous process to a tolerable level. Although selecting a safety integrity level (SIL) is vital to this purpose, an organization must also devote significant effort to supporting safety activities.

Safety life-cycle (SLC) is an engineering process designed to optimize the design of the SIS and to increase safety.

What is SLC?

The concept of a safety life-cycle has been incorporated into many national and international standards, such as ANSI/ISA S84.01-1996 (replaced by ANSI/ISA-84.00.01-2004), IEC 61508 and IEC 61511. And ISA 84.01—the first published functional safety standard—was recognized by the U.S. Occupational Safety and Health Administration as an example of good engineering practices.

All of these standards have gained wide acceptance and are forming the basis for compliance with local, national and international laws and regulations.

As described in several functional safety standards (IEC 61508 and IEC 61511), the SLC is a closed-loop process. In other words, the

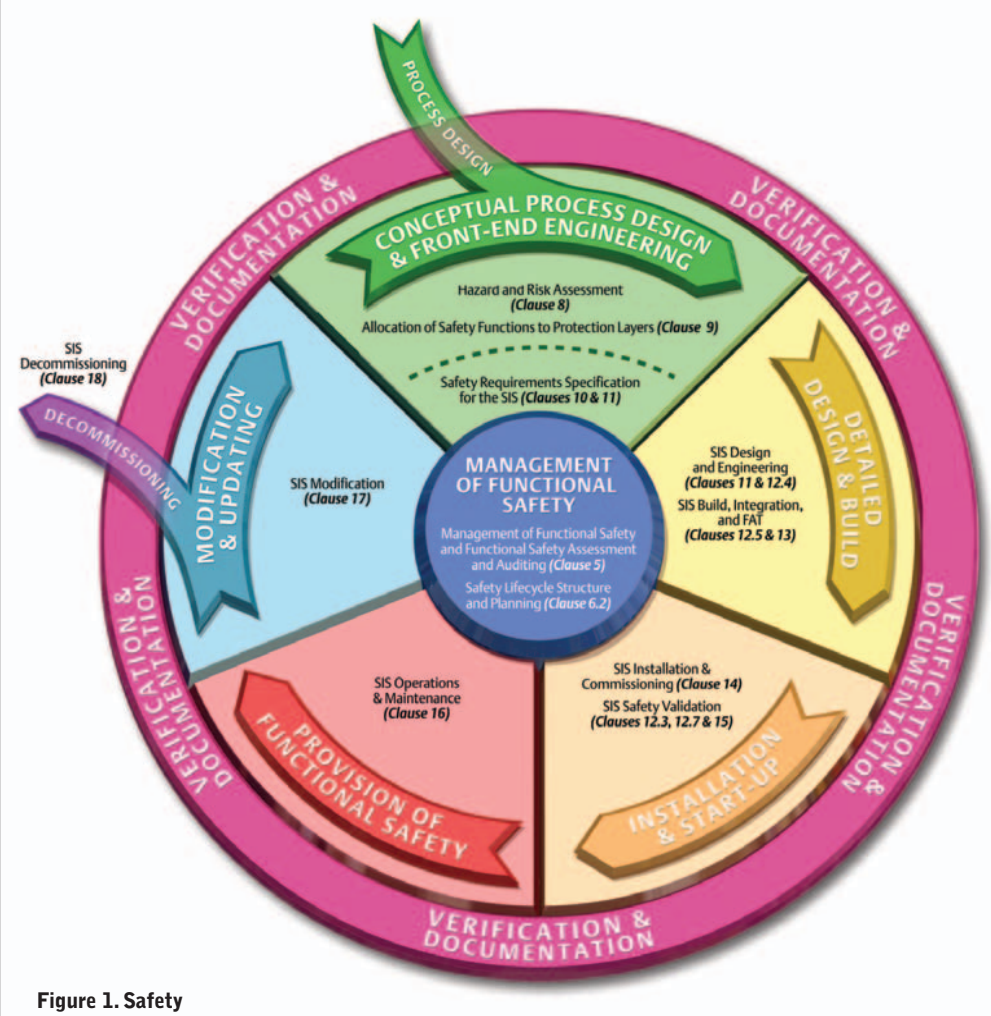


Figure 1. Safety life-cycle "close loop process"

process has no end. Its lifecycle tasks are continuously performed while a process is in operation, and especially when designs are under periodic review and process changes are occurring (Figure 1).

