MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Adapting cause and effects methodology to your Safety instrumented system (SIS) to reduce human errors from engineering, operations and beyond

Charles M. Fialkowski, CFSE & Luis M F Garcia G, CFSE
Siemens Industry Inc.
Charles.Fialkowski@siemens.com & luisgarcia@siemens.com

Keywords: Process Safety, safety instrumented systems, IEC 61508, ANSI/ISA 84, IEC 61511, Safety PLC, safety lifecycle, cause and effects, Safety Integrity Level, SIL, Probability of Failure on Demand, PFD, Risk Reduction Factor

Abstract

A safety instrumented system (SIS) is used to implement one or more Safety Instrumented Functions (SIFs)[1] which are designed to reduce the likelihood of hazardous risk by decreasing the frequency of unwanted events (accidents). The amount of risk reduction that an SIS can provide is represented by its safety integrity level (SIL). The SIS is designed to detect when the process reaches a hazardous condition and respond accordingly to move the process to a safe state, thus preventing the unwanted accident from occurring. Studies indicate however, that over 50% of all SIS failures are related Systematic faults introduced by human error. While many SIS systems boast having SIL 3 certification, it's often the human interactions that render many of these well intended systems to be essentially idle. A cause and effects methodology is an approach many in the industry are exploring to help reduce human errors throughout the entire safety lifecycle of the SIS.

1 Introduction to Cause and Effects Methodology

Logic is defined as the science of correct reasoning, or necessary connection or outcome, as through working of cause and effect. Any problem, if approached logically, will either yield a solution, or verify that a solution is not possible. By examining all eventualities with respect to causes and effects a solution can usually be found.

[1] IEC 61511-1:2016, page 26 - 3.2.66 Safety Instrumented Function - SIF

The cause and effect diagram is used for defining how and when actions are executed in a safety system. This methodology involves organizing process events into categories of causes and effects and then linking them together logically via the intersection which will indicate what effect(s) will result from which active cause(s).
There are, therefore, three key fields of information contained in the cause and effect diagram. A cause occupies a row, an effect occupies a column and the intersection is the cell which is common between a cause row and an effect column and determiners the relationship between both of them. These fields may contain and represent the following functional requirements for a safety instrumented system as shown below in Figure 1:

- Cause - This field reflects a process deviation. When the cause tags meet certain user-configured conditions, it becomes active.

- Effect - This field reflects a process action. When the effect is active, the effect tags will be set to their failsafe values.

- Intersection - This field determines how the effect responds to the cause. If the intersection is empty, the cause does not influence the effect. If the intersection is configured, an active cause will trigger the associated effect and the effect will become active.

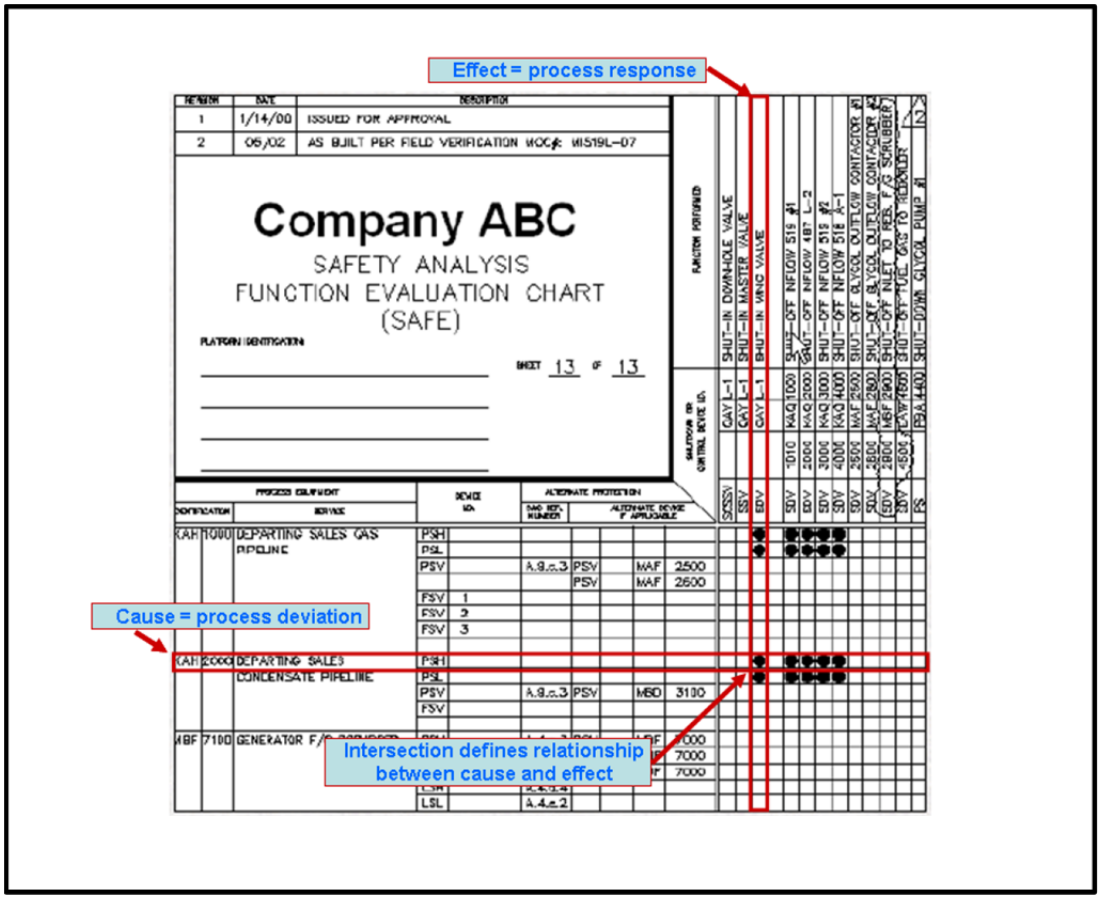


Figure 1 - Cause and Effect Diagram

2 The Safety Lifecycle

In 1995, the U.K. Health and Safety Executive (HSE) published a report titled "Out of Control: Why Control Systems Go Wrong and How to Prevent Failure"[2] where they analyzed the root cause of several industrial accidents that were initiated by failure of the control system and published the chart shown in Figure 2, showing where failure occurred. They updated their publication in 2003 where they noted the analysis of incidents remained unchanged from the first edition.

