contents

"SAFETY LIFE CYCLE" – IMPLEMENTATION BENEFITS AND IMPACT ON FIELD DEVICES

Riyaz Ali, Manager
FIELDVUE Business Development
Emerson Process Management - Fisher Controls Int'l., LLC.
Austin, TX 78717

KEYWORDS

Safety Life Cycle (SLC), Analysis Phase, Realization Phase, Operation Phase, Safety Instrumented System (SIS), Functional Safety, Systematic Failures, Safety Instrumented Function (SIF), Safety Integrity Level (SIL), Digital Valve Controller, Predictive Maintenance, Safety Audit Documentation

ABSTRACT

The ultimate goal of any organization is to execute all activities so as to achieve a desired level of safety as efficiently and effectively as possible. Governmental safety regulations and international standards all support this goal, with varying degrees of clarity. However, one area of strong agreement in all standards and regulations is the definition of an overall Safety Life Cycle.

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, which is same as IEC61511 with a grandfather clause), 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.

A Safety Life Cycle can be defined as all necessary activities required during the implementation of all Safety Instrumented Functions, starting from the concept phase of a project until decommissioning of the project when all the Safety Instrumented Functions are no longer available for use.

This paper will discuss SLC implementation stages as described by ANSI/ISA S84.01-1996 (Which is the same as IEC61511 except for a grandfather clause), IEC 61508, and IEC 61511.

This paper also discusses the benefits of SLC by providing low systematic failures, reduced risk, increased process up-time, decreased cost of engineering, and design consistency.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

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 testing to improve the Safety Integrity Level (SIL) and the mode and methods of testing will be discussed in length.

INTRODUCTION

The purpose of a Safety Instrumented System (SIS) is to reduce the 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 all supporting safety activities. The ultimate goal of any organization's safety effort is to execute as efficiently and effectively as possible all activities required to achieve the desired level of safety.

The key objective of all international safety standards for plant functional safety is to address accident causes by creating a system to manage safety, to assure proper technical requirements, and to ensure competent personnel. This system is called the Safety Life Cycle (SLC). It is an engineering process designed to optimize the design and to increase safety. This SLC combined with well-accepted quality techniques such as verification, validation, and third party certification has the potential to result in safer and more cost effective systems.

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 IEC61511. The ISA 84.01 standard was the first published functional safety standard and was recognized by OSHA in the United States as an example of good engineering practices.

These standards are gaining wide acceptance and are forming a basis for compliance with local, national and international laws and regulations. Many of the authorities responsible for enforcing these laws and regulations view compliance with international safety standards as equivalent to complying with "good engineering practices." Thus, understanding the overall SLC process should be a pre-requisite for selecting a SIL for any safety related system.

The Safety Life Cycle approach is basically a good, common-sense design process with the same fundamental steps that any good design process would follow. First a problem is identified and assessed – then a design is done to solve the problem. Finally the design is verified (checked and tested) to make sure it actually solves the original problem that was identified.

The SLC is a closed-loop process as described in several functional safety standards, including IEC61508 and IEC61511. The Safety Life Cycle process does not end. Its lifecycle tasks are continuously performed while the process is in operation, and especially when the designs are periodically reviewed and process changes occur. Please see Fig. 1.

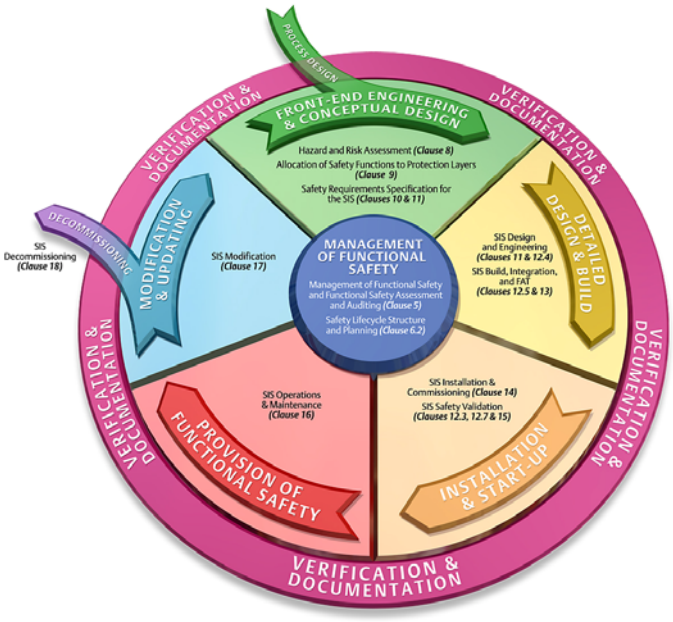

FIG. 1 - SAFETY LIFE CYCLE "CLOSE LOOP PROCESS"