Over the last two decades, the need for a formally defined SLC process has emerged. This is because the inevitable requirement for better processes eventually pushed control systems to a level of complexity where sophisticated electronics and programmable systems have became the optimal solution for control and safety protection.

Standards and Safety Life-Cycle

The SLC per IEC 61508 can be categorized into three broad areas. The first is the analysis phase, which focuses on identifying hazards and hazardous events, the likelihood these hazardous events will occur, potential consequences, and the availability of a layer of protection, as well as the need for any SISs and the allocated SIL.

The second phase is realization, which focuses on design and fabrication of the SIS; and the final phase is operation, which covers startup, operation, maintenance, modification and eventual decommissioning of the SIS. These phases encompass the entire life-cycle process of the safety system from concept through decommissioning.

IEC 61508's safety life-cycle is shown schematically in Figure 2. Each phase of the overall SLC is divided into elementary activities, and the scope, inputs and outputs are specified for each phase. IEC 61508 recommends the information required to execute each step, as well as the output and documentation that should be produced in each step. However, the standard is performance based, not prescriptive—it only has general guidelines and recommendations on the life-cycle phases.

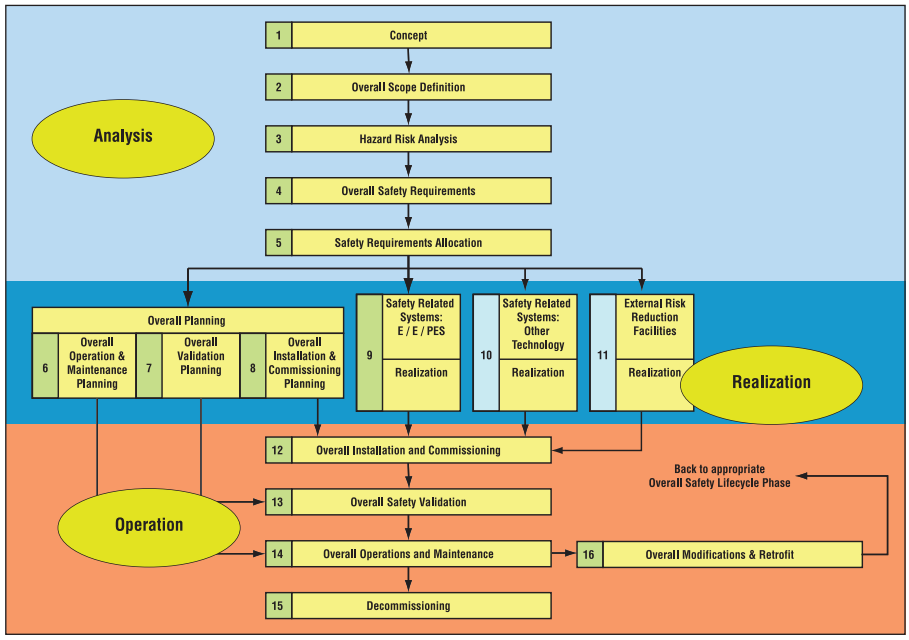


Figure 2. IEC 61508 Safety Life-Cycle

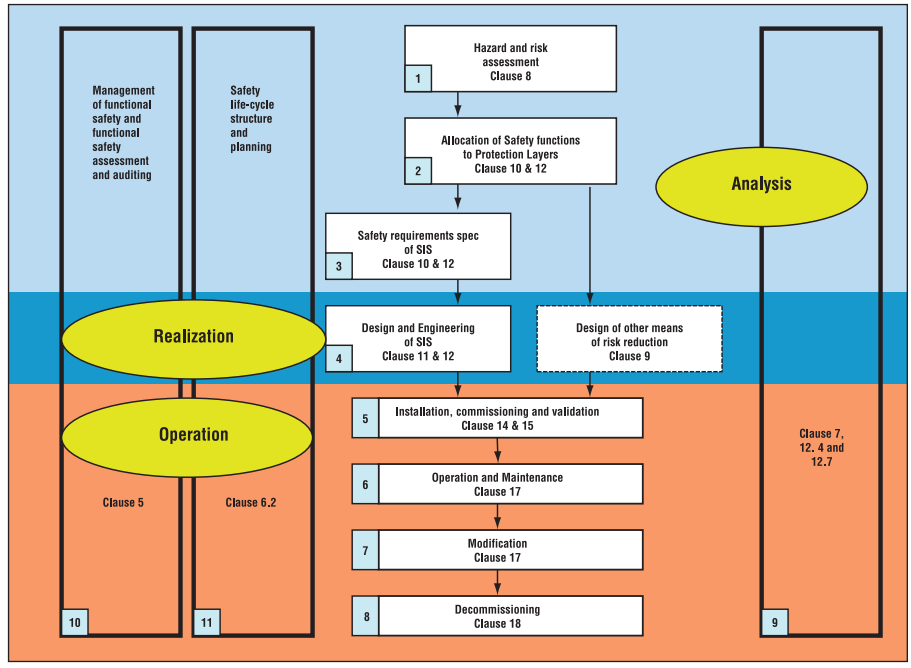


Figure 3. IEC 61511 Safety Life-Cycle

IEC has developed document IEC 61511 to provide specific guidance to the process industry using IEC 61508 as the umbrella standard. The safety life-cycle per IEC 61511[1] is shown in Figure 3. This document also covers the analysis, realization and operation phases. It also stresses the continuous functions of planning, management, assessment and verification, which support the sequential components of life-cycle structure.

To achieve desired safety levels, organizations must devote extra care to the essential safety life-cycle.

SLC Analysis Phase

The initial planning, identification and specification functions needed to properly apply safety systems to a process

are included in the analysis phase of the SLC. The analysis also looks at individual functions and flow of information required to perform these tasks most effectively.

The SLC begins with conceptualizing the initial design of the process through definition of the project's scope. Clear definitions are particularly critical in projects with operational and safety-focused objectives such as grassroots new facility constructions or with process revamps of existing plants. Ideally, an organization should designate the relative importance of objectives, allocate adequate resources to those objectives and establish proper scheduling for those objectives at the outset of the project. Also, the ultimate responsibility for achieving both safety- and non-safety-related goals should be assigned to a single, competent and knowledgeable individual.