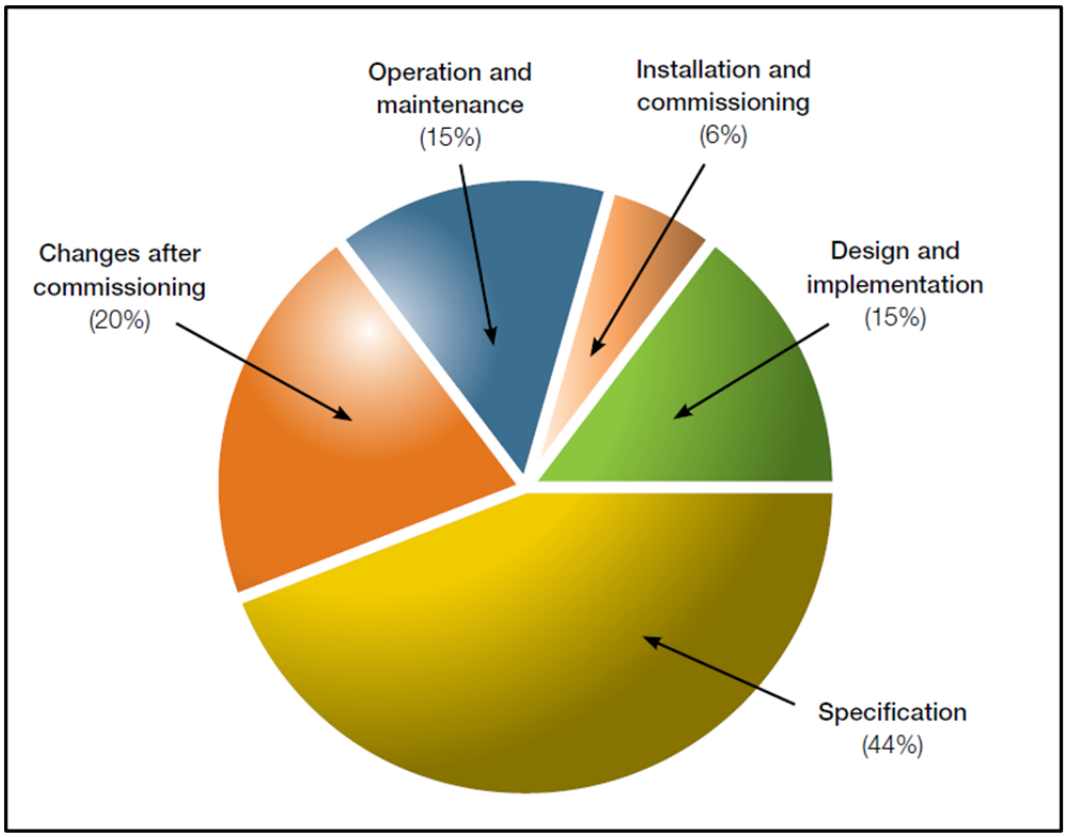


Figure 2 - Root Cause of Control System Failures

In many ways, it was the findings of this study that led to the development of the safety design lifecycle which serves as the basis for international standards on functional safety such as the IEC 61511:2016 standard. The safety design lifecycle is a practical methodology that defines the process necessary to ensure overall plant safety by defining a sequence of steps and deliverables from each phase to help prevent the failures that were identified in the HSE report.

Figure 3, shows the safety life-cycle as described in the IEC 61511 standard[3]. The lifecycle can be divided into three main phases; the analysis phase, the realization phase and the operation phase. The analysis phase is focused on determining and documenting how much safety is

[2] Out of Control – Why Control System go wrong and how to prevent Failure – 2nd Edition 2003 – Page 31
[3] IEC 61511;2016, page 38

needed. The realization phase is focused on the design and implementation of the system and safety achieved. The operation phase is focused on the activities and documentation required in operating and maintaining the system to ensure the performance is maintained.

The safety life-cycle phases are meant to address the root causes of failure as identified by the HSE. The analysis phase is focused on addressing the percent of failures caused by improper specification by requiring quantitative risk analysis and risk reduction techniques resulting in a safety requirements specification (SRS). The realization phase is focused on minimizing the failures caused by design & implementation and installation & commissioning. It does so by requiring documented verification that the design meets the targets defined in the analysis phase. The operation phase is focused on addressing the percentage of failures caused by improper operation & maintenance and changes after commissioning. Again, this is accomplished through mandatory procedures and documentation.