The need for a formally defined SLC process has emerged over last two decades as, the inevitable requirement for better processes eventually pushed control systems to a level of complexity at which sophisticated electronics and programmable systems became the optimal solution for control and safety protection. By adopting the SLC approach, development and engineering time can be reduced, and potentially higher reliability can be achieved.

STANDRDS AND SAFETY LIFE CYCLE

ANSI / ISA S84-01-1996 were the first standard to introduce the Safety Life Cycle concept. A brief SLC of an earlier version of the ANSI/ISA[i] standard is shown in Fig. 2.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

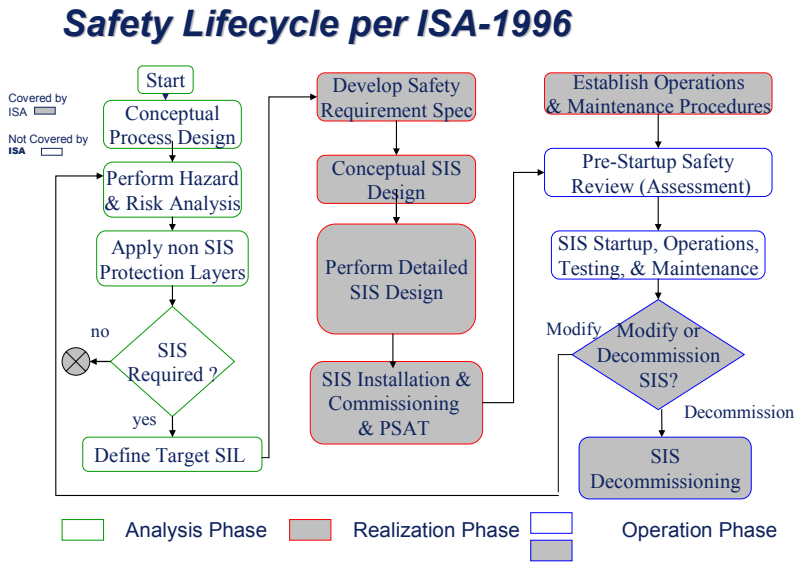

FIG. 2 - SIMPLIFIED SAFETY LIFE CYCLE PER ISA/ANSI S-84.01-1996

The analysis phase covers identification of a hazard, analysis of its consequences and likelihood, and the layer of protection available. It also determines if a Safety Instrumented System (SIS) is required to supplement the currently available layer of protection. Finally, a Safety Integrity Level (SIL) is selected which determines the degree of acceptable risk.

The realization phase focuses on conceptual and detailed design and fabrication of any required SIS. Lastly, the operations phase covers start up, operation, maintenance, and decommissioning of the SIS.

IEC61508 Safety Life Cycle is shown schematically in Fig. 3 below.