The organization's personnel responsible for the safety portion of a project should clearly understand the processes, technologies and equipment under control. They also should have a basic idea of the potential process hazards and a basic understanding of the equipment and materials present.

At the beginning of a project, an organization should also consider the level of risk that will be tolerated in daily operation. This risk level should then be compared to the risks present in the process.

The next function of the SLC is to classify hazard and risk analysis. This step includes identifying any safety instrumented functions (SIF) needed to detect imminent harm and take the process to a safe state in case of demand.

A process hazard analysis (PHA) is structured brainstorming in which a team of experts systematically reviews sections of a process to identify hazards that could occur in the process and lists all events that could cause an accident. The PHA then evaluates outcomes of an accident, the safeguards in place to prevent that accident and measures that can be recommended to reduce the process risks.

Depending upon the hazards, the consequence analysis required to estimate the magnitude of potential harm can be quite complex. This analysis can be done using qualitative, semi-qualitative or quantitative methods.

Analyzing the likelihood of risk involves understanding the different sequences of events that can lead to a harmful event. Layer of protection analysis (LOPA) is the likelihood part of the risk analysis, and it is used to determine the frequency of the potential harmful outcome.

Once potential hazards have been identified and characterized, along with the risks they pose, and once required SIFs and their corresponding SILs have been identified, the analysis phase of the safety life-cycle must be completed to document these efforts and results in the safety requirements specifications (SRS). The purpose of the SRS, according to IEC 61508[2], is "to develop the specifications requirements and safety integrity requirements, for the E/E/PES safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety." During the conceptual phase, end-user and consultant involvement typically is required.

SLC Realization Phase

The realization phase begins with conceptual design of the safety instrumented system based on the safety requirements specification.

This phase of the SLC includes design, fabrication, installation and testing of the SIS specified in the analysis phase of the project.

Based on the SRS, the first task of the realization phase is to select the safety instrumented system technology and architecture needed to meet the specification's requirements. A key part of this planning step is developing maintenance and proof-test schedules to ensure any potential failure in the safety equipment can be found and repaired before the system is required to act.