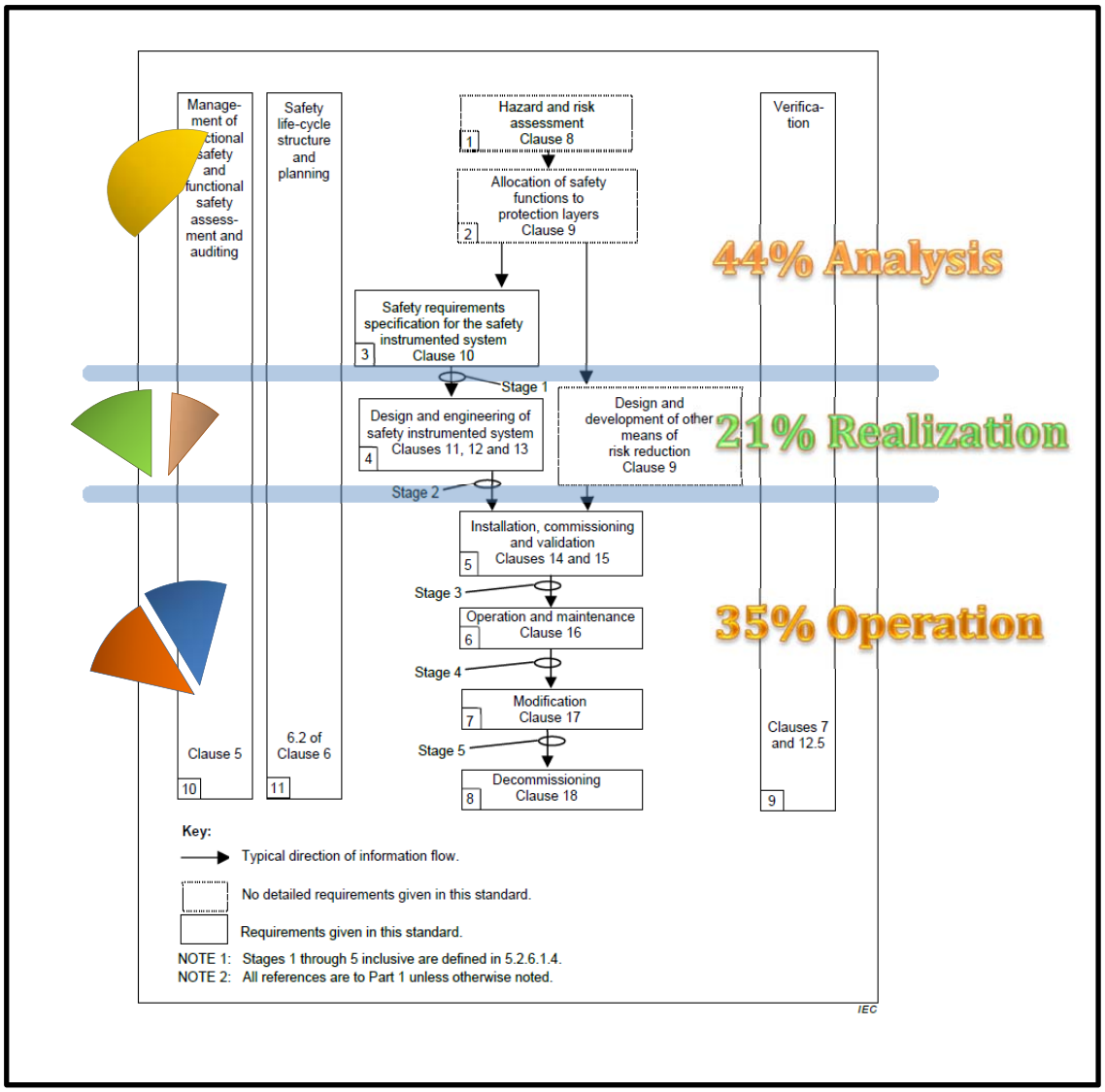


Figure 3 - SIS Safety Life-Cycle Phases

3 The IEC 61511 standard requirements

In June 2016, the IEC technical committee released the 2nd edition of their functional safety standard titled "Safety instrumented systems for the process sector". This edition cancels and replaces the first edition which was published in 2003, and includes a number of editorial improvements (definitions, etc.), and technical changes specifically around the requirements to improve the management of functional safety.

Safety instrumented systems (SISs) have been around for many years to perform safety instrumented functions (SFIs) in the process industries. If instrumentation is to be effectively used for SIFs, it is essential that they can achieve certain minimum performance levels. The IEC 61511 standard drives towards two basic concepts which are fundamental to its application, the SIS safety life-cycle and safety integrity levels (SILs).

Fundamentally, the goals and purpose of the 2nd edition of the IEC 61511 standard is identical to the first edition which maintains the same general title "Functional safety: Safety Instrumented Systems for the process industry sector" as well consisting of the same 3 parts:

1. Part 1: Framework, definitions, system, hardware and software requirements - normative
2. Part 2: Guidelines in the application of IEC 61511-1- informative
3. Part 3: Guidance for the determination of the required safety integrity levels - informative

The principle behind this standard is simple. Follow the activities of the safety lifecycle, make sure you achieve the defined minimum requirements, and document everything. This approach is intended to direct a process that is rational and consistent. To facilitate this approach, this standard requires the following:

- a hazard and risk assessment is carried out to identify the overall safety requirements
- The allocation of the safety requirements to the safety instrumented system(s)
- works within a framework applicable to all instrumented methods of achieving functional safety
- Details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety

Specifically this standard addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning. In order to claim conformance to this standard the owner/operator would have to demonstrate that the requirements outlined in clause 5 through 19 have been satisfied. This paper will discuss how adopting a cause and effects methodology, may be used to satisfy most of these requirements.

Clause 5: Management of functional safety

The objective of clause 5 is to identify the management activities (organizational, planning, assessment, etc.) that are necessary to ensure the functional safety for the SIS is met.

In general it contains the policy and strategy for the organization on how to achieve functional safety. Sub-clause 5.2.7 requires SIS configuration management techniques have to be developed specifically for the application program of the SIS where proper revision control shall be maintained. An example of revision control is shown in Figure 4. This process requires that if further changes are made (after properly reviewed and approved) by the SIS designers, the revision of the cause and effects diagram may be incrementally advanced forward allowing for appropriate descriptions of the changes to be captured as well.