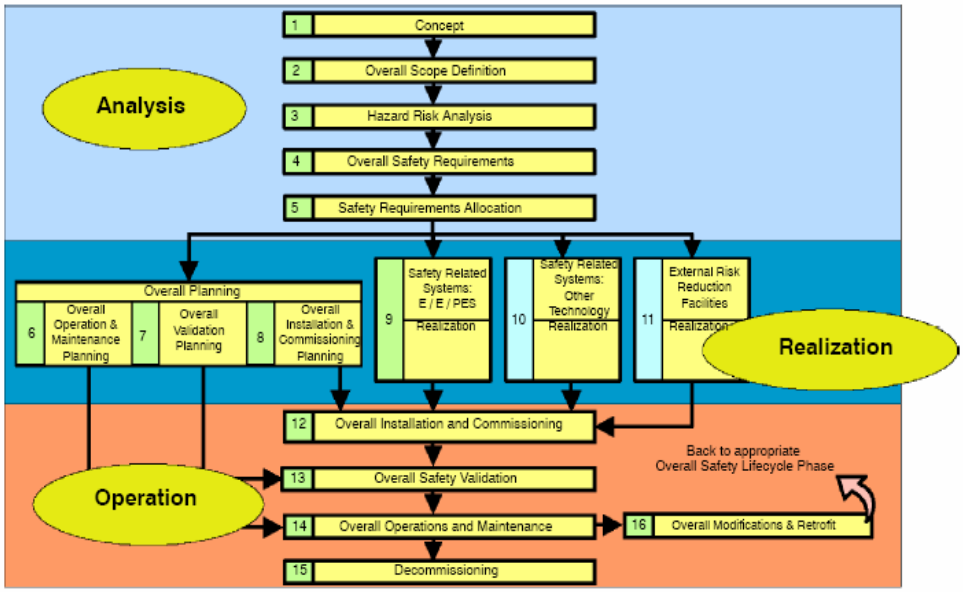

FIG. 3 - IEC61508 SAFETY LIFE CYCLE

The Safety Life Cycle per IEC61508, similar to ISA, can be categorized into three broad areas. First one is the analysis phase that focuses on the identification of hazards and hazardous events, the likelihood of these hazardous events and their potential consequences, the availability of a layer of protection, as well as the need for any Safety Instrumented Systems and the allocated Safety Integrity Level.

The second one is the realization phase, which focuses on design and fabrication of the SIS and the final one is the Operation phase, which covers start up, operation, maintenance, and eventual decommissioning of the SIS. These phases encompass the entire life cycle process of the safety system from concept through decommissioning. Each phase of the overall Safety Life Cycle is divided into elementary activities with the scope, inputs and outputs specified for each phase. Recommendations are provided in IEC61508 regarding the information required to execute each step as well as the output and documentation that should be produced in each step. However, the standard only includes general guidelines and recommendations on the life cycle phases; it is performance based and not prescriptive. It is not meant as a "cook book" for functional safety.

IEC has developed document IEC61511 to provide specific guidance to the process industry using IEC61508 as the umbrella standard . The Safety Life Cycle per IEC61511[ii] is shown in Fig. 4 below. This document also covers the analysis, realization, and operation phases. It emphasizes the continuous functions of planning,

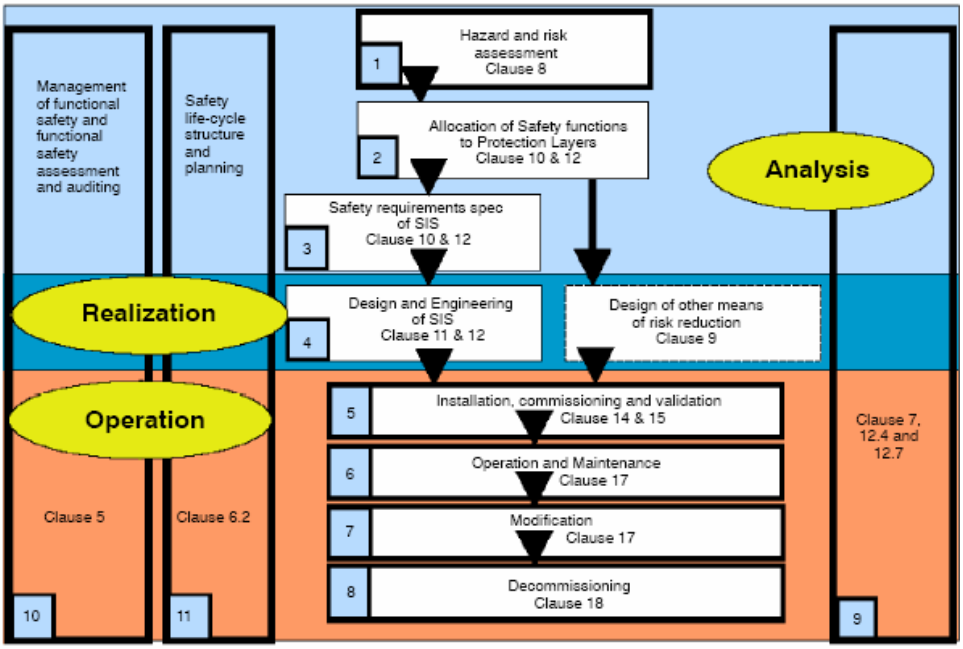

FIG. 4 - IEC61511 SAFETY LIFE CYCLE

management, assessment, and verification, which support the sequential components of life cycle structure.

