

## A New Way to Look at Safety

For a long time, designers of offshore platforms only looked to API RP 14C for guidance when designing safety systems for offshore platforms. However, in recent years another standard is also being considered: IEC-61511. EDG has created **SILPAX** to aid in implementation of IEC-61511. OSHA recognizes IEC-61511 as a “good engineering practice” for reducing process-related risk. The **SILPAX** process produces a unique set of deliverables that ensures the safety system is designed and tested to reduce risk to an acceptable level. A safety system designed using the **SILPAX** process is a highly reliable system of interconnected sensors, final elements, and logic solver meant to back up the control system. The system does not have anything to do when conditions are normal; its job is to “wait” for conditions to get out of control. When that occurs, the system must take action to stop a hazard from taking place. In other words, the safety system must “perform on demand.” This performance is ensured by establishing performance levels for the SIS design and verifying the design will meet these levels with supporting calculations using established failure rate data.

(See inside flap for more information.)



Give the Edge to EDG

### HOUSTON

10777 Westheimer, Suite 700  
Houston, Texas 77042  
713.977.2347

### NEW ORLEANS

3900 N. Causeway Blvd., Suite 700  
Metairie, Louisiana 70002  
504.455.0858

### LAFAYETTE

1819 West Pinhook Rd., Suite 210  
Lafayette, Louisiana 70508  
337.269.5900

### COLUMBUS

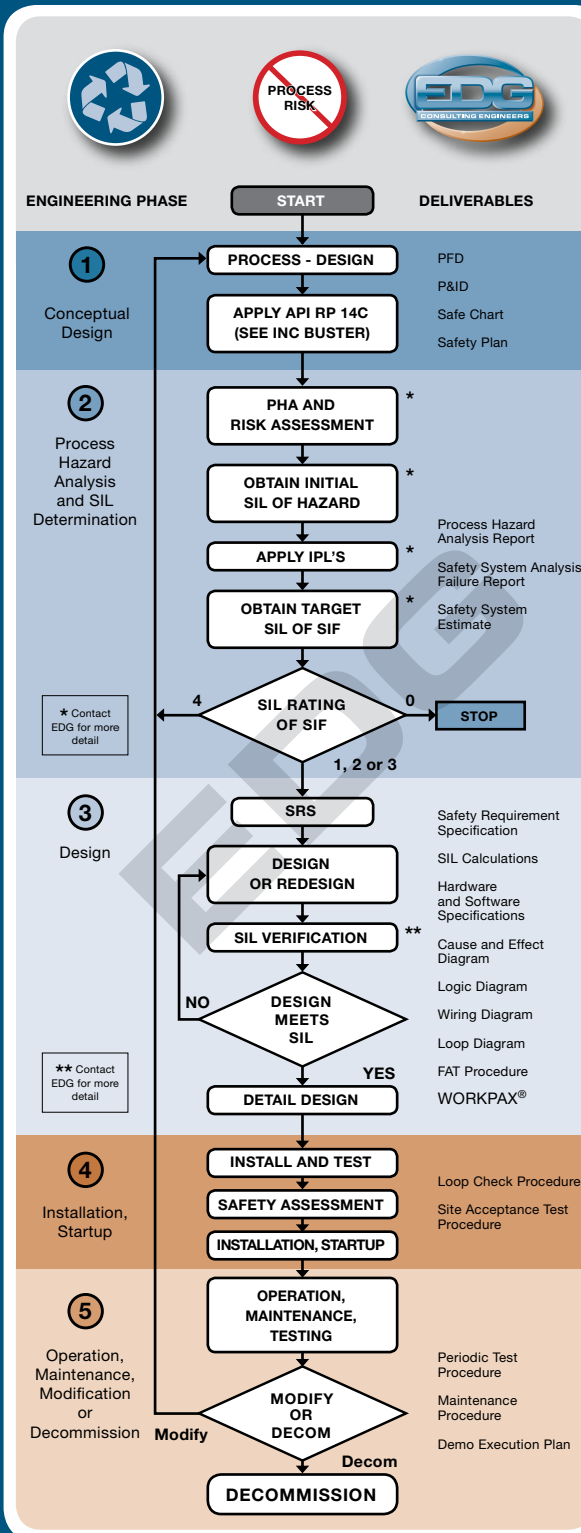
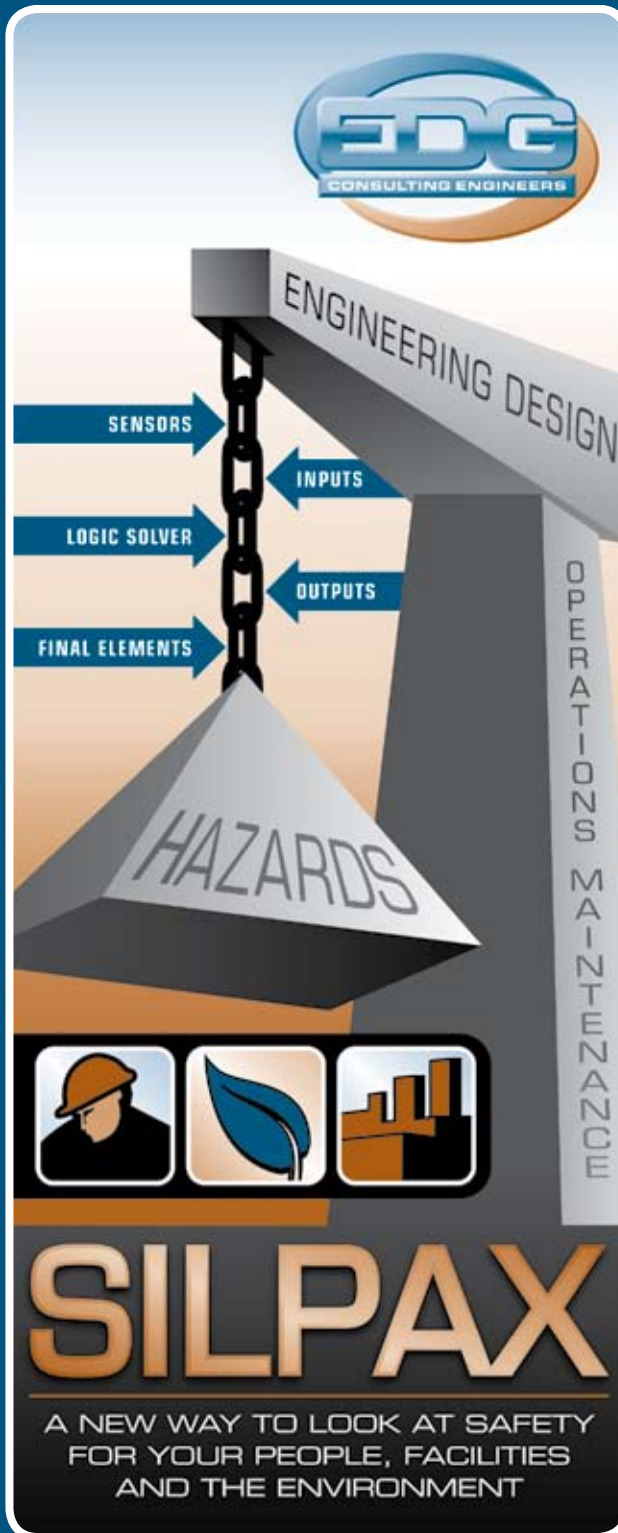
53 Dorchester Square Ln., Suite B  
Westerville, Ohio 43081  
614.891.9920