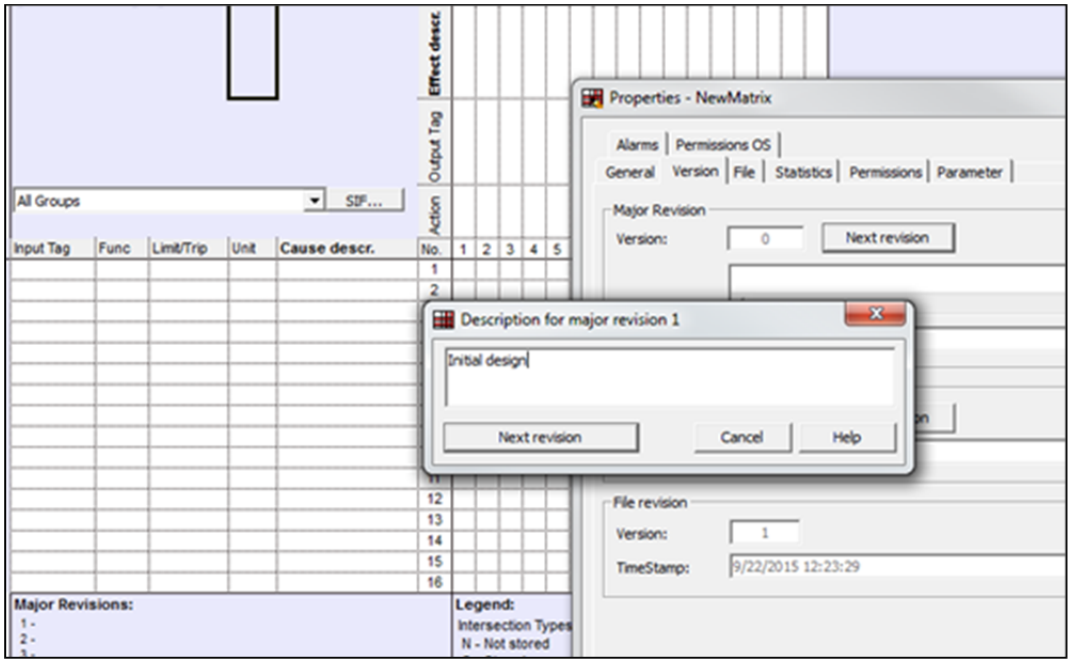


Figure 4 - Example of Revision Control

Clause 6: Safety life-cycle requirements

The main objective of clause 6 is to define the phases and establish the requirements of the SIS safety life-cycle activities and to ensure that adequate planning exists to make certain the SIS meets the safety requirements.

A cause and effects diagram will not only help management organize and define their safety strategy, but will also help to present their safety philosophy in a clear concise manner that various levels can read and understand. Prior to this, a control narrative would have to be derived from reading complex logic charts. This process often took many man hours to compete as it might require the attention of multi-disciplined personnel.

The cause and effects diagram will significantly reduce the time it takes to organize the technical functions of the safety system. It is noted in the standard that the SIS requirements should be expressed and structured in such a way that they are clear, precise, verifiable, maintainable, and written to aid comprehension by those who are likely to utilize the information at any phase of the lifecycle.

Traditionally, safety logic would be in the form of high level programming language such as Boolean algebra or ladder logic. It would consist of several defined "logical connections" or relationships between variables that depend on, or follow each other logically. Either of these procedures are fine for Safety PLC programmers, but additional work would still be required to meet the criteria for properly documenting the safety functions.
Take for example the logic shown below in Figure 5. This indicates how a fired heater shutdown system needs to be operated. This form is again fine for programming but would not be acceptable for documentation. From this logic diagram, a control narrative would still need to be developed to clarify the operation of this "de-energized to trip" logic circuit as many would find this counter-intuitive to the way it is diagramed below where a logic 0 at the final control element would equal an active state (i.e. closed).