The essential details of analyzing, designing, verifying, and documenting are discussed and defined in all safety standards. It is important for an organization to devote extra care to the essential Safety Life Cycle so as to ensure that the desired safety level is achieved. A study of actual causes of industrial accidents, performed by the Health and Safety Executive in the United Kingdom, showed that there are a number of causes. The most significant cause (44%) was poor safety function specifications. Other causes included "changes after commissioning (including online changes)" at 21%, operation and maintenance errors at 15%, design and implementation errors at 15%, and installation and commissioning errors at 6%. There were problems in almost every activity leading to an operational Safety Instrumented System; however, it was apparent that better methods were needed in the front-end of the engineering process as well as the back-end. It appeared that a "life cycle approach" was not being used.

PHASES OF SAFETY LIFE CYCLE (SLC)

SLC ANALYSIS PHASE

The initial planning, identification and specification functions that are needed to properly apply safety systems to a process are included in the analysis phase of the SLC. In addition, the individual functions and the flow of information required to perform these tasks most effectively is analyzed.

The SLC begins with conceptualizing the initial design of the process through definition of the project's scope. It is important and critical to clearly identify the project's purpose in terms of goals and measurable outcomes. If the project's initial definitions are ambiguous, team members can develop different versions of the project's scope and thus emphasize potentially conflicting aspects of work. Clear definitions are particularly critical in projects such as grass root new facility constructions that have both operational and safety focused objectives, or process revamps, production or capacity increases of an existing plant or modification of process bottleneck. Ideally, the organization should designate the relative importance, allocate adequate resources, and establish proper scheduling of these objectives at the outset of the project. Similarly, the ultimate responsibility for achieving both the safety related and non-safety related goals should be assigned to a single, competent and knowledgeable individual.

The organization's personnel responsible for safety portion of the project should clearly understand the process, technology, and equipment under control. This understanding should include a basic idea of the potential process hazards and of the equipment and materials present. The organization should also understand that gaining environmental permissions, particularly in developed countries, is often the long lead critical path item when dealing with all the applicable laws, regulations, legislation, and standards. The scope definition should clearly designate the limits of the process, equipment, and areas of operation.

The organization should also consider at the beginning of the project, the level of risk, it will tolerate in its daily operation. This risk level should then be compared to the risks that are present in the process. In this way the organization will know how much process risk must be reduced and what kind of safety equipment is required.

Classification of hazard and risk analysis is the next function of the Safety Life Cycle. This step includes identification of any Safety Instrumented Functions (SIF) that may be needed to detect imminent harm and take the process to a safe state in case of a Demand (i.e., a signal requiring a safety action). The first task for an organization's safety team is to identify the hazards (potential causes of harm) and the hazardous events that may potentially occur in the operation of the equipment or process. Many regulations, laws, and standards rigorously require this identification process by way of a Process Hazards Analysis (PHA). A PHA is a structured brainstorming process by which a team of experts

reviews sections of a process in a systematic fashion to identify hazards that can occur in the process and lists all events that can cause an accident. It then evaluates outcome of the accident, the safeguards that are in place to prevent the accident, and makes recommendations for other measures that should be implemented to reduce the process risks.

After identifying the hazards and potential SIFs, the organization needs to characterize the hazards in terms of both magnitude of their consequences and the likelihood or frequency of their occurrence. Depending upon the hazard, the Consequence Analysis required to estimate the magnitude of potential harm can be quite complex. Analyzing the likelihood component of the risk involves understanding the different sequences of events that can lead to the harmful event.