Once the conceptual design is completed, the organization needs to analyze the prospective system to confirm it meets the SIL selected and documented in the SRS. The detailed design of the SIS should be executed according to clear, well-defined and established procedures.

The final part of realization phase is planning and executing the system's installation, commissioning and validation. Once these tasks are finished, the SIS should be fully functional at the SIL selected to achieve a tolerable level of risk. With this, the SLC realization phase is complete.

The realization phase is the most resource-intensive part of the overall

THE THREE PHASES OF A COMPLETE SAFETY LIFE-CYCLE

A complete safety life-cycle can be categorized into three major phases:

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).

Realization 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 and maintenance, periodic functional test
- Modification
- Decommissioning

safety life-cycle, and it involves the end user, vendors and contractors.

SLC Operation Phase

The operation phase of the safety life-cycle begins with validation of the design. The most significant part of this phase is maintenance and testing of the SIS. The system's SIL can be affected by the number of times the system is tested and repaired to full functioning condition. A proper testing and maintenance regime begins with good planning and relies on solid documentation to show the plan is being followed. Effective management of change is also important. So, too, is decommissioning. The organization should analyze the effect of the decommissioning on both the equipment and processes directly under control of those two factors and on any closely integrated systems.

The operation phase of the safety life-cycle is the longest phase of SLC. It requires involvement of end users and contractors.

Benefits of the SLC

The primary result of the safety life-cycle process is to provide an optimal SIS design that matches risk reduction with process risks while maintaining internal design consistency.

The SLC and closed-loop verification concepts should result in safer, more cost-effective designs by having fewer systematic failures, lower cost of engineering and more up-time for processes.

If the safety requirements specifications have been defined properly during the SLC analysis phase, risk will definitely be reduced.

Proper selection of technology and correct specification of equipment lessens the likelihood of immature failures, reduces maintenance and causes fewer plant shutdowns.

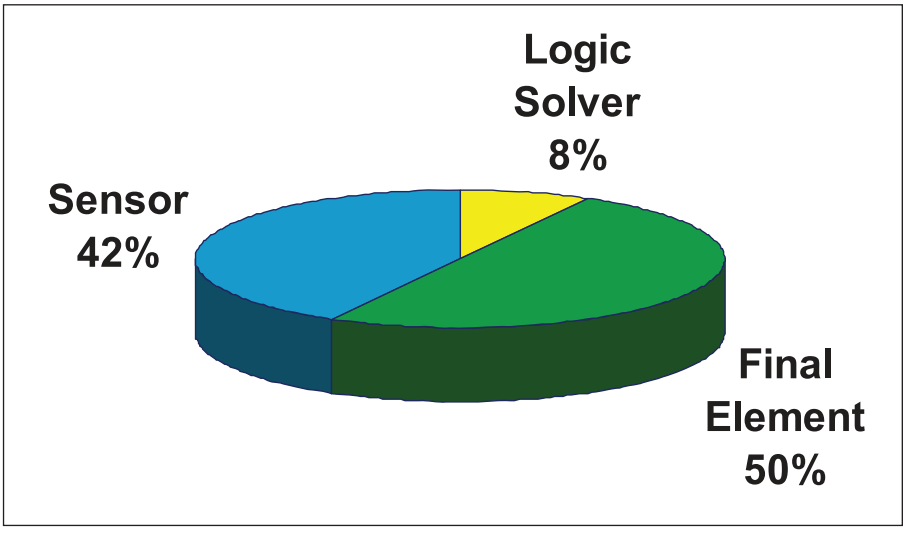
Note that required reliability has been achieved commensurate with required integrity levels. Defensive measures may include using high-reliability elements and automatic diagnostic features to reveal faults and seeking out redundancy (e.g. a 2oo3 configuration for sensors) to provide fault tolerance.

If this step of the realization phase is done properly, it not only reduces the equipment, design, installation, initial training and the start-up system commissioning costs, it can improve safety tremendously as well.

Periodic testing intervals need to be defined. Also, selecting the best technology for that testing allows better diagnostic information, including online testing to meet the periodic intervals required by the target safety integrity level, which can possibly improve the SIL level. Improving SIL through use of fewer field devices can lessen maintenance costs as well as reduce spurious trips.