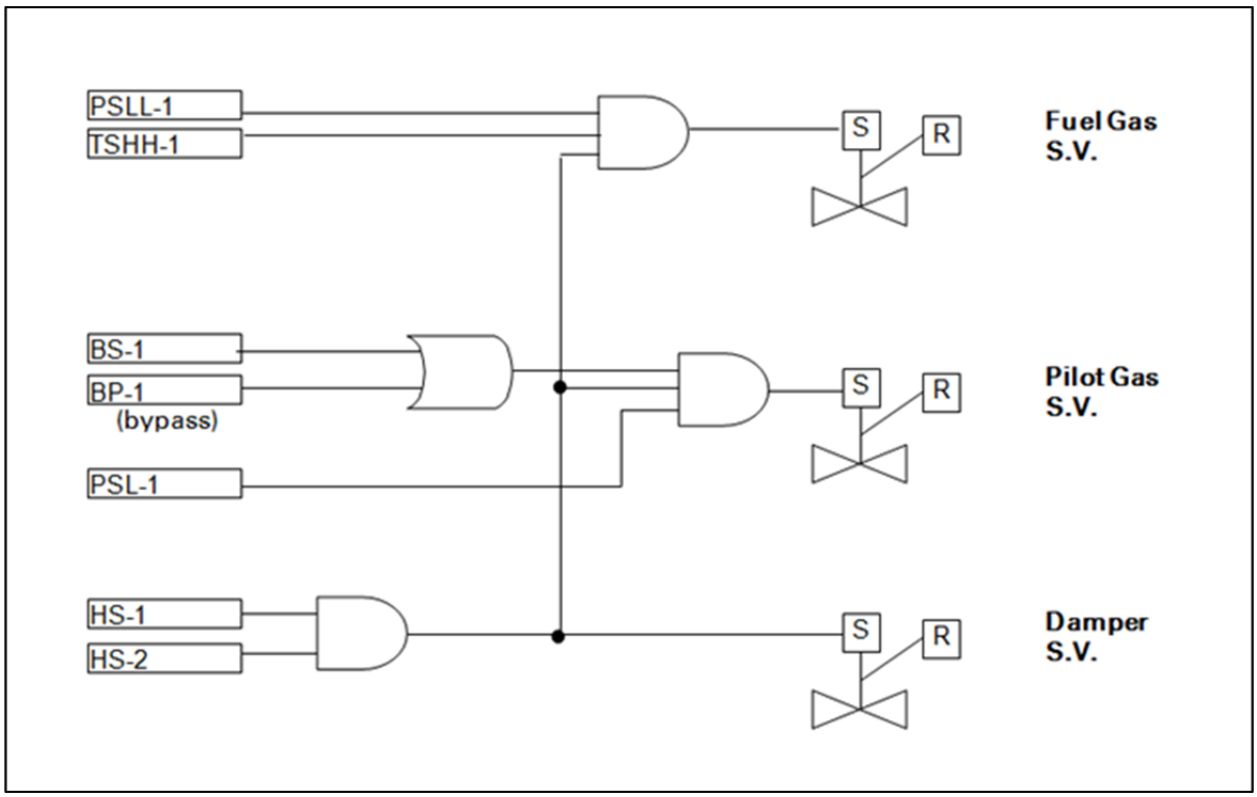
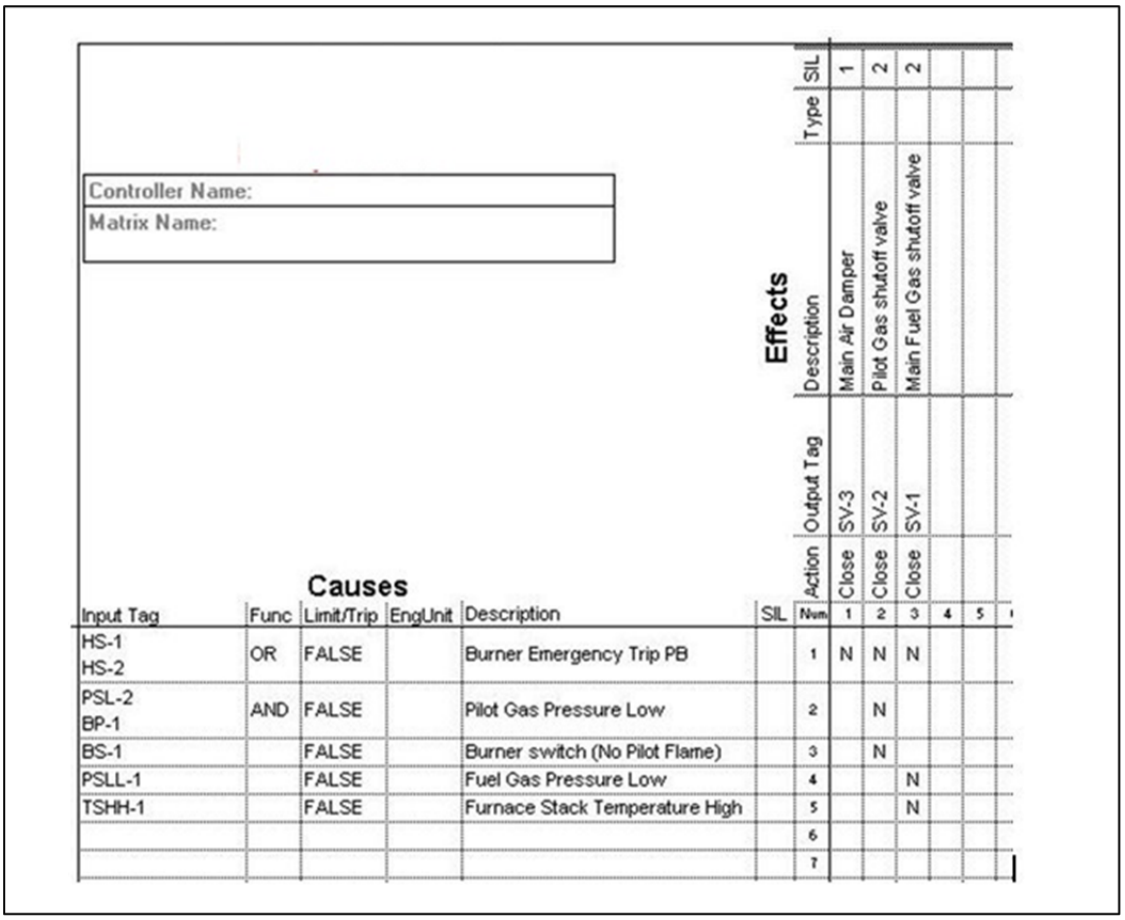


Figure 5 - Sample Shutdown Logic

Figure 6, shows the same fired heater shutdown logic, but illustrated in a cause and effects diagram. This view shows a more concise and descriptive way that when either emergency trip pushbuttons HS-1 or HS-2 are activated, as defined by the relationship of the intersection, they would logically demand that all three control elements (valves and damper) close. In addition, either PSL-2 or BS-1 would demand "close" the pilot gas shutoff valve, and either PSLL-1 or TSHH-1 would demand "close" the main fuel gas shutoff valve.



Controller Name:

Matrix Name:

Effects

							SIL	1	2	2		
							Type					
							Description	Main Air Damper	Pilot Gas shutoff valve	Main Fuel Gas shutoff valve		
							Output Tag	SV-3	SV-2	SV-1		
							Action	Close	Close	Close		

Causes

Input Tag	Func	Limit/Trip	EngUnit	Description	SIL	Num	1	2	3	4	5
HS-1 HS-2	OR	FALSE		Burner Emergency Trip PB		1	N	N	N		
PSL-2 BP-1	AND	FALSE		Pilot Gas Pressure Low		2		N			
BS-1		FALSE		Burner switch (No Pilot Flame)		3		N			
PSLL-1		FALSE		Fuel Gas Pressure Low		4			N		
TSHH-1		FALSE		Furnace Stack Temperature High		5			N		
						6					
						7					

Figure 6 - Cause and Effects Diagram

Clause 7: Verification

The main objective of clause 7 is to demonstrate by review, analysis, and/or testing that the required output for each phase of the safety life-cycle meets the requirements.
Verification planning requires a number of items to be properly addressed throughout the safety life-cycle. One area of concern is the management of change (MOC) of the SIS logic. Most modern day software tools provide an option that allows your cause and effect diagram tool to perform a compare function. This utility would allow the engineer to compare the current program to one that is stored offline, thus being able to identify and record any functional logic changes that might have taken place during the verification phase. Figure 7 below illustrates an example of compare utility; where the output is in a comprehensive report that describes in great detail the differences between the two documents.