Layer of Protection Analysis (LOPA) is associated with the likelihood part of the risk analysis to determine the frequency of the potential harmful outcome. The LOPA identifies and quantifies the non-SIS safety features of the process equipment, as well as identifying any other factors that can prevent a harmful incident from occurring. Determining the probability that each of these layers can prevent harm from occurring, combined with the likelihood the harmful outcome will occur, is an important step before considering any required SIF action.

With the information on magnitude of the consequence, the likelihood of its occurrence, and the level of risk an organization is willing to tolerate, one can determine whether an SIS is required to perform the SIF under consideration. After all non-SIS layers of protection have been credited, if there is still any difference between the risk present in the process and the risk the organization can tolerate, it must be made up for by using an SIS. The size of the risk gap or required risk reduction will determine which SIL should be specified for the SIF in question.

Once potential hazards have been identified and characterized along with the risk they pose, as well as identification of any required SIFs, and their corresponding SILs, one must complete the analysis phase of the Safety Life Cycle by documenting these efforts and results in the Safety Requirements Specifications (SRS). The purpose of the SRS, according to IEC61508[iii], "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." The SRS documents serves as the base and documents the requirement for the safety system, to be designed, installed and operated according to the subsequent life cycle phases. The overall objective of the SRS is to specify everything needed to allow the safe and effective realization of the safety instrumented system. A complete, clear, and accurate SRS saves a lot of misunderstanding and rework.

During the conceptual phase, involvement from the end user and various consultants is typically required.

SLC REALIZATION PHASE

The realization phase begins with conceptual design of the safety instrumented system based on the Safety Requirements Specification.

The realization phase of the Safety Life Cycle includes the design, fabrication, installation, and testing of the SIS that was specified in the analysis phase of the project. The realization phase cannot be properly executed if the specifications are not clearly and correctly developed from the results of the analyses conducted in the first phase of the life cycle.

Based on 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. The organization should address this conceptual design at the same time it plans how the prospective system will be tested and verified to ensure it meets specifications before being put into active use. A key part of this planning step is developing maintenance and proof-test schedules to ensure that one can find and repair any potential failure in the safety equipment before the system is required to act. Both the proof-test and repair intervals must be addressed properly since they affect the SIL of the system.

Once the conceptual design is complete, the organization needs to analyze the prospective system to confirm that it meets the SIL that was selected and documented in the Safety Requirements Specifications. This analysis should include both the individual components of the system as well as the architecture used to configure the components. The objective of conceptual design in the safety lifecycle is to select and configure the equipment used in the safety instrumented system and verify that the design meets target goals. Only if the system can be shown to meet the selected SIL can it then be finally designed and fabricated. The detailed design of the SIS should be executed according to clear, well defined and established procedures. IEC61508 presents additional hardware and software Safety Life Cycles specific to the detailed design functions. The standards also require appropriate documentation of both the SIL verification analysis and the detailed design of the SIS.

Planning and executing the system's installation, commissioning, and validation is the final part of realization phase. Once these tasks are finished, the SIS should be fully functional at the Safety Integrity Level that was selected in order to achieve a tolerable level of risk. With this, the SLC realization phase is completed.

Verification and validation are two terms that describe the integrity of a system. The terms are often confused. Verification is an activity of demonstrating for each phase of the safety life cycle by analysis and or test that, for the specific inputs, the deliverables meet the objectives and requirements set for the specific phase. It has more the connotation of an analysis or test intended to demonstrate the correct operation of the system when it is needed. Verifications have more to do with checking of code before

testing (“back check”). Validation, on the other hand, more strongly suggests demonstration of the actual operation and functioning of the equipment in a field situation to ensure that it actually solves the intended problem. Validation is a physical testing of the completed project output and it is more operation and function oriented.

The realization phase is the most resource intensive part of the overall Safety Life Cycle and involves the end user, vendors & contractors.