### ANGOLA

EDG Projectos Angola, Lda.  
Rua Do Robert Shields #8  
Luanda, Angola  
011.244.222.396308  
011.244.222.396353

### VIETNAM

33 Mac Dinh Chi Street  
Ward DaKao, District 1  
Ho Chi Minh City, Vietnam  
Phone 84.8.291.4086  
FAX 84.8.291.4085



SILPAX



### What is SILPAX?

Experience has shown that attention to detail is an important consideration when designing, operating, maintaining and decommissioning a safety system. The safety life cycle is a series of steps that map out important activities that should take place to ensure a safety system performs as expected throughout its life cycle. When these steps are implemented correctly, one can have peace of mind that process risks have been reduced to an acceptable level.

The life cycle diagram on this document represents EDG's method for implementing requirements found in ANSI / ISA standard 84.00.01 and its international counterpart, IEC-61511.

- The life cycle starts with conceptual design of the process. This is where the objectives of the process are converted to PFDs and where API RP 14C is used to develop initial P&IDs and Safe Charts. It is also where a Safety Plan is developed for the project.
- The next life cycle step is the Process Hazard Analysis and SIL Determination. This is where process risks are assessed and the performance level of the SIS is identified. Good practice would require redesign of the process system if a performance level of SIL 4 was obtained for the SIS.
- The Design step is the next step in the safety life cycle. This is where the SRS is written and the performance of the design is verified. It is also where detail design of the SIS takes place and where documents necessary for testing and installation are produced. It is also where testing and maintenance procedures are made available.
- The next life cycle step is where Installation and Startup take place. This is where the SIS is tested prior to startup.
- The last step of the life cycle addresses Operation and Maintenance modification and decommissioning of the SIS. Modifications must be subjected to all steps of the life cycle. Decommissioning must be done in a way that maintains safety. This is where demolition execution plans are followed.

- SIL** is a term used in ANSI / ISA 84.00.01 and IEC-61511. It is the Safety Integrity Level, and it defines the performance level that is required of a particular safety function.
- IPL** stands for Independent Protection Layer.
- Target SIL** is the SIL rating of a particular safety function.
- API RP 14C** is an API recommended practice for design of safety systems on offshore platforms.
- Safe Chart** is a matrix that defines the causes and effects of an offshore platform. It is required by RP14C.
- The **Safety Plan** contains management activities that are necessary to ensure function safety objectives are met. ANSI / ISA 84.00.01 and IEC-61511 refers to this as “Management of Functional Safety.”
- SIS** stands for Safety Instrumented System. It is a safety system that meets the requirements of ANSI / ISA 84.00.01 or IEC-61511.
- SRS** is the Safety Requirement Specification. It is a requirement of ANSI/ ISA 84.00.01 and IEC-61511. It specifies the requirements of the safety instrument function(s).
- SIF** stands for Safety Instrumented Function.
- WORKPAX®** is EDG's Detailed Construction Procedure.