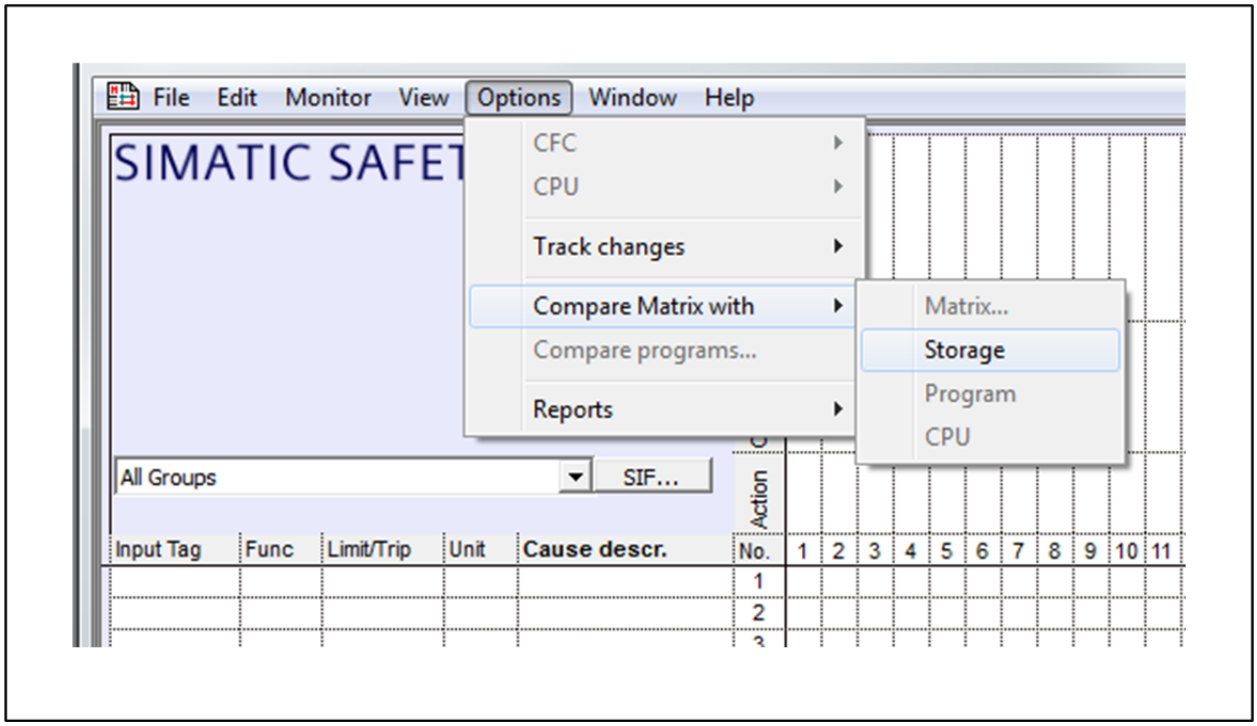


Figure 7 - Management of Change (MOC) Requirements

Clause 8: Process Hazard and Risk Assessment

Identifying the hazards and/or hazardous events of the process along with determining the risk associated with these hazards is the main objective of clause 8. This would also include determining if any safety functions are necessary to reduce the risk and if so, are any of these safety functions SIFs?

While there maybe a number of engineering documents needed to conduct a proper process hazard analysis (PHA) to gain a thorough understanding of the process such as sequential function charts, process flow diagrams and piping and instrumentation diagrams, the output of the PHA could be in the form of a cause and effect diagram to list the identified SIFs as shown in Figure 8.

Clause 9: Allocation of safety functions to protection layers

In this clause, safety functions are allocated to specific protection layers. It should be noted that not all safety functions will be part of the SIS (e.g. mechanical relief device), however those identified as SIFs could be managed and documented within a cause and effects diagram.