SLC OPERATION PHASE

The operation phase of the safety lifecycle begins with a validation of the design. The operation phase has the longest duration of all the SLC phases. It begins at start up of plant and continues until the SIS is decommissioned or redeployed. The most significant part of this phase is the maintenance and testing of the SIS. The system's SIL can be affected by the number of times it 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 that the plan is being followed. Effective management of change is also important so that any potential modifications to the system can be addressed properly. The safety lifecycle continues with a careful look at modifications. For all modifications, the engineer must go back to the appropriate step in the safety lifecycle. Depending on the exact nature of the modifications, such change management should include a full return to the concept phase when circumstances warrant. For an example, if new technology is chosen, the SIL verification must be repeated. Decommissioning is also considered as well in SLC. The effect of decommissioning on the system must be analyzed. Are all safety instrumented functions need to be analyzed, before switched off permanently. The organization should analyze the effect of the decommissioning on both the equipment and process directly under control and on any closely integrated systems.
If some are still needed, then they must be relocated or decommissioning must not proceed. The decommissioning of the SIS ends the Safety Life Cycle.

In short the operation phase of the Safety Life Cycle begins with a validation of the design. Does the system actually solve the problems identified during the hazard analysis? Have all necessary design steps been carried out successfully? Has the design met the target SIL for each Safety Instrumented Function? Have the maintenance procedures been created and verified? Is there a management of change procedure in place? Are operators and maintenance personnel qualified and properly trained? If the answers to these questions are acceptable, the process can proceed with startup and operation. The Safety Life Cycle continues with a careful look at modifications and decommissioning. For all modifications, the engineer must go back to the appropriate step in the SLC. For example, if new technology is chosen, the SIL verification must be repeated. The effect of decommissioning the system must be analyzed. Are all Safety Instrumented Functions no longer needed? If some are still needed, then they must be properly relocated or decommissioning must not proceed. The validation task in the operation phase of the Safety Life Cycle is especially important. It is at this point that all Safety Life Cycle activities are reviewed to ensure that the right steps were carried out and that the documentation is in place.

The longest phase of SLC requires involvement of End User, & 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 risk while maintaining internal design consistency.

The Safety Life Cycle was created not only to help Safety Instrumented System designers build safer systems but to help create more cost effective systems. By precisely analyzing the process risk, a system can be designed to meet that particular risk. Costly problems of the past have included systems that were over-designed in accordance with older "prescriptive" standards, but in reality would not meet the expected risk reduction, and then there were systems with costly redundant logic solvers and ineffective field equipment.

The Safety Life Cycle and closed-loop verification concepts should result in safer, more cost effective system designs by having fewer Systematic failures, lower cost of engineering, and more process up-time.

If the Safety Requirements Specifications have been defined properly during the Safety Life Cycle analysis phase, risk will definitely be reduced. This will certainly be true if the Safety Instrumented Functions, the needed functionality with actions to be taken, process input and trip points, process output and actions, response actions, operator interface, process safety timing, maintenance, manual shutdown, and bypass requirements, and any known special requirements are rigorously defined. If the work is done well, the efficient SLC process of "plan, do and review" significantly reduces waste from over-design of safety systems, as well as limiting unsafe conditions resulting from under-design.

If compliance with the standards is done poorly, following the Safety Life Cycle model is essentially useless and typically rather expensive. During the analysis phase, proper identification of all hazardous situations with their consequences to human life, property, surrounding environment, and business interruption, along with determining the likelihood of their occurrence, will often require only moderate changes to existing company safety system practices with relatively minor cost. Incurring this minor cost at the beginning of the project is more desirable than dealing with the cost of a major accident such as the 1984 Bhopal Gas disaster in India.

The realization phase of the Safety Life Cycle begins with conceptual design of the Safety Instrumented System based on the Safety Requirements Specification. The desired technology is chosen for the sensors, logic solver and final control elements. Often redundant devices are selected based on experience in Safety Instrumented System design. Redundancy configurations (such as 1oo1, 1oo2, 2oo3, 1oo2D, etc.) that can be

used are defined in IEC 61508. The specific architecture chosen depends on safety and process availability needs. The architecture of the protective system should be designed to protect against random hardware failure. Proper selection of technology and correct specification of equipment leads to lesser immature failures, reduced maintenance and fewer plant shutdowns.

It should be demonstrated that the required reliability has been achieved commensurate with the required integrity level. Defensive measures may include high reliability elements, automatic diagnostic features to reveal faults, and redundancy of elements (e.g. a 2oo3 configuration for sensors) in order to provide fault tolerance. Diversity of elements is not effective for protection against random hardware faults, but it is useful in defense against common mode failures within a protective system.