This informative document was produced by the E&I Department of EDG. Questions? Contact Wayne Ruschel, PE at [wjruschel@edg.net](mailto:wjruschel@edg.net).

# IEC-61511 Overview

Clauses in 61511	Topic	Part 1 Summary	Objective
1	<b>Scope</b>	This standard places requirements on the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state.	To define what this standard applies to.
2	<b>Normative References</b>	References other IEC documents that are helpful when applying requirements of 61511.	To identify other standards that are helpful.
3	<b>Abbreviations &amp; Definitions</b>	No summary required.	To define abbreviations and terms used in this standard.
4	<b>Conformance to the Standard</b>	"To conform to this standard it shall be shown that each of the requirements outlined in clauses 5 through 19 has been satisfied to the defined criteria and, therefore, the clauses' objective has been met."	To underline the importance of complying with the entire standard.
5	<b>Management of Functional Safety</b>	Identify the policy and strategy for achieving safety along with the means for evaluating its achievement throughout the project organization.	To identify the management activities that are necessary to ensure the functional safety objectives are met.
6	<b>Safety Life Cycle</b>	Organize technical activities into a safety life cycle to ensure that adequate planning is used to make certain that the Safety Instrumented System (SIS) shall meet the safety requirements.	To define the phases and establish the requirements of safety life cycle activities. To organize the technical activities into a safety life cycle. To ensure that adequate planning exists (or is developed) that makes certain the SIS meets the safety requirements.
7	<b>Verification</b>	Demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phase of the safety life cycle identified by verification planning.	To demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases of the safety lifecycle identified by the verification planning.
8	<b>Process Hazard and Risk Analysis</b>	Determine the hazards and hazardous events associated with the process.	To determine hazards and hazardous events of the process and associated equipment. To determine the sequence of events leading to the hazardous event. To determine the process risk associated with the hazardous events. To determine any requirements for risk reduction. To determine the safety functions required to achieve the necessary risk reduction. To determine if any of the safety functions are safety instrument functions. To allocate safety functions to protective layers.
9	<b>Allocation of Safety Functions To Protective Layers and Determining the Safety Integrity Level (SIL)</b>	Identify layers of protection and their associated SIL rating.	To determine the required safety instrumented function. To determine, for each safety instrumented function (SIF), the associated SIL. To specify the requirements for the safety instrumented functions.
10	<b>Safety Requirement Specification</b>	Comprehensive description of safety system requirements, features, functions and performance levels.	To specify the requirements for the safety instrumented functions.
11	<b>SIS Design and Engineering</b>	Construction documents that can be used to build a safety system containing required safety functions that will operate at a specified performance level.	To design one or multiple SIS to provide safety instrumented functions and meet the specified SILs.
12	<b>Requirements for Application Software</b>	Provide requirements for application software.	To provide requirements for application software.
13	<b>Factory Acceptance Test</b>	A test that confirms the software and associated logic solver hardware will satisfy requirements of SRS.	To test the logic solver and associated software together to ensure that they satisfy the requirements defined in the Safety Requirement Specification (SRS).
14	<b>Installation and Commissioning</b>	Installation of the system in accordance with engineered documents. Commission SIS so that it is ready for final validation.	To install the SIS according to specifications and drawings. To commission the SIS so that it is ready for final system validation.
15	<b>Validation</b>	Confirm that the SIS and its SIFs achieve the requirements of the SRS.	To validate through inspection and testing that the installed and commissioned SIS and its associated SIFs achieve the requirements as stated in the SRS.
16	<b>Operation and Maintenance</b>	Ensure the SIL of each SIF is maintained during operation and testing.	To ensure that the required SIL of each SIF is maintained during operation and maintenance. To operate and maintain the SIS so that the designed functional safety is maintained.
17	<b>Modification</b>	Ensure required SIL of the SIS is maintained before, during and after modifications.	To ensure modifications to any SIS are properly planned, reviewed and approved prior to making a change to the SIS. To ensure that the required safety integrity of the SIS is maintained despite any changes made to the SIS.
18	<b>Decommissioning</b>	Ensure decommissioning activities do not affect SIL requirements.	To ensure that prior to the decommissioning of a SIS from active service, a proper review is conducted and required authorization is obtained. To ensure SIFs remain operational during decommissioning activities.
19	<b>Information and Documentation</b>	Ensure that necessary information is available and documented in order that all phases of the safety life cycle can be effectively performed, verified, validated and assessed.	To ensure that the necessary information is available and documented so that all phases of the safety life cycle can be effectively performed. To ensure that the necessary information is available and documented so that verification, validation and functional safety assessment activities can be effectively performed.