Detailed documentation provides design consistency across all units in a plant; however, it also reduces chances of error by thoroughly verifying all maintenance procedures.

The SLC phase also allows systematic recording of system failures, demand rates, results of audits and tests, procedures for revalidation, procedures for tracking maintenance performance, personnel training and competence, periodic proof testing, procedures for decommissioning, etc., which not only reduces risk of accidents, but improves process up-time considerably.



SOURCE: OREDA

Figure 4. Where in the loop do SIS faults happen?

Impact of SLC on Field Devices

As shown in Figure 4, a study from the Offshore Reliability Data Handbook (OREDA) indicates that 92% of all SIS failures occur in field devices such as final control elements and sensors.

By following the SLC steps, the number of dangerous failures in sensor components of SIF loops can be minimized:

- 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 practices and well-proven techniques for process connections and sample lines to prevent blockage, sensing delays, etc. *(Correct specifications)*
- Use analog 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)*

Discussions in this article are limited to the "final control element" of the SIF loop, which is frequently the most unreliable part of the SIF loop.

Final control elements should all be adequately reliable. Those elements, which are required for the actuator to perform its safety function, include valves (shutdown, isolation, block and bleed), pilot valves, valve actuators, positioners, accessories, power supplies and utilities.

Failures of final control elements of the SIF loop can be minimized by 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.); e.g., use of a spring return actuator. *(De-energize to trip) {Proper specifications during SRS}*
- Provision for uninterruptible power or reservoir supplies of sufficient capacity for essential power. *(Energize to trip) {Proper specifications during SRS}*
- Failure detection and performance monitoring (valve travel diagnostics, limit switches, time to operate, torque, etc.) during operation. *(On-line testing and 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}*

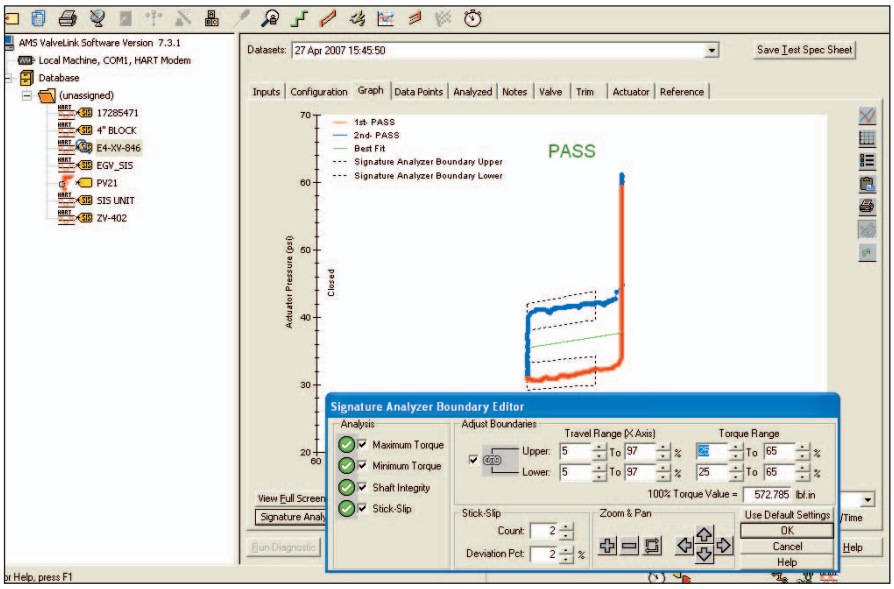


Figure 5. Partial stroke test pass/fail criterion

Other matters that should also be considered are:

- Valves should be properly selected, including choosing the correct sizing for actuator thrust requirements with additional safety cushions as per guidelines. Never assume that a control valve can satisfactorily perform isolation functions without proper design and selection. *(Specifications)*
- Process fluid and physical process conditions should be properly considered for selecting suitable valve type and style. *(Specifications)*
- Metallurgical selection of the valve body, trim material, linkages, etc., should be properly selected *(Technical requirement)*
- Environmental conditions should be taken into account for minimizing stem blockage, corrosion, dust protection, etc. *(Outside environmental conditions)*
- Actuators may also include microprocessor-based digital valve controllers (i.e., smart positioners) with configurable travel, stroking speed, pause time, etc. Normally, it is reasonably practicable for the demand signal to act directly upon the final control element. *(Predictive maintenance)*