If this step of the realization phase is done properly it not only reduces the equipment cost, design cost, installation cost, initial training and the start up system commissioning cost but it can tremendously improve safety as well. The saying is true that, "Cheap products are not Good, and Good products are not Cheap." Higher quality normally brings higher reliability. This means that higher initial procurement cost brings lower future operating cost.

A periodic test interval needs to be defined. This periodic testing is done to insure that all elements of the system are operational and to verify that no failures have occurred. In some industries, a periodic inspection is done more frequently and online test facilities are designed into the system. By selecting suitable technology, better design equipment not only reduces redundancy but also allows diagnostic information to be obtained. If selected equipment can provide the capability for online testing to meet the periodic test interval required by the target Safety Integrity Level, then the possibility of improving the SIL exists. Improving the Safety Integrity Level with fewer field devices can provide fewer burdens on maintenance cost as well as reducing spurious trips.

When the conceptual design is complete, the detail design work, including wiring drawings, installation planning, programming of the logic solver, and selection of field devices, etc. is done. As in normal practice, this work must be documented, typically in a detailed design document. This will provide an advantage of design consistency across all the units in a plant.

The realization phase ends with the system installation, commissioning and startup acceptance testing where the design verification is completed. This step not only provides uniformity of SIS design throughout the plant, but it also reduces chances of error by thoroughly documenting all the maintenance procedures.

After the realization phase is complete, the operation phase of the Safety Life Cycle starts, and it continues until the end of decommissioning the SIS. The operation phase requires proper documentation for maintaining and operating a plant in a safer manner. This is done by systematically recording system failures, demand rates, results of audits and tests, procedure for revalidation, procedure for tracking maintenance performance,

personnel training and competence, periodic proof testing, procedures for decommissioning, etc. Following these steps not only reduces the risk of unwanted accidents, but it improves process up-time considerably. This allows the plant to run more efficiently and effectively to increase production output. Operating cost can overshadow procurement cost in many systems. Depending upon consequences of lost production, operating cost may dominate any life cycle cost study. By not following properly operation phase of SLC, it might become a major cause of accidents like the 1988 Piper Alpha incident in the North Sea, or the Flixborough, UK incident in 1974.

IMPACT OF SLC ON FIELD DEVICES

As shown in Fig. 5, a recent study reports from OREDA (Offshore Reliability Data Handbook) that 92% of all SIS failures occur in field devices such as final control elements and sensors.

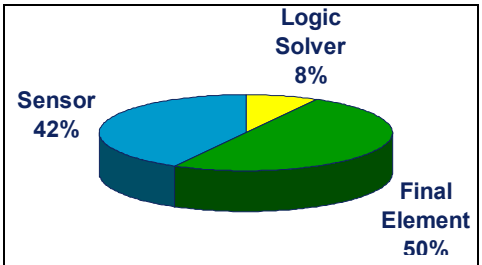

FIG. 5 – WHERE IN THE LOOP DO SIS FAULTS HAPPEN - ? OREDA

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

- 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)

Discussions in this paper will be limited to the "Final Control Element" of the SIF loop. 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 analog 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.

Dangerous failures of final control elements of SIF loop can be minimized 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.); 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 & 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}

Other matters that should also be considered are:

- Valves should be properly selected, including correct sizing for actuator thrust requirement with additional safety cushion as per guidelines. It should never be assumed that a control valve can satisfactorily perform isolation functions without proper design and selection; (Specifications)
- Process fluid and physical process condition should be properly considered for selecting suitable valve type and style. (Specifications)

- Proper metallurgical selection of the valve body, trim material, linkages, etc. (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. It is normally reasonably practicable for the Demand signal to act directly upon the final control element. (Predictive Maintenance)

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 2 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.

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 on-line 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 6).