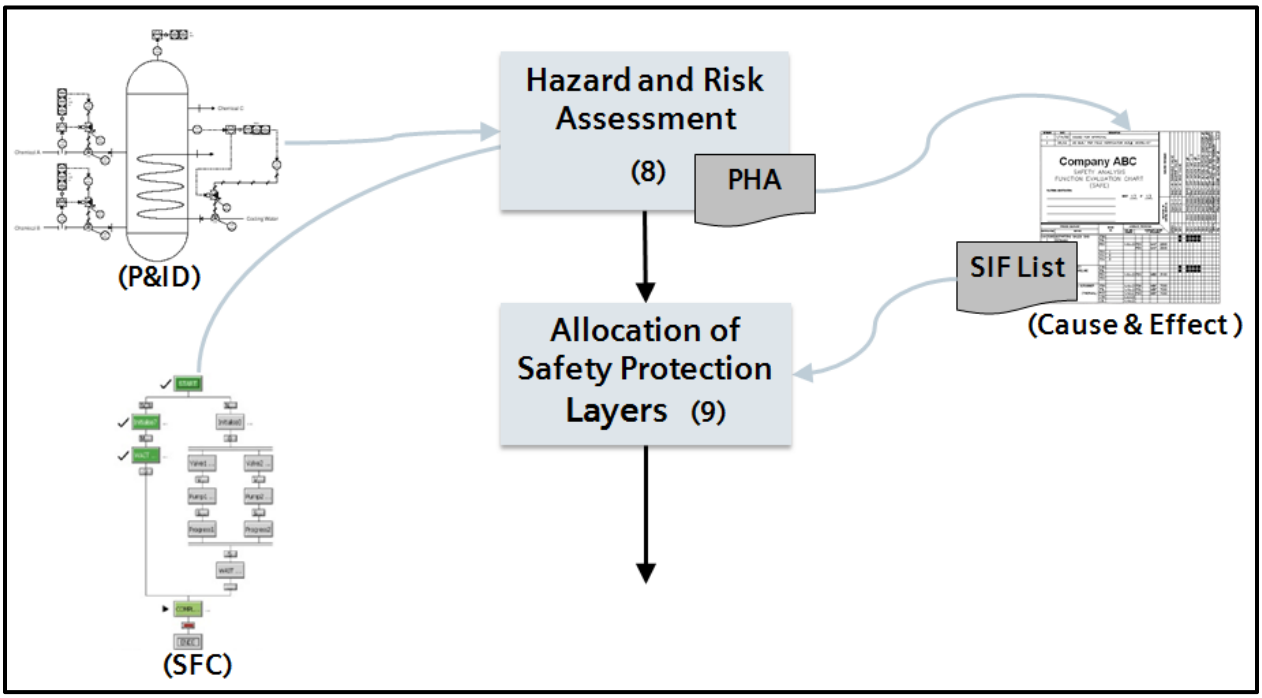


Figure 8 - Hazard and Risk Assessment to Protection Layers

Clause 9: Allocation of safety functions to protection layers

In this clause, safety functions are allocated to specific protection layers. It should be noted that not all safety functions will be part of the SIS (e.g. mechanical relief device), however those identified as SIFs could be managed and documented within a cause and effects diagram.

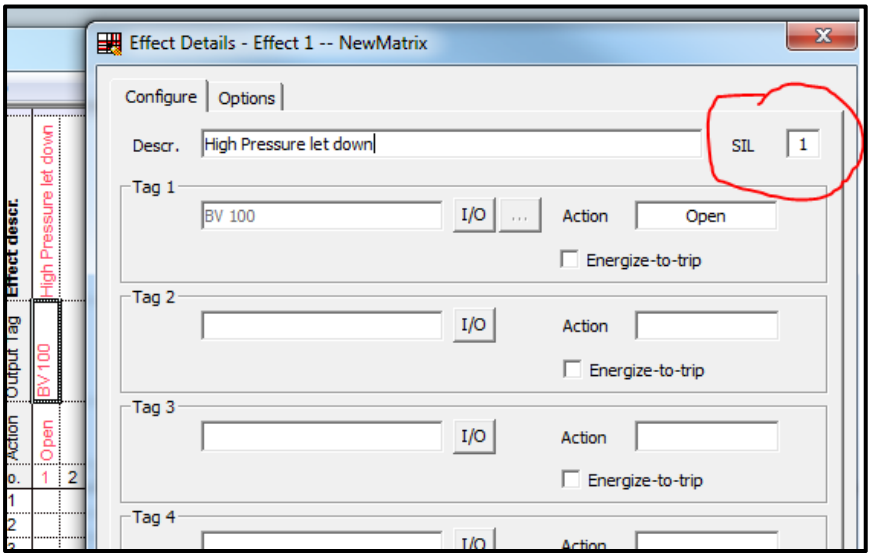


Figure 9 - Recording SIL Requirement for Each SIF

In addition one of the requirements of this phase is to determine the necessary risk reduction or SIL for each SIF. This may also be recorded and documented within the same cause and effect diagram during the configuration of each specific effect as shown below in Figure 9.

Clause 10: SIS safety requirements specification (SRS)

The objective of this clause is to specify the requirements for the SIS including a clear and concise description of the application program as well as the architecture of the SIS.

Cause and effects diagrams play a crucial role in providing an intuitive documentation format for the application program. Conventional programming tools such as ladder logic, or function block diagrams are not considered adequate since they do not convey the ease of comprehension, therefore it would typically require a separate control narrative to verbally describe the safety functions that are being executed in the application program. Cause and effects diagrams will generally contain the configuration details (architecture voting, input and output tags, etc.) along with the options (bypass tags, time delays, etc.) to fully satisfy the requirements of the SRS.

Clause 11: SIS design and engineering

The objective of this clause is to design and engineer the SIS to meet the specified integrity requirements (e.g. SIL, risk reduction, PFD, etc.). In many cases SIS designers have found success leveraging cause and effect diagrams to help meet some of clause 11 requirements for operability, maintainability, diagnostics, inspections and testability to reduce the likelihood of dangerous failures. The level of implementation will vary from using the cause and effects as the design document to a full replication of an active cause and effects diagram running in the SIS logic solver, where the latter would be preferred as it would remove potential human errors during the translation from to the application program. In some cases end-users have reported that this feature alone can reduce their detailed design effort by 50%, not to mention the reduction in translation errors.

Clause 12: SIS application program development

The objective of this clause is to define the requirements for the development of the application program. In the first edition of the standard this clause was 17 pages, it is now 3 and a half pages. This clause has been significantly rewritten to remove life-cycle steps covered in other sections, and now only provides useful information around the requirements for proper application design, development and implementation.

Using a cause and effects tool that is capable of developing the application program will vary from SIS vendors, thus to avoid commercial conflicts this clause will not be covered.

Clause 13: Factory acceptance test (FAT)

The objective of this clause is to test the devices of the SIS to ensure that the requirements defined in the SRS are met. Historically this process involved comparing the functional operation of the application logic (what it is supposed to do) to the traditional programmable logic diagrams (what it's going to do) that are designed and programmed in the system such as ladder logic diagrams, function blocks, etc. A cause and effect diagram could further support the program validation depending on the system and its level of integration using cause and effect diagrams. In some cases it may be available to test the application logic, via an intuitive interface that illustrates the logic in a simple and concise manner such as the cause and effect diagram rather than having to trace the logic thru one of the other conventional methods. This

would require that the system being used is capable of supporting both the ability to monitor online visualization of the logic, as well as a means to 'record' the interaction to generate a validation report to prove that the logic provided the correct outputs as it was designed.