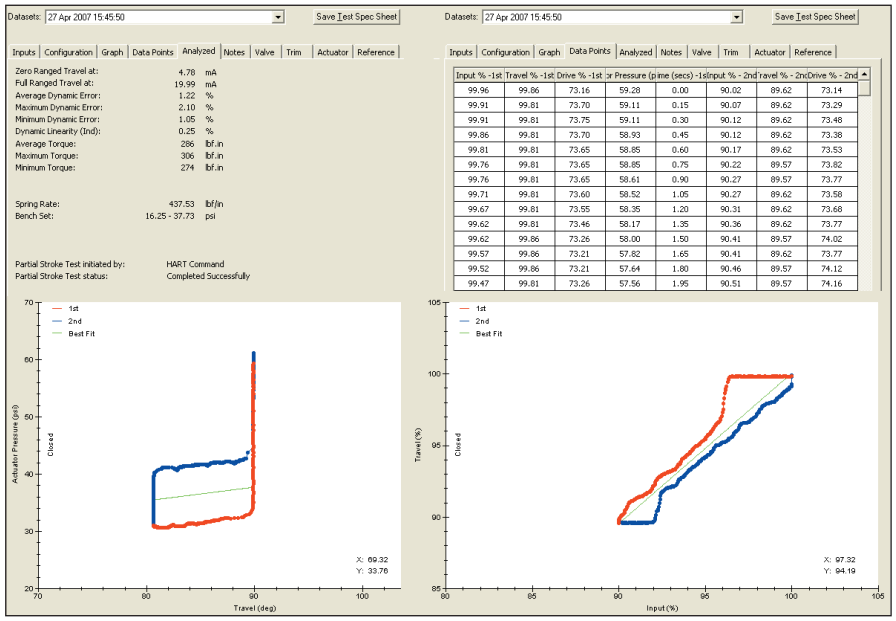


Figure 6. Partial stroke test valve signature analyzed data

Process industries are extending their plant shutdowns from the usual two- to five-year periods. This puts pressure on final control elements, which remain untested for an extended period of time. Following the SLC steps, testing of the final control element should occur at each stage of life-cycle phase. Digital valve controllers are communicating, microprocessor-based devices and have the capability to perform on-line partial stroke testing of final control elements in the SIF loop. Such controllers also provides pass/fail test criterion for easy understanding of test results by operators (Figure 5).

Valve performance trends are monitored and automatically analyzed after each partial-stroke test so that potentially failing valves can be identified long before they become inoperable. The results of a valve signature test (Figure 6) can be used to easily determine packing problems, leakage in the pressurized pneumatic path to the actuator, valve sticking, actuator spring rate and bench set. Therefore, the test can be used to predict when the valve needs maintenance.

Conclusion

The safety life-cycle is an engineering process intended to optimize the design and increase safety of valve processes. This 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 identified problems. A safety life-cycle starts with an initial concept, progresses through design, implementation, operation and maintenance to modification, and finally decommissioning.

Safety life-cycle implementation provides a safer plant with low systematic errors. It decreases the cost of engineering and increases process uptime. It lowers operation and maintenance costs considerably by selecting the right technology.

The SLC process impacts components of the SIF loop. By following SLC guidelines, the right digital valve controller for the "final control element" of the SIF loop can be selected, which can reduce dangerous undetected failures of the field devices. A digital valve controller allows on-line partial stroke testing while the process is running. It also provides remote testing capability allowing for fewer maintenance field trips. In addition, it allows an automated test routine to be established that can produce great savings over time.

For all of these reasons, the safety life-cycle process is certainly a step forward in the direction of improving plant reliability and productivity. **VM**

Riyaz Ali is manager, FIELDVUE Business Development, Emerson Process Management – Fisher Division. Reach him at Riyaz.Ali@emersonprocess.com. ***This article was adapted from a presentation given by the author at ISA EXPO 2005, held Oct. 25-27, 2005, in Chicago.***

REFERENCES

1. International Electrotechnical Commission, "Functional Safety - Safety instrumented systems for the process industry sector" – IEC 61511
3. International Electrotechnical Commission, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems" – IEC 61508