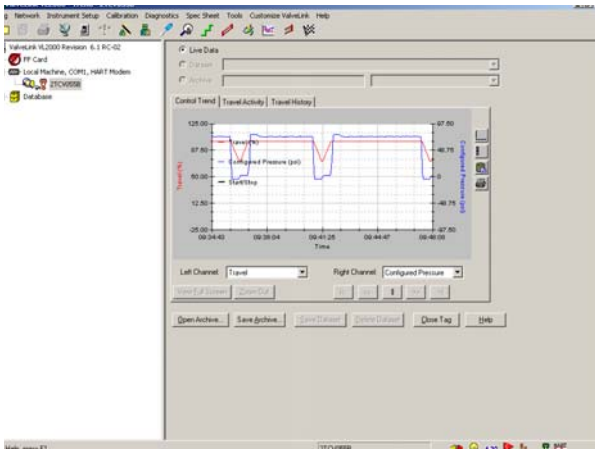

FIG. 6 – VALVE TREDNDING STATUS

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

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. 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 Fig. 7) can be used to easily determine packing problems (through friction data), leakage in the pressurized 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.

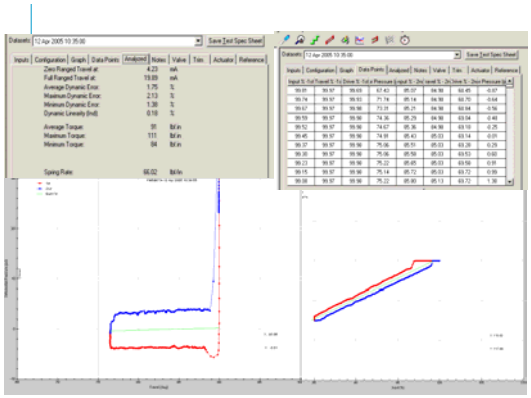

FIG. 7 – VALVE SIGNATURE TEST

A Digital Valve Controller during its normal operation has the capability to continuously check device integrity, and if any component fault is detected it sets an alert which can be assessed by the Field Communicator or Companion software. Digital valve Controller can also notify key plant personnel for critical alerts via email or pager enabling them to take timely and precise corrective action.

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 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.

CONCLUSION

The Safety Life Cycle is an engineering process intended to optimize the 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 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 categorized 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).

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 & Maintenance, Periodic Functional test,
- Modification,
- Decommissioning.

Safety Life Cycle implantation 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 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 establishment of an automated test routine that can produce great savings in time.

Digital Valve Controllers are a great aid to predictive maintenance by providing a Valve Degradation Analysis that is important for critical valves in safety related systems. This feature also reduces the amount of scheduled maintenance. If for any reason the valve is found to be stuck when performing the partial-stroke test, with digital valve controller intelligence, it will not completely exhaust the actuator pressure, thus assuring that, should the valve become unstuck, it will not slam shut. These Digital Valve Controllers will then abort the test and send an alert signal to the operator warning that the valve is stuck.

The Digital Valve Controller provides a time and date stamp on all tests and reports. This is very important for complying with the requirements of statutory authorities. It also provides the capability for comparing and interpreting diagnostic data.

The Safety Life Cycle process is certainly a step forward in the direction of improving plant reliability and productivity. National and international standards stress that these steps should be followed comprehensively in order to reduce associated process risk and cost of engineering. Due to the increased requirements for advanced control measurement in the process industry, single loop controls are a memory of the past. This essentially demands more electronics and programmable electronics technology in the field of control instrumentation. Thanks to the present day development of technology in control instrumentation, industry is able to meet their increasingly complex requirements. However, more microprocessor-based devices in the control room and the field are imposing new challenges from a reliability aspect. The Safety Life Cycle is the right process to provide safety and plant reliability of Safety Instrumented Systems.

Field devices have shown considerable failures in the past, and using Digital Valve Controllers on the "Final Control Elements" of SIF loops can minimize these dangerous failures. The Digital Valve Controller provides testing of the mechanical parts of the final control element and this reduces the PFD (probability of failure on demand). By using a microprocessor-based Digital Valve Controller, diagnostic information about valve health will put the system into a predictive maintenance mode rather than preventive. Finally, safety audit documentation is important for SIS components for future comparison and analysis.

REFERENCES

[i] ANSI/ISA-S84.01-1996 – Application of Safety Instrumented Systems for the Process Industries

[ii] International Electrotechnical Commission, "Functional Safety - Safety instrumented systems for the process industry sector" - IEC61511

[iii] International Electrotechnical Commission, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems" - IEC61508

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org