Clause 14 & 15: SIS installation and commissioning and safety validation

The objective of these two clauses are to ensure that the SIS is properly installed, commissioned and validated according to the requirements as stated in the SRS. Much of the requirements listed in clause 14 are geared toward the field devices (properly installed, grounded, calibrated and configured, etc.) however a detailed cause and effect diagram could be vital in recording and identifying these devices as well as documenting the interactions between the sensors (inputs) all the way thru to the final control elements (outputs).

Clause 15 defines all the required validation planning activities for the entire SIS which is sometimes referred to as the site acceptance test (SAT).

Clause 16: SIS operation and maintenance

The objective of this clause is to ensure that the required SIL for each SIF is maintained during operation and maintenance of the SIS. Depending on how integrated the cause and effect diagram is to the safety PLC operating the SIFs, will vary to what functions are available to meet the requirements of this objective. Owner/operators would need to verify what their current system is capable of covering, but below are a few examples of how a cause and effect diagram maybe used to meet the operation and maintenance requirements:

- System diagnostics that impact the performance of specific SIFs might be displayed on a cause and effect diagram to quickly draw the attention to the operator to reduce the time to repair.
- Inspection and proof testing maybe conducted, recorded and documented using the online capability of the cause and effect diagram to meet SIL verification requirements.

Clause 17 & 18: SIS modification and decommissioning

The objectives of clauses 17 and 18 are to ensure that any changes (modification or decommissioning) to the SIS are properly planned, reviewed, approved and documented. Today it's well understood that depending on the plants circumstances, modifications may be necessary either online or offline and in either case rigorous revision tracking would be required, with the ultimate goal of maintaining the performance of the SIS. In the case where a cause and effect diagram is well integrated with the SIS logic solver, much of the required documentation can be automatically updated as the system goes thru modifications as well as automatically updating the SRS to keep it current.

Clause 19: Information and documentation requirements

The objective of this clause is to ensure that all of the necessary information is available and documented to support all phases of the SIS safety life-cycle. Figure 10 below summarizes the typical workflow between the safety life-cycle and a cause and effect program to minimize human errors through all phases.

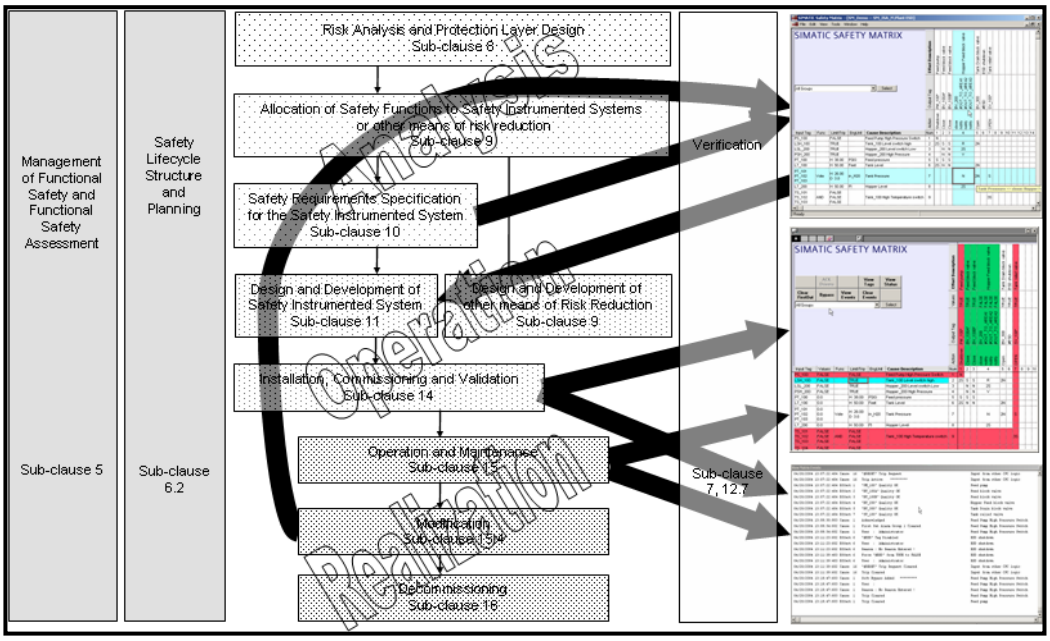


Figure 10 - Safety Lifecycle Workflow

4 Summary

The safety life-cycle is regarded as the foundation of the international functional safety standard for the process industries. It recognized as an important engineering methodology, but documentation intensive process that is prone to errors. A number of tools have been developed throughout the industry to try and address some of the leading contributors to failures (specifications, installation and commissioning, operations and maintenance, etc.) which are largely tied to human errors. One approach the industry is looking towards is how a comprehensive cause and effect methodology that covers the SIS design, programming, operations, and maintenance tool tying together all phases to address the impact of human error through the life-cycle.

5 References

1. U.K. Health and Safety Executive, Out of control: Why control systems go wrong and how to prevent failure, Available at http://www.hse.gov.uk/pubns/books/hsg238.htm Accessed on December 8, 2016
2. IEC 61511-1: 2016, Functional Safety – safety instrumented systems for the process industry sector
3. Permissive Sequencing and ISA 84 -- The Shape of Things to Come By Gene Cammack, PE; Francisco Sanchez, PDVSA and Luis M. Garcia G. CFSE Siemens Energy & Automation, Houston, Texas 2008
4. SIMATIC Safety Matrix V 6.2 Configuration Manual, Copy right 1995-2015, Siemens AG
5. Innovative new tools for automating SAFE Charts as required for API RP 14C Charles M. Fialkowski: Siemens Energy & Automation; Spring House, PA USA Presented at IEEE – PCIC technical conference 2006